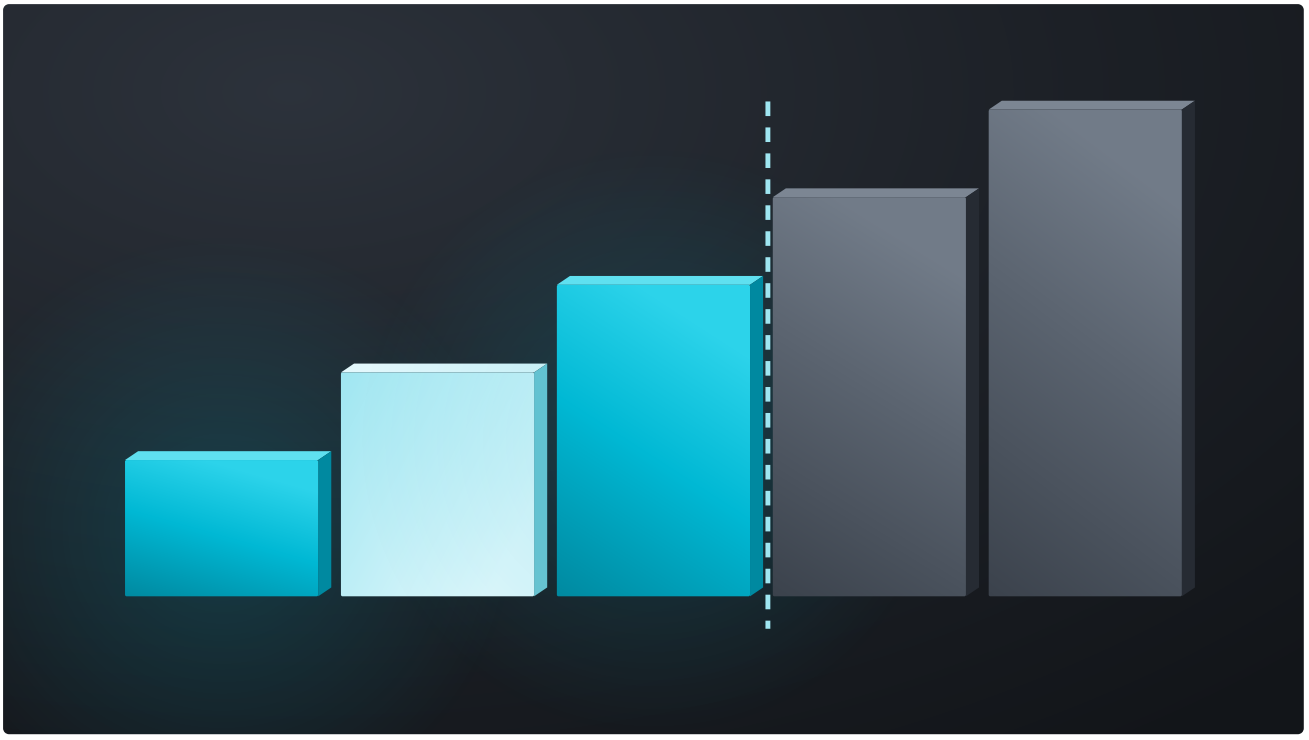
Black Shard

TECHNICAL WHITEPAPER

SMB1001:2026: what each of the five tiers asks of a small business

SMB1001:2026 sets five cumulative levels of cyber security for a small or medium business, Bronze to Diamond. A director attests to the first three and an external auditor checks the top two. The controls at each level in the publisher's words, and the work a firm faces to reach the one its customers ask for.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-10
Classification	Public
Version	1.3
First published	21 July 2026
This edition	16 November 2026
Figures	Standard of 1 Sep 2025, practice statement of 10 Jul 2026

Executive summary

SMB1001:2026 has five levels, Bronze, Silver, Gold, Platinum and Diamond, numbered Levels 1 to 5, and each level carries every control of the levels below it. Dynamic Standards International released SMB1001:2026 on 1 September 2025.

Bronze, Level 1, asks for 7 controls: a technical support specialist, a firewall, antivirus on every device, automatic patching, strong password hygiene, a backup and recovery strategy, and cyber security awareness training for all employees.

Gold, Level 3, carries 27 controls in total, the count printed on our own SMB1001:2026 Gold certificate. A director attests at Levels 1 to 3; an external audit joins the attestation at Levels 4 and 5.

