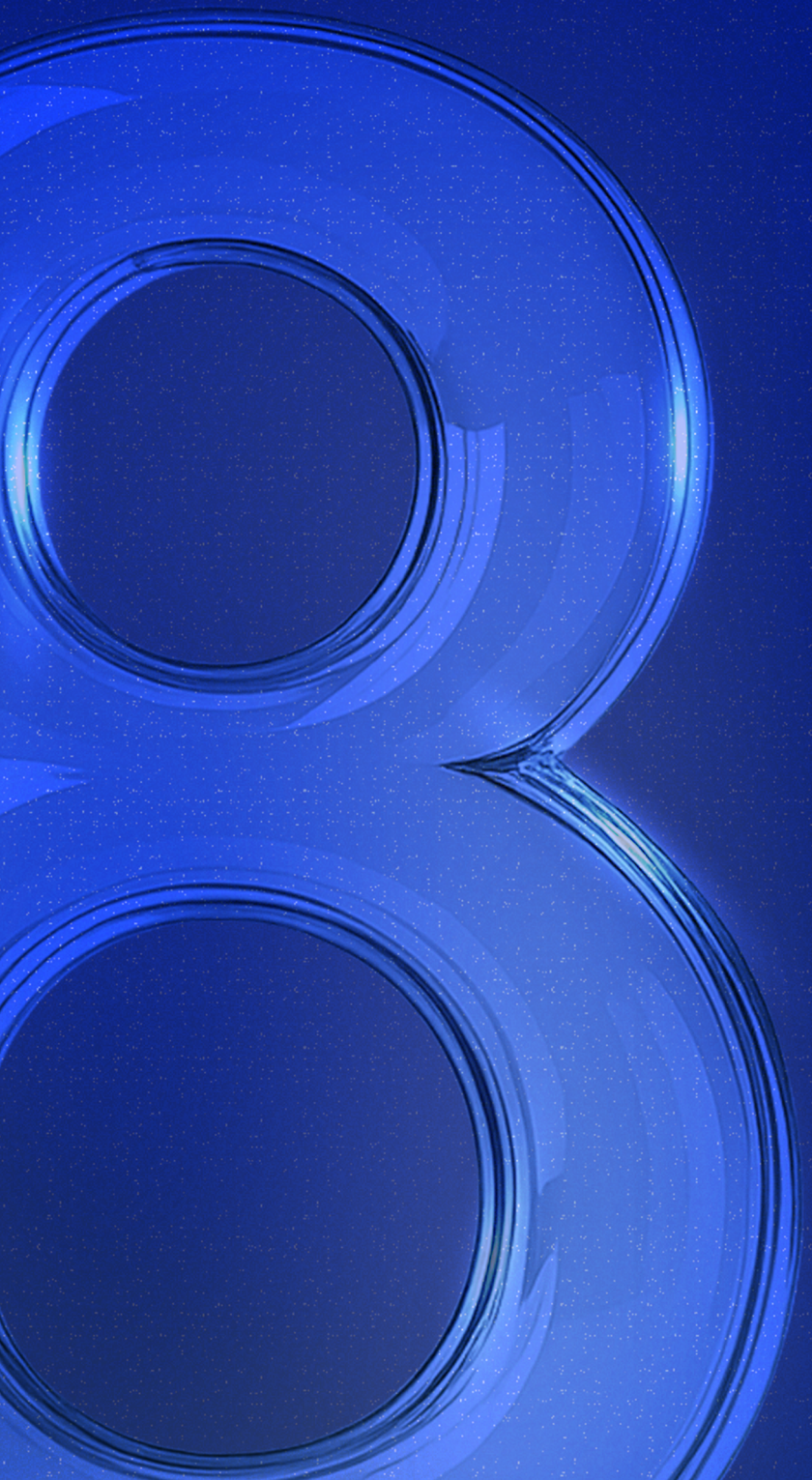
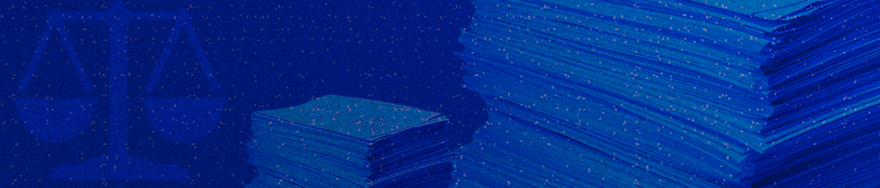
ManageEngine
ServiceDesk Plus

