ManageEngine's guide for complying with the DORA



ManageEngine

Table of contents

What is the Digital Operational Resilience Act? 5

What does DORA mean for your organisation? 7

Five core areas of DORA 8

How ManageEngine solutions can help you comply with DORA 9

Article 5: Governance and organisation 11

Article 6: ICT risk management framework 17

Article 7: ICT systems, protocols and tools 24

Article 8: Identification 28

Article 9: Protection and prevention 34

Article 10: Detection 40

Article 11: Response and recovery 45

Article 12: Backup policies and procedures, restoration and recovery procedures and methods 51

Article 13: Learning and evolving 55

Article 14: Communication 59

Article 15: Further harmonisation of ICT risk management tools, methods, processes and policies 61

Article 16: Simplified ICT risk management framework 65

Article 17: ICT-related incident management process 69

Article 18: Classification of ICT-related incidents and cyber threats 74

Article 19: Reporting of major ICT-related incidents and notification of significant cyber threats 76

Control mapping 79

About ManageEngine 81

Disclaimer

Copyright © Zoho Corporation Pvt. Ltd. All rights reserved. This material and its contents ("Material") are intended, among other things, to present a general overview of how you can use ManageEngine's products and services to implement the Digital Operational Resilience Act (DORA) in your organisation. Fully complying with the DORA requires a variety of solutions, processes, people, and technologies. The solutions mentioned in this Material are some of the ways in which IT management tools can help with some of the requirements under the DORA. Coupled with other appropriate solutions, processes, and people, ManageEngine's solutions help organisations align with the DORA. Organisations must do their independent assessment with respect to ManageEngine's features and to what extent they can help them comply with this directive.

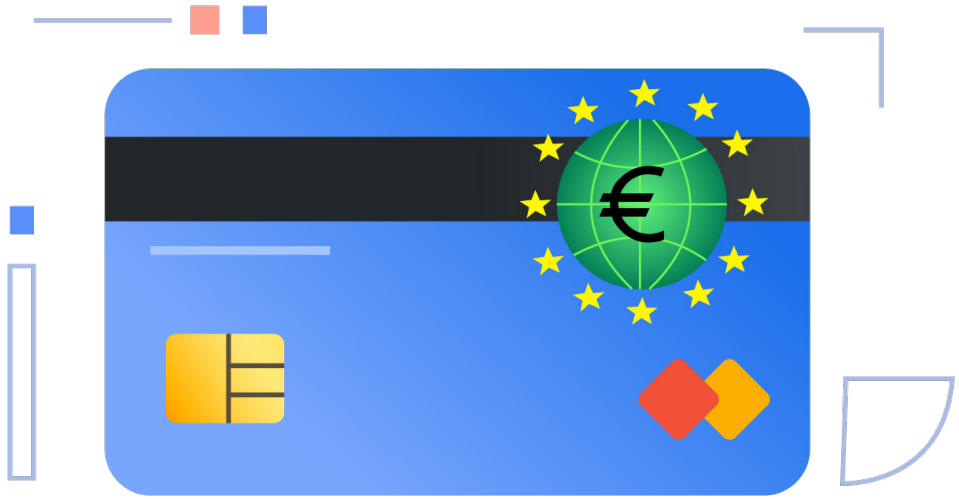
This Material is provided for informational purposes only and should not be considered as legal advice for implementing the DORA. ManageEngine makes no warranties, express, implied, or statutory, and assumes no responsibility or liability as to the information in this Material.

Please contact your legal advisor to learn how the DORA impacts your organisation and what you need to do to comply with the DORA compliance requirements. You may not copy, reproduce, distribute, publish, display, perform, modify, create derivative works, transmit, or in any way exploit the Material without ManageEngine's express written permission. The ManageEngine logo and all other ManageEngine marks are registered trademarks of Zoho Corporation Pvt. Ltd. Any other names of software products or companies referred to in this Material, and not expressly mentioned herein, are the trademarks of their respective owners.

What is the Digital Operational Resilience Act?

Digital transformation in the financial industry has brought numerous advantages, including improved efficiency, enhanced customer experiences, and innovative service offerings. However, this rapid evolution has also exposed financial institutions to various technology-related risks, such as cyberattacks, system failures, and vulnerabilities arising from third-party information and communication technology (ICT) services disruptions.

To tackle these emerging threats and ensure the continuity of essential operations, the European Union implemented the Digital Operational Resilience Act (DORA). This legislation was introduced to create a comprehensive framework aimed at strengthening the operational resilience of financial institutions within the EU.



DORA took effect on January 16, 2023, and full enforcement began on January 17, 2025. The primary goal of DORA is to standardise regulations related to operational resilience across the financial sector, which includes a diverse range of 20 different types of financial entities, such as banks, investment firms, and insurance companies, as well as the third-party ICT service providers that support these institutions.

DORA establishes strict requirements for risk management, incident reporting, and digital operational resilience testing to minimise the potential impact of disruptions. By mandating that financial organisations develop strong frameworks to prepare for, respond to, and recover from operational incidents, DORA aims to enhance the overall stability and security of the financial ecosystem in an increasingly complex technological landscape.

What does DORA mean for your organisation?

The Digital Operational Resilience Act (DORA) is a transformative regulation designed to enhance your organisation's ability to withstand, recover from, and adapt to ICT-related disruptions. Here's what DORA means for your organisation:

Strengthened cyber resilience:

Your organisation needs to implement strong measures to protect your digital infrastructure from cyber threats and operational disruptions. Regular risk assessments and security upgrades will become a core part of your operations.

Governance and oversight:

DORA places accountability at the board level, requiring you to align your governance framework with digital resilience objectives.

Incident reporting and recovery:

Your organisation needs to establish efficient mechanisms to detect, report, and recover from ICT-related incidents, ensuring minimal impact on operations and customer trust.

Third-party risk management:

DORA emphasises the importance of assessing and mitigating risks posed by third-party ICT providers. Your organisation is expected to ensure that your vendors meet the same resilience standards as your organisation.

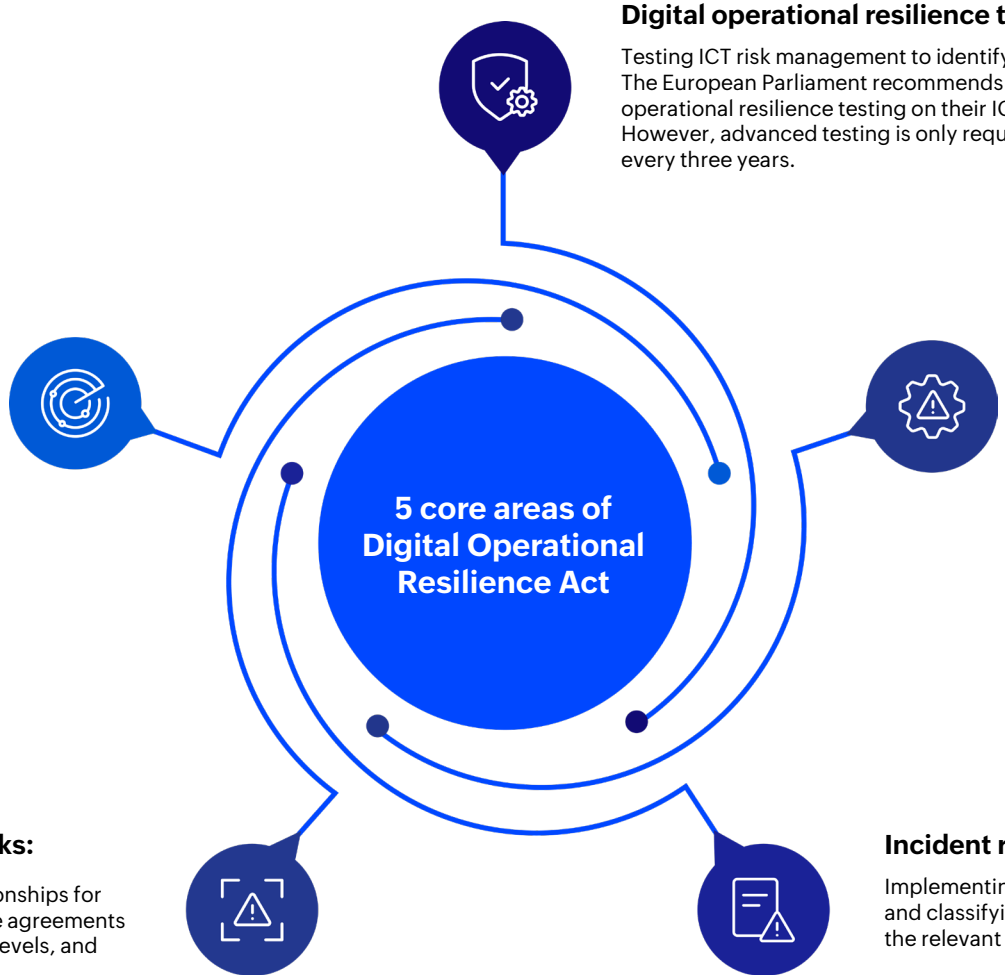
Five core areas of DORA

Digital operational resilience testing:

Testing ICT risk management to identify any weaknesses. The European Parliament recommends annual digital operational resilience testing on their ICT services. However, advanced testing is only required once every three years.

