ManageEngine
ServiceDesk Plus

Championing NIS2 compliance as an ITSM leader

Table of contents

NIS2 and ITSM: What this handbook aims to deliver

Network and Information Systems Directive 2 (NIS2) is the European Union's updated directive aimed at strengthening cybersecurity across mid-sized and large organizations. Building on the original NIS directive, NIS2 introduces stricter requirements and expands its scope to cover 15 critical sectors, up from eight previously.

The NIS2 directive consists of 46 articles spread across multiple chapters, covering a wide range of topics including coordinated cybersecurity frameworks, EU and international cooperation, cybersecurity and risk management measures, incident reporting obligations, jurisdiction, and more.

Unlike popular security and compliance frameworks, NIS2 is a directive. It outlines the cybersecurity objectives and required outcomes but does not prescribe specific technical standards or implementation methods.

The directive requested that each EU member state must transpose NIS2 into national law by October 2024. Organizations within these countries are now obligated to comply with those national laws or risk significant fines and legal consequences.

For ITSM practitioners aiming to align with NIS2, two key articles stand out:

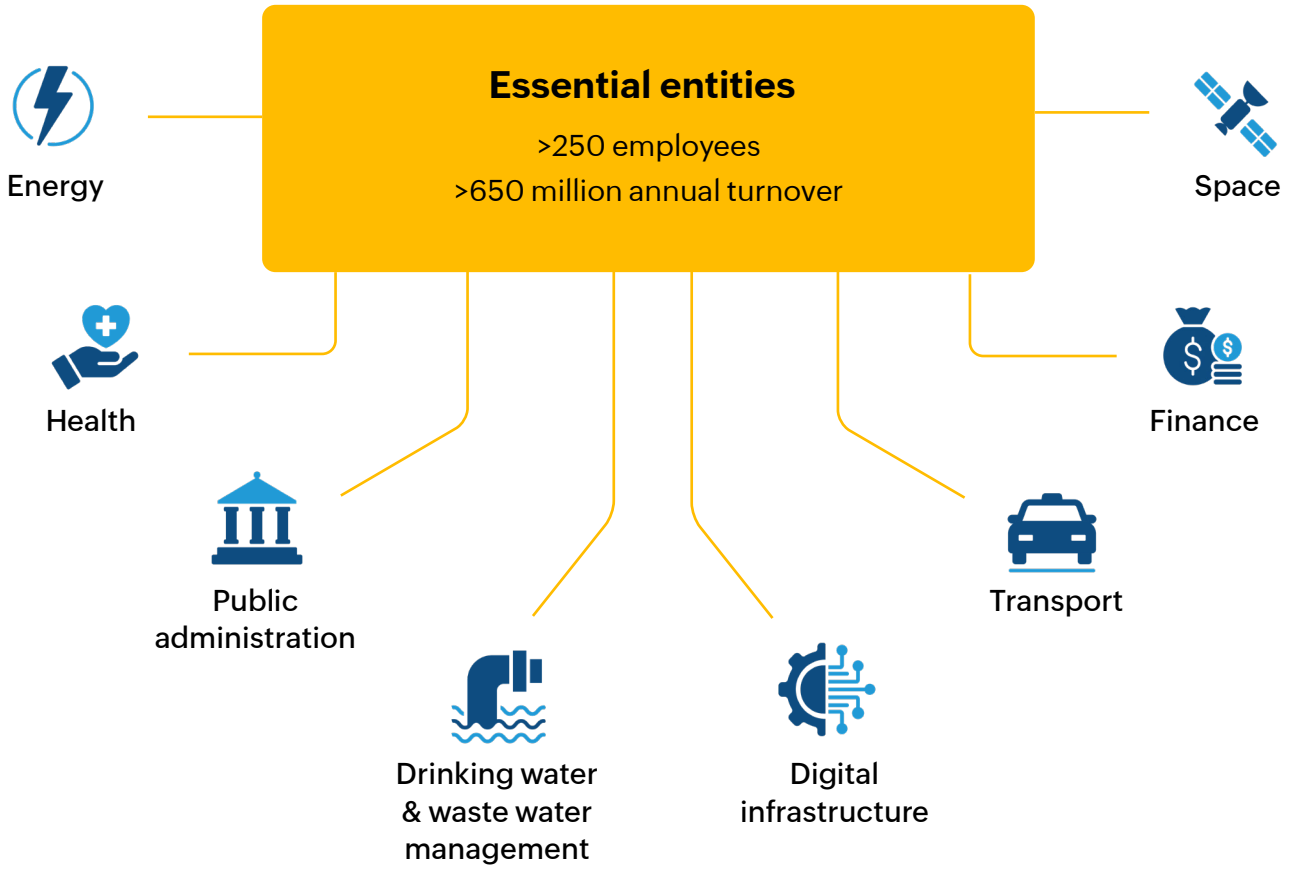
- **Article 21:** Cybersecurity risk-management measures
- **Article 23:** Incident reporting obligations

