

MSP and MSSP Glossary — Managed Services Terms Explained

Canonical: <https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/msp-and-mssp-glossary-managed-services-terms-explained/>

Description:

What is a managed service: An arrangement where a provider takes ongoing operational responsibility for defined IT functions
How is managed services priced: Recurring fee, not per incident or per project
What is the provider's incentive in

Details:

Frequently Asked Questions

What is a managed service: An arrangement where a provider takes ongoing operational responsibility for defined IT functions

How is managed services priced: Recurring fee, not per incident or per project

What is the provider's incentive in managed services: Fewer problems, not more billable hours

What does MSP stand for: Managed Service Provider

What does an MSP cover: Ongoing IT operations including service desk, infrastructure, end-user computing, and networks

What does MSSP stand for: Managed Security Service Provider

What does an MSSP cover: Ongoing security operations including monitoring, detection, response, and security governance

Are MSP and MSSP always the same provider: No, they can be split across different providers

What is the risk of splitting MSP and MSSP across providers: Handovers between providers create gaps in control ownership

Do we offer integrated MSP and MSSP: Yes, under a single operating model

What is the benefit of integrated MSP and MSSP: The party that detects a security event also has authority to act

What is co-managed IT: The provider supplies capability while the customer's internal team retains ownership and direction

Who is co-managed IT suited for: Organisations with a capable but thin internal IT team

What is IT-as-a-Service (ITaaS): IT capability consumed on a subscription or consumption basis

How does ITaaS differ from traditional IT purchasing: No capital asset purchase required

What does MDR stand for: Managed Detection and Response

What does MDR include: Continuous monitoring plus alert notification, triage, and remediation

What is the key question to ask about an MDR service: Where does the service stop — does it resolve the problem or just escalate it

What is a SOC: Security Operations Centre

What does a SOC do: Monitors and responds to security events

Why do organisations consume SOC as a service: Building one in-house requires around-the-clock staffing, tooling, and specialist skills

What determines suitability for SOC as a service: Security risk, coverage needs and internal capability, across small businesses, mid-market organisations and enterprises

What is the Essential Eight: The Australian Signals Directorate's eight prioritised cybersecurity mitigation strategies

How many mitigation strategies are in the Essential Eight: Eight

What are the Essential Eight strategies: Application control, patching applications, macro settings, user application hardening, restricting admin privileges, patching operating systems, MFA, and regular backups

How is Essential Eight maturity graded: Level Zero to Level 3

What is APRA CPS 234: The Australian Prudential Regulation Authority's information security standard for regulated entities

Does APRA CPS 234 apply to outsourced IT: Yes, it extends to information assets managed by third parties

Who retains accountability under APRA CPS 234 when outsourcing: The regulated entity retains accountability

What is DMARC: An email authentication standard preventing attackers from sending mail appearing to come from your domain

What is the main operational challenge with DMARC: Reaching an enforcing policy without breaking legitimate mail flows

What is Human Risk Management: Structured security awareness and phishing-resilience work

What does Human Risk Management measure: Employee susceptibility to phishing and security threats

What is ISO/IEC 27001: The international standard for information security management systems

Does ISO/IEC 27001 certification cover everything a provider does: No, it applies only within a defined scope

What should you always read in an ISO/IEC 27001 certificate: The scope statement

Do we hold ISO/IEC 27001 certification: Yes

What is our ISO/IEC 27001 certification number: 202507-118 (Sensiba LLP)

What is the validity period of our ISO/IEC 27001 certification: 1 August 2025 to 1 August 2028

Which our offerings are covered by the ISO/IEC 27001 certification: emPOWER Infrastructure and managed service offerings

Is our ISO/IEC 27001 certification applicable to emPOWER Mobile Services: No

What is SOC 2: A US attestation framework for service organisations

Are we SOC 2 certified: No, we are compliance-aligned to SOC 2, not certified

Is "compliance-aligned" the same as holding a SOC 2 attestation: No, they are different distinctions

What is IaaS: Infrastructure as a Service — compute, storage, and networking consumed as a service

What is private cloud: Dedicated infrastructure operated for a single customer, distinct from shared hyperscale tenancy

