

The Acronis logo is displayed in white text on a dark blue rectangular background in the top right corner. The background of the entire page features a 3D illustration of a laptop with a line graph and pie chart on its screen, resting on a blue base. Surrounding the laptop are various digital icons: a calendar, a cloud, a database cylinder, and a person icon, all connected by a network of lines. A large, curved white object is visible in the upper left background.

Acronis

WHITE PAPER

How Australian MSPs can help clients meet the new SMB1001 cybersecurity standard

A new cybersecurity
standard for SMBs

SMB1001 is a new global cybersecurity certification standard created by Dynamic Standards International (DSI) for small and medium-sized businesses (SMBs). Unlike the sets of standards that are relevant for organisations of larger sizes or more complexity, SMB1001 is designed specifically for SMBs.

First published in 2023, SMB1001 provides a clear, affordable and scalable roadmap for improving cyber defences without the complexity or cost of enterprise-grade frameworks. DSI created the standard to help SMBs address evolving cyberthreats, meet compliance requirements and build trust with customers and partners.

Requirement 1 of SMB1001 is to engage a technical support specialist — it is partner-powered by design. For managed service providers (MSPs), this presents great opportunity. MSPs that can effectively communicate to clients the importance of compliance can also provide services that enable SMBs to achieve certification. SMBs will not be able to comply with SMB1001 without their own resources, so MSPs have a large potential market to address.

How SMB1001 works

SMB1001 is a dynamic standard that is updated every year to keep pace with emerging cyberthreats. It maps to global security frameworks, including Essential Eight, Cyber Essentials in the U.K. and the Cybersecurity Maturity Model Certification (CMMC) in the U.S.

Though similar frameworks, such as NIST 2.0 and the Centre for Internet Security (CIS) frameworks target businesses of varying sizes, their origins lie with larger organizations. By contrast, DSI designed SMB1001 specifically for small businesses from the outset.

The SMB1001 framework is organised into five progressive levels, each building on the previous one. This tiered approach enables SMBs to enhance their cybersecurity at a pace that matches their resources and risk profile. They include:

Bronze	Silver	Gold	Platinum	Diamond
Start with the absolute essentials: firewalls, antivirus, strong passwords, software updates and a reliable backup plan. These form your cyber hygiene baseline.	Step up with stronger identity protection, increased access controls, server patching, invoice fraud protection and fundamental procedures. This tier qualifies SMBs for cyber insurance.	Introduces formal security governance: cybersecurity policies, data protection, digital asset registers, incident response and employee awareness training. The foundations for SMB cyber compliance and resilience.	Strengthen resilience with vulnerability scanning and testing, stronger MFA, cyber insurance and independent verification. Platinum verifies protection against more serious threats and risks to your SMB.	Demonstrate comprehensive assurance through supplier trust programs, police vetting and live testing of incident response. Independently verified and aligned to advanced regulatory and critical services standards.

SMBs can achieve certification for the first three levels using self-attestation from the business's director. The two highest levels require external audits and ongoing oversight with independent validation of advanced controls.

How MSPs can explain the value of SMB1001

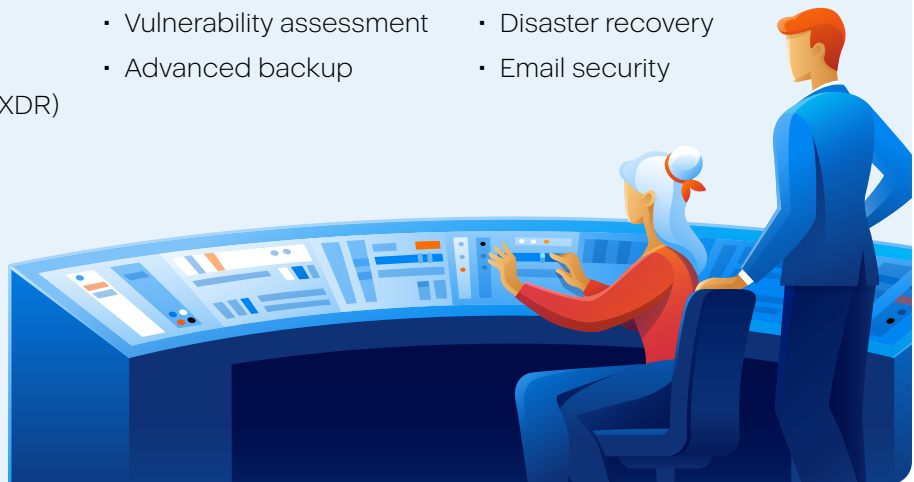
SMB1001 opens cybersecurity certification to smaller businesses that can't necessarily meet enterprise-grade requirements. MSPs can deliver the message that ransomware and other forms of malware are persistent and growing threats, but they can also communicate some advantages specific to SMB1001 certification:

- **Improved protection:** SMBs reduce the risk of cyber incidents and data breaches by implementing at each stage of certification best practices tested and verified by CyberCert, and its independent, expert third parties.
- **Competitive advantage:** Certification demonstrates a commitment to cybersecurity and enables SMBs to build and reinforce trust with clients and partners.
- **Scalability and affordability:** The tiered approach enables businesses to start at a level that matches their needs and scale as they grow.
- **Simplified compliance:** Certification helps SMBs meet regulatory and contractual requirements without taking on too much complexity.

