FSET
INFORMATION TECHNOLOGY

2025

WHITEPAPER

The Three Pillars of a Reliable Managed Service Provider

FSET Inc.
Address: 201-610 Lakeview Drive Kenora, ON P9N 3P7
Phone: (833) 468-0174
Email: info@fset.ca

CONTENTS

Beyond IT Support: The Evolving Role of MSPs

The right managed service provider (MSP) can be one of your most valuable partners and service providers, delivering the insight and technical support your organization needs to operate securely and navigate the fast-moving digital landscape with confidence. An MSP provides outsourced IT services such as infrastructure management, cybersecurity, cloud support, and help desk operations.

As MSPs become more integral to operations across healthcare, education, government, and business, they must also rise to higher standards of accountability.

MSPs are no longer limited to help desk support or patch management. Many providers now oversee sensitive data, public-facing systems, and the daily continuity of critical infrastructure. Your MSP needs to go beyond transactional support and serve as a trusted extension of your team.

The most reliable MSPs invest heavily and extensively in foundational disciplines that are easy to overlook during procurement. Accreditation, hiring practices, and insurance may not be part of the standard evaluation criteria, but they are clear indicators of how a provider operates behind the scenes.

The New MSP Standard

Procurement checklists don't always reflect what matters most. While technical capabilities, SLAs, and toolsets are easy to compare, they reveal very little about whether a provider is equipped to support high-trust environments over time.

The difference isn't always visible on the surface. Two MSPs may offer similar services, but only one may have the internal structure, staffing discipline, and liability protections required to work in regulated sectors or support business continuity under pressure.

Organizations that prioritize due diligence look past service menus and pricing tiers. They ask how providers are audited. How employees are vetted. How insurance coverage is structured. These questions shift the conversation from support to accountability.

Service quality can be evaluated in real time, but structural readiness requires a closer look. The most capable providers don't just respond effectively; they're built to reduce risk, support continuity, and hold up under scrutiny. That foundation is where meaningful differentiation begins.

Accreditation and Certification

A Signal of Trust in a Crowded Market

In a field where every MSP says they offer "secure" or "compliant" solutions, third-party accreditation where available is one of the few tools that separates marketing from reality. It demonstrates that a provider is meeting a globally recognized framework, validated by an external body with no stake in the outcome. It also shows that controls are in place, that processes are consistently followed, and that any claims can be backed by evidence.

While ISO/IEC 27001 remains one of the most globally recognized frameworks, others such as SOC 2, NIST 800-53, the CPCSC, and CCCS SMB Baseline Profile are also common. Not all frameworks offer a formal certification or accreditation process, so it's important to understand what a given standard actually reflects and what level of oversight it includes.

Inside ISO/IEC 27001: What It Covers and Why It Matters

Among the most trusted frameworks in the industry is ISO/IEC 27001, the international standard for information security management systems (ISMS). ISO 27001 outlines 109 detailed controls across administrative, personnel, physical, and technical domains. The standard is split into several categories, each with real-world implications for how an MSP supports clients.

● Organizational and Administrative Controls

This section governs the internal structure of the provider, including inventory and asset management, documented policies, change management, access rights, role definition, and business continuity planning. The related controls establish a formalized framework for managing operational risk and ensuring consistency in day-to-day activities.

● Personnel and Human Resource Controls

Here, the focus shifts to the people behind the platform. Requirements include pre-employment background checks, confidentiality agreements, onboarding and offboarding protocols, and remote work safeguards. The goal is to ensure that staff are properly screened, trained, and supported to handle sensitive systems responsibly.

● Physical Security Controls

These controls govern access to physical infrastructure, such as data centers, secure office spaces, and server rooms, as well as surveillance, visitor logging, and facility-level protections. For MSPs working with sensitive data or public-sector clients, physical security controls form a critical layer of defense.

● Technical Controls

This is perhaps the most widely recognized category, encompassing everything from encryption and endpoint protection to vulnerability scanning, identity management, monitoring, and logging. Each control must be formally addressed, and each claim must be backed by documented procedures and audit-ready evidence.

Once certified, the MSP enters a three-year cycle: a full certification audit in year one, followed by annual surveillance audits conducted by an accredited third-party registrar. Additional internal audits are required and usually performed by an independent consultant to identify gaps, test controls, and maintain readiness year-round.

