Driving DORA compliance with effective ITSM practices

ManageEngine
ServiceDesk Plus

Table of contents

Understanding the Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA), which came into effect January 2025, is a transformative European Union regulation aimed at strengthening the cybersecurity and operational resilience of financial entities. Before DORA, digital resilience rules were fragmented across the EU, creating a complex and inconsistent compliance landscape. DORA establishes a unified framework, ensuring that all financial institutions and their critical third-party providers can withstand, respond to, and recover from all types of information and communication technology (ICT)-related disruptions and threats.

It mandates that banks, insurance companies, investment firms, and their technology partners implement robust systems, controls, and response mechanisms to effectively address digital risks.

Five pillars of DORA

DORA's comprehensive framework is built on five interconnected pillars. Understanding each is critical to developing a successful compliance strategy.

1. ICT risk management

This is the foundation of DORA. Financial entities are required to establish and maintain a comprehensive, well-documented ICT risk management framework. This isn't just about having an antivirus program; it's about a continuous cycle of identifying, protecting, detecting, responding, and recovering.

Key mandates:

- Develop a detailed ICT risk management framework that is integrated with the overall business risk strategy.
- Maintain a continuously updated inventory of all ICT assets and map their interdependencies.
- Conduct regular risk assessments on all ICT systems and processes.
- Implement robust security measures for protection and prevention.
- Establish business continuity and disaster recovery plans based on business impact analyses.

2. ICT-related incident management and reporting

When incidents occur, DORA demands a structured and swift response. The regulation introduces a harmonized incident classification and reporting system across the EU.

Key mandates:

- Implement a process to monitor, manage, log, classify, and resolve all ICT-related incidents.
- Classify incidents based on criteria set by European Supervisory Authorities (ESAs), such as the number of users affected, duration, and geographical spread.
- Report major ICT-related incidents to the relevant national competent authority using a standardized template and timeline. This includes initial, intermediate, and final reports.

3. Digital operational resilience testing

You can't be resilient if you don't test your defenses. DORA mandates a rigorous and comprehensive digital operational resilience testing program to identify vulnerabilities and assess the effectiveness of protective and recovery measures.

Key mandates:

- Implement a process to monitor, manage, log, classify, and resolve all ICT-related incidents.
- Classify incidents based on criteria set by European Supervisory Authorities (ESAs), such as the number of users affected, duration, and geographical spread.
- Report major ICT-related incidents to the relevant national competent authority using a standardized template and timeline. This includes initial, intermediate, and final reports.

4. Managing ICT third-party risk

DORA extends its reach beyond the financial institution itself to its critical ICT third-party providers (TPPs), such as cloud providers, software vendors, and data analytics firms. The principle is simple: you can outsource the service, but you can't outsource the risk management.

Key mandates:

- Maintain a register of all third-party ICT service contracts.
- Conduct thorough due diligence and risk assessments before entering into any new third-party arrangement.
- Ensure contracts with TPPs include specific provisions covering security, availability, data location, and audit rights.
- Critical TPPs will be subject to direct oversight by a lead overseer from the ESAs.

5. Information and intelligence sharing

Recognizing that collective defense is stronger, DORA encourages financial entities to participate in trusted communities to share cyber threat information and intelligence.

Key mandates:

- Entities are permitted to exchange cyber threat intelligence to enhance their individual and collective resilience.
- This sharing must occur within trusted communities and in a manner that protects sensitive data and complies with the GDPR.

Digital Operational Resilience Testing (DORT)

Conduct regular and advanced testing of ICT systems, including threat-led penetration testing for critical functions at least every three years.

ICT risk management

Establish and maintain robust governance and control frameworks to manage all ICT risks—covering people, processes, and technology.

ICT-related incident reporting

Implement standardized processes to detect, classify, and report ICT-related incidents within strict timelines.

ICT third-party risk management

Monitor and manage risks associated with external technology providers, including contractual oversight, risk assessments, and exit strategies.

Information sharing

Voluntarily exchange cyber threat intelligence and best practices with peers, regulators, and information-sharing communities to improve collective resilience.

DORA Articles that ServiceDesk Plus can help you become compliant with

To help organizations navigate DORA, it is important to understand how its key articles translate into actionable IT service management practices. ManageEngine ServiceDesk Plus, with its ITIL-aligned capabilities, enables organizations to align their ITSM workflows with DORA requirements.