How Acronis Cyber Protect Cloud enables MSPs to help clients achieve SMB1001 certification

MSPs need a platform that will enable them to grow and scale as their clients' businesses grow. Acronis Cyber Protect Cloud provides a foundation for growth by offering multiple services in one natively integrated platform, including:

- RMM
- Security plus extended detection and response (XDR)
- Patch management
- Microsoft 365 posture management
- Vulnerability assessment
- Advanced backup
- Disaster recovery
- Email security



Acronis Cyber Protect Cloud also delivers comprehensive cybersecurity protection with antivirus, endpoint detection and response (EDR) and extended detection and response (XDR) capabilities. All solutions in the platform work together seamlessly, so MSP technicians can manage them all from a single console. Onboarding clients is easy, as is adding and expanding services.

With Acronis Cyber Protect Cloud, MSPs can take SMBs from Bronze-level SMB1001 certification all the way to Diamond level. A specific map of SMB1001 requirements to Acronis Cyber Protect Cloud features reveals how Acronis enables MSPs to guide clients through the layers of certification.

Bronze certification

- Engage a technical support specialist MSP or IT specialist to provide regular and reliable assistance to manage your organisation's day-to-day IT related cybersecurity requirements, including assistance implementing requirements in this certification.

Acronis Cyber Protect Cloud is designed for MSPs, who fill the role of specialists for clients.

- Install antivirus software on all devices or endpoints in use within your organisation, including all workstations, laptops and personal devices, such as phones and tablets. All antivirus software must be set to automatically install new updates and software versions.

Acronis Cyber Protect Cloud offers antivirus protection on the most AV on widely used endpoint operating systems, including Windows, MacOS and Linux. It also offers endpoint detection and response (EDR) on Windows and Linux.

- Ensure all software installed on the workstations, laptops and personal devices such as phones and devices that are used within your organisation, including their operating systems and applications, are set to update automatically with tested and approved updates and patches.

MSPs can automate both patching for Windows and application updates with minimal need for maintenance or management.

- Ensure all new devices have their passwords reset when first installed or used. Change or update passwords to all networking devices (including firewalls and Wi-Fi access points), workstations, mobile devices and servers in use within your organisation at least once every 12 months.

The Acronis Cyber Protect Cloud platform enables MSPs to keep clients in compliance by requiring a password change after a first-time login. Microsoft 365 management via the Acronis Ultimate 365 solution, natively integrated into Acronis Cyber Protect Cloud, ensures baseline security policy compliance for Microsoft 365.

- Implement a strategy to back up the important digital data and systems your organisation needs to operate so they can be recovered and restored to an operational state in a timely manner.

MSPs have natively integrated backup and disaster recovery capabilities.

Silver certification

Silver certification includes all the requirements of the Bronze level and adds another layer.

- Install Transport Layer Security (TLS) and / or Secure Sockets Layer (SSL) certificates on all public internet-facing websites the organisation has deployed. All certificates must be issued by a trusted certificate authority (CA).

Acronis Cyber Protect Cloud encrypts all data "in flight" (as it is transferred) and uses digital certificates.

- Enable multifactor authentication (MFA), or two step verification on all email accounts that are used within your organisation. This includes any administrator accounts.

Acronis Ultimate 365, natively integrated into Acronis Cyber Protect Cloud, enforces Microsoft 365 baseline policies, including MFA.

Gold certification

Gold certification includes all the requirements of the Silver level and adds another layer.

- Ensure a regular routine for maintenance, patching and updating is in place for all servers your organisation uses. This includes all on-premises servers, cloud-hosted servers and servers from external providers, such as web servers.

Acronis Cyber Protect Cloud enables MSPs to automatically patch the Windows Server operating system and third-party applications automatically without the need for technician intervention.

- Conduct cybersecurity awareness training for all employees to educate them on the cyberthreats they face, the responsibilities they have to protect the organisation and how they should respond in the event they are involved in, or suspect they are involved in, a cyber incident.

Acronis Security Awareness Training gives MSPs prepackaged courses specific to countries and industries that service providers can deliver to clients. Partners can also create their own training content based on the Acronis curriculum.

Platinum certification

Platinum certification includes all the requirements of the Gold level and adds another layer.

- Ensure all public internet-facing resources, including web servers, API programmable web services, VPN authentication sites and any publicly addressable content are regularly scanned and remediated for malware and known vulnerabilities.

Acronis Cyber Protect Cloud performs daily vulnerability assessment scans on endpoints. The platform then compares those scans to the Acronis databases of known vulnerabilities, which include a wide variety of sources.

Diamond certification

Diamond certification includes all the requirements of the Platinum level and adds another layer.

- Ensure that important digital data (specifically all critical, confidential, sensitive and personally identifiable data required to run your organisation) is encrypted where it is stored (at rest).

Acronis Cyber Protect Cloud encrypts all backups — both in flight and at rest. MSPs can set their own Advanced Encryption Standard-level encryption and passwords.

- Implement a digital trust agreement with all of your organisation's suppliers.

Acronis can provide documented certification for many standards, including ISO27001.

Move at the pace of SMB1001 with Acronis

With Acronis Cyber Protect Cloud, MSPs can enable their clients to achieve all levels of SMB1001 certification. And since DSI updates the framework annually, the opportunities for MSPs can expand services as the framework evolves.