Achieving Essential Eight compliance with ITSM best practices





Today, organisations operate in an IT landscape that's surrounded by vulnerabilities and risks. Vast cloud environments, expanding SaaS ecosystems, remote workforces, and interconnected business systems have created an unprecedented flow of data. While this continuous exchange of data drives efficiency, it also generates business risks. According to the ACSC Annual cyber threat report for 2024-25, a cybercrime is reported in Australia every six minutes. In the short time it takes to step away from your desk, another business has already become a statistic. To counter this relentless threat, the Australian Cyber Security Centre (ACSC) provides a crucial, non-negotiable directive: the implementation of the Essential Eight cybersecurity controls.

So, how do you operationalise this critical mandate within the complexity of a modern IT environment? In this ebook, you'll discover how best practices for IT service management (ITSM) can help strengthen your cyber resilience and make compliance with the Essential Eight more achievable. Furthermore, you will see how ManageEngine ServiceDesk Plus helps turn these best practices into action, embedding security and compliance into the daily workflows of your IT team.

A brief introduction to the Essential Eight framework

The Essential Eight is a set of prioritised cybersecurity mitigation strategies developed by the ACSC, Australia's national technical authority on cybersecurity. It was designed to help organisations protect themselves against a wide range of common cyberthreats, particularly those that exploit weak controls, unpatched systems, excessive privileges, and poor recovery practices. Rather than prescribing an exhaustive security program, the Essential Eight focuses on eight practical, high-impact strategies that address frequently observed attack techniques, such as ransomware, credential compromise, and malicious code execution. Together, these strategies form a baseline that helps organisations reduce their attack surface, limit the spread of incidents, and recover quickly when security events occur.

At the core of the Essential Eight is a simple principle: Cybersecurity controls are only effective if they are implemented consistently and operated reliably over time. For this reason, the framework is accompanied by a maturity model that evaluates how rigorously controls are applied across an organisation.

The Essential Eight is widely adopted across Australian government agencies and is increasingly referenced by private-sector organisations looking to strengthen their cybersecurity posture or align with broader standards such as ISO/IEC 27001. While it originated as a government-led initiative, its principles are industry-agnostic and apply equally to organisations of all sizes that rely on digital systems to deliver services and manage sensitive information.

The Essential Eight mitigation strategies explained

The Essential Eight mitigation strategies are designed to reduce cyber risk by addressing weaknesses that attackers commonly exploit at different points during an intrusion. Taken together, the strategies help organisations reduce exposure, constrain attacker actions, and maintain operational continuity.

Strategies focusing on reducing exposure at the point of entry

1) Application control

This strategy focuses on limiting what software is allowed to run within the environment. By permitting only trusted and approved applications to execute, organisations reduce the risk of malicious or unauthorised programs being used to compromise systems.

2) Patching applications

Applications are frequent targets for exploitation due to publicly known vulnerabilities. This strategy emphasises keeping applications up to date so that attackers cannot take advantage of outdated or unsupported software.

3) Configuring Microsoft Office macro settings

Microsoft Office macros are a commonly abused delivery mechanism for malicious code. This strategy reduces risk by controlling when and how macros can run, particularly in documents obtained from external or untrusted sources.

4) User application hardening

Many applications expose features that are rarely needed for business use but are attractive to attackers. This strategy involves disabling or restricting such functionality to narrow the attack surface available to adversaries.

Strategies intended to constrain attacker capability after access is gained

5) Restricting administrative privileges

Elevated access increases the potential impact of compromise. This strategy ensures administrative privileges are granted only when necessary, approved through appropriate processes, and removed when no longer required.

6) Patching operating systems

Operating systems form the foundation of every endpoint and server. This strategy focuses on keeping them current reduces the likelihood that attackers can exploit known weaknesses to gain persistence or escalate access.

7) Multi-factor authentication

Passwords alone are often insufficient to protect user accounts. This strategy strengthens identity assurance by requiring additional verification factors, particularly for privileged accounts and remote access.

Strategy to maintain operational continuity

8) Regular backups

Data loss can occur through ransomware, system failure, or human error. Regular backups ensure that critical information can be restored and operations can resume without permanent damage.

