ManageEngine
ServiceDesk Plus

Conforming to ISO 27001 with ITSM best practices

A handy guide to help you strengthen information security and accelerate your ISO compliance journey with ManageEngine ServiceDesk Plus.

Table of contents

01 A brief introduction to the ISO27k family and the ISO 27001 standard

The ISO 27000 series is a family of mutually supporting information security standards jointly proposed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards are meant to help organizations secure their information assets by implementing and maintaining an information security management system (ISMS).

Focus

ISO 27001 is a globally recognized information security standard that focuses on implementing and maintaining an information security management system (ISMS) to help organizations guard sensitive information.

Scope

From small businesses to multinational corporations, any organization that stores and handles sensitive information can benefit.

Global adoption

The number of organizations with ISO 27001 certifications continue to rise. According to ISO's 2022 survey, there are over 70,000 organizations with this certification across150 countries.

Recent updates

The latest version of this standard is ISO 27001:2022. Organizations have until October 31, 2025 to transition to the 2022 version.

The series encompasses more than 40 individual standards like ISO 27000 (overview and vocabulary), ISO 27001 (specifications for ISMS requirements), ISO 27002 (guidance for controls implementation), ISO 27005 (risk management), and many others.

In this series, ISO/IEC 27001 is the main certifiable standard that specifies and mandates the risk-based requirements for implementing an ISMS. ISO 27001:2022 is the latest revision built upon the 2013 version to reflect modern security challenges and updated best practices. It provides a comprehensive framework that helps organizations protect and manage their sensitive information. Organizations are audited against the requirements of this standard, and if found compliant, they are awarded certification by an accredited certification body, and the certificate remains valid for a period of three years from the date of issuance.

02

But first, what is an ISMS?

ISMS

?

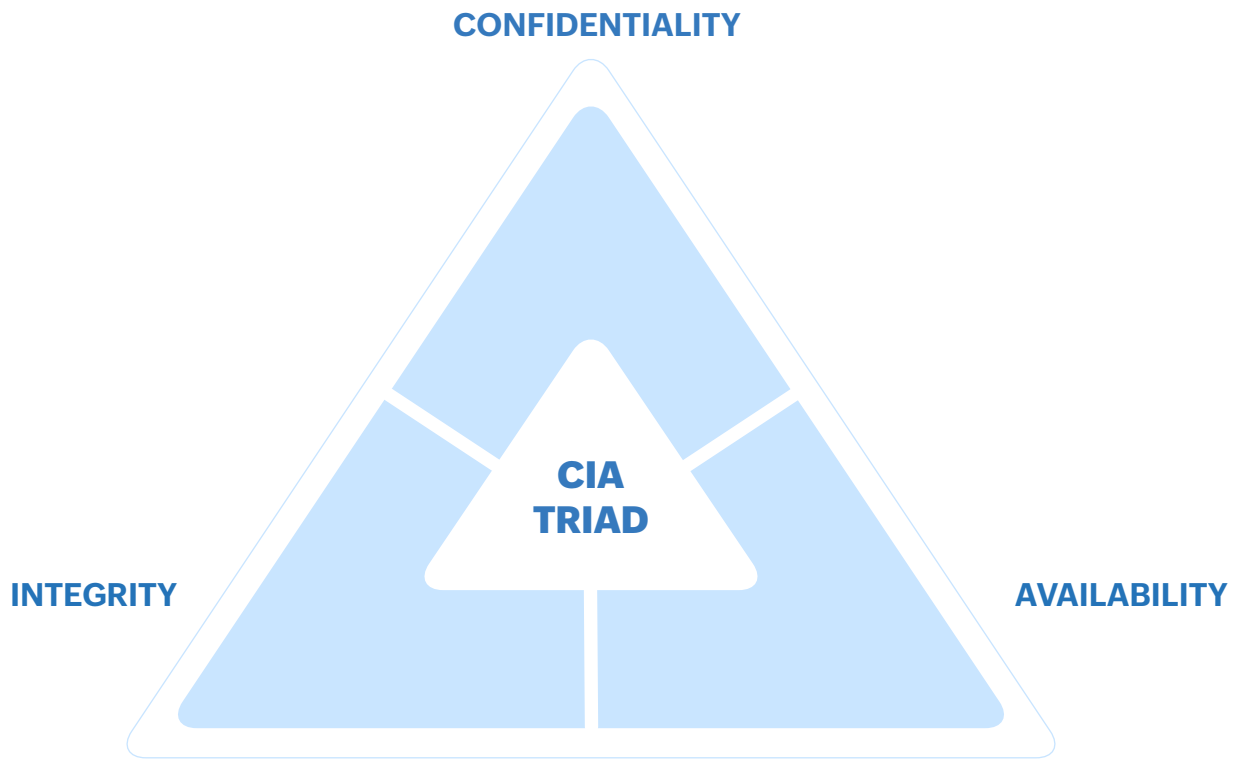
An ISMS is a systematic approach that combines people, processes, and technology to help organizations identify, assess, and mitigate information security risks. Specifically one that conforms to the requirements of ISO 27001, an ISMS can further aid in complying with data protection laws like the GDPR. It establishes a clear set of controls, policies, and procedures that help organizations safeguard their information from threats like data thefts, unauthorized access, or breaches by ensuring the confidentiality, integrity, and availability of the information. This security model is commonly called the CIA triad.