Information sharing and threat intelligence:

Facilitating the sharing of cybersecurity threat information—while safeguarding confidential data—to stay abreast of any recent threats and risks.



ICT risk management framework:

Developing a framework to monitor and manage risks with third-party ICT providers, covering critical aspects like capabilities, levels, and locations.

Managing third-party risks:

Ensuring effective service relationships for better risk management. Service agreements must cover monitoring, service levels, and data processing locations.

Incident reporting and management:

Implementing uniform procedures for monitoring and classifying ICT incidents and reporting them to the relevant authorities.

How ManageEngine solutions can help you comply with DORA

ManageEngine's suite of IT management solutions can assist you in meeting the technical measures with some of the requirements of DORA, thereby supporting compliance with this standard.

However, Articles 5 to 15 of this regulation do not apply to small and non-interconnected investment firms, payment institutions exempt under Directive (EU) 2015/2366, institutions exempt under Directive 2013/36/EU where the Member States have opted not to apply the provision in Article 2(4) of this regulation, electronic money institutions exempt under Directive 2009/110/EC, and small institutions for occupational retirement provision. These firms only need to comply with Articles 16 to 27.

Moreover, Member States have the authority to exclude specific entities from the scope of DORA as outlined in Article 2(5), points (4) to (23) of Directive 2013/36/EU. This flexibility enables Member States to customise the application of DORA in accordance with their regulatory frameworks and the unique situations of particular entities, ensuring that the regulation is applied effectively where it is deemed most necessary.

Article

05

Governance and organisation

Financial entities must have a governance framework for effective ICT risk management to ensure digital operational resilience. Key responsibilities of the management body include:

- Overseeing overall ICT risk management.
- Maintaining standards for data availability and confidentiality.
- Setting roles and governance for ICT functions.
- Approving the digital resilience strategy and risk tolerance.
- Reviewing business continuity and response plans.
- Overseeing ICT audits and budget allocations for resilience training.
- Reviewing policies for third-party ICT services.
- Establishing reporting for ICT arrangements and incidents.

ManageEngine products to help you comply with Article 5

PAM360: Organisations can set up password request-release workflows. These workflows will mandate an approval mechanism for every access request generated. Users are required to enter a reason for their access request, which is relayed to admins. After that, upon verification, the admin may choose whether to allot access or not. This access provisioning can also be combined with a just-in-time (JIT) condition that lets admins allot time-restricted access to users. The workflow can be combined with app-only access control to enforce much more granular security practices, including the principle of least privilege (PoLP).

With PAM360's endpoint privilege management capabilities, IT admins can enforce access controls tailored to endpoints and applications. These access controls include allowlisting and blocklisting applications, implementing child process controls, removing admin rights at the endpoint level, provisioning JIT access to applications, and configuring privilege elevation specific to endpoints.

PAM360 helps organisations implement PoLP access through controls like role-based access control (RBAC) and policy-based access control, granting users only the permissions necessary for their tasks. In addition, PAM360 monitors and records privileged sessions, ensuring accountability and bolstering overall security.

ServiceDesk Plus: Incident response teams (IRTs) can move fast and respond to outages with powerful orchestration capabilities. From omni-channel detection of incidents—from security information and event management (SIEM), observability, and unified endpoint management (UEM) solutions—to real-time notifications in Microsoft Teams and GenAI-powered summaries, ServiceDesk Plus puts every aspect of incident response on auto-pilot. IRTs can further investigate the root-cause of incidents through a dedicated ITIL-compatible problem management practice.

IT teams can regulate access to critical services and applications by building access request forms and publishing them to specific role-based user groups. Every access request can be vetted, authorised, and fulfilled with automated workflows that notify the right service owners and stakeholders at contextual touchpoints.

IT teams can enforce change governance through visual change management workflows, dynamic change templates, change roles, multiple change advisory boards (CABs), and AI-driven change risk predictions. From routine, standard changes like router upgrades to major changes like cloud migrations, IT teams can ensure change success while minimising risks by embedding notifications, condition checks, fine-grained approvals, and orchestrations into change workflows.

IT asset managers can rely on ServiceDesk Plus as the single source of truth for all hardware, software, and non-IT assets. From discovering IT assets across networks and domains to scanning barcodes and QR codes, ServiceDesk Plus offers multifarious discovery techniques. Every IT asset can then be governed over its entire lifecycle—from procurement to disposal—using visual workflows. Software assets can also be scanned and accounted for, ensuring compliance with software license agreements. Any deviation in asset states or software license compliance can be notified to the right stakeholders, thereby establishing strong asset governance.

IT teams can also create entirely new, bespoke governance practices beyond the traditional ITSM practices using Custom Modules in ServiceDesk Plus. Every practice can be monitored and optimised using tailored reports and dashboards.

OpManager Nexus: With its RBAC feature, OpManager Nexus' Network Configuration module enforces strict access controls and maintains detailed audit trails. This ensures that the roles and governance for ICT functions are properly implemented. This also ensures accountability and visibility for ICT risk management, directly supporting DORA's requirements for ICT audits and incident reporting.

Log360: Log360 provides centralised visibility and control over ICT risks, helping management oversee security operations effectively. Its real-time monitoring, risk analytics, and compliance reporting enable financial institutions to maintain high standards of data availability and confidentiality, ensuring a robust governance framework for ICT risk management.

AppCreator: Applications created on AppCreator can be used to add controls for ICT risk management. Automated reporting and real-time dashboards built on the platform can offer insights into the organisation's ICT obligations. Workflows created based upon roles facilitate incident monitoring, enforce policies, and enable data security and integrity. Compliance tracking through dedicated dashboards built on the platform helps to ensure seamless ICT governance.

Article

06

ICT risk management framework

Financial entities must establish a comprehensive ICT risk management framework to ensure digital operational resilience. This includes strategies and tools to protect information and ICT assets from risks such as damage and unauthorised access.
Key points include:

- Assign ICT risk management to an independent control function.
- Document and review the framework annually, as well as updating after major incidents or audits.
- Conduct internal audits with knowledgeable and independent auditors.
- Implement a follow-up process for critical audit findings.
- Include a digital operational resilience strategy that aligns with business objectives and manages incidents effectively.
- Entities can define a multi-vendor strategy and may outsource compliance verification while maintaining overall responsibility.
- Updated information on the framework must be provided to authorities upon request.

ManageEngine products to help you comply with Article 6

Endpoint Central: Offers extensive reporting functionality. In addition to offering detailed insights into endpoint assets, Endpoint Central can also serve governance and auditing needs.

PAM360: Dynamic trust scoring and privileged user behaviour analytics (PUBA) enable organisations to manage risks in real time. With PAM360, businesses can identify critical security policies and parameters, allowing them to prioritise and enforce them effectively. PAM360 helps organisations fit privileged access management (PAM) seamlessly into their security framework, understand user behaviour to spot anomalies and take the appropriate action, and weave security into their business workflows.

