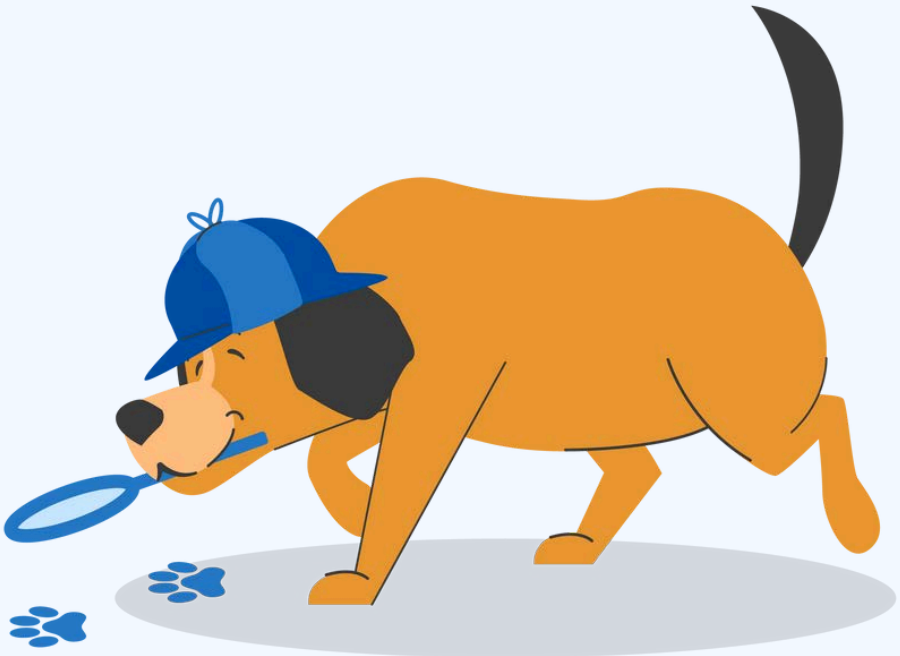
Mirazon

MSP Key Term Glossary

A Guide to Managed IT Terminology

www.mirazon.com
(502) 240-0404
info@mirazon.com

Let’s be real—tech jargon can get out of hand fast. If you’ve ever sat in a meeting and heard terms like “Zero Trust,” “RMM,” or “SIEM” thrown around like everyone just gets it, you’re not alone. Whether you’re a business leader trying to navigate your MSP partnership, an IT pro looking to brush up on key terms, or just someone tired of nodding along in confusion, we’ve got you covered. This glossary breaks down the most common MSP lingo in a way that actually makes sense—no tech-speak, no fluff, just clear and simple explanations. Let’s decode the language of Managed IT termoniology together!



IT Terminology Glossary

Backup & Disaster Recovery (BDR)

The process of securing data backups and having a recovery plan in place in case disaster strikes—whether it's a data breach, hardware failure, or natural disaster. The goal is to ensure business continuity.

- *Why it matters: BDR ensures your data is safe and recoverable, minimizing downtime and preventing catastrophic losses.*

Best Practices

A set of recommended actions, processes, or methods that are considered the most effective for achieving desired outcomes in a specific area, such as IT, security, or management.

- *Why it matters: Following best practices helps ensure consistent results, improves efficiency, reduces errors, and enhances overall performance by applying proven, industry-recognized strategies.*

Business Continuity Plan (BCP)

A strategic approach to preparing for and responding to disruptions ensures your business can continue to operate during and after a crisis.

- *Why it matters: A solid BCP minimizes downtime, protects critical assets, and enables rapid recovery, safeguarding your business against potential threats and disasters.*

Change Management

A structured process for making changes to IT systems. Whether it's a new software installation or a system upgrade, change management ensures that updates are made smoothly without causing disruptions.

- *Why it matters: Structured change management reduces risks, ensuring IT updates don't cause unexpected downtime or issues.*

Cloud Services

Remote IT services hosted on the internet, such as data storage, computing power, and applications. MSPs manage these environments for clients to ensure security, availability, and performance.

- *Why it matters: Cloud services improve flexibility, scalability, and performance, while the MSP ensures these resources remain secure and available.*

Commitment

This refers to the promises made by the MSP regarding the level of service and support they'll provide, including specific timeframes, resources, and deliverables.

- *Why it matters: Commitments ensure your MSP's promises are defined and measurable, keeping service delivery transparent and making sure everyone is on the same page.*

Cybersecurity

A set of practices and tools used to protect networks, systems, and data from cyberattacks, unauthorized access, and other digital threats. MSPs help safeguard their clients' operations with comprehensive cybersecurity measures.

- *Why it matters: Strong cybersecurity measures protect your business from costly breaches, downtime, loss of reputation, and more.*

Data Protection & Compliance Services

A service that ensures your business complies with industry regulations and standards while protecting sensitive data from breaches or misuse.

- *Why it matters: Compliance reduces legal and financial risks, while strong data protection fosters trust and safeguards your reputation.*

Documentation

The process of creating and maintaining detailed records of your IT systems, processes, and assets to ensure clarity, consistency, and operational efficiency.