The certification process is both rigorous and labor-intensive. Preparing for an audit can take weeks of focused internal work, in addition to continuous documentation, internal monitoring, and process improvements throughout the year. Every control is reviewed not only for its existence but for its effectiveness. Even seemingly simple controls often involve multiple layers of review. A remote work policy, for example, might need to account for device hardening, VPN configuration, identity management, session timeout, and user training along with the logs and change history to prove that each of these controls is functioning.

Although ISO certification is a meaningful differentiator, it does not prescribe which specific technologies or tools a provider must use. It plainly requires that each control be selected based on documented risk, implemented in policy, and supported by evidence. In practice, certification demonstrates that a formal structure is in place, and one that has been independently audited and maintained through ongoing internal and external review. It also shows a significant investment of time, resources, and organizational commitment to risk management.

When comparing multiple certified MSPs, it's helpful to ask how key controls have been implemented and whether their approach aligns with the level of protection your business requires. Even with the same certification, providers may tailor controls differently based on client needs, industry demands, and risk assessments.

ITSG-33: Canada's Highest Standard for Secure IT Services

For organizations in Canada's public sector (or those serving public sector clients), ISO 27001 alone is not enough. The Government of Canada relies on its own security framework, ITSG-33, developed by the Canadian Centre for Cyber Security, and outlining how government departments and service providers must manage IT security risk throughout the system lifecycle.

The ITSG-33 framework centers on two key components:

1. Security Control Profiles (SCPs):
   A catalog of safeguards across 13 control families, including access control, audit and accountability, configuration management, and incident response. These profiles help determine which security controls must be implemented based on the sensitivity of the system and its use case.

2. Security Assessment & Authorization (SA&A):
   A process that requires documented evidence of how controls are implemented, tested, and reviewed. For service providers, it means being prepared to demonstrate compliance to external auditors or clients at any time.

There is no formal certification for ITSG-33. However, FSET voluntarily aligns its internal practices to the framework to support public-sector clients and others in regulated industries. While ISO 27001 validates that FSET has an audited, documented, and accountable system of internal controls, ITSG-33 reflects how that system aligns to Canadian public-sector expectations.

Hiring Practices
Accountability in Action

Technology may run the systems, but people build, configure, and protect them. The individuals behind your MSP often have the most access to your data, infrastructure, and environment. How they're vetted, trained, and managed directly affects your risk profile. Yet hiring practices remain one of the most overlooked areas when evaluating an MSP.

Organizations often ask about ticket resolution times or hardware compatibility, but rarely do they press for details about the humans doing the work. In sectors where data sensitivity is high and regulatory scrutiny is sharp, strong personnel vetting translates to operational integrity.

Sector-Focused Background Checks

Every MSP will say they "do background checks." **The real question is: what kind, and are they aligned with the sectors they support?**

At FSET, working with police services and community healthcare organizations has required us to go well beyond standard screenings. It starts with enhanced criminal record checks, but often extends to vulnerable sector screenings, especially in environments involving mental health, developmental services, or direct support roles. These deeper checks surface information that conventional screenings might miss and are often mandated by the clients themselves.

Even when not mandated, a layered screening process exhibits operational maturity. Beyond criminal checks, providers should verify employment history, education credentials, and professional references. For roles involving client interaction, administrative access, or regulated sectors, these steps help validate both qualifications and intent.

ID verification is another critical step that's often overlooked. Background checks are only as reliable as the identity they're tied to. In the past, this verification was done in person with scanned government-issued ID. Today, the process is more often digital, but with digital ease comes new risk. Without strong controls, it's possible for a different person to show up on Day 1 than was screened during hiring. Some providers now leverage biometrics to confirm identity, improving fraud detection beyond what the human eye can catch.

Elevated screening across the board builds consistency and confidence. If an MSP supports multiple sectors, their hiring practices should meet or exceed the most rigorous of them, not just the lowest common denominator. Vetting is not a one-time checkbox, either. Secure onboarding, periodic rescreening, access reviews, and tight separation of duties all help build long-term integrity into the workforce.

Personnel as Part of Security Protocol

Cybersecurity remains one of the most pressing concerns for organizations across sectors. While much of the focus tends to fall on systems and software, the more common (and often more dangerous) threat vector is human behavior.