Further, PAM360 delivers Zero Trust architecture by design, helping organisations adhere to the PoLP. PAM360 offers organisations the ability to provision time-based access, time-based access elevation, ticket ID verification, application and command-level allowlisting, and comprehensive endpoint privilege management, among others.

Digital Risk Analyzer: Helps organisations manage domain-related risks by providing comprehensive visibility into their security posture. Digital Risk Analyzer identifies potential threats such as domain theft, hijacking, and DNS spoofing. Through detailed checks, it ensures SSL certificate validity, verifies domains against blocklists, and monitors domain expiry. By assessing these risks and taking corrective actions, Digital Risk Analyzer enables organisations to develop a robust web of security strategies, safeguard sensitive data, and maintain customer trust.

Analytics Plus: Provides in-depth insights that help organisations proactively monitor and manage risks across their IT environment. With granular insights into your infrastructure's health and performance, Analytics Plus allows you to track risk indicators, detect potential vulnerabilities, and assess the effectiveness of your risk mitigation strategies.

AD360: Identify and assess potential security risks—like failed logon attempts and users whose passwords never expire in Active Directory and Microsoft 365 environments—with the Identity Risk Assessment report. Take on-the-fly actions to prevent any security breaches. The built-in user behaviour analytics (UBA) features help detect insider threats in your organisation by monitoring rogue users and identifying compromised user accounts and privilege abuse.

Generate pre-configured, detailed reports that can not only provide insights about the environment but also help with governance and auditing requirements. Protect information and ICT assets from unauthorised access using strong multi-factor authentication (MFA) methods.

ServiceDesk Plus: Minimises ICT risks, specifically around availability and uptime, by helping IRTs build highly responsive incident playbooks. From ingesting alerts from different solutions to AI-driven triage and routing, ServiceDesk Plus enables organisations to adopt a proactive incident response and problem management approach that is critical to ensuring digital operational resilience.

Any change to the ICT infrastructure can be controlled using ServiceDesk Plus' fine-grained visual change management workflows. From dynamic change submission forms to intelligent risk predictions and comprehensive workflow-driven approvals, every change to an organisation's ICT systems and networks can be scrutinised to minimise the risk of change failures.

Organisations can also ensure an audit-ready IT asset management (ITAM) posture by relying on ServiceDesk Plus to discover, track, and manage IT and non-IT assets.

IT assets can be discovered and inventoried by scanning networks and domains, importing assets from third-party tools like Intune, or by scanning barcodes and QR codes. Every IT asset can be managed through its entire lifecycle by establishing standard operating procedures (SOPs) as ITAM workflows. IT asset managers can also minimise risks by tracking unlicensed software installations and prohibited software (also known as shadow IT). Every software license agreement and contract can be managed within ServiceDesk Plus—including associations to the corresponding IT asset—enabling faster and accurate audits.

OpManager Nexus: The security audit feature strengthens firewall security, providing needed reporting capabilities and improving security posture. This aligns with DORA's requirement for protecting information and ICT assets from damage and unauthorised access. The network configuration module in OpManager Nexus helps ensure that configurations remain compliant with security policies and that any changes are properly documented, supporting DORA's emphasis on a well-defined and auditable ICT risk management framework.

Perform vulnerability assessments on network devices, identifying potential weaknesses that could be exploited by attackers. This proactive approach to risk management helps organisations address vulnerabilities before they can be exploited.

Log360: Log360's detailed audit-ready reports simplify compliance verification by providing comprehensive logs of security events, user activities, and system changes. These reports help financial institutions conduct internal audits, review ICT risk management frameworks, and demonstrate regulatory adherence to authorities. By offering customisable compliance reports aligned with DORA requirements, Log360 ensures transparency in risk assessments, incident response measures, and digital resilience strategies.

AppCreator: Risk assessment and mitigation tools can be engineered as low-code apps on the AppCreator platform. A centralised risk management framework with automated reviews can also be established and maintained. Workflows for incident management, compliance verification, and vendor oversight can be automated on the platform, each of which help organisations ensure data security. Regulatory updates can be tracked using real-time dashboards built on the platform.

Article

07

ICT systems, protocols and tools

In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are:

- Appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4.
- Reliable.
- Equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services and to deal with peak orders, messages, or transaction volumes, as needed, including where new technology is introduced.
- Technologically resilient, in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.

ManageEngine products to help you comply with Article 7

Endpoint Central: Endpoint Central utilises FIPS 140-2 approved algorithms, allowing users to activate FIPS mode for enhanced security. Endpoint Central's multi-tenant architecture (Summary Server) enables easy enrolment of additional endpoints as your business expands, making it adaptable for organisations with a global footprint. Endpoint Central also offers various third-party software integrations for seamless integration into your IT infrastructure.

OpManager Nexus: Provides in-depth performance monitoring for network devices and servers, allowing organisations to track key metrics such as CPU utilisation, memory usage, and network traffic. This data can be used for capacity planning, ensuring that ICT systems have sufficient resources to handle peak demands and evolving technological challenges. The configuration of automated alerts based on performance thresholds and other criteria enables proactive identification and resolution of performance issues before they impact service delivery. OpManager Nexus itself is designed to be scalable and highly available, ensuring that the monitoring system itself remains operational even during peak loads or unexpected events.

AppCreator: A repository containing information about software system updates can be maintained on AppCreator. Solutions engineered for ICT processes (including process automation solutions) on the AppCreator platform are resilient, scalable, and reliable. The security controls and failover mechanisms ensure consistent uptime of the AppCreator applications—even under strenuous conditions.



Article

08

Identification

Financial institutions must regularly review and document all business functions, roles, and assets supported by ICT. This includes identifying and addressing potential risks, such as cyber threats, and conducting assessments for any changes in network infrastructure or legacy systems. It is also important to maintain an updated inventory of critical information, ICT assets, and third-party dependencies.

ManageEngine products to help you comply with Article 8

Endpoint Central: Endpoint Central's agents gather complete inventory details from your IT environment. It offers extensive vulnerability management by providing continuous assessment and visibility of threats through a single interface. In addition to evaluating vulnerabilities, it includes built-in solutions for each detected vulnerability. Administrators can set up inventory alerts to notify them of unauthorised alterations within their IT network.

Moreover, Endpoint Central assists administrators in identifying high-risk applications such as outdated software, peer-to-peer programs, and insecure remote sharing tools, allowing for their removal. The Custom Group feature in Endpoint Central allows administrators to logically separate critical systems for better management and security. With Network Access Control offered by Endpoint Central, administrators can isolate end-of-life operating systems.

PAM360: PAM360's audit trails will instantly record all events around privileged accounts and key activities, login attempts, and scheduled or completed tasks. This data helps in complying with regular internal audits and forensic investigations, demonstrating who accessed what resource or files, where, when, and why.

Site24x7: Site24x7's network discovery tool automatically scans and identifies all devices and connections within an organisation's IT infrastructure, providing a comprehensive inventory and visual map of the network. This tool supports multiple protocols—like SNMP, WMI, and SD-WAN APIs—enabling real-time monitoring and vulnerability detection. The Network Configuration Management (NCM) feature allows users to compare device configurations against baselines, startup, running, or previous setups. It highlights and validates changes, facilitating effective change management. By comparing version numbers in real-time, organisations can quickly identify and rectify discrepancies, ensuring optimal performance and compliance. This combination enhances network visibility, security, and efficiency.

Analytics Plus: Analytics Plus integrates data from various IT sources to provide a unified view of the IT environment, helping identify potential risks and maintain an up-to-date inventory of critical assets and information. It detects unauthorised changes, tracks vulnerabilities, and assesses third-party dependencies, enabling proactive risk management and regulatory compliance.

AD360: Use the detailed Identity Risk Assessment report to identify and analyse potential cybersecurity risks, such as failed logon attempts and licence changes in Active Directory (AD) and Microsoft 365 platforms.

Take appropriate measures to prevent any security breaches and keep an eye on any suspicious activity happening in your environment. Audit user activities taking place in your organisation with detailed, pre-configured audit reports. Periodically verify and manage user access permissions with access certification campaigns.

ServiceDesk Plus: Enables IT teams to build a comprehensive and up-to-date IT asset inventory through a range of agent-based and agentless discovery techniques. Every asset—both IT and non-IT located either on-premises or remote—can be governed throughout their lifecycle with automated multi-path workflows that are embedded with condition checks, notifications, and low-code scripts.