Below are the specific DORA Articles that ServiceDesk Plus can support compliance with by strengthening risk management, incident response, operational resilience, and audit readiness.

ICT Risk Management

- Article 5, Governance and organisation
- Article 6, ICT risk management framework
- Article 8, Identification
- Article 9, Protection and prevention
- Article 10, Detection
- Article 11, Response and recovery
- Article 13, Learning and evolving
- Article 14, Communication
- Article 16, Simplified ICT risk management framework

ICT-Related Incident Management

- Article 17, ICT-related incident management process
- Article 18, Classification of ICT-related incidents and cyber threats
- Article 19, Reporting of major ICT-related incidents and notification of significant cyber threats

Article 5 - Governance and organisation

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Financial entities must establish an internal governance and control framework to manage ICT risk and ensure digital operational resilience.	• ITIL-aligned ITSM processes • Custom module for risk register	Implement ITIL-aligned ITSM processes such as incident management, problem management, and change management to log, track, and resolve ICT disruptions and operational risks. Support ICT risk identification and tracking by creating bespoke modules for risk register that allow organizations to document risk details, assess impact and likelihood, define mitigation actions, and monitor risk treatment status as part of their internal governance and control framework.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
2.The management body is accountable for establishing and overseeing the organization's ICT risk management framework. It shall: (c) Define clear roles, responsibilities, and governance arrangements for ICT-related functions to ensure effective communication and coordination. (e) Approve, oversee, and periodically review ICT business continuity policies and response and recovery plans. (f) Approve and review ICT internal audit plans, audits, and significant modifications. (h) Approve and review policies governing ICT third-party service provider arrangements.	• User roles • Role-based access control (RBAC) • SLAs • Workflow • Automated notifications • Tasks • Knowledge base • Vendors in asset management	Define clear roles and responsibilities for ICT-related functions through RBAC, configurable user roles, and granular permission settings. Enable effective ICT governance through structured workflows, approval mechanisms, SLAs, ensuring timely communication, coordination, and accountability across ICT functions. Automated notifications, task assignments, and collaboration features keep the right stakeholders informed at the right time. Document ICT policies, business continuity procedures, response and recovery plans, and internal audit plans within the knowledge base. Route these documents through structured approval workflows, define review

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
(i) Establish reporting channels to keep management informed about: • ICT third-party service arrangements. • Planned material changes to those arrangements. • Impact of such changes on critical or important functions. • Major ICT incidents and the related response, recovery, and corrective measures.		schedules, and maintain version control in the solutions module to ensure management oversight, accountability, and periodic review. Maintain vendor and contract records within asset management and the CMDB to track ICT service providers and their relationships to critical business functions. Capture and route planned modifications to vendor services via change management workflows for review. Record major vendor-related incidents and corrective actions through incident and problem management. Consolidate updates using reports and dashboards to provide management with corporate-level visibility.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
3. Financial entities, other than micro enterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.	• User roles	Create dedicated roles to monitor ICT third-party service arrangements. Provide access to vendor records, related vendor or asset records, reports and dashboards so the designated role or senior management can oversee vendor services, associated risks, and contractual arrangements.
4. Members of the management body must maintain sufficient knowledge and skills to understand and assess ICT risk and its operational impact, including through regular training appropriate to the level of ICT risk managed.	• Knowledge base	Document ICT risk policies, incident analyses, mitigation procedures, and response guidelines in the ServiceDesk Plus solutions module to create a structured knowledge repository for ICT risk management. Provide role-based access so management body members and relevant stakeholders can review validated risk documentation and operational guidance. Maintain accuracy throughapproval, custom expiry dates, and automated review cycles to ensure risk documentation reflects evolving threats,

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		incident learnings, and regulatory expectations. Surface relevant insights from historical incidents and documented risks using AI-powered solution generation and RAG-based recommendations, helping leadership continuously strengthen their understanding of ICT risk and its operational impact.