- *Why it matters: Comprehensive documentation improves troubleshooting, reduces downtime, and simplifies onboarding, knowledge transfer, and system management.*

Downtime

When a system or service is unavailable, often due to issues or maintenance. Reducing downtime is a key part of what MSPs do to keep systems running smoothly.

- *Why it matters: Less downtime means fewer disruptions, keeping your business operational and minimizing lost revenue.*

Endpoint Detection & Response (EDR)

A security solution that continuously monitors and responds to suspicious activity on devices like desktops, laptops, and mobile phones, identifying and addressing threats in real-time.

- *Why it matters: EDR enables early detection of cyber threats, provides detailed insights into potential attacks, and allows for rapid remediation to prevent data breaches.*

Endpoint Management

Managing all the devices (laptops, desktops, smartphones, etc.) connected to a network to ensure they are secure and properly configured.

- *Why it matters: Proper endpoint management protects your network from vulnerabilities, ensuring every device performs as it should and does not put your business/IT infrastructure at risk.*

Escalation

When an issue needs to be handed off to a higher level of expertise within the MSP, either because it's more complex or more urgent. This ensures that problems are resolved by the right person as quickly as possible.

- *Why it matters: Escalation ensures critical problems are addressed efficiently by the experts best equipped to resolve them.*

Helpdesk

A service that provides technical support to end users. Whether it's solving software glitches, password resets, fixing hardware issues, or troubleshooting network problems, the helpdesk is there to help when things go wrong.

- *Why it matters: A responsive helpdesk ensures your employees can stay productive by quickly resolving their IT problems.*

Incident Management

The process of managing IT issues or disruptions. It's about identifying, responding to, and resolving incidents that affect the business's ability to function.

- *Why it matters: Effective incident management minimizes downtime, restores functionality quickly, and reduces business impact.*

Incident Response Plan (IRP)

A documented strategy outlining how an organization will respond to cybersecurity incidents, including breach detection, containment, investigation, and recovery.

- *Why it matters: An effective IRP enables a quick, coordinated response to minimize damage, restore operations, and prevent future incidents.*

Identity & Access Management (IAM)

A solution that controls user access to systems and applications, ensuring the right people have the right access at the right time.

- *Why it matters: IAM helps secure sensitive information, ensures compliance with regulations, and minimizes the risk of unauthorized access or data breaches.*

Internet Service Provider (ISP)

The company that provides the internet connection for businesses or individuals. They are often part of the MSP conversation when it comes to managing network infrastructure.

- *Why it matters: Reliable internet is critical to your operations, and your MSP can help ensure it's stable, optimized, and supported when issues arise.*

Managed Detection & Response (MDR)

A comprehensive security service that provides 24/7 monitoring, detection, and response to threats across your IT environment, combining advanced technology and expert analysis.

- *Why it matters:* MDR offers proactive threat hunting, quick incident response, and expert-driven security oversight, ensuring your organization is protected from emerging and sophisticated cyber threats.

Managed Services

Ongoing IT support and management provided by the MSP, which can include everything from network monitoring to data backups and security measures. It's about keeping your systems running smoothly without having to worry about it.

- *Why it matters: Managed services allow you to focus on your business while experts handle your IT, reducing risks and improving efficiency.*

Multi-Factor Authentication (MFA)

A security measure that requires users to provide two or more forms of identification before accessing systems or applications, such as a password and a verification code.

- *Why it matters: MFA significantly reduces the risk of unauthorized access by ensuring that stolen credentials alone are not enough to compromise sensitive data.*

Network Monitoring

Constantly watching a company's network to spot any performance issues, security threats, or problems. This is key to proactive support and ensures systems are always running as they should.

- *Why it matters: Network monitoring helps prevent downtime, maintain security, and ensure optimal performance across your IT environment.*

Offboarding

When the service relationship ends, the MSP will help transition the client out, making sure all data is transferred and the systems are properly shut down or handed over.

- *Why it matters: Proper offboarding ensures a smooth transition, preventing data loss or lingering access issues.*

Onboarding

The process of getting a new client set up with the MSP's services. This typically involves assessments, tool deployment, and making necessary configurations, ensuring that all systems are ready for ongoing support and expectations are set.

- *Why it matters: A smooth onboarding process minimizes disruptions and ensures your IT environment is optimized from the start.*

Patch Management

The practice of keeping software up to date by applying updates and patches. This ensures security vulnerabilities are fixed, and systems stay secure and functional.

- *Why it matters: Regular patching keeps your systems protected from cyberattacks and ensures they operate smoothly.*

Privileged Access Management (PAM)

The process of controlling and monitoring access to critical systems and accounts for users with elevated privileges.

- *Why it matters: PAM minimizes the risk of insider threats and unauthorized actions, ensuring sensitive systems remain secure and compliant.*

Proactive Support

This is when the MSP takes steps to prevent issues from happening before they even arise—whether that's monitoring systems, performing regular maintenance, or optimizing your environment to avoid downtime.

