SecurityScorecard

INSIGHT PAPER

Singapore's Cyber Trust Mark

Turning a National Mandate into a Certification-Ready Cybersecurity Program



How Singapore's tiered cybersecurity certification is reshaping vendor requirements and procurement decisions, and where SecurityScorecard supplies evidence across all 22 domains



Executive Summary

The Cyber Security Agency of Singapore (CSA) refreshed the Cyber Trust Mark (CTM) in April 2025 to cover cloud. In March 2026, CSA confirmed the mark will become mandatory for Critical Information Infrastructure Owners (CIIOs), Critical Information Infrastructure (CII) auditors, and licensed cybersecurity providers, with deadlines through 2027. For those organizations, it is now a compliance obligation with a countdown clock. For everyone else, it is the direction the market and procurement are heading.

This paper covers three things security and risk leaders need to know: what the framework requires tier by tier, who must certify and by when, and how a continuous, evidence-based platform like SecurityScorecard maps onto the 22 Cyber Trust domains. That mapping turns certification from a periodic scramble into an always-on state of readiness.

©2026 SecurityScorecard Inc. All rights reserved.

Why Cyber Trust, Why Now

A framework built for a more digital Singapore

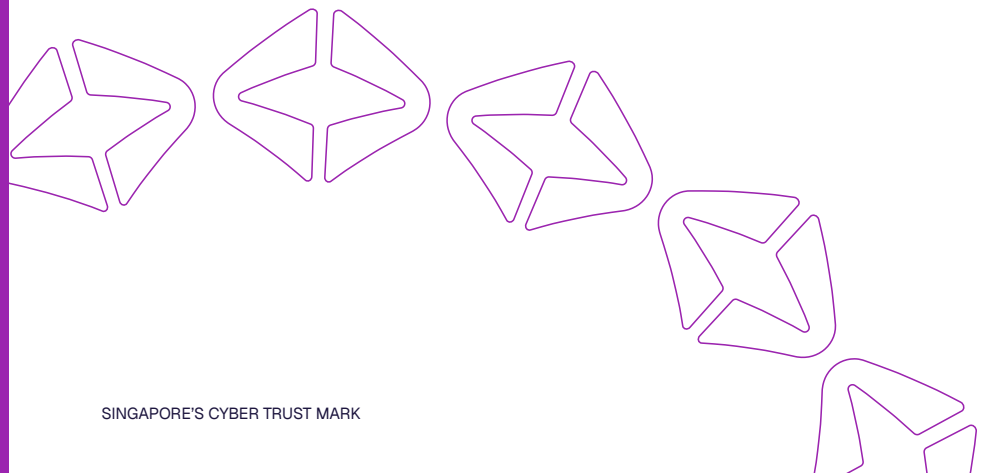
Cyber Trust is CSA's certification for organizations with more extensive, higher-risk digital operations. CSA refreshed it in April 2025 as "Cyber Trust (2025)" (Singapore Standard SS 712:2025) to explicitly cover three new pillars alongside classical IT: cloud, OT, and AI security. Each of the framework's 22 domains now carries pillar-specific guidance, so certification can be scoped to cloud and AI systems, not just traditional IT.

From voluntary mark to national mandate

On March 2, 2026, CSA announced fixed deadlines for three groups. CIIOs must reach CTM Tier 5 by December 31, 2027. CII auditors must reach Tier 5 by December 31, 2026. Licensed cybersecurity providers, such as penetration testers and managed Security Operations Center (SOC) providers, must reach Tier 3 by December 31, 2026. The mandate focuses on supply-chain risk. CIIOs must also oversee interconnected systems beyond their core CII, precisely the blind spot continuous, outside-in monitoring is built to close.

Why this matters beyond the mandatory list

On 14 Oct 2026, CSA said GovTech will require Cyber Essentials and/or Cyber Trust by the end of 2027 for government vendors that handle critical systems or sensitive data. Any vendor in a CIIO's ecosystem should expect Cyber Trust-aligned due diligence, mandate or not.



©2026 SecurityScorecard Inc. All rights reserved.