Article 6 - ICT risk management framework

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Maintain a comprehensive ICT risk management framework to quickly, efficiently, and effectively manage ICT risks and ensure digital operational resilience.	• Custom module • Incident, problem, and change management • Knowledge base	Provide structured risk identification, assessment, and remediation workflows through the bespoke risk assessment module, enabling organizations to document risk details, mitigation plans, and supporting evidence in structured, auditable records.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		Enable rapid ICT risk response through an integrated ITSM framework that includes incident, problem, and change management. Centralize all risk management documentation in the knowledge base with version control to ensure the framework remains well documented and audit-ready.
2. Protect all ICT and information assets, including hardware, software, servers, infrastructure, and sensitive areas, from damage or unauthorized access.	• Asset management • CMDB • Incident management • Fine-grained access	Maintain a detailed inventory of hardware, software, and configurations using asset management and CMDB. Enforce controlled access to asset records, configuration items (CIs), and related incident data through role-based and fine-grained access permissions.
3. Minimize ICT risk impact and provide updated ICT risk information to competent authorities upon request.	• Custom module • Incident management • Problem management • Custom reports	Define and track risk mitigation strategies in the custom risk assessment module. Minimize impact through rapid response and root cause elimination using incident and problem management. Generate on-demand regulatory reports delivering complete ICT risk information and mitigation status.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
4. Assign ICT risk oversight to an independent control function and ensure segregation of risk management, control, and audit functions.	• Custom roles • Technician groups • Approval workflows	Create separate roles for ICT risk management, control, and internal audit through custom roles with distinct permissions. Enforce segregation via technician groups. Prevent self-approval conflicts through approval workflows, aligning with the three lines of defense model.
5. Document and review the ICT risk framework at least annually or after major incidents; continuously improve and submit review reports to authorities.	• Incident management • Major incident workflow • Reports • Knowledge base with version control and next review date	Store ICT risk framework documentation in the knowledge base with solution versioning, revision history, and approval workflows, and define review dates to ensure periodic updates. Schedule periodic maintenance tasks to trigger annual framework review activities and configure a major incident workflow in incident management to automatically create review tasks or notifications after major incident closure. Generate exportable review reports for submission to competent authorities.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
7. Establish formal follow-up for timely verification and remediation of critical ICT audit findings.	• Problem management • Change management • Tasks and checklists	Log findings as problem records and assign to responsible teams. Apply change management workflows for controlled execution with approvals. Break remediation actions into tasks and checklists for systematic closure.

Article 8, Identification

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Identify, classify and document all ICT-supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies. Review at least yearly.	• ITAM • CMDB • Custom CI types	Maintain up-to-date hardware and software inventories through ITAM, organize assets using custom CI types to represent business functions and roles, and use the CMDB to document these functions and link them to owners for auditable coverage.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
2. Continuously identify all sources of ICT risk, including exposure to/from other entities; assess cyber threats and ICT vulnerabilities; review risk scenarios regularly.	• Risk assessment module • Scheduled reports • Integrations	Log cyber threats and vulnerabilities in the risk assessment module, integrate with tools like Endpoint Central, Vulnerability Manager Plus, or a SIEM to ingest threat data, and use scheduled reports to notify owners for periodic review of risk scenarios.
3. Perform risk assessment upon major changes in network/infrastructure, processes, or procedures affecting ICT-supported functions or assets.	• Change management • Change workflow with Wait for Condition node	Plan, evaluate, approve, and implement IT changes systematically using change management. Configure change workflows with a “Wait for Condition” node to pause major changes until the required risk assessment is completed.
4. Identify all information assets and ICT assets (including remote sites and hardware), map critical ones, and document configurations and interdependencies.	• ITAM • Asset discovery • CMDB • Relationship mapping	Track and manage all IT and non-IT assets through ITAM, employ agent-based or agentless asset discovery methods to maintain accurate inventories, and map critical assets and their interdependencies in the CMDB using relationship mapping.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
5. Identify and document all processes dependent on ICT third-party providers, and map interconnections with providers supporting critical/important functions.	• Vendor in asset management • CMDB relationship mapping	Record and manage external service providers within asset management module, link them to business services in the CMDB to visualize dependencies, and synchronize vendor and risk data through integrations with vendor risk management tools where needed.
6. Maintain relevant inventories from paras 1, 4, and 5; update periodically and after major changes.	• Asset discovery schedule • CMDB • Change triggers	Keep asset and CI inventories current through automated discovery schedules, maintain updated records in the CMDB, and automatically adjust asset statuses and configurations after major changes using change management triggers.
7. Conduct yearly ICT risk assessments on all legacy ICT systems and before/after connecting technologies, applications, or systems.	• Change templates • Groups in ITAM • CMDB • Maintenance module	Use asset groups to classify legacy ICT systems, with asset state to flag EOL status. Schedule maintenance activity via the maintenance module to generate annual ICT risk review for the legacy asset group. Apply change templates to enforce pre- and post-implementation risk assessment stages for every change involving these systems.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		Leverage relationships in the CMDB to identify impacted legacy systems during integration events.