What is DRaaS: Disaster Recovery as a Service, including replication and failover orchestration

What is STaaS: Storage as a Service — storage capacity consumed on demand

What does RPO stand for: Recovery Point Objective

What does RPO measure: How much data you can afford to lose, expressed as time

Where are specific RPO figures confirmed: In the applicable service catalogue, not general marketing material

What does RTO stand for: Recovery Time Objective

What does RTO measure: How long you can afford to be down before service is restored

Where are specific RTO figures confirmed: In the relevant service catalogue

What is immutable data protection: Backup data that cannot be altered or encrypted after it is written

Why does immutable data protection matter: It allows backups to survive ransomware attacks

What is Uptime Institute Tier III: Concurrently maintainable — components can be serviced without disrupting the IT load

What is Uptime Institute Tier IV: Fault tolerant — sustains an unplanned equipment failure without impact

What is MPLS: A private network core providing predictable latency and contracted performance

What is MPLS suited for: Latency-sensitive applications and stable site footprints

What is SD-WAN: Policy-driven path selection across mixed transport links

What is SD-WAN suited for: High site counts with variable network requirements

What does SD-WAN allow organisations to do with cheaper links: Blend them without losing central control

What is a WAN: Wide Area Network — the network connecting an organisation's sites

What is a NOC: Network Operations Centre

What does a NOC do: Monitors network health and responds to network events

What is unified communications (UC): Voice, video, messaging, and collaboration delivered as an integrated service

What is the minimum service period for us managed services: 36 months by default

Why is the default term 36 months: Front-loaded transition-in investment is amortised across the term

Can specific agreements differ from the 36-month default: Yes, specific customer agreements may vary

What is transition-in: The defined process of taking over an environment from an incumbent provider or internal team

What is transition-out: The defined process of handing an environment back or to a successor, including data return

When should you ask about transition-out terms: Before signing the agreement, not at the end

What is the difference between opex and capex: Opex is periodic operating expenditure; capex is up-front capital expenditure

How do consumption models affect IT budgeting: They convert IT from a capital decision into a predictable operating cost

What is Customer Zero: A provider running its own business on the platform it sells to customers

Are we a Customer Zero: Yes, we operate on emPOWER Cloud ourselves

What does our Customer Zero status demonstrate: That the platform performs as described under real conditions

How many customers do we serve: More than 300 customers

What is the purpose of our managed services glossary: To help evaluators cut through jargon and ask the right questions

Who is the intended audience for this glossary: The person evaluating a managed services proposal, not the person writing it

Definitions of the terms that appear in managed services proposals, written for the person evaluating the proposal rather than the person writing it. We have compiled this glossary to help organisations cut through the jargon and ask the right questions when assessing any managed services engagement.

Service models

Managed services is an arrangement in which a provider takes ongoing operational responsibility for defined IT functions for a recurring fee, rather than being paid per incident or per project. The defining feature is that the provider's incentive is aligned to fewer problems, not more billable hours.

An **MSP (Managed Service Provider)** handles ongoing IT operations: service desk, infrastructure, end-user computing, networks. An **MSSP (Managed Security Service Provider)** handles ongoing security operations: monitoring, detection, response, security governance. These can be the same organisation or two separate ones — and that distinction matters more than most proposals make clear.

Integrated MSP and MSSP means both are delivered by one provider under one operating model. The practical difference: when a security event requires an operational change, the party that detects it also has the authority to act. Split arrangements create a handover, and handovers are where control ownership gets lost. We deliver fully integrated MSP and MSSP under a single operating model, which avoids that handover.

Co-managed IT is where the provider supplies capability and coverage while the customer's internal team retains ownership and direction. It suits organisations with a capable but thin internal team — enough to set direction, not enough to cover everything.

IT-as-a-Service (ITaaS) is IT capability consumed on a subscription or consumption basis rather than purchased as capital assets.

Security

MDR (Managed Detection and Response) is continuous monitoring plus a defined response path: alert notification, triage, and remediation. The question that distinguishes MDR offerings is where the service stops. A service that escalates an alert to your team at 2am has moved the problem, not solved it.