Five Tiers, Twenty-Two Domain

Organizations assess their own risk to see which of five tiers they fall into, from Supporter (the simplest) to Advocate (the most demanding). The five tiers are T1 Supporter, T2 Practitioner, T3 Promoter, T4 Performer, and T5 Advocate. The higher the tier, the more of the 22 domains apply, grouped into five areas: Governance and Oversight, Cyber Education, Information Asset Protection, Secure Access and Environment, and Cybersecurity Resilience.

Source: CSA, Cyber Trust (2025), Table 7:
https://isomer-user-content.by.gov.sg/36/2cff8d23-0f79-4477-9629-377d3bccbcaf/cyber-trust-v202504.pdf

Domain	T1	T2	T3	T4	T5
1. Governance			✓	✓	✓
2. Policies and procedures			✓	✓	✓
3. Risk management	✓	✓	✓	✓	✓
4. Cyber strategy					✓
5. Compliance	✓	✓	✓	✓	✓
6. Audit				✓	✓
7. Training and awareness*	✓	✓	✓	✓	✓
8. Asset management*	✓	✓	✓	✓	✓
9. Data protection and privacy*	✓	✓	✓	✓	✓
10. Backups*	✓	✓	✓	✓	✓
11. Bring Your Own Device (BYOD)			✓	✓	✓
12. System security*	✓	✓	✓	✓	✓
13. Anti-virus / anti-malware*	✓	✓	✓	✓	✓
14. Secure Software Development Lifecycle (SDLC)			✓	✓	✓
15. Access control*	✓	✓	✓	✓	✓
16. Cyber threat management				✓	✓
17. Third-party risk and oversight			✓	✓	✓
18. Vulnerability assessment			✓	✓	✓
19. Physical/environmental security		✓	✓	✓	✓
20. Network security		✓	✓	✓	✓
21. Incident response*	✓	✓	✓	✓	✓
22. Business continuity/disaster recovery		✓	✓	✓	✓

*These domains also appear in Cyber Essentials, CSA's baseline mark for organizations with simpler IT needs -organizations already certified under it have a head start.

©2026 SecurityScorecard Inc. All rights reserved.

Since April 2025, each applicable domain can extend across cloud, OT, and AI, not just classical IT. That is the biggest operational challenge in the refresh, since most organizations have far weaker continuous visibility into cloud, OT/Industrial Control Systems (ICS), and AI/Application Programming Interface (API) estates than into traditional IT. Driftnet, a high-fidelity internet discovery engine that maps exposed hosts, services, and misconfigurations across the global internet, now part of SecurityScorecard, recently identified more than 816,000 internet-exposed OpenClaw AI agent deployments, and the same outside-in discovery surfaces ICS services reachable from the internet. These are the cloud, OT, and AI exposures Cyber Trust now expects organizations to know about.

Organization type	Required tier	Deadline
Critical Information Infrastructure Owners (CIIOs) for non-CII systems supporting operations	Tier 5 (Advocate)	December 31, 2027
CII auditors, at the organization level	Tier 5 (Advocate)	December 31, 2026
Licensed cybersecurity service providers (pen testing, managed SOC)	Tier 3 (Promoter)	December 31, 2026
Government vendors handling critical systems or sensitive data (GovTech)	Cyber Essentials and/or Cyber Trust	December 31, 2026

Compliance doesn't stop with the organizations on CSA's mandatory list. Even companies outside the mandate may need to prove they meet Cyber Trust standards — for example, if they supply a CIIO, work with a licensed provider, or bid on a tender that requires it. That's because CIIOs must vet their entire vendor base, so suppliers should expect the same scrutiny, whether or not it's mandated. Vendors that can provide continuous, threat-informed evidence instead of a once-a-year questionnaire response will clear due diligence faster.

©2026 SecurityScorecard Inc. All rights reserved.

Mapping SecurityScorecard to the Cyber Trust Domains

The standard asks for about three months of operating evidence before the audit, then an annual audit across the three-year certification cycle; continuous, dated evidence makes both far easier to produce. The table below maps each Cyber Trust control group to the SecurityScorecard capability that most directly supports it.