Article 9 - Protection and prevention

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Continuously monitor and control ICT security and functioning, and minimize the impact of ICT risk through appropriate security tools, policies and procedures.	• Integration with monitoring tool • Incident management • Problem management • Change and release management	Integrate with network and security tools like OpManager or other third-party monitoring systems to automatically log and track incidents from alerts, ensuring visibility and accountability. Through incident, problem, and change management modules, minimize ICT risk impact by enforcing structured response workflows, performing root cause analysis, and tracking corrective actions. Get support for controlled deployment of ICT security tools and procedures through change

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		and release management, while policies and best practices can be documented and shared via the knowledge base.
4. Develop and document an information security policy protecting availability, authenticity, integrity and confidentiality of data and ICT assets; establish risk-based network and infrastructure management including isolation during incidents; implement access controls restricting physical and logical access to authorized personnel; enforce strong authentication and encryption based on data classification; implement documented ICT change management controls; maintain documented patch and update policies.	• Knowledge base • RBAC • Technician roles • Request approvals • Audit logs • Change management • CAB • Approval workflows	Create and store information about security policies in the knowledge base, use version control to track updates, and route policies through approval workflows so documented standards exist for protecting availability, integrity, confidentiality, and authenticity of data. Enforce least privilege through role-based permissions, automate access request/approval, and maintain complete access modification audit trails. Establish and maintain a risk-based ICT change management process requiring all ICT changes to be initiated, recorded, and managed through change requests (RFCs). Identify, assess, and document the risks and potential impacts associated with each RFC

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		prior to approval. Ensure that ICT changes are subject to defined testing and validation activities, authorized through appropriate management and CAB approvals, and implemented in accordance with approved procedures. Perform and document post-implementation reviews to verify the effectiveness of changes and to prevent ICT-related incidents, ensuring full traceability and auditability across the ICT change life cycle.

Article 10 - Detection

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Prompt detection of anomalous activities, ICT performance issues, incidents, and single points of failure. Detection mechanisms must regularly be tested.	• Incident management • CMDB relationship map • Integrations with monitoring and observability tools	Integrate with monitoring and observability tools like OpManager or Site24x7 to feed performance anomalies directly into ServiceDesk Plus as incidents. Use the CMDB relationship map to visually identify and flag

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
	• Zia Cluster Analysis	single points of failure within critical business services. Zia Cluster Analysis detects emerging patterns across incoming incidents.
2. Detection must include multiple layers of control, thresholds, and automatic alerts to trigger ICT incident response.	• Integrations • Email to ticket conversion • API integrations • Business rules • SLAs • Escalation rules	Forward alerts from security and monitoring tools into ServiceDesk Plus via email-to-ticket, or API integrations, enabling automatic incident creation. Through the Site24x7 integration, you can configure which monitor types (e.g., server, website, application), monitor groups, and alert statuses (Down, Trouble, Critical) automatically create incidents in ServiceDesk Plus. This ensures that only meaningful, threshold-breaching events generate tickets, preventing minor alerts from cluttering your incident queue. Business rules and templates allow these security incidents to be classified, prioritized, and assigned to the appropriate security or IT teams based on severity. SLA and escalation rules ensure that high-priority security events are promptly

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		escalated, while major incident workflows enable structured response and coordination for critical incidents. Activity logs, audit trails, and ticket history provide traceability of all actions taken during investigation and response, supporting governance and compliance requirements.
3. Allocate resources and capabilities to monitor user activity, ICT anomalies, and especially cyberattacks.	• Technician groups • Request list view • Technician auto-assign	Define specialized technician groups, such as Incident Response Team (IRT), Cyber Incident Response Team (CIRT), and Security Operations Center (SOC), composed of trained technicians who manage major incidents arising from reported anomalies, ensuring qualified staff are assigned and accountable for tracking and resolving the issue. Request list views allow operations staff to monitor open, escalated, and unassigned incidents by category or priority. Technician auto-assign immediately routes incidents to available resources.