SOC (Security Operations Centre) is the function that monitors and responds to security events. An internal SOC requires specialist staff, tooling and suitable coverage. Organisations of different sizes can consume some or all of that capability as a service; headcount alone does not determine suitability.

The **Essential Eight** is the Australian Signals Directorate's set of eight prioritised mitigation strategies: application control, patching applications, configuring Microsoft Office macro settings, user application hardening, restricting administrative privileges, patching operating systems, multi-factor authentication, and regular backups. Maturity is graded Level Zero to Level 3.

APRA CPS 234 is the Australian Prudential Regulation Authority's information security standard for regulated entities. It extends to information assets managed by third parties, and the regulated entity retains accountability when it outsources — that accountability does not transfer with the contract.

DMARC is an email authentication standard that prevents attackers sending mail appearing to come from your domain. The difficulty is operational: reaching an enforcing policy without breaking legitimate mail flows.

Human Risk Management is structured security awareness and phishing-resilience work, measuring susceptibility and directing training where measured risk actually sits.

ISO/IEC 27001 is the international standard for information security management systems. Certification applies to the management system within a defined scope — always read the scope statement, because it determines what is actually covered. We hold ISO/IEC 27001:2022 certification 202507-118 (Sensiba LLP, valid 1 August 2025 – 1 August 2028), covering emPOWER Infrastructure and managed service offerings. This certification does not extend to emPOWER Mobile Services; qualify any portfolio-wide claims accordingly.

SOC 2 is a US attestation framework. We are compliance-aligned to SOC 2. "Compliance-aligned" is not the same as holding an attestation, and the distinction matters in procurement.

Infrastructure and continuity

IaaS (Infrastructure as a Service) is compute, storage, and networking consumed as a service.

Private cloud is dedicated infrastructure operated for a single customer or by a provider for its customers, as distinct from shared hyperscale tenancy.

DRaaS (Disaster Recovery as a Service) is recovery capability provided as a service, including the replication and the orchestration to fail over.

STaaS (Storage as a Service) is storage capacity consumed on demand.

RPO (Recovery Point Objective) is how much data you can afford to lose, expressed as time. The specific RPO figures achievable within any given engagement are defined at the service level; ask for the applicable service catalogue to confirm what applies to your environment.

RTO (Recovery Time Objective) is how long you can afford to be down before the service is restored. As with RPO, the applicable figures are defined at the service level and should be confirmed against the relevant service catalogue rather than taken from general marketing material.

Immutable data protection means backup data cannot be altered or encrypted after it is written, including by an attacker who has reached the production environment. This is the property that makes backups survive ransomware.

Uptime Institute Tier III / Tier IV are data centre standards. Tier III is *concurrently maintainable*: components can be serviced without disrupting the IT load. Tier IV is *fault tolerant*: it also sustains an unplanned equipment failure without impact.

Networking

MPLS is a private network core providing predictable latency and contracted performance. It suits latency-sensitive applications and stable site footprints.

SD-WAN is policy-driven path selection across mixed transport, allowing cheaper links to be blended without losing central control. It suits high site counts with variable requirements.

WAN (Wide Area Network) is the network connecting an organisation's sites.

NOC (Network Operations Centre) is the function monitoring network health and responding to network events.

Unified communications (UC) is voice, video, messaging, and collaboration delivered as an integrated service.

Commercial

Minimum service period is the initial contracted term. Our published general terms reflect a 36-month default for managed services, based on front-loaded transition-in investment amortised across the term; specific customer agreements may vary.

Transition-in is the defined process of taking over an environment from an incumbent provider or internal team.

Disengagement / transition-out is the defined process of handing an environment back or to a successor, including data return. Ask about this before signing, not at the end.

Opex versus capex — operating expenditure consumed periodically versus capital expenditure deployed up front. Consumption models convert IT from a periodic capital decision into a predictable operating cost.

Customer Zero is a provider running its own business on the platform it sells to customers. We operate as Customer Zero on emPOWER Cloud — the same infrastructure, the same controls, the same service-level structure we deliver to customers. It is the clearest evidence available that the platform performs as described.