Together, these strategies establish a baseline for managing cyber risk in modern IT environments. Their real value, however, lies in how well they are operationalised. Whether controls hold up under pressure is determined by consistency of application, breadth of enforcement, and ongoing oversight. To capture this distinction between control design and day-to-day execution, the Essential Eight is underpinned by a maturity model that evaluates the operational strength of each control, not just its presence.

What is the Essential Eight maturity model?

The Essential Eight maturity model categorises organisations based on the types of cyber threats their environments are able to withstand. Rather than treating cybersecurity as a simple checklist exercise, the model assesses the consistency, coverage, and reliability of control implementation across the environment.

The maturity model consists of four levels: maturity level zero through to maturity level three. Each level represents a progressively stronger and more disciplined approach to managing cyber risk. Advancement through the levels reflects improvements not only in technical configuration, but also in governance, operational execution, and oversight.

Maturity levels corresponding to adversary behaviour and attack capability

3

Applies to organisations that are prepared to withstand highly targeted and resourceful attacks. Adversaries at this level may spend significant time researching their targets, probing for weaknesses such as outdated software, misconfigurations, or monitoring blind spots. Organisations at this maturity level are equipped to detect, contain, and respond to these attacks before they result in widespread compromise or data loss.

2

Reflects an ability to defend against more deliberate and capable adversaries. These advanced attackers invest effort in impersonation, privilege misuse, and control evasion to move laterally or escalate access. Organisations operating at this level apply controls in a way that restricts attack paths and limits the effectiveness of such techniques.

1

Represents organisations that can reduce risk from opportunistic threat actors who rely on commonly available tools and well-known techniques to identify exposed systems and vulnerable applications. At this level, organisations are positioned to handle prevalent attack methods, including common forms of phishing and social engineering that attempt to execute malicious content on user endpoints.

0

Applies to environments where cybersecurity controls provide minimal resistance to attack. These organisations are exposed to compromise by threat actors using basic techniques and widely available tooling. Weak control enforcement, inconsistent operational practices, or limited visibility can allow attackers to gain access with little effort.

Maturity levels

Here’s how to use ITSM to support Essential Eight controls

Many organisations already operate mature ITSM practices that govern how incidents are handled, access is granted, and assets are managed. These practices are embedded into daily IT operations and supported by defined workflows, clear ownership, and built-in audit trails. By applying a cybersecurity lens, these same ITSM practices can be reoriented to support Essential Eight objectives. Incident management can drive consistent security incident response and recovery actions, while access management and joiner–mover–leaver (JML) workflows ensure end-to-end management of user access and privilege controls aligned with security requirements.

Using ITSM in this way allows organisations to meet Essential Eight requirements without reinventing new processes as security controls become part of routine service delivery model rather than standalone tasks. This approach reduces duplication, avoids silos, and produces compliance evidence as a natural outcome of day-to-day IT service operations.

Many of the requirements defined under the Essential Eight are drawn directly from the ACSC’s Information Security Manual (ISM). The ISM defines a comprehensive set of security controls that organisations are expected to implement. The Essential Eight is a prioritised subset of these ISM controls, selected for their proven effectiveness in reducing cyber risk. While the ISM outlines what good security looks like at a broad level, the Essential Eight focuses on how organisations should implement and mature the most critical controls. Driving Essential Eight compliance with ITSM best practices, therefore, is about operationalising ISM-aligned controls through existing service management workflows.

Driving Essential eight compliance with ITSM best practices

User access management

Automated workflows for employee onboarding, offboarding, and access requests help enforce least-privilege access through governed approvals and controlled execution.

Asset & configuration management

Accurate inventories of hardware, software, and cloud resources forms the foundation of application control, patch management, and vulnerability monitoring. A centralised CMDB helps teams understand dependencies, prioritise remediation, and anticipate the impact of incidents.

Change management

Patching applications and operating systems, enforcing secure configurations, or applying software updates are managed through formal change workflows. This reduces human error, ensures approval oversight, and creates a record for compliance audits.

Incident management

Security alerts from endpoints, network tools, or vulnerability scanners can automatically generate incident tickets. ITSM ensures these incidents are tracked, prioritised, and resolved efficiently, providing an auditable trail that demonstrates timely response and containment.

