Singtel Business

Product Brochure
Cyber Security Readiness Assessment

Enhance Your Cyber Risk Awareness and Readiness.

Much focus is on "knowing one's enemy" in today's fast-evolving threat landscape. However, to build an effective defence, it is equally critical to know one's current security posture. Singtel Cyber Security Readiness Assessment service provides a view of your readiness in detecting and responding to attacks. Benchmarked against an established outside-in security posture rating and industry standards, we provide a point-in-time validation of your cyber readiness and propose a remediation roadmap to fortify your cyber defence.

Singtel

Cyber Security Readiness Assessment

Cyber Readiness: Being Ready for What's Next

Enterprises today constantly juggle between increasing legislative calls for better security protection, while balancing business costs and performance. Facing ever-mutating threats, there is an urgency to elevate one's risk awareness and preparedness to successfully tackle threats head-on.

One way to better align security management to business performance is to conduct a point-in-time validation of your security posture. This includes reviewing how well your existing security architecture, designs and processes have been implemented; how well they are operating; and how effective they have been in addressing incidents.

A health check should be proactive and this involves 3 steps:

- **Conduct cyber security readiness assessment**
- **Identify security gaps**
- **Establish security roadmap to prioritise remediation action and enhance cyber security readiness**

Do you know your cyber security readiness?

Check against these 4 levels:

Level 0: None	Security practices are not performed.
Level 1: Reactive	Existing security practices are ad-hoc or reactive.
Level 2: Repeatable	Existing security practices are established, performed and managed as part of day-to-day business operations.
Level 3: Adaptive	Existing security practices are periodically reviewed and continually evolved to cope with emerging vulnerabilities and new legal/regulatory requirements.

Singtel Cyber Security Readiness Assessment (CSRA) Service

Many enterprises lack a holistic understanding of their cyber risks and therefore, an effective strategy to address these risks. Singtel Cyber Security Readiness Assessment (CSRA) will help you establish an effective review of your preparedness against industry-recognised standards. Backed by proven security expertise and industry benchmarking data, this service helps assess your readiness in detecting and responding to incidents.

An inside-out and outside-in approach is undertaken to achieve these objectives:

- **Perform an inside-out assessment to check how one's current cyber security readiness fares against the desired state**
- **Provide an outside-in security posture rating and industry benchmark against industry players**
- **Assess if IT resources are deployed or invested optimally to best manage cyber risks**
- **Establish a roadmap of recommended remediation over proposed timeframe in journey towards desired state**

How It Works

Scope of Assessment

Backed by our cyber security framework, Singtel CSRA's comprehensive scope of assessment helps to:

- Identify crown jewels like sensitive information or core systems/applications, which would have detrimental impact on the organisation when they are breached.
- Assess how adequately they are protected.
- Detect cyber security threats/vulnerabilities through security monitoring and assess availability of access to threat intelligence.
- Check effectiveness in responding to and recovering from incidents.

Focus: 7 Key Domains

Domain	Areas examined during assessment
Asset management	• Examine if an asset inventory is maintained and kept current (e.g., physical devices, systems, software platforms and applications). • Assess if the asset inventory is classified (e.g., by criticality, business impact/value etc.) to determine the required security controls to protect them.
Security compliance and vulnerability management	• Investigate if proper security hygiene is adhered to (e.g., by having security policy in place and ensuring that employees/third party vendors comply to them). • Conduct risks and vulnerability assessment to identify potential/known vulnerabilities and prevent opportunistic attacks.
Data protection	• Establish sensitive data footprint and their security classification. • Determine if necessary data protection controls (e.g., endpoint security and encryption) to prevent data leakage, infringement of PDPA (Personal Data Protection Act) and more have been established.
Security monitoring	• Review if security is continuously monitored via an effective detection mechanism to identify threats when they occur. • Examine if security alerts are being monitored and responded to promptly.
Threat management	• Appraise if there is real-time access to global threat intelligence (e.g., adversaries, IP reputation, security trends) that enables proactive management of emerging threats before they strike.
Security incident response	• Review if response/recovery plans and/or procedures are in place. • Check if such response plans have been tested for effectiveness, to ensure effective response to a security breach and minimise potential damages.
Security awareness	• Appraise if your staff are aware of the potential cyber threats such as social engineering, email phishing, etc. and whether they know how to handle them.