In this handbook, we'll explore the relevant measures outlined in Articles 21 and 23, how your organization can align your ITSM strategy to meet these requirements, and how ManageEngine's ServiceDesk Plus can support your compliance journey.

Types of organizations regulated by NIS2

It's important to first assess whether your organization falls under the scope of the NIS2 directive.

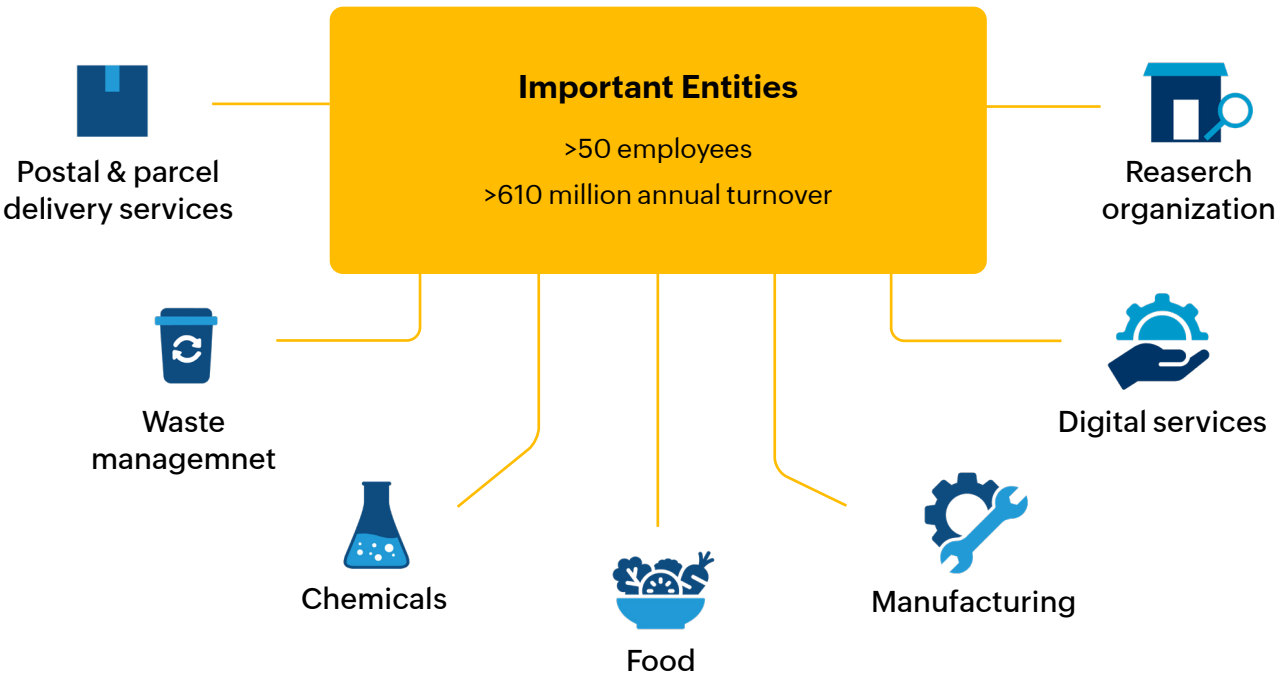
The NIS2 directive applies to organizations across 15 sectors, categorized into two groups: **Essential entities** and I**mportant entities.**



Essential entities operate in high-impact sectors such as:

- **Energy:** Supply, distribution, transmission, and sales
- **Transport:** Air, rail, road, and maritime
- **Finance:** Banking, trading platforms, and financial market infrastructure
- **Health:** Healthcare providers, medical device manufacturers, and pharmaceutical research and production
- **Drinking water and wastewater management**
- **Digital infrastructure:** DNS service providers, trust service providers, data centers, cloud computing, electronic communications, MSPs, and MSSPs
- **Public administration:** Central, regional, and municipal bodies
- **Space:** Operators of space-based services and related software

To be classified as an Essential Entity under NIS2, an organization must operate within one of the sectors listed above and meet at least one of the following thresholds: more than 250 employees, an annual turnover exceeding €50 million, or a balance sheet total of €43 million or more. Additionally, the organization must offer products or services within an EU member state.



Important entities under NIS2 operate in sectors that, while not as critical as those of essential entities, are still vital to economic and societal stability. These sectors include:

- **Postal and parcel delivery services**
- **Waste management**
- **Chemical industry:** Production and distribution
- **Food sector:** Production and distribution
- **Manufacturing:** Pharmaceuticals, electronic and optical equipment, machinery, and motor vehicles
- **Digital services:** Online marketplaces, search engines, and social media platforms
- **Research organizations**

To qualify as an **Important Entity,** an organization must operate in one of the sectors listed above and meet at least one of the following criteria: more than 50 employees, an annual turnover exceeding €10 million, or a balance sheet total of at least €13 million. The organization must also offer products or services within any EU member state.

The cost of ignoring NIS2 requirements

Organizations that fail to meet NIS2 requirements face significant administrative and legal consequences. While EU member states can define the exact penalties, the directive sets strict minimum thresholds:

- **Essential entities:** Fined up to €10 million or 2% of global annual turnover, whichever is higher.
- **Important entities:** Fined up to €7 million or 1.4% of global annual turnover, whichever is higher.

But the penalties don't stop at fines. NIS2 also holds executive leadership accountable for non-compliance, recognizing that security and governance responsibilities extend beyond the IT team.

EU member states are empowered to:

- Order organizations to publicly disclose compliance violations.
- Issue public statements naming the individuals or legal entities responsible and describing the nature of the violation.
- In the case of essential entities, temporarily ban individuals from holding management roles after repeated violations.

Achieve NIS2 compliance through ITSM excellence

A robust ITSM framework, enhanced by modern technologies, can play a critical role in helping organizations meet the requirements of the NIS2 Directive. The following ITSM practices, when implemented using today's advanced tools, directly support this compliance effort.

1. **Proactive incident management:** Automated incident detection and response directly supports NIS2 compliance. By triggering incident workflows based on IT events, enforcing SLAs, and maintaining detailed audit trails, ITSM teams can ensure swift detection, timely escalation, and rapid resolution of security incidents. These capabilities align with the directive's requirements for prompt response and transparent reporting.
2. **Context-rich CMDB:** A well-maintained CMDB is a critical asset for NIS2 compliance, enabling accurate risk assessments and structured risk management. By enriching it with contextual data, IT teams can better understand the impact of component or service failures especially during high-impact changes, IT projects, or security evaluations.
3. **Streamlined communications channels:** If you're already maintaining effective collaboration channels for technicians and keeping leadership well-informed of ground-level incidents, you're on the right track. The NIS2 Directive emphasizes timely incident reporting to both authorities and stakeholders across the EU, making this level of visibility and communication a key compliance requirement.

4. **Service continuity and resilience:** From a business continuity perspective, if your organization has automated backups, a clear fallback plan for disruptions, and a robust IT service continuity management setup, you're already well on your way to NIS2 compliance. The directive mandates the availability of essential services through effective backup management, disaster recovery strategies, and crisis response planning.
5. **Accessible knowledge hub for user awareness:** A continuously updated knowledge base that users can rely on plays a key role in promoting awareness of the latest security practices and emerging attack vectors. NIS2 places strong emphasis on regular training and user awareness, making such a resource essential for compliance. Organizations that invest in accessible, up-to-date knowledge sharing are naturally better positioned to meet these requirements.

Simplifying NIS2 compliance for ITSM teams

Fortunately, NIS2 compliance doesn't have to be overwhelming. As an ITSM leader, the key articles to focus on are mentioned below. We've outlined what each article requires, what your team needs to meet those requirements, and how ManageEngine ServiceDesk Plus can help you achieve them.