The standard is written for the business that has never been asked to show its security before. Bronze is a short list a sole trader can complete with its IT provider. Gold is where a buyer, an insurer or a government panel starts to read the certificate as evidence, because it reaches governance: policies, an incident response plan, detection on every endpoint and authenticated email. Platinum and Diamond are for the firm whose customers want an auditor's signature.

The practical question for a small firm is which level the people who pay it will ask for, and how far its current controls sit from that level. A firm that runs its email in a hosted suite with a managed IT provider usually has part of Bronze and Silver in place without naming it. What is missing is the evidence, and the handful of controls that need a decision from the owner.

- Find out which level your customers, your insurer and your contracts name, and aim at that one.
- List the controls at that level against the systems that enforce them, and write down what proves each one.
- Treat Gold as the level that buyers read; above it, book the auditor before the work starts.

Method

We read the publisher's public page for the 2026 edition and print the five levels and their descriptions as Dynamic Standards International states them. The Bronze controls come from the Level 1 certification requirements workbook CyberCert publishes; the Gold count comes from the certificate issued to us, which carries it. The full control text of the standard is a licensed document, so the control counts at Silver, Platinum and Diamond are not printed; the description of each of those levels is the publisher's own, and the controls each adds are as the issuer's published tier descriptions state them.

The verification rules come from CyberCert's certification practice statement, version 1.1 of 10 July 2026, and its site copy: who attests at which level, when an audit is required, and how long a certificate runs. Every SMB1001 certificate is valid for 12 months and names the edition of the standard it was issued against.

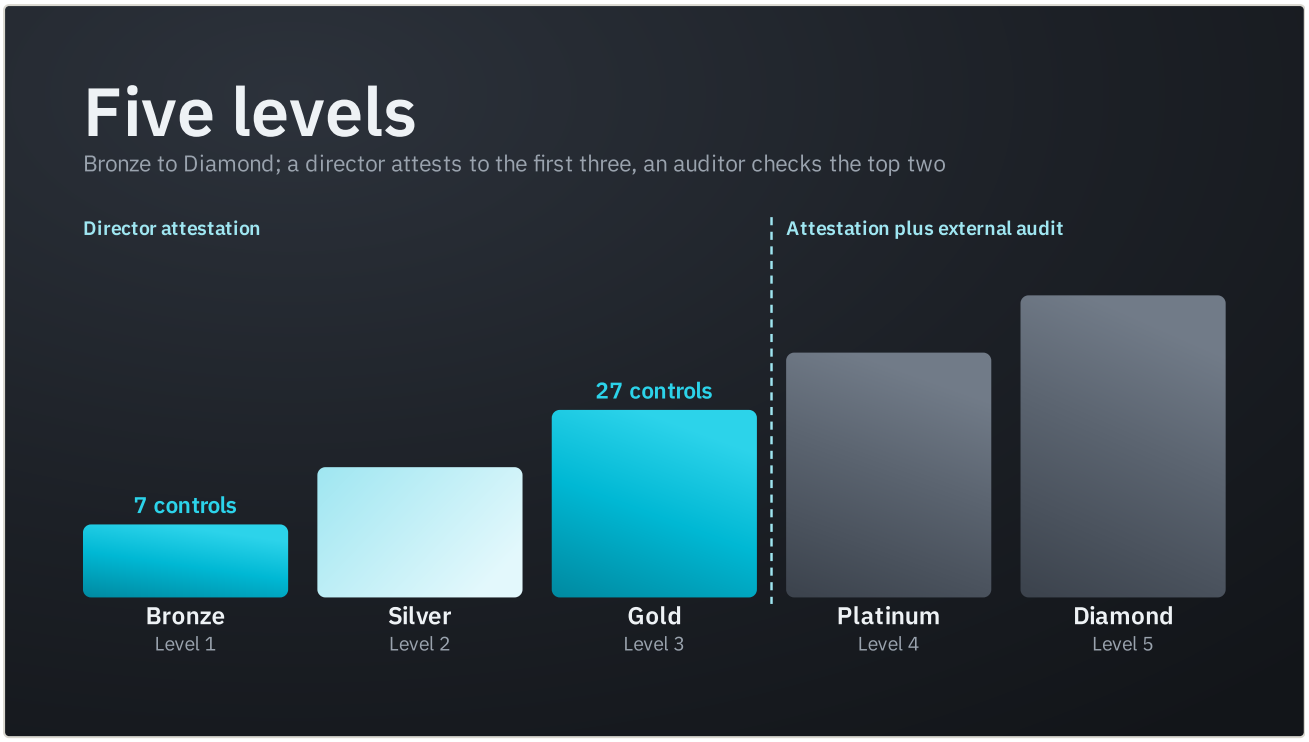
To use the levels in your own business, start from the end. Ask the three parties who can refuse you work what they expect: a contract clause, an insurance proposal form and a tender questionnaire each name a level or describe one without naming it. The highest of those is the target.