The CIA triad

The CIA triad is a security model that guides information security policies and is embedded within many security frameworks, including ISO/IEC 27001.

The three principles of the CIA triad are:

Confidentiality	Keeping information secure by protecting it from unauthorized exposure.	Data encryption, access controls, and authentication mechanisms help ensure confidentiality of data.
Integrity	Maintaining the accuracy and trustworthiness of information by ensuring that it is not altered or tampered with.	Version control, file integrity checks, and audit trails help identify and address unauthorized modifications to data.
Availability	Making sure that information is readily available when authorized users require access.	Real-time system monitoring, regular data backups, and disaster recovery planning help ensure proper availability of data.



03 Why ISO/IEC 27001 matters and who needs it

According to IBM's 2025 cost of a data breach report, the average global cost of a data breach is $4.44 million. Today, information is one of the most valuable assets an organization can hold. Safeguarding this information is crucial in a time that's filled with rising cyberthreats and sophisticated attacks. However, the complexity of modern IT environments and cyberthreats makes managing cyber risks more challenging than ever. This is where an ISO backed ISMS can make all the difference.

Implementing an ISMS based on ISO/IEC 27001 can help organizations:

- ✓ Enhance cyber resilience against evolving threats
- ✓ Reduce risk exposure and close security gaps
- ✓ Preserve the confidentiality, integrity, and availability of data
- ✓ Lower costs associated with information security risks and non-compliance
- ✓ Improve operational excellence through a structured and risk-based approach

Now the question is, does your organization need it?

To answer simply, if you handle sensitive information of any kind, then yes, your organization can benefit tremendously. The standard is designed to be flexible and applies to organizations of any size, whether large or small, public or private, across all industries. ISO 27001 compliance can be non-negotiable for organizations in verticals like BFSI, healthcare, life sciences, government, etc. Achieving this certification can help you demonstrate a strong commitment to information security and further build trust with customers, partners, and other stakeholders.

ISO/IEC 27001 applies to any organization, regardless of size or industry, including:

- **Information technology companies:** To secure customer information, employee records, and infrastructure systems.
- **Healthcare providers:** To safeguard sensitive patient health information (PHI) and meet compliance obligations like HIPAA or the GDPR.
- **Financial institutions:** To protect financial records, transaction data, and customer information from fraud.
- **Manufacturers:** To protect intellectual property, product designs, and supply chain data.
- **Government agencies:** To protect classified or sensitive public sector data and ensure regulatory compliance.

04 Clauses, controls, and objectives: The structure behind it all

ISO 27001 clauses

The ISO 27001 standard consists of 10 clauses that specify the requirements for an ISMS. The first three clauses define the scope, normative references, and terms and definitions that lay down the purpose of getting certified for this standard. Clauses 4 through 10 list the requirements that the ISMS must meet before it can be ISO 27001 certified.

