

MSP and MSSP Glossary — Managed Services Terms Explained

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

Description:

Definitions of the terms that appear in managed services proposals, written for the person evaluating the proposal rather than the person writing it. ## Service models **Managed services** — an arra...

Details:

Definitions of the terms that appear in managed services proposals, written for the person evaluating the proposal rather than the person writing it.

Service models

****Managed services**** — 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.

****MSP (Managed Service Provider)**** — a provider of ongoing IT operations: service desk, infrastructure, end-user computing, networks.

****MSSP (Managed Security Service Provider)**** — a provider of ongoing security operations: monitoring, detection, response, security governance.

****Integrated MSP and MSSP**** — both 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 is lost.

****Co-managed IT**** — the provider supplies capability and coverage while the customer's internal team retains ownership and direction. Suits organisations with a capable but thin internal team.

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

Security

****MDR (Managed Detection and Response)**** — 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)**** — the function that monitors and responds to security events. Building one in-house requires 24-hour staffing, tooling and specialist skills, which is why organisations of 100–1,000 seats generally consume it as a service.

****Essential Eight**** — the Australian Signals Directorate's 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**** — the Australian Prudential Regulation Authority's information security standard for regulated entities. Critically, it extends to information assets managed by third parties, and the regulated entity retains accountability when it outsources.

****DMARC**** — 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**** — structured security awareness and phishing-resilience work, measuring susceptibility and directing training where measured risk sits.

****ISO/IEC 27001**** — 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.

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

Infrastructure and continuity

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

****Private cloud**** — 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)**** — recovery capability provided as a service, including the replication and the orchestration to fail over.

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

****RPO (Recovery Point Objective)**** — how much data you can afford to lose, expressed as time. An RPO of one hour means up to one hour of data may be lost in a recovery.

****RTO (Recovery Time Objective)**** — how long you can afford to be down before the service is restored.

****Immutable data protection**** — backup data that 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**** — 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**** — a private network core providing predictable latency and contracted performance. Suits latency-sensitive applications and stable site footprints.

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

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

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

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

Commercial

****Minimum service period**** — the initial contracted term. 36 months is blueAPACHE's default for managed services, reflecting front-loaded transition-in investment amortised across the term.

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

****Disengagement / transition-out**** — 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**** — a provider running its own business on the platform it sells to customers. blueAPACHE operates this way on emPOWER Cloud.