Then read each control at the target back from the system that enforces it. A firewall is proved by its configuration export; automatic patching by the update policy and the last patch date on each device; a backup strategy by the schedule, the location of the copy and the date of the last restore test. A control with no artefact behind it cannot be attested.

Where a control is missing, the gap is usually a decision and a few hours of work. Where the control is a process, such as awareness training or an incident response plan, the gap is a calendar entry and an attendance list.

The five levels, in the publisher's words

THE FIVE LEVELS OF SMB1001:2026



Bronze asks for 7 controls and Gold carries 27 in total; a director attests at the first three levels and an external audit joins at the fourth. Source: Dynamic Standards International, SMB1001:2026, released 1 September 2025; CyberCert Bronze workbook, Certification Practice Statement, version 1.1 of 10 July 2026, and the firm's Gold certificate.

SMB1001:2026 has five levels, Bronze, Silver, Gold, Platinum and Diamond, numbered Levels 1 to 5, and each level carries every control of the levels below it. The publisher describes Level 1 as basic preventive controls, such as firewalls and antivirus software, that stop threats before they can harm a system.

Level 2 introduces more advanced preventive measures, adding layers of protection against more sophisticated threats. Level 3 expands to a holistic risk management approach, where risks related to people, processes and technology are identified, assessed and addressed in a coordinated manner. The top two levels the publisher describes as elite risk governance, each tier reinforcing the business's reputation as a secure, reliable partner.

Three things follow from the design. The levels are cumulative, so a Gold certificate carries Bronze and Silver inside it, and a buyer reading a certificate reads everything beneath the level named. The first three levels are attested by the business itself, so their worth rests on the evidence the director had in hand when signing. The top two add an auditor, so a certificate at those levels rests on a finding by someone outside the business.

The standard numbers its controls under five areas: technology management, access management, backup and recovery, policies, plans and procedures, and education and training. The numbering runs through every level, so a control keeps its number as the levels climb and a firm can map what it already has against the standard before buying anything.

Bronze: seven controls

Bronze, Level 1, asks for 7 controls: a technical support specialist, a firewall, antivirus on every device, automatic patching, strong password hygiene, a backup and recovery strategy, and cyber security awareness training for all employees.

AREA	CONTROL
Technology management	Engage a technical support specialist for your organisation.
Technology management	Install and configure a firewall.
Technology management	Install anti-virus software on all organisation devices.
Technology management	Automatically install tested and approved software updates and patches on all organisation devices.
Access management	Ensure strong password hygiene is maintained.
Backup and recovery	Implement a backup and recovery strategy for important digital assets.
Education and training	Conduct cyber security awareness training for all employees.

The Bronze controls as the CyberCert workbook words them, by the area of the standard each sits in.

Each one answers a route attackers use against the smallest businesses. The technical support specialist is the person who will be called when something breaks, named before it breaks. The firewall and antivirus close the two doors malware walks through first. Automatic patching removes the window between a vendor's fix and the exploit that follows it. Password hygiene stops a password reused from a breached site opening the business email. The backup strategy is what the business restores from after ransomware. The training reaches the people who receive the messages an intrusion begins with.

The issuer puts Bronze at a business with low cyber risk exposure. In practice that is a firm with few staff, no servers and standard business applications in the cloud. A firm that holds client files, takes payments or moves money on emailed instructions sits above it, whatever its size.

Silver and Gold: from protection to governance

Silver, the second level, adds stronger identity protection, tighter access control, server patching and protection against invoice fraud, the controls that matter once a business runs on email and shared applications. The issuer describes it as the level at which a business becomes insurable.

Gold, Level 3, carries 27 controls in total, the count printed on our own SMB1001:2026 Gold certificate. At Gold the standard reaches governance: written cyber security policies, an incident response plan, a responsible AI use policy, endpoint detection and response, authenticated email, and an insurance policy in place. The business is asked to show that someone owns security, that there is a plan for the day it fails, and that its outbound mail cannot be forged in its name.

Gold is the level most buyers read as evidence. A tender questionnaire, a supplier security review and an insurance renewal each ask for the artefacts Gold produces: the policies, the incident plan, proof of detection on endpoints and

the email authentication settings. A firm that holds Gold answers those with a certificate and a short evidence pack. A firm at Bronze answers each one from scratch.