IT teams can also manage software assets with ServiceDesk Plus. Every software that's discovered can be mapped to the software licenses purchased by the organisation. ServiceDesk Plus aids in software license compliance by spotlighting unlicensed installations and prohibited software.

The native CMDB in ServiceDesk Plus helps organisations to discover and map out each component in their hybrid IT infrastructure and its relationship to other systems, networks, and components. With visual relationship maps, organisations can accelerate incident responses, identify risks proactively, and improve change success rates.

ServiceDesk Plus enables IT teams to record and evaluate every request for a change with dynamic templates. It also aids in accurately pinpointing the risk associated with a change through Zia, ManageEngine's AI powerhouse. Alternatively, organisations can also build out elaborate risk questionnaires within the change template. Change workflows can be built to handle the different types of changes, such as standard, normal, and emergency changes. These workflows can trigger approvals, send notifications in Microsoft Teams, invoke low-code scripts and webhooks, and execute workflow automations with just a single touch.

ServiceDesk Plus aids in risk identification and mitigation through proactive, AI-driven incident triage and response. Every service process that is connected to risk management, like access provisioning requests, can be mapped and governed using visual workflows. Purchase orders and contracts with third-party vendors can be managed within ServiceDesk Plus where IT teams can stay on top of contract expiry and financials.

OpManager Nexus: Automatically discovers and maps network devices, helping organisations identify critical infrastructure supporting business functions. Real-time monitoring allows for proactive identification and mitigation of performance issues, ensuring operational resilience. Service impact analysis links network issues with business services, facilitating efficient recovery and minimising downtime.

Log360: Aggregates logs from across the IT infrastructure—including servers, network devices, applications, and cloud environments—ensuring organisations maintain an updated and documented inventory of critical ICT assets.

With real-time log correlation and automated alerting, Log360 detects potential vulnerabilities, unauthorised access attempts, and risky changes in network infrastructure or legacy systems. Security teams receive instant alerts on suspicious activities, enabling proactive risk mitigation and compliance enforcement. This ensures that financial institutions can regularly review, assess, and strengthen their ICT environment.

AppCreator: Repositories containing critical information such as inventory status, ICT assets, and third-party dependencies can be developed and maintained on the AppCreator platform. These custom repositories can enable financial institutions to regularly review and document all business functions, roles, and assets supported by ICT.

Article

09

Protection and prevention

Financial entities must continuously monitor and control the security of their ICT systems to minimise ICT risks. Key objectives for ICT security include ensuring the resilience, continuity, and availability of systems—especially those supporting critical functions—while maintaining high standards of data availability, authenticity, integrity, and confidentiality. To achieve these objectives, they should:

- Use appropriate ICT solutions to secure data transfer, minimise data loss and unauthorised access, and protect against various risks.
- Develop an information security policy that safeguards data and ICT assets.
- Establish a robust network and infrastructure management structure, implementing automated mechanisms to isolate affected assets during cyberattacks.
- Limit access to information and ICT assets based on necessity, with clear policies and controls for access rights.
- Implement strong authentication mechanisms and protect cryptographic keys, ensuring data encryption according to approved classifications and risk assessments.
- Maintain documented policies for ICT change management, ensuring all changes are thoroughly managed, recorded, and validated.
- Design network infrastructure to enable quick severance or segmentation to prevent contagion among interconnected processes.
- Ensure that the ICT change management process has approval and established protocols from appropriate management levels.

ManageEngine products to help you comply with Article 9

Endpoint Central: Offers strong endpoint security features, including endpoint DLP, browser security, risk-based vulnerability management, next-gen antivirus, and anti-ransomware. It provides patching for Windows, Linux, macOS, and over 1,000 third-party applications. With FIPS 140-2 compliant algorithms, it enhances security through encryption on Windows and Mac devices. Admin capabilities include Windows Firewall configuration, port auditing, secure browsing enforcement, blocking downloads from malicious sites, and addressing security misconfigurations while implementing least privilege and conditional access policies.

PAM360: Ensures secure authentication with two-factor authentication via leading MFA tools and IDPs, requiring users to pass two verification stages. It also centralises credential management by securely storing, managing, and rotating sensitive data like passwords, certificates, keys, etc.

Analytics Plus: Provides in-depth security analytics enabling organisations to track access control violations, detect security misconfigurations, and monitor changes in asset infrastructure.

Provides real-time insights into endpoint risks, failed authentication attempts, and security incidents, thereby ensuring proactive threat management and timely remediation.

AD360: Regularly back up data from AD, Microsoft 365, Google Workspace, and Exchange servers, storing multiple encrypted versions in immutable storage repositories for secure recovery. Protect data records, assets, resources, and endpoints from unauthorised access using strong, phishing-resistant MFA methods, thereby safeguarding the entire business network. Detect and analyse potential risks in your AD and Microsoft 365 accounts using the Identity Risk Assessment report. Take immediate actions to reduce the risk of security breaches. Periodically review the access permissions of users and groups with comprehensive access certification campaigns.

Identity360: Manage access permissions with automated role synchronisation and bulk access management to protect your organisation’s resources. Use robust MFA methods to protect data, assets, and resources from unauthorised access, securing the entire business network.

ServiceDesk Plus: ServiceDesk Plus offers automated incident response workflows that streamline the management of security incidents. From incident detection through integrations with monitoring and SIEM tools to AI-driven triage and escalation, ServiceDesk Plus ensures that critical cybersecurity issues are addressed rapidly. IRTs can leverage Zia's GenAI capabilities to create detailed post-incident reviews that summarise conversations and notes and then drill down into the root causes of security incidents through ITIL-compatible problem management. Access requests to critical ICT services, applications, and assets can be regulated through comprehensive service request templates and workflows that route such requests through multiple approval layers with timely notifications to stakeholders.

Change workflows in ServiceDesk Plus help safeguard against unauthorised or high-risk changes, reducing the change failures that lead to outages. Change workflows can be incorporated with approvals at the right touchpoints, condition checks, contextual notifications, orchestrations, and more, maintaining control and minimising risks—from submission and planning to UAT and release. Organisations can further map and track the asset and service dependencies in the CMDB for better risk assessment. Each and every information security policy and procedure in the organisation can be documented within the knowledge base in ServiceDesk Plus .These policies and documents can be published to selected groups of end-users and technicians.

OpManager Nexus: Provides round-the-clock monitoring of critical ICT systems, enabling proactive threat detection and rapid response to security incidents. Real-time alerts and comprehensive visibility into network and application performance empower organisations to identify and address potential vulnerabilities before they can be exploited, strengthening the organisation's security posture and ensuring operational resilience.

Log360: Log360's continuous security monitoring, privilege access management, and real-time threat detection safeguards ICT systems and ensures operational resilience. Its centralised security monitoring tracks user activities, system changes, and network traffic, helping organisations prevent unauthorised access, data breaches, and cyber threats. By detecting and responding to security incidents instantly, Log360 strengthens data integrity, availability, and confidentiality across critical business functions.With privileged access monitoring and RBAC, Log360 ensures that only authorised users can access critical ICT assets, enforcing least privilege policies and minimising insider threats.

AppCreator: Data stored in AppCreator is encrypted at rest with industry-grade encryption standards, compliant with global data safety regulations. RBAC ensures that only those with relevant permissions can access and modify the stored data. For example, access control policies can be enforced from AppCreator applications to CRM software.

Article

10

Detection

Financial entities must implement mechanisms to quickly detect anomalous activities, including ICT network issues and incidents, as outlined in Article 17. These detection mechanisms should be tested regularly per Article 25, enabling multiple control layers, defined alert thresholds, and automatic alerts for ICT incident response staff. Additionally, sufficient resources must be allocated to monitor user activity, ICT anomalies, and cyberattacks. Data reporting service providers must have systems to check trade report completeness, identify errors, and request re-transmissions.

ManageEngine products to help you comply with Article 10

Endpoint Central: In the event of a malware attack, Endpoint Central can alert the SOC team and IT admins to safely quarantine the infected system. After forensic analysis, the system can be restored to production. It also protects endpoints against ransomware, offering instant, non-erasable backups every three hours using Microsoft's volume shadow copy service. If a file is infected, it can be restored with the latest backup.