- *Why it matters: Preventing problems saves time, money, and headaches, keeping your systems reliable and minimizing disruptions.*

Quarterly Business Review (QBR)

A quarterly meeting between the MSP and the client to evaluate performance, resolve issues, and discuss future objectives. It's an opportunity to ensure the service is staying aligned with the client's needs.

- *Why it matters: QBRs provide a regular touchpoint to address concerns, plan improvements, and ensure your IT investment delivers maximum value.*

Remote Monitoring & Management (RMM)

Tools and processes that allow the MSP to monitor and manage a client's IT systems remotely. It's all about catching issues early, applying patches, and ensuring everything runs smoothly without needing to be on-site.

- *Why it matters: RMM enables your MSP to manage systems efficiently, resolve problems faster, and ensure uptime without disruptions.*

Security Awareness Training (SAT)

A program designed to educate employees on cybersecurity best practices, phishing identification, and safe IT usage. It helps prevent human error, which is one of the most common causes of cyber incidents.

- *Why it matters: Educated employees are your first line of defense against cyber threats, reducing risks and protecting your business from costly breaches.*

Security Assessments

A process that evaluates your organization's IT infrastructure, policies, and systems to identify vulnerabilities, risks, and areas for improvement.

- *Why it matters: Regular assessments help uncover weaknesses before attackers exploit them, ensuring your systems remain secure, compliant, and resilient against evolving threats.*

Security Information & Event Management (SIEM)

A system that collects, analyzes, and responds to security events and incidents in real time, providing comprehensive visibility and threat intelligence.

- *Why it matters: SIEM enables proactive threat detection and response, helping organizations defend against cyberattacks and maintain compliance with security regulations.*

Service Level Agreement (SLA)

A written agreement that defines the level of service an MSP will provide. It outlines key details like response times, resolution times, and uptime guarantees. Essentially, it's a promise to deliver the agreed-upon service.

- *Why it matters: It sets clear expectations for both you and the MSP, ensuring accountability and helping you measure the quality of service you receive.*

Service Level Objective (SLO)

A specific, measurable target set within an SLA. For example, it could be the goal to resolve 90% of service requests within four hours. It helps both the MSP and client know what to expect in terms of performance.

- *Why it matters: It provides benchmarks to track performance and helps you hold your MSP accountable for agreed-upon terms and goals.*

Staff Augmentation

A service that provides skilled IT professionals to supplement your existing team, helping you bridge talent gaps, manage workloads, or execute specialized projects efficiently.

- *Why it matters: Flexible access to qualified experts ensures your business stays on track, meets deadlines, and adapts to changing demands without the long-term commitment of hiring full-time employees.*

Technology Business Review (TBR)

A regular check-in where the MSP reviews the client's tech environment, performance, and future needs. It's a proactive way to make sure everything's running smoothly and aligned with the business's goals.

- *Why it matters: TBRs keep your IT strategy aligned with your business goals, ensuring no gaps or inefficiencies arise. It also helps with budgeting and making sure your MSP is also prepared for what's in store for your business.*

Uptime

The percentage of time that a system or service is fully operational. An MSP will often guarantee a certain level of uptime, like 99.9%, to ensure that clients experience minimal downtime.

- *Why it matters: High uptime guarantees ensure your systems are reliable, supporting business productivity, customer satisfaction, and brand reputation.*

Value-Added Reseller (VAR)

A service provider that enhances third-party hardware, software, or IT solutions with additional services like installation, configuration, and support to deliver a complete solution.

- *Why it matters: VARs simplify IT procurement, provide tailored solutions, and ensure businesses get maximum value and functionality from their technology investments.*

Virtual Private Network (VPN)

A technology that creates a secure, encrypted connection over a public network, allowing users to access a private network remotely while keeping their data protected.

- *Why it matters: A VPN ensures privacy and security for sensitive data, even when users are connected to unsecured networks, such as public Wi-Fi, reducing the risk of cyberattacks and data breaches.*

Virtualization

The creation of virtual versions of physical IT components, like servers or storage devices. This allows for better flexibility, scalability, and efficiency in managing IT resources.

- *Why it matters: Virtualization allows you to optimize resources, reduce costs, and scale IT systems efficiently as your business grows.*

Zero-Trust Architecture

A security model that assumes no one, inside or outside the organization, should be trusted by default and requires verification for every user and device attempting to access systems.

- *Why it matters: Zero Trust minimizes the risk of internal and external threats by continuously verifying access requests and minimizing the attack surface.*

Technology moves fast, and keeping up with all the industry jargon can feel like a full-time job. But now that you've got this glossary in your back pocket, you're one step ahead of the game. Whether you're working with an MSP, leading an IT team, or just trying to make sense of all the buzzwords, understanding these key terms can help you make smarter decisions and have more productive conversations. And if you ever come across a new acronym that makes you scratch your head—don't worry, we've all been there. Just reach out, and we'll help you decode it!

Check Out Our Managed IT Services!

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com