Most incidents involving data loss, unauthorized access, or service disruption can be traced to individual actions, whether reused passwords, misconfigured permissions, phishing clicks, or poorly managed credentials. In a managed service environment, where technicians may have broad access across multiple clients, even one misstep can expose multiple systems. That level of access turns every hiring decision into a security decision.

Treating hiring as part of security architecture means building in safeguards from day one, including:

- Structured onboarding that aligns access levels with job roles and provides training on acceptable use, data handling, and organizational protocols.
- Security awareness programs that adapt to current threat patterns, including social engineering, MFA fatigue, and zero-trust expectations.
- Internal oversight and monitoring that goes beyond system uptime to track permission usage, behavioral anomalies, and access logs.
- Immediate offboarding protocols that revoke all access the moment a role changes or employment ends.

The rise of remote work introduces further complexity. MSPs must now account for home network variability, shared personal devices, VPN hygiene, and secure hardware delivery. A robust hiring process extends beyond screening to encompass how employees are supported to work securely in every environment.

When evaluating a provider, look for signs that they treat internal accountability as part of their security discipline:

- Do they log and audit who accessed what, when, and why?
- Are roles strictly permissioned, or is admin access loosely distributed?
- Can they clearly explain how they train, monitor, and manage staff?
- Is there operational separation between technical personnel and oversight?

At the end of the day, it’s culture that shapes how seriously people take their responsibilities when no one’s watching.

How to Vet Your Provider’s Vetting

Hiring practices are rarely detailed in an MSP pitch or proposal. Conversations with potential providers are your opportunities to get specific about how personnel are screened, onboarded, and monitored. The answers reveal not just process, but mindset.

Key questions to ask:

1. What levels of background checks do your employees undergo, and how often are they updated?
2. Are your screening protocols adapted for sectors with heightened regulatory or privacy expectations?
3. Do you verify identity as part of your screening process?
4. What types of verifications do you conduct beyond criminal, such as education, employment, and licensing?
5. How do you handle role-based access, particularly in remote or hybrid environments?
6. What controls are in place for onboarding, offboarding, and access transitions?
7. How is internal behavior monitored, and who oversees the reviewers?
8. Is screening conducted in-house, or do you partner with a vetted third-party provider who specializes in those services?

These questions can help distinguish whether a provider treats personnel risk as a checkbox or as a critical element of service delivery.

Insurance

The Safety Net You Need to See

Outsourcing IT doesn't automatically transfer liability. It's one of the most common misunderstandings in the MSP-client relationship. When something goes wrong, whether it's a breach, a ransomware attack, or a system outage, who carries the burden depends not only on contracts, but also on how well both parties are insured.

Many organizations assume that if they're paying a managed service provider, the provider's insurance will automatically protect them. That's not always the case. If the MSP lacks proper coverage, or if the coverage is structured narrowly around internal operations, your business could be left exposed, despite doing everything right on your end.

Exposure can also arise when an incident stems from a system or responsibility area not covered under the MSP's scope, such as a new service that hasn't been added to the contract, a tool outsourced to a different vendor, or a gap in the Shared Responsibility Matrix. Regularly reviewing contracts and keeping an up-to-date responsibility matrix is essential for aligning coverage to actual operations.

The most security-conscious MSPs recognize that their insurance posture directly affects their clients' ability to recover from potential incidents, qualify for cyber insurance, and satisfy compliance obligations, especially in regulated industries. However, despite its significance, insurance is one of the least-discussed aspects of MSP evaluation.

Why Your MSP's Insurance Is Part of Your Risk Profile

MSPs operate at the convergence of digital risk. They manage your systems, access your data, and often serve as your first line of defense and recovery. If an MSP is underinsured or carrying policies with significant exclusions, potential insurance gaps loom large, such as:

- Multi-tenant environments where one breach can impact multiple clients.
- Remote access tools that link directly into sensitive systems.
- Cloud misconfigurations that may be managed by third-party providers.
- Delays or errors in response during an active incident.

A well-insured MSP doesn't just protect its own bottom line. It becomes part of your organization's resilience strategy.

What Coverage Should Your MSP Have?

An MSP's insurance portfolio should reflect the complexity of the services they provide and the risk they inherit by operating within your environment. The following are the core policy types. Each plays a distinct role in managing liability and supporting continuity when things go wrong.