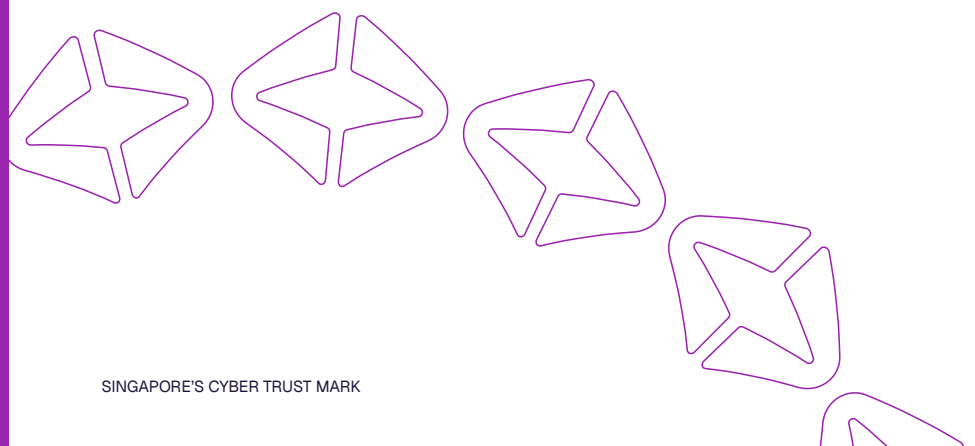
SecurityScorecard runs on TITAN AI, our threat-informed and predictive operating system for third-party risk management. The mapping turns certification from a periodic scramble into an always-on state of readiness. That shift — from a point-in-time snapshot to a constant, audit-ready record — is what TITAN AI is built to deliver.

Domain group	Tiers	How SecurityScorecard helps
Governance, policies & procedures, strategy, compliance, audit (1-2, 4-7)	1-2: T3-T5 / 4: T5 / 5, 7: T1-T5 / 6: T4-T5	**Governance evidence:** Board-ready Reporting, A-F Security Ratings with ten factor scores, and peer Benchmarks give governance, audit, and compliance teams a continuous, independent evidence trail. **Policy monitoring:** Continuous Monitoring and Alerts flag externally visible deviations (weak TLS, missing SPF/DMARC, unpatched CVEs) and material score changes. **Third-party attestations:** Questionnaires collect and validate attestations (e.g. ISO 27001 alignment, licensed CSP status). This outside-in data supplements, not replaces, internal governance and audit processes. **Training and awareness:** This is an internal HR/LMS record that external ratings can't observe directly. Hacker Chatter and Leaked Credentials act as indirect proxies, since rising credential exposure often signals an awareness gap, while Questionnaires can capture completion-rate attestations.
Risk management (3)	3: T1-T5	Digital Footprint and Automatic Vendor Detection continuously discover the organization's externally reachable assets, cloud services, and third/fourth-party dependencies. Security Ratings, Issues/Findings, and Benchmark turn that exposure into a severity-weighted, trend-tracked risk register that refreshes daily rather than annually or monthly. Alerts flag new or worsening findings, and a recommendations/resolution workflow supports treatment and closure evidence.
Asset management, data protection, backups, BYOD, system security, anti-malware, SDLC (8-14)	8-10, 12-13: T1-T5 / 11, 14: T3-T	Digital Footprint continuously discovers internet-facing hardware, software, and cloud assets, including shadow IT. Issues/Findings across the Network Security, Application Security, Patching Cadence, and Hacker Chatter factors evidence device/app hygiene, patch currency, and leaked-credential exposure, while Vulnerability Intelligence correlates CVEs against the discovered footprint. Where a function sits with a CSP or vendor — data deletion, backup redundancy, BYOD device posture — Questionnaires collect and analyze the provider's attestations.

©2026 SecurityScorecard Inc. All rights reserved.