Site24x7: Offers robust monitoring and advanced anomaly detection for servers, applications, and user activities, ensuring comprehensive IT oversight. With customisable alert thresholds and dynamic thresholds that adapt to normal usage patterns, it provides precise tuning to specific needs. Real-time notifications keep staff informed of any irregularities. Automatic alerts are triggered based on pre-defined or dynamic criteria, enabling rapid response to threats. This proactive approach helps prevent downtime, maintain security, and ensure efficient operation, empowering organisations to manage their IT environments effectively and with confidence.

Analytics Plus: Analytics Plus' AI-driven anomaly detection spots and alerts on irregular security patterns across the IT landscape. With real-time alerts and predictive analytics, IT teams can proactively identify and eliminate threats. Custom IT analyses and insights help facilitate faster detection and response to potential cyber threats.

AD360: Identify potential security risks and take on-the-fly actions for AD and Microsoft 365 environments with the Identity Risk Assessment report. Its UBA capability helps detect, investigate, and mitigate malicious threats such as suspicious logins, privilege abuse, data breaches, and malware.

ServiceDesk Plus: Detects incidents by ingesting alerts and alarms from ITOM, SIEM, and IT alert management tools. These incidents are categorised, prioritised, and assigned to the right incident response teams, either through rule-based automations or by Zia's predictive AI capabilities. IRTs can build unique incident response workflows for every type of incident, ensuring consistency in incident response. Notifications can be triggered to stakeholders at every stage of the incident workflows, both within ServiceDesk Plus and in tools like Microsoft Teams.

OpManager Nexus: OpManager Nexus' anomaly detection engine uses machine learning to establish baseline performance patterns and identify deviations that could indicate malicious activity or system malfunctions. When anomalies are detected, OpManager Nexus triggers real-time alerts, notifying designated ICT incident response staff. This ensures prompt awareness and facilitates swift action to address potential threats or disruptions. With customisable alert thresholds, organisations can define specific criteria for triggering alerts based on their risk tolerance and operational needs. This flexibility ensures that detection mechanisms are tailored to the organisation's unique environment.

Log360: Provides advanced anomaly detection, real-time alerts, and automated incident response to quickly identify and mitigate ICT security threats. Log360's behavioural analytics engine continuously monitors user activity, network traffic, and system logs, detecting unusual patterns, privilege escalations, and suspicious access attempts. This proactive approach enables organisations to detect and respond to ICT anomalies, cyberattacks, and potential security breaches before they escalate.

With customisable alert thresholds and multi-layered detection mechanisms, Log360 ensures that critical incidents trigger automatic notifications to ICT security teams, allowing for rapid investigation and response. Its incident response automation streamlines containment, mitigation, and forensic analysis, helping financial entities meet DORA's requirement for timely incident detection and resolution.

Article

11

Response and recovery

Financial entities must develop a comprehensive ICT business continuity policy as part of their risk management framework. This policy should ensure the continuity of critical functions and effective incident response. ICT response and recovery plans should be established and audited internally, excluding micro enterprises. Regular testing of these plans is essential, particularly for outsourced functions. A business impact analysis must evaluate the effects of severe disruptions, including dependencies of critical functions. Entities are required to test their crisis communication and recovery plans annually and update them based on results. A crisis management function is necessary for communication during disruptions, and records must be maintained for accessibility. Central securities depositories must provide test results to authorities, and non-microenterprises must report estimated annual costs from major ICT incidents. As of July 17, 2024, the European Supervisory Authorities (ESAs) have issued guidelines for estimating these costs and losses.

ManageEngine products to help you comply with Article 11

Endpoint Central: Protects enterprise endpoints from ransomware and provides instant, non-erasable backups. It can quarantine suspicious endpoints and restore them after a forensic analysis. Files on your network are backed up every three hours using Microsoft's Volume Shadow Copy Service, allowing for easy restoration if a file is infected. Additionally, Endpoint Central integrates with SIEM tools like Rapid7, Splunk, and EventLog Analyzer.

PAM360: For enterprises with multiple sites and service providers managing multiple clients, the application scaling design of PAM360 will allow them to have multiple application servers, all using a single SQL availability group or cluster or a Cloud RDS on the back end. PAM360 comes with a read-only (RO) server for the PostgreSQL database. The RO servers function as mirror servers, synchronising all of the primary server's operations. In the event of the primary server failing, admins can convert any RO server into the primary server and reconfigure all other RO servers to point to the new primary server. In the event of network connectivity loss or degradation between PAM360 application servers, each application will provide local resiliency by operating independently for days to weeks until the connectivity gets restored.

A dedicated RO server can be deployed to handle all API requests and other machine identity-based requests. This will eliminate the need to cater service to both human and non-human entities using a single application. High availability enables regulated entities to operate PAM360 in an active-active configuration.

Site24x7: Helps organisations ensure business continuity by providing real-time monitoring of critical systems, enabling prompt identification of disruptions. Site24x7's automated alerting and reporting tools ensure that incidents are quickly addressed, minimising downtime. By facilitating regular testing of response plans, Site24x7 ensures that staff are prepared to handle emergencies effectively. This proactive approach helps maintain operational stability, safeguard against potential threats, and ensures that business processes continue smoothly without significant interruptions.

Analytics Plus: Analytics Plus facilitates effective incident response and recovery by catching security incidents at their onset and automating root cause analysis. AI-powered capabilities provide a hassle-free approach to optimising risk management strategies, arming key stakeholders with the tools to spot and fix inefficiencies in resolution and recovery practices.

AD360: Regularly back up data from AD, Microsoft 365, Google Workspace, and Exchange servers, storing multiple encrypted versions in immutable storage repositories for secure restoration. Safeguard data records from unauthorised access by implementing robust MFA methods.

ServiceDesk Plus: Enables organisations to efficiently detect and log incidents, ensuring that all issues impacting critical services are promptly recorded and categorised. It automates notification alerts, immediately notifying the appropriate personnel when an incident occurs. This ensures that response teams are promptly made aware of issues, allowing for quicker mitigation efforts.

It features a comprehensive incident management workflow, ensuring that each incident is assigned, escalated, and resolved in a structured manner, along with service level agreements (SLAs) that define clear response and recovery times for different types of incidents.

IRTs can leverage Zia's GenAI-powered summarisation to generate post-incident reviews. With tightly integrated problem management, it aids in conducting comprehensive RCA, empowering teams to identify underlying causes and implement corrective actions to prevent recurrence, thereby promoting long-term operational resilience.

To further support compliance, ServiceDesk Plus maintains a comprehensive audit trail of incidents, actions taken, and resolutions, with robust reporting capabilities that allow organisations to generate detailed logs for audit and compliance purposes.

OpManager Nexus: With real-time monitoring of critical ICT systems and support for automated failover mechanisms, OpManager Nexus ensures the continuity of essential functions in case of disruptions. It also enables the creation of automated workflows for incident response, streamlining recovery processes and minimising downtime. Facilitate regular configuration backups for network devices, which enables swift recovery and data protection in case of system failures or cyberattacks.

Log360: Automated incident response and recovery mechanisms help minimise downtime and ensure business continuity. Log360 enables real-time threat detection, automated remediation workflows, and forensic analysis to contain security incidents efficiently.

AppCreator: On AppCreator, custom repositories of risks, disruptions, and incident management can be developed and maintained for accessibility and future reference.

Article

12

Backup policies and procedures, restoration and recovery procedures and methods

Financial entities must create and document backup and recovery policies to minimise downtime. Key points include:

- **Backup policies:** Define backup scope and frequency based on data importance.
- **Secure systems:** Implement backup systems that protect network security.
- **Regular testing:** Test backup and recovery processes periodically.
- **System segregation:** Use separate systems for data restoration to maintain security.
- **Central counterparties:** Ensure recovery plans allow for transaction continuity.
- **Service provider resources:** Maintain adequate backup resources for uninterrupted services.
- **Redundant capacity:** Non-microenterprises must maintain backup capacities; micro enterprises should evaluate their needs.
- **Secondary sites:** Central securities depositories need a distant secondary site for critical functions.
- **Recovery objectives:** Set recovery time and point objectives considering function importance.
- **Integrity checks:** Perform checks during recovery to ensure data integrity.