Article 11 - Response and recovery

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. As part of the ICT risk management framework referred to in Article 6(1) and based on the identification requirements set out in Article 8, financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.	• Knowledge base with version control	Store and maintain the ICT business continuity policy as part of the overall business continuity policy, with versioning and approval records in the knowledge base.
2. The ICT business continuity policy must be implemented through documented plans and mechanisms that ensure continuity of critical functions, limit damage from incidents, activate containment plans without delay, estimate impacts, and set out crisis communication actions.	• Incident workflow • Tasks • Notification rules • CMDB • SLA management • Problem management	Activate predefined response procedures through incident workflow upon incident classification, trigger containment task assignments based on incident type, and escalate critical cases to crisis management teams without delay. Identify affected critical functions and dependencies via CMDB linkage, enforce response and restoration timelines through SLA management, ensure

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		real-time communication to relevant internal staff using notification through incident workflow, and capture preliminary impact and damage estimates through linked problem management processes.
3. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to independent internal audit reviews.	• Incident workflow • Tasks • Checklist • Knowledge base	Provide structured recovery and response workflows through incident, problem, and change management, enabling organizations to document recovery steps, mitigation actions, and supporting evidence in structured, auditable records. Enable rapid ICT response during incidents through integrated task assignment and checklist tracking. Centralize all recovery documentation in knowledge base, ensuring plans remain well-documented.
6. Financial entities must test ICT business continuity and response/recovery plans at least annually, including cyberattack and	• Change management • Problem management • Knowledge base	Manage annual and event-triggered testing exercises as formal change records with assigned owners, approvals, and due dates. Record post-test findings as linked problem

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
failover scenarios, and review plans based on test results, audit recommendations, and supervisory feedback.		records to drive corrective actions and plan updates. Update knowledge base documentation based on test outcomes and audit findings while preserving a complete audit trail of reviews and modifications for supervisory inspection.
7. Non-microenterprises must establish a crisis management function with clear procedures for managing internal crisis communications upon activation of continuity or recovery plans.	• Announcement • Notifications • Email templates • Integrations with collaboration tools	Enable synchronized internal and external communication by configuring notifications via incident workflow, notification rules, announcements, and integrating with collaboration tools like Microsoft Teams, Zoho Cliq, and email systems. Use preconfigured communication templates to standardize messages to all stakeholders.
8. Financial entities must maintain readily accessible records of all activities conducted before and during disruptions when continuity or recovery plans are activated.	• Ticket history • Worklogs and notes in tickets • Custom reports	Maintain timestamped audit logs of all incident actions, task completions, notifications, and approvals during disruption events. These records are readily accessible

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		and exportable, providing regulators and auditors with a complete chronological account of activities as required.
10. Financial entities, other than microenterprises, shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.	• Custom field • Reports and dashboards	Aggregate incident data across the year using custom fields capturing estimated downtime, service impact, and affected users per major incident. Reports and dashboards consolidate this into structured annual summaries ready for submission upon regulatory request.

Article 13 - Learning and evolving

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyberattacks,	• Ask Zia • ChatGPT integration • Azure OpenAI integration • CMDB	Leverage Ask Zia—powered by ChatGPT or Azure OpenAI integration—to explore and summarize information on emerging vulnerabilities, cyber threats, and attack