Technology Errors and Omissions (Tech E&O)

This is the foundational policy for any IT service provider. Tech E&O covers financial losses stemming from mistakes, failures, or negligence in service delivery. If the MSP misconfigures a system, misses a critical patch, or causes downtime due to an oversight, this is the policy that responds. An established MSP should carry sufficient E&O coverage to protect both its own business and its clients from the ripple effects of service disruption.

Importantly, tech E&O should account for both first-party (the MSP's own costs) and third-party (client-related) damages. That distinction becomes critical when the issue impacts your ability to operate, comply with regulations, or meet your own customer obligations.

Cyber Liability Insurance

Cyber insurance fills in the gaps that traditional E&O policies often exclude, especially when it comes to digital threats and data breaches. Strong cyber coverage for an MSP encompasses:

- Third-party coverage for client damages resulting from a breach or failure in the MSP's systems.
- First-party response costs, including breach notification, legal support, forensics, public relations, and ransomware remediation.
- Cybercrime-specific protections, such as social engineering, spoofing, MFA fatigue exploits, and dual extortion. These scenarios increasingly fall outside traditional definitions of negligence, but they still call for a coordinated response.

The most forward-looking MSPs also maintain a cyber policy that includes forensic coordination, incident response vendors, and pre-negotiated ransomware settlements, because speed and experience are everything during a breach.

General Liability, Property, and Business Interruption

These are more conventional commercial policies, but they're still necessary, particularly for MSPs that manage physical infrastructure or perform onsite work. General liability covers bodily injury and property damage, while property insurance protects the MSP's assets (including client-owned hardware housed in MSP facilities). Business interruption coverage can also be relevant if the provider experiences a facility-wide outage that delays service delivery.

Clients often overlook these lines of coverage because they seem unrelated to IT. But in environments where physical security, uptime, or hosted systems are involved, they can become just as relevant as cyber protections.

Retroactive Coverage and Contractual Liabilities

Two often-misunderstood areas can lead to significant exposure if they're not addressed:

- **Retroactive coverage:** Many MSP policies only cover incidents that occur after the policy is in force. But if a vulnerability existed months earlier—or if the MSP had been serving you under a prior policy without adequate coverage—you may not be protected. Strong policies should include retroactive dates that go back to the start of the relationship, or even earlier.
- **Contractual coverage alignment:** If your MSP contract includes indemnification clauses, minimum insurance requirements, or service level guarantees, those obligations should be backed by actual policies. A gap between what's promised in the contract and what's covered in insurance creates unnecessary risk.

A Truly Tailored Policy

The cyber insurance market is one of the fastest-moving and least-understood sectors in risk management. Many MSPs rely on automated platforms to purchase generic, low-cost policies, only to discover at claim time that the coverage doesn't hold up. Exclusions, low sub-limits, and narrow definitions of covered events can turn a six-figure recovery process into a legal fight.

Established MSPs usually work with insurance brokers who specialize in technology and cyber risk. A broker helps:

- Evaluate the MSP's business model, sector exposure, and system access.
- Design layered coverage to match those realities rather than generic risks.
- Identify ambiguous policy language and close gaps proactively.
- Recommend appropriate limits based on client size, industry, and data sensitivity.

More importantly, insurance brokers help MSPs explain their insurance posture to you as a client. That transparency helps you understand what protections are already in place, what risks remain shared, and what your own insurer may expect from third-party vendors.

You don't need to be an insurance expert to assess whether your MSP is putting you at risk. But you do need to ask the right questions and treat their coverage as a piece of your broader security posture.

A well-insured MSP will:

- Carry policies that name you as a third party or cover third-party damages related to their services.
- Understand your own cyber insurance requirements and help you meet them.
- Support annual risk assessments, incident response planning, and documentation required for your own policy renewal.
- Maintain policy limits that reflect the real-world consequences of failure.

That last point can't be overstated. A $1 million cyber policy may have been sufficient a decade ago, but today's ransomware events regularly exceed that number, especially for municipalities, healthcare providers, and education systems with widespread IT dependencies. Your MSP should be prepared to absorb risk at the scale of the environments they serve.