ManageEngine products to help you comply with Article 12

Endpoint Central: Protects enterprise endpoints from ransomware and offers instant, non-erasable backups in the event of an attack. It can quarantine endpoints that show suspicious behaviour and, following a thorough forensic analysis, safely redeploy them into the production environment. Additionally, Endpoint Central provides instant, non-erasable backups of files on your network every three hours by utilising Microsoft's Volume Shadow Copy Service. If a file becomes infected with ransomware, it can be restored from the most recent backup copy.

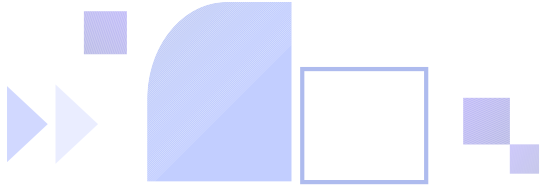
AD360: Regularly back up data from AD, Microsoft 365, Google Workspace, and Exchange servers, keeping multiple encrypted versions in immutable storage repositories for secure recovery. Protect data from unauthorised access by implementing strong MFA methods.

OpManager Nexus: Automates the backup of network device configurations, ensuring readily available, up-to-date backups for rapid restoration. By automating backups and providing tools for rapid restoration, OpManager Nexus supports business continuity and minimises downtime in case of system failures or cyberattacks.

Perform compliance checks for configurations and ensure that organisations adhere to security standards and maintain network integrity during recovery processes.

Log360: Provides automated log collection and long-term storage, ensuring that critical security events, system activities, and compliance records are backed up at defined intervals to meet regulatory retention policies.

With secure backup systems and integrity checks, Log360 ensures that stored logs are tamper-proof and protected from unauthorised access and data corruption. Its segregated backup and archival mechanisms enable organisations to restore critical logs and security data from isolated storage, minimising downtime during cyber incidents or system failures.



Article

13

Learning and evolving

Financial organisations must gather information on vulnerabilities and cyber threats to assess their impact on digital operations. After major ICT incidents, a thorough review is needed to identify causes and improve ICT operations or business continuity plans. Except for micro enterprises, organisations must inform relevant authorities of any changes made.

These reviews should evaluate responses to security alerts, forensic analysis, and communication effectiveness. Insights should contribute to the ICT risk assessment process to enhance risk management. Organisations should monitor ICT risk trends and incident types to improve cyber maturity and preparedness, with senior ICT staff reporting annually to management.

Furthermore, organisations need to provide tailored ICT security awareness and resilience training for employees and, when appropriate, third-party service providers. Continuous monitoring of technological developments is essential for understanding their impact on ICT security and resilience. Staying updated on ICT risk management processes is crucial for effectively addressing evolving cyber threats.

ManageEngine products to help you comply with Article 13

ServiceDesk Plus: Ensures that every incident response action, affected CIs, impact, team conversation, and incident-related notes are recorded within the incident ticket. Zia, powered by ChatGPT, can help generate post-incident reviews instantly. Its Text Assist capability helps incident responders generate replies, notes, descriptions, etc. at speed.

Organisations can set up timers within incident response workflows that trigger timely notifications to both internal stakeholders and other competent authorities.

Multiple related incidents can be linked or merged together and once the IRT identifies the resolution to reported incidents, it can be automatically applied to every incident at the same time. Resolutions can be documented in the knowledge base and published to both IT technicians and end users to foster a culture of continuous learning. Problem management in ServiceDesk Plus helps IT teams to pinpoint the root causes of recurring incidents. If necessary, IT changes may be initiated from within a problem to fix these root causes.

Log360: Aggregates and analyses security event data from across the IT environment, enabling organisations to identify vulnerabilities, assess cyber threats, and refine risk management strategies. With customisable reports and dashboards, Log360 ensures that security teams can evaluate incident response effectiveness, track ICT risk trends, and enhance business continuity planning.

Its real-time alerting system ensures that security teams are promptly notified of critical vulnerabilities, unauthorised access attempts, and anomalies. Log360 also provides forensic analysis tools, helping organisations investigate security incidents, identify root causes, and implement corrective actions to strengthen ICT operations. The platform supports audit-ready compliance reports, enabling senior ICT staff to report annually to management and demonstrate compliance improvements to regulatory authorities.

Article

14

Communication

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans that enable a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate. 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 particular the staff responsible for response and recovery, and staff that needs to be informed. At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT related incidents and fulfil the public and media function for that purpose.

ManageEngine products to help you comply with Article 14

ServiceDesk Plus: Offers automated alerts, announcements, and notifications to internal teams and external parties, ensuring timely and responsible incident disclosure. It also integrates with popular collaboration channels like Microsoft Teams and Slack for quick communication. ServiceDesk Plus further empowers IT teams to restrict or share notifications and announcements to specific groups of technicians and end users.

Article

15

Further harmonisation of ICT risk management tools, methods, processes and policies

The ESAs and ENISA have established regulatory technical standards to enhance ICT security in financial entities. These standards cover network strength, data integrity, access management, incident response, continuity plans, and ICT risk management. They have also been adopted by the European Commission. Key areas include:

- Strengthening networks against intrusions and ensuring data confidentiality and integrity.
- Defining processes for managing access rights and monitoring anomalous behaviour.
- Improving mechanisms for detecting anomalies and triggering incident responses.
- Detailing components and testing scenarios for continuity plans, considering critical function failures and third-party risks.
- Elaborating on response and recovery plans.
- Specifying the review process for the ICT risk management framework.

ManageEngine products to help you comply with Article 15

Endpoint Central: Helps companies meet Regulatory Technical Standards (RTS) for ICT risk management and streamlines their frameworks. In case of suspicious activity, Endpoint Central can isolate and securely redeploy affected endpoints after examination. The system utilises algorithms compliant with FIPS 140-2 and offers FIPS mode for increased security. It also supports encryption on Windows and Mac devices through BitLocker and FileVault, respectively. Moreover, Endpoint Central allows for strong endpoint privilege management, including application-specific controls, JIT access, and conditional access policies to safeguard critical systems and sensitive information.

AD360: Protect business networks using strong, phishing-resistant MFA methods. Detect and analyse risks in your AD and Microsoft 365 accounts using the Identity Risk Assessment report and take actions to eliminate any security breaches. Regularly review access permissions of users and groups with access certification campaigns.

Identity360: Manage access permissions with automated role synchronisation and bulk access management to keep resources secure. Use robust MFA methods to protect data, assets, and resources from unauthorised access, securing the entire business network.

OpManager Nexus: Provides real-time monitoring and alerting for performance issues and security threats based on anomaly detection, enabling rapid incident response and supporting the ESAs and ENISA focus on improving anomaly detection and response mechanisms. Enforce granular access controls, aligning with ESAs and ENISA standards for managing access rights and strengthening network security.

Log360: With robust access control and privilege monitoring, Log360 enables financial entities to define, enforce, and audit access rights, ensuring compliance with regulatory requirements for user authentication, role-based access, and anomaly detection. The platform's automated incident detection and response mechanisms trigger alerts, correlate threat intelligence, and initiate security workflows to contain and mitigate ICT threats, enhancing overall digital resilience.

AppCreator: Offers audit trails and real-time alerts that facilitate financial entities to monitor anomalies and enforce access controls on the applications built on the platform.

Article

16

Simplified ICT risk management framework

Organisations must establish an ICT risk management framework with a clear plan, continuously monitor systems, and respond quickly to risks. They should recognise their reliance on third-party providers and develop business continuity plans with backups. Regular testing and updates of these plans are essential, along with reviews of the framework. The ESAs will set regulatory standards for ICT risk management and reporting.

Note: This article is only applicable to small, non-interconnected firms as described above on our guide. You can refer to the DORA regulation for more details.