Formalities

Mandatory for certification

Clause 1
Scope

Clause 2
List of references

Clause 3
Terms and definitions

Clause 4
Context of the organization

Clause 5
Leadership

Clause 6
Planning

Clause 7
Support

Clause 8
Operation

Clause 9
Performance evaluations

Clause 10
Improvement

PDCA cycle

ISO 27001 is based on the plan-do-check-act (PDCA) cycle, a 4-step iterative process that helps organizations establish, implement, monitor, and continually improve their information security management systems. The stages in the PDCA cycle help organizations systematically manage information security risks and strengthen their security posture.

Phase	Clause	What's done in each stage
Plan Establishing the ISMS	**Clauses 4-7**	Define ISMS scope and establish the context, leadership commitment, objectives, and necessary support
Do Implementing the ISMS	**Clause 8**	Implement controls and run the ISMS as planned
Check Monitoring and evaluating the ISMS	**Clause 9**	Monitor and evaluate the implemented processes to see if they are effective
Act Continually improving the ISMS	**Clause 10**	Take corrective actions and continually improve the ISMS

Controls in Annex A

Annex A in ISO 27001 outlines a list of security controls that organizations use to demonstrate compliance with the standard.

It comprises 93 controls divided across four categories that address a wide range of topics like access control, asset management, incident response, and more.

Annex A controls are spread across these four categories:

1. Organizational controls (37)
2. People controls (8)
3. Physical controls (14)
4. Technological controls (34)

So, how does all of this work?

The ISO/IEC 27001 certification requires organizations to conduct a risk assessment and identify which controls are necessary to treat those risks. The organization must then prepare a Statement of Applicability (SOA), specifying which of these 93 controls they conform to and provide clear justifications for any excluded controls. During the audit, the auditor would then verify if the implemented controls are effective and assess the rationale behind the exclusions.

05 How to approach ISO 27001 through ITSM best practices

For the longest time, IT service management has been centered around the delivery of IT services with a focus on efficiency, productivity, and user satisfaction. ITSM does this by providing a structure for managing incidents, fulfilling service requests, tracking assets, and executing IT changes with minimal disruption. But as cybercrimes become more complex, service excellence alone is no longer enough. Organizations need to go a step further and look into embedding security checks within their everyday service management workflows to keep up with cyberthreats.

Best practice service management, refined through years of ITIL adoption, can be retrofitted with a security lens to help meet with ISO 27001 controls. This means that instead of having to reinvent the wheel, organizations can leverage the service management practices they already rely on to demonstrate commitment to information security and move closer to getting ISO 27001 certified. For example, service request workflows can be used to enforce access control and governance measures defined in Annex A. Real-time incident reporting and incident management processes can be used to proactively kick start response workflows during data breaches. Asset management can help maintain a real-time inventory of information assets to support risk assessments.

The controls that ITSM practices can help you comply with

06

How then can you accelerate your compliance journey with ServiceDesk Plus?

ServiceDesk Plus is the AI-driven unified service management solution from ManageEngine, the enterprise IT management division of Zoho Corporation. It helps you align with some ISO 27001 controls by assisting you with retrofitting core ITSM processes with a security-first approach. We've mapped some ServiceDesk Plus capabilities to ISO 27001 controls to demonstrate how this solution supports your compliance journey for access governance, incident response, asset management, and more!

Access controls and governance

- Provide role-based access to access provisioning requests through a unified service catalog.
- Trigger predefined workflows to automate provisioning and also revoke privileges if needed.
- Enforce fine-grained scrutiny with multi-tiered approvals to minimize the risk of unauthorized access.
- Have complete visibility into all access requirements from a single system of record.

Incident response

- Ingest alerts from observability solutions for proactive detection and quick resolution.
- Ensure diligent evidence collection through templates with prebuilt ticket fields and custom fields.
- Kick-start incident response with AI-powered triaging.
- Establish standard operating procedures and pilot governance through prebuilt incident response workflows.
- Document detailed root cause analyses and generate post-incident reviews (PIRs) to reduce recurrence and strengthen response posture.