Domain group	Tiers	How SecurityScorecard helps
Access control, threat management, third-party risk, vulnerability assessment (15-18)	15: T1-T5 / 16: T4-T5 / 17-18: T3-T	This is SecurityScorecard's core strength: Automatic Vendor Detection surfaces third and fourth parties, Portfolio holds every vendor under continuous reassessment, and Security Ratings plus Alerts flag meaningful score changes. Together, they turn third-party oversight into an ongoing program rather than a point-in-time review. **Third-party risk (17) by tier**. T3 Vendor SLAs: Questionnaires collect SLA and security attestations, and Portfolio holds the vendor inventory. T4 Checks before onboarding: Security Ratings and Questionnaires support pre-onboarding due diligence. T5 Assessing vendors' own third parties regularly: Automatic Vendor Detection surfaces fourth parties, and Portfolio with Alerts supports continuous reassessment. **Vulnerability assessment and threat management.** Issues/Findings (Network/Application Security, Patching Cadence) support vulnerability assessment (18) with continuously refreshed, externally observed findings. For threat management (16), SecurityScorecard's recently acquired Driftnet engine (Internet Intelligence) supports threat hunting (B.16.11), and Board-ready Reporting supports board dashboards (B.16.10). Internal log management, SIEM, and behavior analytics remain internal controls.
Physical/ environmental and network security (19-20)	19-20: T2-T5	Network Security findings cover exposed or openly accessible internet-facing services, providing independent evidence that network access controls hold at the boundary. Physical/environmental security sits outside the natural scope of external ratings. Where a CSP or data center operator delivers it, Questionnaires collect and validate the provider's physical security attestations (e.g., ISO 27001, SOC 2).
Incident response, business continuity/ disaster recovery (21-22)	21: T1-T5 / 22: T2-T5	Incidents surface confirmed breach events, active malware/botnet infections (via sinkhole and honeypot sensors), and ransomware-victim domains directly on the scorecard, with Alerts accelerating awareness, giving the incident response team an outside-in detection feed. For business continuity, Questionnaires collect and validate third-party redundancy arrangements, such as Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Service Level Agreement (SLA) commitments and ISO 22301 alignment. Security Ratings and Continuous Monitoring then provide an ongoing, dated record of vendor and infrastructure dependency posture.

SecurityScorecard is an external, continuous-monitoring platform. It strongly accelerates the domains above, but complements internal controls like physical security, training curricula, and backup configuration, which auditors will still verify directly.



©2026 SecurityScorecard Inc. All rights reserved.

A Tiered Path to Readiness

T1-T2

SUPPORTER/PRACTITIONER

The baseline: risk management, compliance, training, asset and data protection, backups, system security, anti-malware, access control, and incident response (T1), with physical security, network security, and BC/DR added at T2. Start with an external baseline rating to find exposure you didn't know about, especially across cloud, OT, and AI.