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
and analyze the impact they are likely to have on their digital operational resilience.	• Zia Cluster Analysis	patterns through natural language queries, supporting proactive awareness and investigation. Identify recurring incident patterns and potential systemic issues using Zia Cluster Analysis on historical data. Analyze potential impact using the CMDB CI relationship map to trace affected configuration items, services, and business functions.
2. Financial entities must conduct post-incident reviews after major ICT incidents to evaluate root causes, response effectiveness, and required improvements. These reviews should assess whether established procedures were followed and whether response actions were effective. The review should evaluate: (a) Timeliness of responding to security alerts and assessing incident impact and severity. (b) Quality and speed of forensic analysis,	• AI-generated post incident reviews through Zia • Problem management • Change management • Reports • SLAs • Incident management	Upon major incident closure, incident workflow triggers a formal post-incident review task assigned to the responsible team. Problem management records root cause findings, links them to the originating incident, and tracks improvement actions to completion. Audit logs provide a timestamped record of all response actions, enabling assessment of whether procedures were followed. Structured reports consolidate review findings into exportable outputs ready for submission to competent authorities upon request.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
where applicable. (c) Effectiveness of incident escalation processes. (d) Effectiveness of internal and external communication during the incident.		
3. Continuously incorporate lessons from digital operational resilience testing, real ICT incidents, cyberattacks, and challenges from activating business continuity and response plans into the ICT risk assessment process.	• Problem management • Knowledge base • Risk register • Change management • Workflow	Capture lessons learned as knowledge base articles, creating a structured and searchable repository of findings from incidents, tests, and audits. Feed conclusions into the risk register to update identified risks and controls. Change management workflows translate improvement actions into formally tracked and approved changes to ICT processes and procedures, ensuring lessons result in tangible framework improvements.
4. Financial entities shall monitor effectiveness of digital operational resilience strategy; map evolution of ICT risk over time; analyze frequency, type, magnitude, and patterns of ICT-related incidents (especially	• Reports • Dashboards • Custom fields • SLA management • Incident management	Track incident trends over time—including frequency, severity, type, affected services, and resolution times— using reports and dashboards. Custom fields enable consistent incident categorization that makes pattern and

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
cyberattacks); understand ICT risk exposure for critical functions; enhance cyber maturity and preparedness.		magnitude analysis meaningful and auditable. SLA data provides measurable indicators of response and resolution effectiveness, supporting continuous monitoring of resilience strategy performance.
5. Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.	• Dashboard and reports • Integration with Analytics Plus	Generate structured annual summaries of incident trends, post-incident review outcomes, and improvement actions from problem management using reports and dashboards, directly supporting the preparation of the yearly management body report. Zia's AI-driven analytics highlight key patterns and anomalies across incident data, supporting data-driven recommendations to the management body.

Article 14 - Communication

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.	• Announcements • Email template • Incident management workflow	Enable responsible disclosure by defining crisis communication plans within incident management, send approved messages using email templates, publish public or internal updates via announcements, and record all disclosures in communication logs for auditability.
2. As part of the ICT risk management framework, financial entities shall implement communication policies for internal staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed.	• Roles • User groups • Notifications via incident workflow • Self-service portal	Differentiate internal communication using roles and user groups, deliver detailed incident information to response and recovery teams through role-based access, and share high-level status updates with general staff via notifications through an incident workflow and the self-service portal, ensuring appropriate and controlled information flow.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
3. At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfill the public and media function for that purpose.	• Roles • Technician groups • Audit logs	Assign responsibility for ICT incident communications by configuring roles and technician groups to designate a named communications owner and record all communication actions in audit logs to demonstrate accountability for public and media disclosures.

Article 16 - Simplified ICT risk management framework

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Entities must: (a) Document and maintain a sound ICT risk management framework. (b) Continuously monitor security and functioning of all ICT systems. (c) Minimize ICT risk through resilient,	• Risk register • Knowledge base • CMDB • Incident management and workflow • Change management	Document a sound ICT risk management framework by recording risks in the risk register, storing policies and procedures in the knowledge base. Monitor ICT system security and availability by capturing alerts and anomalies as

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
updated systems protecting data availability, integrity, and confidentiality. (d) Promptly identify, detect, and swiftly handle ICT incidents and anomalies. (e) Identify key dependencies on ICT third-party service providers. (f) Ensure continuity of critical functions through BCPs, response, recovery, and backup measures. (g) Regularly test plans and effectiveness of ICT risk controls. (h) Implement lessons from testing and post-incident analysis into ICT risk assessment.		incidents through incident management and integrations with monitoring tools. Reduce ICT risk by governing system changes through change management and maintaining accurate asset data in the CMDB. Detect ICT anomalies and respond quickly using incident management, major incident workflows, and escalation rules. Identify dependencies on ICT third-party providers by maintaining vendor records and linked services in the CMDB, supported by integrations where available. Ensure continuity of critical functions by documenting continuity, backup, and restoration procedures in the knowledge base. Update post-incident and post-test findings using the risk register and store training materials for staff and management using the knowledge base.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
2. The framework must be documented, regularly reviewed after major incidents, and continuously improved. A review report must be submitted to regulators upon request.	• Knowledge base with version control • Reports	Maintain up-to-date ICT risk management documentation with version control, tracking changes after major incidents or supervisory reviews. Generate audit-ready summaries using Reports for quick submission to authorities.