Asset management

- Maintain a centralized asset inventory and CMDB as your single source of truth for all information assets.
- Perform better impact analyses and risk assessments with a built-in CMDB.
- Implement visual workflows to stage-gate every phase of the asset life cycle, from procurement to disposal, and stay audit-ready.
- Trigger automated workflows via UEM integrations to wipe sensitive data during asset disposal or restrict unauthorized software installations.

Change management

- Govern changes to information systems through visual workflows with distinct stages, approvals, and tasks.
- Use AI-driven risk evaluations to assess the impact of changes on information security.
- Enforce multi-tiered approval mechanisms to ensure only authorized changes are implemented.
- Maintain detailed records of all change activities to support audit readiness.

Knowledge management

- Compile and maintain your organization's information security policies, procedures, and best practices as knowledge articles in a centralized repository.
- Ensure the quality of knowledge articles with streamlined approval mechanisms and expiry cycles.
- Restrict visibility to these knowledge documents with role-based access.
- Promote knowledge reuse to accelerate incident response, security awareness, and consistent service delivery.

Here are some ServiceDesk Plus capabilities that we've mapped to the corresponding ISO 27001 controls to show how they can support your compliance journey:

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.5 Organizational controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	• Agent-based and agentless asset discovery • Centralized asset inventory • Asset classification based on product types • Asset mapping to designated owners • Relationship maps to visualize asset dependencies	Discover and identify all IT and non-IT assets using various discovery methods such as domain scans, network scans, self-scan scripts and agent-based scans. Once the assets are brought into the system, classify them based on product types, assign them to specific owners, and consolidate them in a centralized repository for complete visibility. From there, implement ITIL-certified asset management practices to keep the inventory accurate and up-to-date.
5.11 Return of assets	Personnel and other interested parties, as appropriate, should return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.	• An asset inventory as the single source of truth • Visual ITAM workflows with no-code automations • Notification rules • Native integration with ManageEngine PAM360	When an employee or a contractor is about to be relieved, ensure that all organizational assets tied to them are properly returned by referring to a centralized asset inventory that clearly maps out user and asset associations. Leverage predefined workflows to track the return of assets and automatically trigger notifications if an asset is marked as lost. Plug your privilege access management solutions into your offboarding workflows in ServiceDesk Plus to automate tasks like password rotation, privilege revocation, disabling AD accounts, and more.

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.5 Organizational controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
5.15 Access Control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	• Centralized service catalog • Role-based access controls • Multi-tiered approvals • Workflow orchestration for access provisioning • Single system of record for all access requests	Receive, authorize, and administer access provisioning requests with the ITIL-certified service request management capabilities in ServiceDesk Plus. Centralize the access provisioning services through a unified service catalog that would have dynamic templates with role-based access to specific groups of employees. Implement fine-grained scrutiny through visual workflows embedded with multi-level approvals. The entire access provisioning request can then be orchestrated through single touch workflow automations that are triggered based on events like approvals.
5.18 Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with the organization's topic specific policy and rules for access control.	• Centralized service catalog with dynamic templates • Role-based access to access request templates • Workflow orchestration for access provisioning and deprovisioning • Multi-tiered approvals	Enable and manage access modifications through fine-grained access request forms. Collect accurate information through template fields whenever a modification of access rights is requested. Align with your organization's access policies by establishing SOPs to standardize and pilot access governance through visual workflows embedded with multilevel approvals.
5.19 Information security in supplier relationship	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	• Custom modules for supplier risk assessments • Custom templates with risk questionnaires • Low code scripts to auto assign risk scores • Notification rules	Create bespoke custom modules for handling supplier risk assessments. Store your suppliers/vendors in a central repository and embed these custom modules with fields that help capture and categorize risks. Initiate mitigative actions such as notifying stakeholders and creating tickets with the risk scores auto-assigned based on the responses to the risk assessment questionnaires through low-code automations.