Article and measures	Your responsibility	ServiceDesk Plus capabilities	Outcomes that accelerate compliance
Article 21 - Cybersecurity risk-management measures (2)(a) Policies on risk analysis and information system security	Draft, comply, support, and actively participate in the enforcement of InfoSec and risk management policies, as part of service delivery workflows.	• Governed knowledge base with version control, and draft-to-expiry life cycle. • Controlled visibility of knowledge articles through role-based access. • Customizable self-service portal accessible via mobile and desktop.	**Better policy management:** ServiceDesk Plus can help document, manage versions, and routinely review your InfoSec and risk management policies in a structured Knowledge-Centered Service aligned knowledge base. **Frictionless policy rollout:** The knowledge base in ServiceDesk Plus can help you publish the policies and announce them to specific user groups, IT technician groups, or the entire organization through every employee's self-service portal.
Article 21 - Cybersecurity risk-management measures (2)(b) Incident handling	Implement measures and protocols to prevent, detect, mitigate, and recover from an incident.	• Out-of-the-box ITIL certified modules. • Native integrations with popular apps, plus custom integrations via extension builder. • Visual workflow automation and orchestration. Built-in CMDB with auto-sync of configuration items (CIs) and a visual service dependencies map.	**Streamlined incident and problem management:** The ITIL-certified incident and problem management modules in ServiceDesk Plus help establish robust processes that accelerate response and resolution through AI-driven triaging, automated workflows, and cross-team collaboration. Beyond just tackling incidents, they enable teams to identify root causes, maintain a known error database, and implement lasting fixes to prevent recurring disruptions.

Article and measures	Your responsibility	ServiceDesk Plus capabilities	Outcomes that accelerate compliance
			Omnichannel detection and logging of issues: ServiceDesk Plus provides native integrations with leading IT monitoring tools like SolarWinds, ManageEngine Site24x7, and PRTG, automatically converting alerts into incidents to speed up response times. It also integrates with IAM and SIEM tools, including Microsoft Entra ID, Zoho Directory, and ManageEngine Log360. Additionally, business communication tools like Microsoft Teams, Outlook, and Slack connect seamlessly, enabling end users to report and track incidents with ease. **Workflows that enforce process discipline:** With visual workflow builders, ServiceDesk Plus helps standardize and automate processes across the enterprise such as deploying predefined playbooks for incident response and enforcing structured frameworks for root cause analysis. Beyond automating actions within the platform, it can also trigger operations in third-party tools, enabling end-to-end workflows that connect teams, departments, and systems of record. **Precise impact assessment with CMDB:** The built-in CMDB features an interactive map of business services and their dependencies, enabling precise impact assessment during incidents. Each CI includes detailed insights such as issue history and related change failures, helping teams identify root causes more accurately and resolve issues faster.

Article and measures	Your responsibility	ServiceDesk Plus capabilities	Outcomes that accelerate compliance
Article 21 - Cybersecurity risk-management measures (2)(f) Policies and procedures to assess the effectiveness of cybersecurity risk management	Ensure ITSM processes comply with cybersecurity risk policies and that security incidents are reported to the appropriate authorities within the required timeframe.	• An intuitive report builder featuring instant and query-able reports. • Real-time bespoke dashboards to track any metric. • Automated notifications across various channels, including SMS. • Custom modules for unique use cases.	**Real-time visibility on compliance:** The visually rich, customizable dashboards displays real-time operational oversight of your IT service delivery. You can track metrics that matter to you, such as known risks, security breach rates, compliance project statuses, and more. **Timely notifications:** The automated notification system can generate and share custom alerts including data from ongoing incident tickets via email with both internal stakeholders and external contacts, ensuring timely updates. **Centralized IT risk tracking:** The custom module builder caters to niche use cases, perfect for tracking IT risks, as part of broader corporate strategy. With a custom-built risk management module, you can monitor IT infrastructure risks as they arise during incidents, changes, releases, or projects, ensuring all IT risks are logged and managed in one centralized location.
Article 21 - Cybersecurity risk-manage-ment measures (2)(g) Basic cyber hygiene practices and cyber security training	Make employees aware of IT best practices and train them to recognize common cyber threats, including social engineering attacks.	• Governed knowledge base with version control, and draft-to-expiry life cycle.	**Knowledge articles that drive awareness:** Employees can gain awareness and training materials through role-based access to knowledge articles, enhanced with embedded videos and images to make learning more engaging and effective. This simplifies and strengthens your organization's awareness and training efforts.