Reporting

Dashboards and reports offer visibility into compliance status, control effectiveness, and areas needing attention.

Here's how ServiceDesk Plus capabilities help implement some of the Essential Eight strategies through everyday ITSM workflows.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Patch applications Patch operating systems	M1, M2, M3	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ISM-1807	**ServiceDesk Plus capabilities** • Agent-based and agentless scanning of domains and networks • Remote asset scan • Self-scan script • Barcode scan, QR code scan, and RFID scan • Integration with vulnerability and patch management tools like ManageEngine Vulnerability Manager Plus • ServiceDesk Plus integrates with ManageEngine Vulnerability Manager Plus to provide direct access to vulnerability scanning and assessment capabilities within the ServiceDesk Plus environment. • Vulnerability Manager Plus performs automated asset discovery and vulnerability scanning at configurable intervals, detecting endpoints, identifying vulnerabilities, and flagging missing patches to maintain continuous visibility into the security posture of managed assets. • IT teams can access Vulnerability Manager Plus dashboards and reports directly from ServiceDesk Plus via an embedded interface, enabling them to identify vulnerable assets, review severity levels, and prioritise remediation without switching platforms.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Patch applications Patch operating systems	M1, M2, M3	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. Patches, updates, or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. Patches, updates, or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	ISM-1876 ISM-1690 ISM-1691	**ServiceDesk Plus capabilities** • Emergency and standard change management workflows • Integration with ManageEngine Endpoint Central • Through ServiceDesk Plus' integration with ManageEngine Endpoint Central, asset inventory data is synchronised to the ServiceDesk Plus CMDB in real time, providing IT teams with visibility into managed endpoints across the organisation. • Endpoint Central also maintains patch status tracking and compliance monitoring, which can be accessed directly from ServiceDesk Plus through an embedded interface. This allows IT teams to monitor affected systems, assess patch severity, and prioritise remediation without switching between platforms. • ServiceDesk Plus also supports the design of custom change workflows, allowing organisations to configure emergency change processes with expedited approval chains and automated notifications when rolling out patches for critical vulnerabilities, and normal change workflows that include review and testing stages for non-critical patches. • Endpoint Central automatically deploys patches to endpoints based on preconfigured deployment policies during agent refresh cycles, reducing manual effort and ensuring timely remediation. When manual intervention is required, technicians can initiate patch deployment or perform other patch management tasks directly from ServiceDesk Plus tickets through the embedded interface.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Application control	M1, M2, M3	Application control is implemented on workstations. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, and control panel applets to an organisation-approved set.	ISM-0843 ISM-1657	**ServiceDesk Plus capabilities** • Software scan • Notification rules • Integration with ManageEngine Endpoint Central • ServiceDesk Plus, through its integration with ManageEngine Endpoint Central, enforces application control on workstations, ensuring only organisation-approved applications run, while preventing unauthorised applications from executing (even if already installed). • Endpoint Central uses allowlists to permit trusted applications and blocklists to prevent unauthorised applications from running. It also supports prohibited software lists where administrators can designate specific applications as prohibited. Asset scans then automatically detect these prohibited applications on endpoints, with auto-uninstallation removing them during the next refresh cycle. • When prohibited software is detected, alerts are also automatically logged as requests in ServiceDesk Plus, giving IT teams visibility into policy violations for audits and compliance tracking. For immediate remediation, IT teams can remotely uninstall prohibited software directly from these requests using the Endpoint Central extension.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Restricting administrative privileges	M1, M2, M3	Requests for privileged access to systems, applications, and data repositories are validated when first requested. Privileged access to systems, applications, and data repositories is limited to only what is required for users and services to undertake their duties.	ISM-1507 ISM-1508	**ServiceDesk Plus capabilities** • Service catalogue • Service request templates • Multi-stage approvals • Orchestration of access provisioning and de-provisioning through Zoho Flow and Qntrl Circuit • Integration with ManageEngine PAM360 • ServiceDesk Plus helps organisations manage privileged access requests through dynamic service request templates. Field and form rules (FFR) provide dynamic, condition-based control of fields in the request forms—allowing them to be shown or hidden, made mandatory, populated with default values, or validated based on user role, department, or request context—making the service request template dynamic. For example, if during the JML process the employment type is chosen as a contract employee, the form can be configured to display only the resources relevant to their role and mandate fields like contract start and end dates, ensuring requests are properly validated and scoped to only the access needed. Using FFR, custom scripts can also be executed to block request submission entirely if predefined conditions are not met. • Multi-tiered approval workflows can ensure requests cannot proceed without required managerial and system-owner authorisation.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Restricting administrative privileges				• Once approved, both access provisioning and de-provisioning can be orchestrated through single-touch workflow automation in ServiceDesk Plus. • ServiceDesk Plus also supports integration with ManageEngine PAM360 to deliver time-bound privileged access for change-related tasks. For approved changes, PAM360 can grant elevated permissions that automatically expire after the change window, ensuring technicians have privileged access only for the duration required to complete their tasks.
Restricting administrative privileges	M2, M3	Privileged access events are centrally logged. Privileged account and group management events are centrally logged.	ISM-1509 ISM-1650	**ServiceDesk Plus capabilities** • Custom modules • Service request management workflows • Custom triggers • In ServiceDesk Plus, Custom Modules can be used to establish a dedicated access event management practice, enabling organisations to log, audit, and report on privileged access activity from a single system of record. • Privileged access events can also be recorded directly within service requests whenever users are granted, modified, or revoked access to applications using Zoho Flow, Qntrl Circuits, or Custom Functions. • Triggers can be configured to notify relevant stakeholders when privileged access is granted or modified.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Restricting administrative privileges	M2, M3	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	ISM-1819	**ServiceDesk Plus capabilities** • Incident management • Problem management • Knowledge management • Automated workflows • AI-powered ticket triaging, post-incident review generator, resolution generator • CMDB • ServiceDesk Plus enables organisations to automatically enact incident response plans using structured incident management and automation capabilities. Security incidents can be logged using predefined incident templates that embed roles, responsibilities, SLAs, mandatory evidence fields, and response tasks. • Once identified, automated workflows can trigger actions such as automated task assignment or stakeholder notifications via Microsoft Teams or Slack. AI-powered triage assists with accurate categorisation, prioritisation, and routing of information security incidents to the appropriate response teams.