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.5 Organizational controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
5.21 Managing information security in the ICT supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	• Bespoke custom modules • Custom templates with risk questionnaires • Low-code custom automations	Leverage custom modules and create custom risk assessment questionnaires to capture the risks associated with the ICT supply chain vendor. Trigger custom automations depending upon the identified risk.
5.23 Information security for use of cloud services	Processes for acquisition, use, management, and exit from cloud services should be established in accordance with the organization's information security requirements.	• Custom templates for access requests to cloud services • Service request workflows • Purchase management • Contract management	Build dedicated visual workflows and streamline the process to request and acquire cloud services. Associate and manage purchase orders and contracts alongside approvals and keep track of their expiry dates with automated notifications.
5.24 Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security management processes, roles, and responsibilities.	• Incident templates • SLAs specifying response and resolution timelines • Integrations with collaboration hubs to notify stakeholders in the channels they use most • A native CMDB for impact analyses • An easily accessible knowledge base	Develop structured incident management templates that define roles, responsibilities, SLAs, tasks, and response procedures. Create predefined workflows with automated notifications via Microsoft Teams and Slack to keep stakeholders updated. Perform in-depth impact analyses with an integrated CMDB to identify affected assets, services, and dependencies for quicker resolutions. Quickly refer to the resolutions documented in the knowledge base to accelerate incident response.
5.25 Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	• AI powered triaging with Zia's smart predictions • Incident response workflows with no-code automations	Leverage AI-powered triage to accurately categorize, prioritize, and route information security incidents to the right incident response teams. Fire up visual workflows that guide incident response team members in assessing impact and making decisions with embedded automations.

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.5 Organizational controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
5.26 Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	• Custom incident templates • Incident response workflows • A tightly integrated problem management module • An easily accessible knowledge base • Auditable records	Collect evidence through prebuilt ticket fields and custom fields across the incident response process. Establish SOPs and pilot governance through pre-built incident response workflows. Perform detailed RCAs and address underlying causes with a tightly integrated problem management module. Easily access and refer to previous resolutions documented as knowledge articles to accelerate resolutions. Maintain an auditable trail of every action performed in the incident response process with detailed and time-stamped logs.
5.27 Learning From information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	• AI-generated post incident reviews through Zia • Zia's conversation summaries • Knowledge capture from these findings	Generate detailed post-incident reviews with Zia's Generative AI capabilities. Summarize conversations within the ticket for better context understanding. Transfer these summaries and insights as notes to clearly communicate incident histories. Document the resolution in a central knowledge repository to establish SOPs and reduce the impact of future incidents.
5.28 Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	• Custom templates for evidence collection • Workflows with mandated fields to capture crucial information • AI-generated PIRs to collate evidence	Ensure diligent evidence collection through prebuilt ticket fields and custom fields across incident response and other ITSM practices. Generate post-incident reviews with GenAI. Establish SOPs and playbooks for evidence collection using visual workflows where fields are mandated and stakeholders are notified.

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.5 Organizational controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
5.31 Legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented, and kept up to date.	• Goverened knowledge base with approvals and expiry cycles • Role-based access to the KB articles • A self-service portal for end users for easy access to these articles	Ensure compliance by identifying, documenting, and regularly updating knowledge articles on legal, statutory, regulatory, and contractual requirements. Embed the self-service portal with these articles to provide employees easy access to these requirements and related guidance.
5.34 Privacy and protection of PII	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	• Options to encrypt fields containing PII • Settings to erase the data when needed	Within the IT and enterprise service requests you receive, encrypt fields containing PII to secure the personal information of requesters. Configure privacy settings in ServiceDesk Plus to anonymize and erase the data from the application when required.
5.36 Compliance with policies, rules, and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules, and standards should be regularly reviewed.	• A governed KB backed by approval mechanisms and expiry cycles	Document and manage the organization's information security policies and rules as knowledge articles in a central repository. Set up document review and approval mechanisms with role-based access to keep the information up-to-date and accessible to the right people.
A.6 People controls			
6.8 Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	• Omni-channel incident logging • AI-powered triage • Incident response workflows with no-code automations	Leverage an omni-channel incident logging system integrated with various collaboration tools. Once the ticket is logged, triage, manage, and resolve incidents through end-to-end workflow automations and AI assistance.