The step from Silver to Gold is where most of the work of certification sits, because the controls stop being installable and start being organisational. A policy has to be written and adopted, an incident plan rehearsed, a detection product deployed and watched, and the insurance bought. For a small firm that is the owner's attention over several weeks, and the sequence matters: detection before the policy that refers to it, email authentication before the insurer asks.

Where attestation ends and audit begins

At Levels 1 to 3 a director, owner or authorised senior executive attests that every control at the level is implemented, and the certificate issues on that attestation. At Levels 4 and 5 an external audit joins the attestation, and CyberCert cannot issue a Level 4 or Level 5 certificate until the audit succeeds.

LEVEL	TIER	HOW IT IS VERIFIED
Level 1	Bronze	Director attestation
Level 2	Silver	Director attestation
Level 3	Gold	Director attestation
Level 4	Platinum	Attestation plus external audit
Level 5	Diamond	Attestation plus external audit

Who verifies each level, from the issuer's certification practice statement, version 1.1 of 10 July 2026.

An attestation is a signature by the person who carries the consequences. It is quick, and it holds only when the evidence for each control is in hand before the signature, so the evidence pack is what a Bronze to Gold program produces.

Platinum and Diamond add the auditor. The issuer's practice statement separates the roles: the auditor examines and cannot issue a certificate, and the issuer cannot issue a Level 4 or Level 5 certificate until the audit succeeds. Platinum adds vulnerability scanning and testing, stronger multi-factor authentication and independent verification of the controls. Diamond adds supplier trust programs, police vetting, live testing of incident response and application control. The audit is a cost in fees and in fieldwork days, and it is the reason the top two levels belong to the firm whose customers are regulated or are government.

Every SMB1001 certificate is valid for 12 months and names the edition of the standard it was issued against. A certificate against an earlier edition tells a buyer when the attestation was made and that the controls were read against an older list.

What to do

The order below is the one we run for a firm aiming at Gold. A firm aiming at Bronze stops after the fourth step.

1. Ask your largest customers, your insurer and your contracts which level they name, and set the target at the highest of them.
2. Write the control list for the target level in a single sheet, one row per control, with the system that enforces it and the artefact that proves it.
3. Close the installable gaps first: the firewall, antivirus on every device, automatic patching, a password manager with multi-factor authentication, and a backup with an off-site copy and a tested restore.
4. Run the awareness training, keep the attendance list, and put the next session in the calendar.
5. Write the policies the target level asks for in plain words your staff will read, adopt them at a board or owner meeting, and date them.
6. Deploy endpoint detection and response and set up the email authentication settings before the policy that refers to them is signed.
7. Assemble the evidence pack against the control numbers, then subscribe through the issuer, attest, and put the renewal date in the calendar a year out.
8. For Platinum or Diamond, engage the auditor before the remediation starts, so the fieldwork is planned around your dates.

We hold SMB1001:2026 Gold, issued by CyberCert, and we run the same program for clients: a gap review against the target level, remediation sequenced to the date the certificate is needed, the policies the standard asks for, and an evidence pack built against the control numbers for the director’s attestation or the auditor’s fieldwork. A scoping call settles the level and the quote before any work starts.

Our record

Black Shard builds and defends the systems Australian organisations run on. The Gold certificate the figures above draw on is our own, and the controls behind it are the ones we run every day.

The record is as held at 16 November 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Approved supplier on the Tasmanian Government Technology Services List (TSL) for Application Development Services, Operational Technical Services and Cyber Security.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.

— More than 1,500 deploys and releases shipped since 27 April 2026.

> 24/7 incident line: 1800 370 270.

Sources

— Dynamic Standards International, SMB1001:2026 Cybersecurity Standard for SMBs, released 1 September 2025: https://dsi.org/smb1001

— CyberCert, SMB1001:2026 Level 1 Bronze Certification Requirements Workbook: https://www.cybercert.ai/

— CyberCert, SMB1001 Certification Practice Statement, version 1.1, 10 July 2026: https://www.cybercert.ai/SMB1001CPS.pdf

— CyberCert, SMB1001:2026 certification tiers, Bronze to Diamond, published tier descriptions: https://www.cybercert.ai/

— Black Shard Pty Ltd, SMB1001:2026 Gold certificate on the CyberCert registry: https://certification.cybercert.ai/issued/3b8d8245-6bdb-4cd2-b073-b727020cc058