Questions to Ask Your MSP About Insurance

1. What insurance policies do you carry, and how are they structured for your services?
2. Do your policies include third-party coverage that protects us as a client?
3. What are your current coverage limits, and how often are they evaluated?
4. Who is your broker, and are they experienced in tech and cyber risk?
5. Can you share a certificate of insurance or summary that confirms these details?

Supporting Your Own Cyber Insurance Application

The cyber insurance market has become significantly more selective. Underwriters now ask detailed questions not only about your internal controls, but also about your vendors. That means your MSP plays a direct role in how insurable you are and what rates or exclusions you may face.

A credible MSP can help you navigate the cyber insurance process in several ways:

Providing Documentation for Underwriters

Cyber insurance applications often require proof of security policies, network diagrams, response plans, and access controls. Your MSP may maintain or manage many of these elements. A responsive provider should be able to supply relevant documentation or attestations that show how systems are secured and monitored.

Aligning Practices to Meet Insurability Standards

Whether MFA enforcement, privileged access management, backup encryption, and incident response protocols, insurers look for evidence of specific safeguards. Your MSP should not only implement these, but also explain how they function in your environment, particularly when they manage those controls on your behalf.

Supporting Pre-Binding Risk Assessments

Some carriers conduct technical scans or require third-party assessments before binding coverage. Your MSP may need to participate in these evaluations, whether to remediate vulnerabilities, clarify system architecture, or demonstrate that high-risk areas are under active management.

Advising on Shared Risk Posture

An MSP familiar with cyber underwriting standards can help you understand which controls are your responsibility versus theirs. This clarity reduces finger-pointing, improves application accuracy, and may help prevent policy disputes during a claim.

Participating in Post-Breach Claims Support

If an incident does occur, your MSP may be required to provide logs, timelines, and technical forensics to support your claim. An experienced provider will understand how to package that information in a way that aligns with what insurers need, minimizing delays and increasing the likelihood of a smooth payout.

Including Insurance in Your Incident Response Plan

One of the most overlooked but critical connections is between insurance and incident response planning. Reviewing your incident response plan with your MSP before an event occurs helps clarify when and how insurance should be activated. That conversation should include who contacts the insurer, when legal counsel gets involved, and what documentation needs to be preserved. The best time to map this out isn't during a breach; it's in a tabletop exercise with all the key players in the room.

Ultimately, a well-insured and cyber-savvy MSP can help you secure cyber coverage for your organization and stay insurable over time.

Partnership

What Separates a Vendor from a Partner

The most capable MSPs are rarely the flashiest. They may not lead with jargon, dashboards, or bold claims, but behind the scenes, their structure tells a different story. It's visible in how they're certified, how they hire, and how they mitigate risk. For organizations that rely on continuity, privacy, and public trust, those factors are often what determine whether an MSP relationship thrives or breaks under pressure.

When you ask about certification, you're asking whether a provider's processes have been tested and enforced. When you examine hiring practices, you're probing the integrity of the people with access to your environment. And when you dig into insurance, you're exploring whether the provider is prepared to share and manage risk.

Looking at these elements in isolation is useful. But the deeper insight comes from understanding how they interact. A provider that earns ISO certification but hires carelessly is still introducing risk. A provider that vets staff thoroughly but carries minimal insurance may leave you exposed after a breach. A provider with good insurance but no formalized policies might have coverage, but not credibility. Strong MSPs show strength across the board. They operate as if each decision carries long-term consequences—because it does.

When your provider's internal practices reflect your external obligations, you gain more than a vendor. You gain a partner who's prepared to grow with you and carry weight where it counts. That's what separates a name on a contract from a team you can trust with your systems, your staff, and your goals.

About FSET

Founded in 1999 and based out of Northwestern Ontario, FSET is a managed service provider that delivers progressive and forward-thinking solutions for both the public and private sectors.

FSET Inc. offers a unique blend of proactive IT security solutions and managed services, ensuring protection and operational excellence for businesses. In addition to providing a full range of Information Technology services, we assist other organizations with digital transformation and collaborate with SpaceX to help deliver Starlink broadband internet to the far North.

We believe in Innovation Empowering People and will forever be on a mission to improve the world with technology.

Learn more at fset.inc.

FSET Inc.

Address: 201-610 Lakeview Drive Kenora, ON P9N 3P7

Phone: (833) 468-0174

Email: info@fset.ca

Innovation Empowering People.

Developed by:
FSET Inc.
©December 2025