Annex A-ICT
(normative)

Cyber Essentials mark for Infocomm Technology (ICT) vendor – Requirements

A-ICT.1 Introduction

The Infocomm Media Development Authority (IMDA) leads Singapore's digitalisation journey by developing a vibrant digital economy and an inclusive digital society. The Personal Data Protection Commission (PDPC) serves as Singapore's main authority in matters relating to personal data protection. With digital transformation, cybersecurity has become a critical area for all organisations – in an inter-connected digital environment, organisations need to protect their own assets and environment, as well as to ensure the security of their vendors and business partners.

To this end, CSA, IMDA and PDPC have worked on an extension of the Cyber Essentials mark that is targeted at ICT vendors, and this is intended for ICT vendors that are SMEs. This extension of Cyber Essentials mark is referred to as "Cyber Essentials for ICT Vendors".

The document describes the ICT cybersecurity requirements for ICT vendors for Software-as-a-Service (SaaS) and non-SaaS[1] implementations.

A-ICT.2 Additional terms and definitions

There are no additional terms and definitions in this annex.

A-ICT.3 Cyber Essentials mark for ICT vendor

A-ICT.3.1 Boundary of scope and statement of scope

The scope of assessment and certification shall cover at least the following:

- For SaaS solution: The production and development environment of the ICT Vendor for the service; and
- For non-SaaS solution: The production environment used by the ICT Vendor for hosting the service and/or the development environment of the ICT Vendor for the service.

The statement of scope shall minimally include classical cybersecurity.

The requirements for Cyber Essentials mark shall apply to all devices, systems[2] and software that are within this boundary of scope.

A-ICT.3.2 Pre-certification preparation by the ICT vendor

Prior to engaging a certification body, the ICT vendor shall complete the guided self-assessment template required for Cyber Essentials mark certification for ICT vendors.

[1] Applicable only to ICT vendors that store and process customer's business-critical data.
[2] For ICT vendor that adopts cloud-based software, the scope of assessment and certification shall include such cloud-based services.

This consists of a list of requirements and recommendations that the ICT vendor shall assess and indicate if these have been implemented in the organisation.

A-ICT.3.3 Independent assessment by certification body

Following the completion of its self-assessment, the ICT vendor shall approach any of the certification bodies appointed by CSA for independent assessment and issuance of the Cyber Essentials mark certification for ICT vendor.

For the organisation to be certified for Cyber Essentials mark for ICT vendor, the organisation shall meet all the requirements for full scope of assessment and certification.

A-ICT.3.4 Provisions for Cyber Essentials for ICT vendor

Following shows the provisions for Cyber Essentials mark for ICT vendor.

Clause	Provisions in Cyber Essentials	Additional provisions for ICT vendor
A.1 Assets: People – Equip employees with know-how to be the first line of defence		
A.1.4 (a)	Requirement	Requirement
A.1.4 (b)	Requirement	Requirement
A.1.4 (c)	Recommendation	Recommendation
A.1.4 (d)	Recommendation	Recommendation
A.1.4 (e)	Recommendation	Recommendation
A.2 Assets: Hardware and software – Know what hardware and software the organisation has and protect them		
A.2.4 (a)	Requirement	Requirement NOTE: – The asset inventory shall include 3rd party software and tools deployed; – ICT vendor shall include what is hosted on the cloud instances, e.g., software and Operating System (OS). – The asset inventory shall track expiry of all digital assets, such as certificates, software licenses, software renewal, etc; and – The asset inventory shall be reviewed at least once a year.
A.2.4 (b)	Recommendation	Recommendation
A.2.4 (c)	Recommendation	Recommendation
A.2.4 (d)	Recommendation	Recommendation
A.2.4 (e)	Recommendation	Recommendation
A.2.4 (f)	Requirement	Requirement
A.2.4 (g)	Requirement	Requirement NOTE: – The ICT vendor shall identify and implement mitigating stop-gap measures.
A.2.4 (h)	Requirement	Requirement
A.2.4 (i)	Requirement	Requirement
A.2.4 (j)	Requirement	Requirement
A.2.4 (k)	Requirement	Requirement
A.2.4 (l)	Recommendation	Recommendation