T3

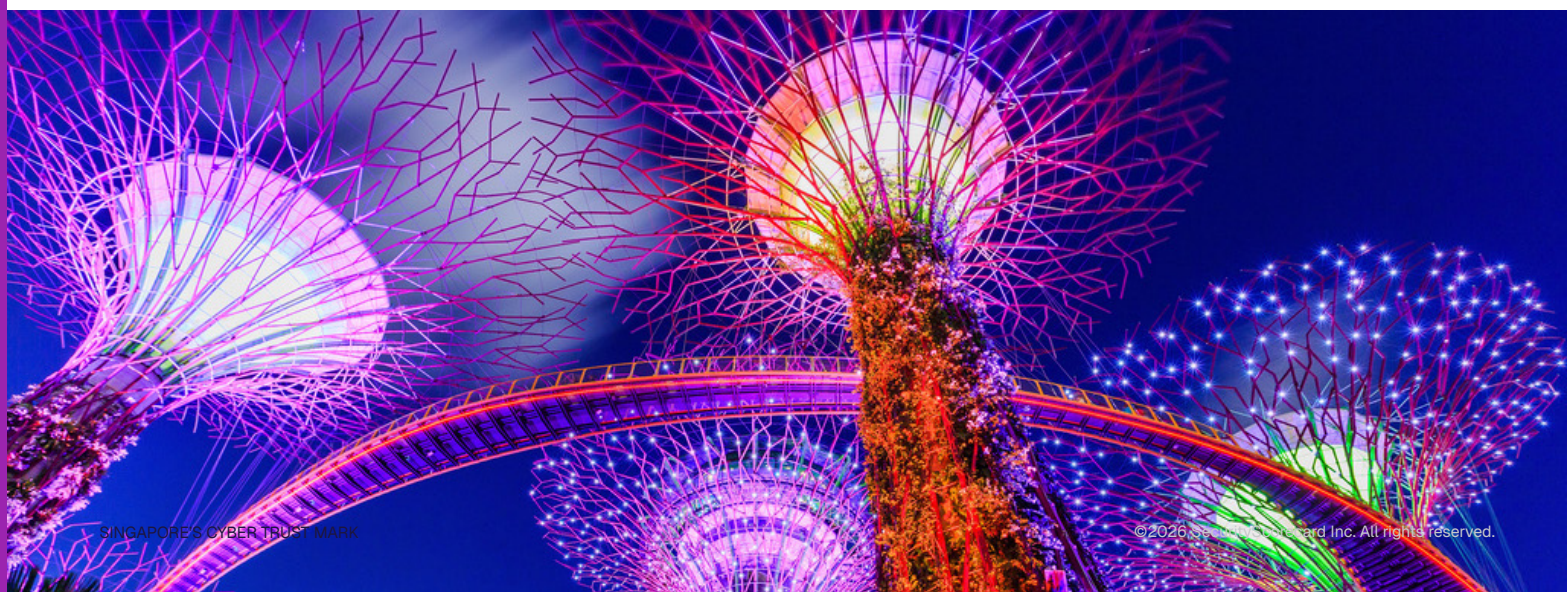
PROMOTER

The floor for licensed cybersecurity providers. This is where governance, policies, secure development, third-party risk, and vulnerability assessment enter the framework; vendor risk management is no longer optional here.

T4-T5

PERFORMER/ADVOCATE

T4 adds audit and cyber threat management. T5, the CIIO and CII auditor bar, adds cyber strategy, so every domain applies. With deadlines at the end of 2026 and the end of 2027, standing up continuous evidence generation now avoids a scramble.



©2026 Schellman Compliance, LLC. All rights reserved.

Why SecurityScorecard

- Continuous visibility across more than 12 million continuously rated companies, enough scale to evidence both your own posture and your extended supply chain.
- Purpose-built third-party risk management, including automatic vendor/fourth-party detection, addressing CSA's interconnected-systems requirement head-on.
- We own our own data rather than relying on third-party feeds, with a real-time trust page showing dispute and correction outcomes: accuracy you can audit, not just take on faith.

Next Steps

1. Whether you're on CSA's mandatory list, a supplier to a CIIO, or positioning ahead of the market, the first move is the same. Get an independent read on your external cyber hygiene, then run it against CSA's domain self-assessment to see where the real gaps sit, before a formal assessor does.
2. Run a free baseline security rating to surface existing exposure as a starting input.
3. Work through CSA's domain self-assessment for your target tier, using your asset and vendor inventory to inform the relevant domains, such as asset management, third-party risk, and access control.
4. Build a roadmap to Tier 3, 4, or 5 readiness aligned to your CSA deadline, if one applies, closing the gaps the self-assessment identifies.

Talk to a SecurityScorecard specialist about how SecurityScorecard can support your Cyber Trust readiness.



Protect the supply chain behind your business. Learn more at securityscorecard.com or connect with us on LinkedIn.

©2026 SecurityScorecard Inc. All rights reserved.

About SecurityScorecard

SecurityScorecard is transforming how organizations defend against the fastest growing threat vector – supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while our AI-powered (or threat-informed) TPRM solutions continuously monitor third-party risks using our factor-based ratings, automated assessments and proprietary threat intelligence, to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity to safeguard business continuity. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

©2026 SecurityScorecard Inc. All rights reserved.