ManageEngine products to help you comply with Article 16

Endpoint Central: Assists in complying with the RTS for ICT risk management tools, methods, processes, and policies, as well as the simplified ICT risk management framework. This RTS includes a Simplified ICT Risk Management Framework (designed for small and non-interconnected investment firms, exempted payment institutions, electronic money institutions, and small occupational retirement provision institutions). Articles 30 to 38 of the RTS provide a comprehensive overview of the Simplified ICT Risk Management Framework.

AD360: Detect security risks in your AD and Microsoft 365 environments and take immediate measures to prevent any potential breaches. Regularly back up data from AD, Microsoft 365, Google Workspace, and Exchange servers. Securely store multiple encrypted versions in immutable storage repositories to ensure quick recovery in case of data loss.

ServiceDesk Plus: Enables small and non-interconnected firms to swiftly adopt ITIL best practices by offering a range of core ITSM practices out of the box. Incident response workflows can be built for various scenarios without implementation overheads. ServiceDesk Plus' high-value AI capabilities enable intelligent triage of incidents, accelerating incident responses and minimising downtime and risks.

Post-incident reviews can be generated by Zia, powered by ChatGPT, accelerating RCA through problem management. Service request management in ServiceDesk Plus helps IT teams at smaller organisations build and publish a service catalogue with the IT services being offered to specific groups of end users. Access provisioning requests can be governed through multiple approval layers with contextual notifications sent to the right stakeholders throughout the lifecycle of the provisioning request.

Every IT asset and non-IT asset can be identified, inventoried, and managed within ServiceDesk Plus. From procurement and assignment through disposal, standard operating procedures can be codified using visual asset workflows.

Software asset management in ServiceDesk Plus helps small financial firms sidestep the risk of unlicensed installations while also identifying any prohibited software installations. Every change to the IT infrastructure can be recorded and controlled using advanced change management workflows. These multi-path workflows can be embedded with prebuilt automations such as condition checks, approvals, notifications, tasks, orchestrations, and more. Change risks can be accurately identified, either through Zia's predictive intelligence or using a detailed questionnaire.

OpManager Nexus: Automates configuration backups and provides compliance checks, ensuring rapid recovery and adherence to security standards. Real-time firewall monitoring and alerts enable proactive threat detection and swift response to security incidents. Centralised dashboards and reporting tools facilitate continuous monitoring and assessment of the ICT risk management framework.

Article

17

ICT-related incident management process

Financial entities must establish and implement a process for managing ICT-related incidents, which includes detecting, managing, and notifying stakeholders of such incidents. Key requirements include:

- Recording all ICT-related incidents and significant cyber threats.
- Implementing consistent monitoring and follow-up procedures to identify, document, and address root causes to prevent recurrence.
- Establishing early warning indicators and procedures for identifying, tracking, logging, categorising, and prioritising incidents based on severity and criticality.
- Assigning roles and responsibilities for different incident types and scenarios.
- Planning communication strategies for staff, stakeholders, and clients, as well as internal escalation procedures.
- Reporting major incidents to senior management and informing them of impacts, responses, and required additional controls.
- Developing response procedures to mitigate impacts and ensure timely recovery of services.

ManageEngine products to help you comply with Article 17

Endpoint Central: Offers critical details to the network administrator or SOC team—including detection time, attack status, agent actions, and endpoint information—in case of any suspicious events in your IT network, such as malware or ransomware.

Site24x7: Aids organisations in detecting, managing, and notifying stakeholders about incidents through real-time monitoring and advanced anomaly detection across servers, applications, and user activities. Its customisable alert thresholds and dynamic thresholds ensure precise tuning. Automated alerting swiftly informs staff upon the detection of anomalies, enabling immediate response. Detailed reporting tools facilitate effective incident management and ongoing communication with stakeholders, ensuring transparency and rapid resolution. This comprehensive approach enhances system reliability and stakeholder confidence in the organisation's IT operations.

Analytics Plus: Consolidated dashboards provide extensive insights into incident management, impact assessments, and response effectiveness. AI and ML capabilities foresee the onset of warning indicators, alert relevant stakeholders, and trigger workflows to mitigate their impact and prevent security incidents.

ServiceDesk Plus: Provides an omni-channel incident logging mechanism—that's integrated with various ITOM, UEM, and SIEM solutions—which can trigger early warning alerts based on any observed deviations. Alongside rule-based automations, ServiceDesk Plus' Zia AI can also classify ICT-related incidents based on priority, severity, and impact on critical services. IT teams can establish incident response playbooks using visual workflows embedded with notifications and statuses that stage gate every step of the incident response, while keeping stakeholders in the loop. ServiceDesk Plus facilitates the assignment of roles and responsibilities to incident responders for different incident types and scenarios. It can automate incident escalation to specific IT teams and incident responders when incidents breach SLAs or mandated timelines.

IT teams can generate post-incident reviews with Zia, powered by ChatGPT. They can also document and manage incident resolutions in a central repository and establish SOPs to develop proper response procedures for future incidents. IT teams can also address the root-causes of incidents to prevent recurrence using ITIL-compatible problem management capabilities in ServiceDesk Plus. The platform provides detailed reporting and analytics capabilities that allow organisations to monitor key performance indicators (KPIs) and incident response times. Additionally, ServiceDesk Plus enables organisations to maintain detailed records of incident responses, resolutions, and compliance activities through its ticketing system, which logs every action associated with each incident.

OpManager Nexus: Real-time monitoring, customisable alerts, and automated response procedures enable proactive incident detection and swift mitigation. Centralised incident recording, tracking, and follow-up facilitate efficient incident management and RCA. Workflow automation and service desk integrations streamline communication and collaboration for effective incident resolution.

Log360: Log360's security orchestration, automation, and response (SOAR) capabilities streamline incident detection, classification, and resolution, ensuring that financial entities can quickly mitigate security threats and minimise operational disruptions.
With real-time incident monitoring and automated alerting, Log360 ensures that early warning indicators are triggered when anomalous activities, cyber threats, or system failures occur. It automatically logs, categorises, and prioritises security events based on severity and impact, allowing IT teams to assign roles, escalate incidents, and implement predefined response procedures.

AppCreator: A custom repository containing information about all ICT-related incidents and significant cyber threats can be created and maintained on AppCreator. Audit-ready reports for stakeholders that assist in impact assessments, mitigation efforts, and remediation efforts can be generated on the platform.

Article

18

Classification of ICT-related incidents and cyber threats

Financial entities must assess and categorise ICT-related incidents based on criteria such as the number of affected clients, the significance of those clients, the duration of the incident, geographical impact, data losses, importance of the affected services, and economic impact. Cyber threats should be labelled significant based on the importance of at-risk services, targeted clients, and the geographical areas affected.

The ESAs—in collaboration with the Joint Committee, ECB, and ENISA—will create regulatory technical standards to clarify criteria for recognising and reporting major ICT-related incidents and significant operational or security payment incidents. These standards will also address significant cyber threats and the needs of micro enterprises and small to medium-sized enterprises.

ManageEngine products to help you comply with Article 18

ServiceDesk Plus: Offers both condition-based and AI-driven classification of ICT incidents and security threats. Incidents are created from alerts triggered through ITOM, UEMS, and SIEM tools and can be reported by end users. Depending on multiple parameters—like the affected service or system, the business impact, and urgency—the incident can be contextually prioritised and routed to the right incident response group. Once the incident is classified, a suitable incident response workflow can be triggered, which guides incident response teams.

Article

19

Reporting of major ICT-related incidents and notification of significant cyber threats

Financial entities are required to report major ICT-related incidents to the appropriate authority as per Article 46. If overseen by multiple authorities, Member States will designate one to manage these responsibilities. Significant credit institutions must report major ICT incidents to the designated national authority, which will subsequently notify the ECB.

Financial entities should gather relevant information, create initial notifications and reports using templates from Article 20, and submit them to the authority. In case of technical issues with the templates, they must notify the authority through alternative means. Reports must provide enough detail for the authority to assess the incident's seriousness and potential cross-border effects. Member States may require additional reporting to relevant authorities or CSIRTs as per Directive (EU) 2022/2555. Financial entities can voluntarily report significant cyber threats if they believe these threaten the financial system or clients. Significant credit institutions may also choose to inform CSIRTs of any voluntary notifications.