Clause	Provisions in Cyber Essentials	Additional provisions for ICT vendor
A.3 Assets: Data – Know what data the organisation has, where they are and secure the data		
A.3.4 (a)	Requirement	Requirement
A.3.4 (b)	Recommendation	Recommendation
A.3.4 (c)	Requirement	Requirement NOTE: – The ICT vendor shall encrypt business-critical data at rest, e.g. full disk encryption, encryption of databases containing personal data; and – The ICT vendor shall encrypt business-critical data in-motion using industry accepted protocols, e.g. Transport Layer Security (TLS), Secure Shell (SSH), when transmitted over the network, during backup or migration.
A.3.4 (d)	Requirement	Requirement
A.3.4 (e)	Requirement	Requirement
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware		
A.4.4 (a)	Requirement	Requirement
A.4.4 (b)	Requirement	Requirement NOTE: – Virus and malware protection solutions shall detect anomalous malware behaviour in real-time and provide constant protection.
A.4.4 (c)	Requirement	Requirement
A.4.4 (d)	Recommendation	Recommendation
A.4.4 (e)	Requirement	Requirement NOTE: – The ICT vendor shall implement a Web Application Firewall (WAF) to mitigate threats, e.g., Open Web Application Security Project (OWASP) Top 10, from external sources. – The ICT vendor shall segment networks by isolating critical systems, such as databases, are in network segments away from public-facing web services network segments.
A.4.4 (f)	Recommendation	Requirement NOTE: – This is a requirement for the ICT vendor, i.e. firewall configurations and rules shall be reviewed and verified annually to protect the organisation's Internet-facing assets.
A.4.4 (g)	Recommendation	Recommendation
A.4.4 (h)	Requirement	Requirement
A.4.4 (i)	Requirement	Requirement
A.4.4 (j)	Requirement	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for ICT vendor
A.5 Secure/Protect: Access control – Control access to the organisation's data and services		
A.5.4 (a)	Requirement	Requirement
A.5.4 (b)	Requirement	Requirement
A.5.4 (c)	Requirement	Requirement
A.5.4 (d)	Requirement	Requirement NOTE: – The ICT vendor shall apply the principle of least privilege to all accounts, e.g., users, services, to ensure excessive privileges are not granted.
A.5.4 (e)	Requirement	Requirement
A.5.4 (f)	Requirement	Requirement
A.5.4 (g)	Requirement	Requirement
A.5.4 (h)	Requirement	Requirement
A.5.4 (i)	Recommendation	Recommendation
A.5.4 (j)	Requirement	Requirement
A.5.4 (k)	Recommendation	Recommendation
A.5.4 (l)	Requirement	Requirement
A.5.4 (m)	Requirement	Requirement
A.5.4 (n)	Requirement	Requirement
A.5.4 (o)	Requirement	Requirement
A.5.4 (p)	Recommendation	Recommendation
A.6 Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software		
A.6.4 (a)	Requirement	Requirement NOTE: – For web applications, security configuration shall address the top 10 web application security concerns in OWASP. – The ICT vendor shall have vulnerability management processes to identify and manage vulnerabilities in the ICT solution, as well as production and development environment. – The ICT vendor shall perform security testing (such as vulnerability assessment and/or penetration testing) on the ICT solution and production environment before commissioning, periodically and upon major changes. – The ICT vendor shall remediate identified vulnerabilities that have a risk rating of "High". The risk rating should be based on industry best practices as well as consideration of potential impact, e.g. the criteria for the rating may include consideration of the CVSS base score, and/or the classification by the vendor, and/or impact to application functionality.
A.6.4 (b)	Requirement	Requirement
A.6.4 (c)	Requirement	Requirement
A.6.4 (d)	Requirement	Requirement
A.6.4 (e)	Recommendation	Recommendation
A.6.4 (f)	Requirement	Requirement

Clause	Provisions in Cyber Essentials	Additional provisions for ICT vendor
A.6.4 (g)	Requirement	Requirement NOTE: – The ICT vendor's solution shall provide "out-of-the-box" default installation that log all user access and be able to link all activities to individual users. – The ICT vendor's solution shall store logs at secured locations to protect the integrity and ensure availability of the logs. It should have the capability to store logs in 3rd party solutions. – The ICT vendor shall store logs at secured locations to protect the integrity and ensure availability of the logs. – The ICT vendor shall ensure that a log review process is defined, documented and implemented to detect suspicious activities and early indicators of security breaches. – The ICT vendor shall ensure that security logs are generated and monitored timely to detect suspicious or malicious activity, e.g., unusual administrative activities during off peak hours, creation of unknown administrator accounts, escalating privileges for user accounts, lateral traversal across multiple segments and attempted download/upload by single system within a short period, disabling security controls such as disable audit log etc. – The ICT vendor shall ensure that security monitoring mechanisms are in place to monitor all security related events for timely detection of suspicious events or malicious activities.
A.6.4 (h)	Recommendation	Recommendation
A.6.4 (i)	Recommendation	Recommendation
A.6.4 (j)	Recommendation	Recommendation
A.7 Update: Software updates – Update software on devices and systems		
A.7.4 (a)	Requirement	Requirement NOTE: – The ICT vendor, who is supplying the ICT solution to customers, shall notify its customers of the availability of updates/patches, and deliver those updates/patches to its customers in a secure and prompt manner and, if possible, guide/assist its customers to ensure the updates/patches are implemented successfully.
A.7.4 (b)	Recommendation	Recommendation
A.7.4 (c)	Recommendation	Recommendation
A.7.4 (d)	Recommendation	Recommendation
A.8 Backup: Back up essential data – Back up the organisation's essential data and store them separately and securely		
A.8.4 (a)	Requirement	Requirement NOTE:

Clause	Provisions in Cyber Essentials	Additional provisions for ICT vendor
		– The ICT vendor shall establish backup strategies, e.g. scope and frequency for data backups is determined and implemented, etc. and aligned with its Recovery Point Objective (RPO). – The ICT vendor shall implement a version control system where developers can roll back to a previous version in the event of any show-stopping bug being discovered.
A.8.4 (b)	Requirement	Requirement
A.8.4 (c)	Recommendation	Recommendation
A.8.4 (d)	Recommendation	Recommendation
A.8.4 (e)	Recommendation	Recommendation
A.8.4 (f)	Requirement	Requirement NOTE: – The backup shall minimally include configuration, source code and data. The backup shall be encrypted with cryptographic algorithms and key lengths that follow the recommendations from industry standards, e.g. National Institute of Standards and Technology (NIST) or equivalent.
A.8.4 (g)	Requirement	Requirement
A.8.4 (h)	Recommendation	Recommendation
A.8.4 (i)	Recommendation	Requirement NOTE: – This is a requirement for ICT vendors, i.e. backups shall be tested at least bi-annually, or more frequently.
A.9 Respond: Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents		
A.9.4 (a)	Requirement	Requirement
A.9.4 (b)	Requirement	Requirement
A.9.4 (c)	Recommendation	Recommendation
A.9.4 (d)	Recommendation	Recommendation