Article and measures	Your responsibility	ServiceDesk Plus capabilities	Outcomes that accelerate compliance
Article 21 - Cybersecurity risk-management measures (2)(i) Human resources security, access control polices, and asset management	Empower business service teams to publish and manage security and access control policies and maintain oversight of their assets.	• Independent service desk instances for non-IT teams, with full autonomy over personnel, work-flows, and data. • Dynamic request templates. • IT and non-IT asset inventory. • Agent-based and agentless IT asset discovery. • Software asset man-agement. • Asset audits.	**Extend compliance to every function:** ServiceDesk Plus acts as a unified platform to streamline service delivery for both IT and non-IT teams. For instance, security-centric workflows like employee offboarding, ServiceDesk Plus, when integrated with privilege management solutions like ManageEngine PAM360, enables streamlined control and governance over user access and privileges across the organization. **Standardized access logging for compliance:** Service owners can leverage the versatile templates to accurately capture access requirements and maintain complete visibility into requester access within a single system of record. **Time-stamped logs for every action:** IT and non-IT teams can design and execute service workflows across the enterprise, with every action logged and time-stamped to maintain full audit compliance. **Comprehensive asset management for compliance:** IT teams can discover assets in their environment using either agents or probes, and track them accurately within the IT asset inventory. Asset management also covers non-IT assets, enabling teams like Facilities to track utility items such as fire extinguishers, desks, projectors, and more. **Visibility that minimizes software installation risk:** IT teams can monitor software installed across organizational assets and quickly detect any unauthorized or prohibited applications on end-user devices.

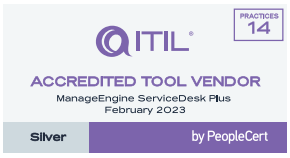
Article and measures	Your responsibility	ServiceDesk Plus capabilities	Outcomes that accelerate compliance
Article 23 - Reporting obligations (4)(a) Within 24 hours, an early warning should be communicated, as well as some first presumptions regarding the kind of incident to the competent authority or CSIRT	Consolidate details from initial incident detection and response, along with estimated impact of the incident, and report them to the appropriate authorities.	• Time bound automations.	**Auto-notify authorities with live incident data:** ServiceDesk Plus delivers a wide range of automation capabilities within its workflows. These include timer-based actions that ensure incident details are automatically compiled and shared with the appropriate authorities within the required time window, using real-time data from the ongoing resolution process.
Article 23 - Reporting obligations (4)(b) After 72 hours, a full notification report must be communicated, containing the assessment of the incident, severity and impact, and indicators of compromise	Prepare an incident report outlining the containment steps, likely root causes, severity, and other key details, and submit it to the appropriate authorities.		
Article 23 - Reporting obligations (4)(d) After 1 month, a final report must be communicated	Review the containment actions and long-term solutions implemented to prevent recurrence and share the final incident report.	• Low-code custom actions to extend the functionality of the platform.	**Timely authority updates on closure:** With ServiceDesk Plus Custom Actions, the final root cause summary and resolution details can be automatically shared with the relevant authorities as soon as the problem status is marked as closed, ensuring timely communication.

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.

Read our customer success stories here. And for more information, visit www.servicedeskplus.com.



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 your ITSM align with the NIS2 Directive?

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).

Disclaimer:

The complete implementation of the NIS2 directive requires a variety of process, policy, people, and technology controls.The solutions mentioned above are some of the ways in which IT management tools help with the NIS2 requirements. Coupled with other appropriate solutions, processes, people controls, and policies, ManageEngine's solutions can help organizations comply with the NIS2 directive.

This material is provided for informational purposes only, and should not be considered as legal advice for the NIS2 compliance. ManageEngine makes no warranties, express, implied, or statutory, as to the information in this material. Please contact your legal advisor to learn how NIS2 impacts your organization and what you need to do to comply with the NIS2 Directive.