Mitigation strategy	Maturity level	Essential Eight requirement	Associated ISM control	How can ServiceDesk Plus capabilities help
Restricting administrative privileges				• ServiceDesk Plus helps organisations manage privileged access requests through dynamic service request templates. Field and form rules (FFR) provide dynamic, condition-based control of fields in the request forms—allowing them to be shown or hidden, made mandatory, populated with default values, or validated based on user role, department, or request context—making the service request template dynamic. For example, if during the JML process the employment type is chosen as a contract employee, the form can be configured to display only the resources relevant to their role and mandate fields like contract start and end dates, ensuring requests are properly validated and scoped to only the access needed. Using FFR, custom scripts can also be executed to block request submission entirely if predefined conditions are not met. • Post-incident activities are supported through problem management and RCA workflows, along with GenAI-powered post-incident reviews and resolutions, helping teams document lessons learned and standardise future response playbooks.

About ServiceDesk Plus

ServiceDesk Plus is the AI-driven unified service management solution from ManageEngine, the enterprise IT management division of Zoho Corporation. It combines ITSM essentials, asset management, and a CMDB with enterprise service management capabilities, providing a comprehensive platform for designing, managing, and delivering IT and business services. Powered by proprietary AI technologies and public LLM integrations, ServiceDesk Plus unlocks unparalleled efficiencies and experiences for employees, technicians, and process owners.

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

Gartner Peer Insights™ 4.7

ITIL® PRACTICES 14 ACCREDITED TOOL VENDOR ManageEngine ServiceDesk Plus February 2023 Silver by PeopleCert

PinkVERIFY® Certified 10 PROCESSES

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

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

About ManageEngine

ManageEngine is a division of Zoho Corporation that offers comprehensive on-premises and cloud-native IT and security operations management solutions for global organisations 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 200+ channel partners worldwide to help organisations 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 compliant with Essential Eight. Using ServiceDesk Plus may help customers align with specific controls and requirements outlined in Essential Eight and their certification is contingent on multiple factors as may be prescribed by a certifying authority. Coupled with other appropriate solutions, processes, people, controls, and policies, ManageEngine ServiceDesk Plus can help organisations align with the Essential Eight guidelines.

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