If a major ICT incident impacts clients' financial interests, entities must promptly inform clients of the incident and any mitigating measures. For significant cyber threats, clients should receive guidance on protective actions.

Financial entities must provide the following to the relevant authority within the timelines stated in Article 20: (a) an initial notification, (b) an intermediate report for significant status changes or new information, and (c) a final report after the RCA and impact assessment. Reporting duties may be outsourced to third-party providers, but the financial entity remains responsible for compliance. Following the initial notification and subsequent reports, the authority must quickly share details with relevant bodies, including EBA, ESMA, EIOPA, and the ECB.

ManageEngine products to help you comply with Article 19

ServiceDesk Plus: Helps financial organisations notify the competent authorities and any internal or external stakeholders at specific time intervals or at a particular stage within the incident response workflow. Financial organisations can send condition-based notifications (via email, Microsoft Teams, Slack, etc.), as well as customise the notification content with data extracted from the reported incidents in ServiceDesk Plus. Timers in ServiceDesk Plus will trigger these notifications within the time limits established by regulatory authorities. These notifications can be triggered when an incident is reported, at any intermediate stage within the incident response workflow, and when the incident is resolved.

Control mapping

ManageEngine products	Requirements they help meet							
	Article 5: Governance and organisation	Article 6: ICT risk management framework	Article 7: ICT systems, protocols and tools	Article 8: Identification	Article 9: Protection and prevention	Article 10: Detection	Article 11: Response and recovery	Article 12: Backup policies and procedures, restoration and recovery procedures and methods
Endpoint Central		✓	✓	✓	✓	✓	✓	✓
PAM360	✓	✓		✓	✓		✓	✓
Site24x7				✓		✓	✓	
Digital Risk Analyzer		✓						
Analytics Plus		✓		✓	✓	✓	✓	
AD360				✓	✓	✓	✓	✓
Identity360					✓			
ServiceDesk Plus	✓	✓		✓	✓	✓	✓	
OpManager Nexus	✓	✓	✓	✓	✓	✓	✓	✓
Log360	✓	✓		✓	✓	✓	✓	✓
AppCreator	✓	✓	✓	✓	✓		✓	

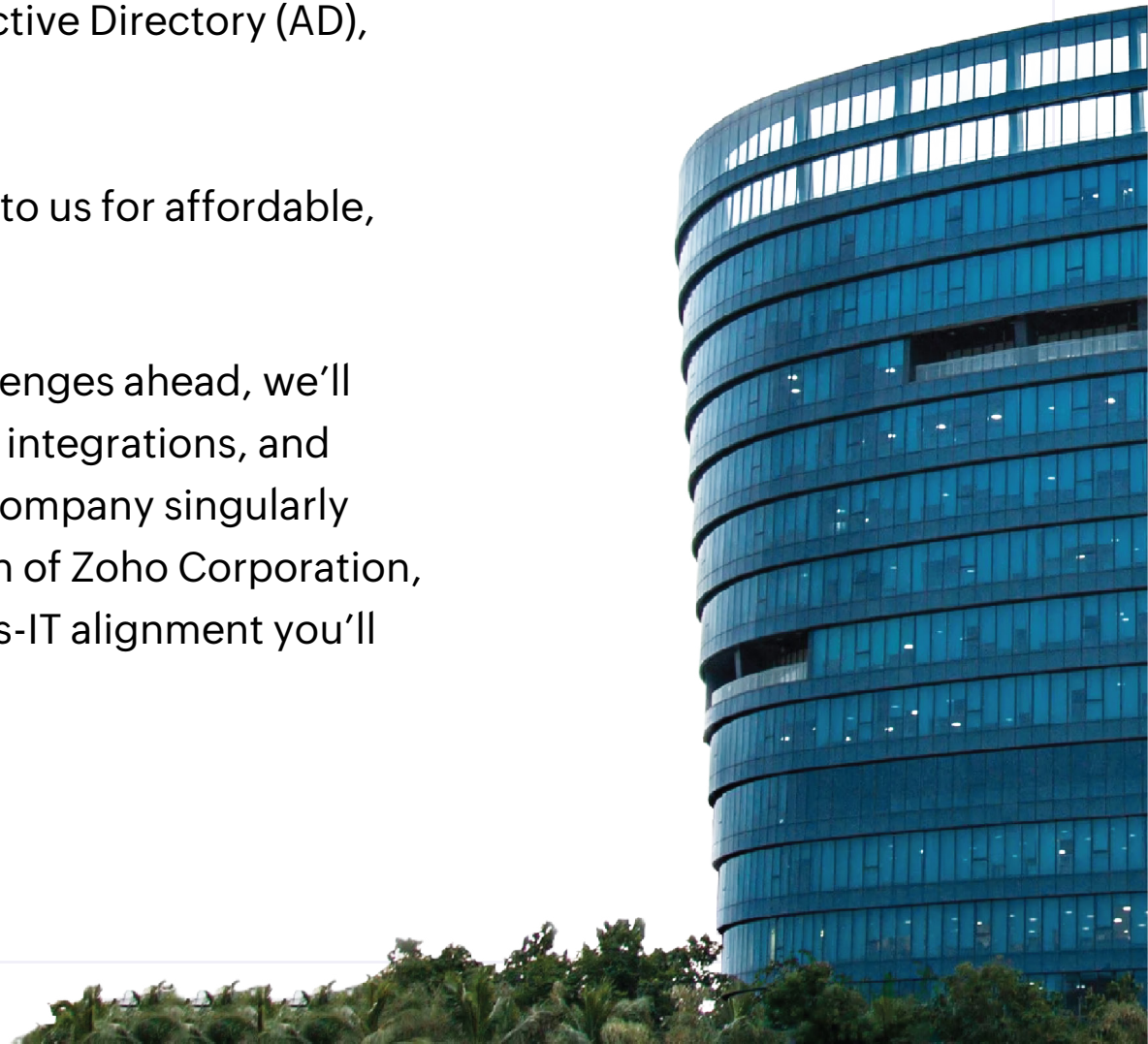
ManageEngine products	Requirements they help meet						
	Article 13: Learning and evolving	Article 14: Communication	Article 15: Further harmonisation of ICT risk management tools, methods, processes and policies	Article 16: Simplified ICT risk management framework	Article 17: ICT-relaed incident management 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
Endpoint Central			✓	✓	✓		
PAM360							
Site24x7					✓		
Digital Risk Analyzer							
Analytics Plus					✓		
AD360			✓	✓			
Identity360			✓				
ServiceDesk Plus	✓	✓	✓	✓	✓	✓	✓
OpManager Nexus			✓	✓	✓		
Log360	✓		✓		✓		
AppCreator					✓		

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory (AD), security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.



Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine.



Manage digital identities and access

Manage, govern, and secure digital identities across your organisation with identity orchestration, privileged access security, CIEM, MFA, SSO, role-based access controls, and more.

manageengine.com/iam

Control and secure every endpoint

Manage, secure, and control all your endpoints across diverse functions like end-user computing, cybersecurity, governance, risk and compliance, I/O, and more.

manageengine.com/uems

Enhance IT security and compliance

Detect, investigate, and respond to security threats with UEBA, threat intelligence, and log monitoring. Be compliant with standards and mitigate risks with audit-ready reports.

manageengine.com/siem

Optimise IT with low-code apps

Extend the capabilities of your IT process by combining low-code and GenAI. Rapidly address IT challenges and innovate with minimal coding, making your organisation more agile.

manageengine.com/lowcode

Deliver smart service experiences

Enhance your service delivery workflows through industry-recommended ITSM best practices, powerful orchestration, and native AI capabilities.

manageengine.com/usm

Strengthen network and IT operations

Achieve visibility across your network and application stack with AI-driven observability. Proactively resolve issues, optimise performance, and enhance IT security.

manageengine.com/itom

Unified insights into all of IT

Visualise every facet of IT effortlessly. With decision intelligence, preemptively identify and tackle risks, and gain practical contextual strategies for operational bottlenecks.

manageengine.com/ita

Trusted by


at&t


BARCLAYS




L'ORÉAL
PARIS


SONY


ERICSSON
TAKING YOU FORWARD


NEC


SAINT-GOBAIN