Assessment Process: 3-Step Approach

The target cyber security readiness profile is established based on 2 factors:

- One's risk tolerance through risk components such as data leakage, system downtime, legal/regulatory compliance and reputation impaired/loss
- An established outside-in security posture rating which rates your organisation based on externally observable data such as botnet, spam, malicious code, security configurations (e.g., SSL, SPF, DKIM, DNSSEC), DDoS, user behaviors, news feeds and social media. The security posture rating is then benchmarked against ratings from relevant industry players.

- Workshops or interviews are conducted with your stakeholders to understand current cyber security practices pertaining to the 7 key domains (refer to table above).
- Determine current cyber security readiness based on findings from these sessions.

- Assess cyber security readiness obtained in step 2 against the target cyber security readiness profile established in step 1 using a Singtel Cyber Security Readiness map.
- Identify any gaps, complete with assessment observations.
- Propose a roadmap recommending potential short-, mid- to long-term remediation actions to close the identified gaps.

Service Offerings

An effective CSRA cannot be a one-size-fits-all service and we will work with you to tailor one to your needs.

Singtel CSRA service is available as 2 offerings:

Standard	Advanced
Covers approximately 40 security practices/controls*	**Covers approximately 100 security practices/controls**
Deliverables:	
• Observations on identified security gaps • Cyber Security Readiness maps current cyber security readiness against target cyber security readiness profile • Outside-in security posture rating/benchmarking • Proposed roadmap with recommended remediation actions	
Optional add-ons:	
• Review: Network architecture security design review • Test: Application or network vulnerability assessment and penetration tests • Compromise assessment • Investigation: Incident response and forensics investigation • Training: Security awareness training	

* Security controls refer to safeguards or counter-measures to identify, protect, detect, response and recover from security risks or minimise risks to your IT assets.

Benefits

Identify critical assets and understand current cyber security readiness

Gain proactive insight into potential security gaps that can lead to security risks/ vulnerabilities

Discover ways to effectively respond to security incidents when they occur

Optimise IT resources by better aligning cyber security initiatives to business requirements, based on resource availability and organisation's risk tolerance

Empower better prioritisation of IT investments on activities that have greater impact in managing cyber security risks

Establish a roadmap with remediation actions to close identified security gaps

Why Singtel

A team of security-cleared and experienced professionals with over 30 years of deep domain knowledge and professional certification in CISSP, SABSA, CISM, CISA, GCIA, GCIH, GCFA, CEH, ECSA, CHFI, Mile2, HP ArcSight, Tipping Point, McAfee, Trustwave and more.

9 audit-ready Security Operations Centre (SOCs) –- 4 in North America, 4 in Asia Pacific and 1 in Europe, and together with Spiderlabs' global leading intelligence research team, we provide expert security and penetration testing services, incident readiness and data breach forensic investigations, innovative security research and major threat discoveries, and more.

End-to-end security capabilities as a solution provider in deploying enterprise-wide, mission-critical systems; trusted security advisors to help our customers identify, track, monitor and respond to security vulnerabilities; and independent security reviewer to determine compliance gaps and propose remediation measures.

About Singtel

Singtel is Asia's leading communications group providing a portfolio of services including voice and data solutions over fixed, wireless and Internet platforms as well as infocomm technology and pay TV. The Group has presence in Asia, Australia and Africa with over 610 million mobile customers in 24 countries, including Bangladesh, India, Indonesia, the Philippines and Thailand. It also has a vast network of offices throughout Asia Pacific, Europe and the United States.

Awards

Frost & Sullivan Singapore Excellence Awards 2016
Managed Security Service Provider of the Year

Frost & Sullivan's Asia Pacific ICT Awards 2016
Telco Cloud Service Provider of the Year

NetworkWorld Asia Info Mgmt Awards
Security-as-a-Service (2012 - 2016)

NetworkWorld Asia Readers' Choice Awards
Managed Infrastructure Services (2012 - 2015)
Managed Security Services (2014 - 2015)

NetworkWorld Asia Info Mgmt Awards
Disaster Recovery & Business Continuity (2014 - 2016)

Telco Cloud Forum Awards 2016
Telco Cloud of the Year

October 2016