Acronis

SG Cyber Safe Programme

What is it?

In Singapore, cybersecurity is quickly becoming a buying criterion, not just an IT line item. Customers and enterprise partners want confidence that your security is real, maintained and resilient when something goes wrong.

The SG Cyber Safe Programme, led by the Cyber Security Agency of Singapore (CSA), includes two certifications that help organisations demonstrate cybersecurity readiness aligned to their risk profile: Cyber Essentials Mark and Cyber Trust Mark.

Start with Cyber Essentials and build toward Cyber Trust

Cyber Essentials Mark is the starting point for many SMEs. It focuses on essential cyber hygiene across five areas: Assets, Secure / Protect, Update, Backup, Respond.

Cyber Trust Mark is designed for organisations with greater digital exposure and maturity. It is tiered and risk based, and best described as outcome focused and evidence backed. The emphasis is whether security practices are operating effectively in the real world, supported by evidence during assessment and audits.

CSA has also expanded its certification scope beyond traditional IT, including areas like cloud security, OT security, and AI security, reflecting how modern risk is changing.

What makes Cyber Trust Mark different

Cyber Trust Mark focuses on cyber resilience and operational preparedness. It validates that your organisation can protect itself, detect and respond to threats and recover reliably when incidents happen.

It can help you:

- Strengthen trust with your customers, partners and suppliers.
- Support your tender and procurement requirements.
- Improve your cyber resilience and reduce business disruption.
- Support your cyber insurance discussions and risk posture.

Cyber Trust Mark also scales with your business maturity. It uses a tiered preparedness model, so organisations can start with strong cyber hygiene and progress toward higher levels of resilience over time.

While the program is outcome focused, certification still requires evidence during assessment and audits. The emphasis is on whether security measures are operating effectively, not whether you have the most documentation.

Preparedness tiers

Cyber Trust Mark has five tiers. As you move up, the certification covers more of CSA's preparedness domains and expects a stronger, more consistent operating model behind them. The assessment starts at **10 domains (Supporter)** and scales up to **22 domains (Advocate)**. We will work with you to assess where you fit today, identify any gaps and build a practical plan to reach the tier you are aiming for.

Supporter	Practitioner	Promoter	Performer	Advocate
10 domains	**13** domains	**19** domains	**21** domains	**22** domains
Foundational cyber hygiene and basic controls.	Structured protection, detection and recovery.	Managed security with governance and risk ownership.	Advanced controls, resilience and assurance.	Adaptive, intelligence-led cyber resilience.

Funding support and certification cycle

CSA has worked with appointed certification bodies to offer funding support for Cyber Trust Mark certification.

"CSA's Cyber Trust Mark offers a three-year certification with annual audits, funding support up to S$3,600 and benefits including insurance discounts."

Click here or scan QR code for official details on process and funding

Acronis Cyber Protect Cloud mapped to Cyber Essentials Mark

Cyber Essentials Mark is built around five areas. Here's how we cover each one through one platform.

Assets

Acronis RMM gives us asset discovery, inventory, health monitoring and policy visibility across endpoints and key workloads, so nothing falls through the cracks.

Secure / Protect

Acronis Advanced Security plus EDR / XDR helps prevent and contain threats. For Microsoft 365 environments, Acronis Email Security and Collaboration Security add protection where most attacks start, and Security Awareness Training helps reduce user-driven risk.

Update

Acronis patch management keeps OS and third-party apps current, with centralized scheduling and reporting so patching stays consistent.

Backup

Acronis Backup for endpoints / servers plus Backup for Microsoft 365 (Exchange, OneDrive, SharePoint, Teams) supports recoverability after ransomware, deletion or disruption with fast, granular restores.

Respond

Acronis MDR and incident response workflows help triage and contain alerts faster, supported by EDR / XDR telemetry and reporting for evidence during assessment and audits.

Building cyber resilience for Cyber Trust Mark

Most SMEs don't struggle because they have no security tools. The bigger challenge is keeping security consistent over time, avoiding configuration drift, staying on top of patching, and being able to demonstrate what is actually in place.

We use Acronis Cyber Protect Cloud to operationalize Cyber Essentials and support your path to Cyber Trust Mark while keeping policies, patching, protection, backup, and reporting consistent in one natively integrated platform.

AI-assisted robust security

Advanced, AI-powered threat protection against ransomware and modern cyberattacks.

Resilience you can prove

We implement and validate backup and recovery processes so your business can recover quickly from ransomware, deletion or disruption.

Proactive management

Continuous monitoring, patch management and automation to prevent issues before they impact you.

Greater efficiency

One integrated platform that reduces complexity, lowers risk and improves response times.

With Acronis, we ensure you get consistent security controls, quicker support and stronger resilience across the systems your organization relies on, so you can grow with confidence.

Next steps

Cyber Trust Mark should feel practical and less paperwork heavy. We can run a quick readiness check to confirm your likely tier, highlight the key gaps and outline the simplest path to certification based on your environment and budget.

Acronis

Learn more at
acronis.com