Article 17 - ICT-related incident management process

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related incidents.	• Incident management • Incident templates and workflow • Omni-channel incident logging	Establish a structured ICT incident life cycle using incident management and customizable workflows to ensure all incidents are processed in a standardized, auditable manner. Detect incidents promptly by integrating real-time monitoring tools and automating ticket creation. Capture incidents via omni-channel

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
	• SLA • Notification rules	logging, including portal, email, SMS, and calls. Standardize incident reporting using incident templates to capture required details at logging. Enforce timely response and resolution using SLAs and escalation mechanisms. Notify internal and external stakeholders through incident workflow notifications, while notification rules determine the channel and when notifications needs to be triggered across the incident life cycle.
2. Record all ICT incidents and significant cyber threats; ensure consistent monitoring, handling, follow-up, and root cause prevention.	• Incident management • Problem management • Change management • Workflow • SLA management • Knowledge base • Zia Cluster Analysis • RCA by Zia	Record all ICT-related incidents and significant cyber threats using incident management with complete, timestamped activity history. Ensure consistent monitoring, handling, and follow-up through incident workflow, SLA management, and escalation rules. Identify and document root causes using problem management by linking recurring incidents to underlying issues. Detect recurring patterns

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		using Zia Cluster Analysis to support early intervention. Accelerate root cause analysis using RCA by Zia by identifying related incidents, highlighting contributing factors, and surfacing patterns across incidents. Implement permanent fixes through change management to address root causes and prevent recurrence.
3. The ICT-related incident management process referred to in paragraph 1 shall: • Implement early warning indicators; • identify, track, log, categorize, and classify incidents by priority, severity, and service criticality; • assign roles and responsibilities; • set communication and escalation plans; • report major incidents to management; establish response procedures to mitigate impacts and restore services.	• Monitoring tool integrations • Incident templates, • Categories, priority matrix, impact/urgency fields • SLAs • Technician auto-assignment • Business rules • Roles • Notification rules • Announcements	• Detect potential incidents proactively through monitoring integrations and automated alerts. • Log, categorize, and prioritize incidents consistently using incident template with categories, subcategories, impact and urgency fields, and a configurable priority matrix to prioritize incidents based on severity and service criticality. • Define and enforce roles and responsibilities using role-based access controls, technician groups, and

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
	• Collaboration tool integrations • Linked incident, problem, and change management • CMDB relationship mapping	technician auto-assignment to ensure the appropriate teams are engaged for each incident scenario. • Communicate timely updates to staff, stakeholders, and clients via notifications, emails, announcements, and collaboration channels. Set proactive and reactive escalate rules for incidents. • Mitigate service impacts and restore operations efficiently by linking incidents to problem and change tickets, referencing CMDB relationships for impact analysis.

Article 18 - Classification of ICT-related incidents and cyber threats

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
1. Financial entities shall classify ICT-related incidents and determine their impact based on criteria such as number of clients affected, duration, geographical spread, data losses, criticality of services, and economic impact.	• Incident templates • Custom fields • Categories and subcategories • Priority matrix • Service catalog • CMDB • SLAs • Reports and dashboards	Classify ICT-related incidents based on measurable impact criteria by: • Capturing affected users, impacted services,number of users, and urgency through customizable incident templates and custom fields. • Automatically determining severity using the priority matrix (impact × urgency) to ensure consistent classification. • Linking incidents to CIs and business services via the CMDB to assess service criticality. • Tracking downtime, response, and resolution times through SLA management to measure incident duration. • Tagging incidents by site or location and using dashboards to assess geographicalor multi-entity impact.

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		• Generating structured reports to document customer impact and service disruption scope for formal regulatory classification.
2. Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.	• CMDB • Priority matrix • Reports and dashboards • SLA management • Workflow	Establish predefined thresholds for major ICT incidents by combining CMDB-mapped service criticality, impact data (such as affected users, services, and duration), and priority matrix rules, automatically flag and escalate high-severity incidents through workflow automation and SLA breach conditions, and use dashboards and structured reports to identify, monitor, and formally document incidents that qualify as major ICT-related incidents.