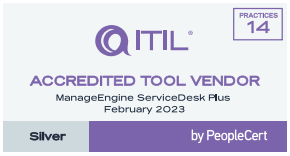
Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.7 Physical controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
7.10 Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.	• An asset inventory with asset classification • Visual ITAM workflows	Classify IT assets as storage media, manage them from a central repository, and have dedicated visual workflows to stage gate every step of the asset's life cycle from procurement to disposal.
7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	• ITAM workflows • Integration with UEM solutions to wipe sensitive data or remove any software	When an IT asset reaches its end of usable life or needs to be disposed of, automatically notify the required stakeholders to remove any sensitive data or licensed software.
A.8 Technological controls			
8.1 User Endpoint Devices	Information stored on, processed by, or accessible via user endpoint devices shall be protected.	• Software scan • Notification rules • Native integration with ManageEngine Endpoint Central	Integrate with UEM solutions like Endpoint Central and Microsoft Intune to perform remedial actions like associating/dissociating profiles, wiping corporate data, uninstalling prohibited software, or geolocating mobile devices.
8.9 Configuration management	Configurations, including security configurations of hardware, software, services, and networks, shall be established, documented, implemented, monitored, and reviewed.	• Built-in CMDB with visual dependency mapping • Information sync from data sources like observability solutions	Build and maintain a high-integrity CMDB that provides accurate dependency data through visual maps. Capture and track downstream dependencies with relationship mapping powered by integrations with observability solutions like Site24x7.

Control	Control definition/ requirements	How ServiceDesk Plus can help	
A.8 Technological controls		**ServiceDesk Plus capabilities**	**What these capabilities can translate to**
8.19 Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	• Software scan • Mark specific software as prohibited • Notification rules • Integration with ManageEngine Endpoint Central • Bespoke software compliance dashboards	Scan and identify the software installed on workstations and classify them as managed or prohibited. Alert the designated personnel when a prohibited software is identified. Create a compliance dashboard to identify software policy violations like instances of unlicensed software.
8.32 Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	• Change workflows with distinct stages and embedded automations • CAB approval mechanisms • AI-powered change risk predictions	Manage changes to information processing facilities and systems with ITIL-certified change enablement capabilities. Govern changes with defined workflows, AI-driven risk evaluation mechanisms, and authorization procedures to minimize risks and compliance violations.

About ServiceDesk Plus

ServiceDesk Plus is the AI-driven unified service management solution from ManageEngine, the enterprise IT management division of Zoho Corporation. It combines ITSM essentials, asset management, and a CMDB with enterprise service management capabilities, providing a comprehensive platform for designing, managing and delivering IT and business services.

Powered by proprietary AI technologies and public LLM integrations, ServiceDesk Plus unlocks unparalleled efficiencies and experiences for employees, technicians, and process owners.



Here are five reasons why ServiceDesk Plus is trusted by some of the leading global enterprises

- High-value AI capabilities for IT and enterprise service management are not paywalled behind add-ons but included within your subscription.
- Powerful, modern ITIL workflows orchestrate enterprise and IT services from end to end.
- From servers, networks, and switches to workstations and peripherals, it's your single system of record for the entire digital infrastructure.
- Platform capabilities power up ServiceDesk Plus to digitize and optimize workplace service delivery.
- ServiceDesk Plus integrates natively with every ManageEngine application and other third-party business apps as well.

Want to consult our product experts on how ServiceDesk Plus can help you conform to ISO 27001 requirements?

Reach out to us at hello@servicedeskplus.com

About ManageEngine

ManageEngine is a division of Zoho Corporation that provides comprehensive on-premises and cloud-native IT and security operations management solutions for global organizations and managed service providers. Established and emerging enterprises rely on ManageEngine's real-time IT management tools to ensure the optimal performance of their IT infrastructure, including networks, servers, applications, endpoints, and more. ManageEngine has 18 data centers, 20 offices and more than 200 channel partners worldwide to help organizations tightly align their business to IT. For more information, please visit the company site, follow the company blog, and get connected on LinkedIn, Facebook, Instagram, and X (formerly Twitter).