Article 19, Reporting of major ICT-related incidents and voluntary notification of significant cyber threats		
Regulatory intent	**ServiceDesk Plus capabilities**	**How these capabilities help organizations comply**
1. Financial entities shall report major ICT-related incidents to the relevant competent authority in a structured manner at different stages, ensuring timely updates with relevant and complete information.	• Incident workflow-based notification • Notification rules	Define structured, stage-by-stage major ICT incident response workflows using incident workflow, with customizable notifications configured at each transition—detection, containment, resolution, and closure—ensuring competent authorities receive timely status updates at every defined reporting point. Configure outbound notification rules triggered at specific workflow transitions to automatically dispatch incident status updates to designated contacts with consistent and accurate information at each stage.
2. Financial entities may voluntarily notify significant cyber threats to the competent authority when deemed relevant to the financial system, service users, or clients.	• Incident workflow • Notification action node	Configure the incident workflow to trigger a dedicated, optional notification path when an incident is categorized as a significant cyber threat distinct from the mandatory major incident reporting workflow. The notification

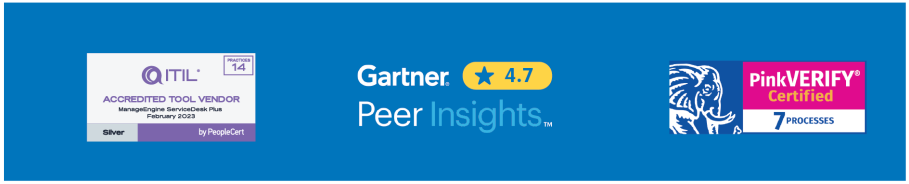
Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
		action node within the workflow dispatches a notification containing incident details to the competent authority's designated contact.
3. Where a major ICT incident impacts the financial interests of clients, financial entities must inform affected clients without undue delay, and for significant cyber threats, advise clients on protective measures they should consider.	• Incident workflow • Notification templates	Extend the incident workflow to trigger client-facing notifications upon classification of a client-impacting incident. Use notification templates to prepare preapproved, client-ready communications explaining the incident, and for significant cyber threats, recommended protective measures. Delivery channels and dynamic variables are handled by the existing notification rules configuration. Enforce the "without undue delay" obligation through SLA management, setting breach thresholds on client notification tasks with automatic escalation if the window is at risk of being missed.
4. Financial entities must submit reports to the competent authority within the required timeframes:	• Incident workflow • Notification rules	Trigger automatic stakeholder notifications using incident workflow at every stage of the incident life cycle—including initial alert,

Regulatory intent	ServiceDesk Plus capabilities	How these capabilities help organizations comply
(a) Initial notification: When the incident is first detected. (b) Intermediate report: Whenever the incident status changes significantly or new information emerges; updated notifications may follow as needed. (c) Final report: After completing root cause analysis and confirming the actual impact.		status changes, and closure—to ensure clients and stakeholders are informed promptly. Configure notification rules to define delivery channels (e.g., email, SMS, push notification) and message templates with dynamic incident variables, ensuring accurate and contextual updates. Enforce the "without undue delay" obligation through SLA management, with escalation rules alerting responsible teams if notification tasks breach the defined timeframe. Record all notifications in audit trails to maintain a complete, verifiable history for regulatory review and compliance.

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 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 applications.

Want to consult our product experts on how ServiceDesk Plus can help you conform to DORA 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).

Disclaimer:

ManageEngine does not claim that the entities using ServiceDesk Plus or its other products will be DORA compliant. Using ServiceDesk Plus might help customers align with specific controls and requirements outlined in the standard and their certification is contingent on multiple factors as might be prescribed by a certifying authority. Coupled with other appropriate solutions, processes, people, controls, and policies, ManageEngine ServiceDesk Plus can help organizations conform to DORA requirements.

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

About the Author

With eight years' experience in IT services, Suganya has hands-on experience handling key IT service management (ITSM) practices. As an avid ITSM evangelist, she is also a ServiceDesk Plus product expert. She creates best-practice articles and blogs that can help ITSM practitioners address their everyday challenges with ServiceDesk Plus, the flagship IT and enterprise service management platform from ManageEngine. Besides her passion for writing, she also enjoys trekking, reading books, playing basketball, and stargazing with her daughters.

Explore more from Suganya