ACCREDITATION SCHEME FOR
MANAGEMENT SYSTEMS CERTIFICATION BODIES

CT 14

SAC CRITERIA FOR CERTIFICATION BODIES (MULTI-TIERED CLOUD COMPUTING SECURITY)

CT 14, 02 March 2020
The SAC Accreditation Programme is managed by Enterprise Singapore

1 Introduction

1.1 This document specifies the supplementary SAC criteria for certification bodies on Multi-Tiered Cloud Computing Security (MTCS) certification to SS 584 *Specification for multi-tiered cloud computing security*, and is to be used with ISO/IEC 17021-1 and the applicable IAF Mandatory Documents.

2 Criteria for MTCS Auditors

2.1 A certification body shall appoint qualified auditors to conduct MTCS audits. Auditors shall meet the criteria as defined in Annex 1 of this document.

3 Duration of MTCS Audits

3.1 For initial audit, the audit duration (Stage 1 + Stage 2) shall be as indicated in Table 1. Duration for stage 1 audit is usually 1 man-day.

Table 1 – Initial Audit Duration

Effective Number of Personnel	Minimum Initial Audit Duration (Man-day)
1-10	5
11-25	6
26-45	7
46-65	8
66-85	9
86-175	10
176-275	11
276-425	12
426-625	13
626-875	14
876-1,175	15
1,176-1,550	16
1,551-2,025	17
2,026-3,450	18
3,451-4,350	19
4,351-5,450	20
5,451-6,800	21
6,801-10,700	22
>10,700	Follow progression above

Note 1: Please refer to Clause 9.3 of ISO/IEC 17021-1 for requirements for stage 1 and stage 2 audits.

Note 2: The numbers of employees in Table 1 should be seen as a continuum rather than a stepped change.

Note 3: The certification body's procedure may provide for audit duration for a number of employees exceeding 10700. Such audit duration should follow the progression in Table 1 in a consistent fashion.

3.2 Impact Level (as defined in table 4 of SS 584)

Impact Level	**Additional day needed (minimum)**
Level 1- Low impact	0 day added
Level 2- Moderate impact	1 day added
Level 3- High impact	2 days added

Note: The above is for IaaS (Infrastructure as a Service) or SaaS (Software as a Service) with IaaS together.

For certification of SaaS running on MTCS certified infrastructure, the audit man-days may be reduced up to 30%. The reduction is due to SaaS certification being done on a MTCS certified infrastructure.

3.3 Multi-sites Audit

The size of the sample shall be the square root of the number of remote sites i.e. y = square root of x where x is the number of sites, rounded up to the upper whole number. 'y' is the number of audit sites needed.

3.4 Other Factors to be considered for determination of audit duration

- No. of platforms or complexity of the cloud environment
- No. of data centres

3.5 For Organisations with ISO/IEC 27001 certification

If the existing organization has already been certified to ISO/IEC 27001, the Certification Body (CB) may reduce the minimum number of man-days as specified in table 1 by up to 50% provided the following conditions are met:

a. The certification scope of the ISO/IEC 27001 is similar to that of the SS 584

b. The computed man-day after the reduction is equal or more than 5 man-days

3.6 Surveillance audit duration = 1/3 of initial audit duration

3.7 Recertification audit duration = 2/3 of initial audit duration

4. Scope Statement

4.1 The scope statement shall include at least the following:

a) Level of MTCS to be certified
b) Name of Service provider (legal entity)
c) Business address (office/operation address)
d) Name of services being certified, if the Cloud Service Provider is offering different services or products
e) The service model or the role CSP. Infrastructure provider, application programming interface (API) or platform provider etc.
f) For MTCS level 2 and 3 certification - the data storage locations must be listed in appendix for information.

4.2 For example,

Level 2 of Multi-tier Cloud Security System (MTCS) of Company A located at <address> supporting the provision of ABC <service name> services using IaaS <service type> model

ABC's services comprise of:

a) Compute Services <At location One>
b) Storage Services <At location One and location Two>

Annex 1

Criteria for MTCS Auditors

The summary of the criteria for MTCS Auditors is tabulated below.

Criteria	MTCS Auditor	MTCS Lead Auditor
Ethics & attributes	Demonstrates personal attributes for effective and efficient performance of audits	
Qualifications and Experience	Degree in Information Technology/Computing 4 years full time working experience which includes minimum of 3 years full time professional work experience in Information Systems auditing, control or security work experience **or** Diploma in Information Technology/Computing 5 years full time working experience which includes minimum of 3 years full time professional work experience in Information Systems auditing, control or security work experience	
Auditor Training	Successfully completed and passed a • Certified Information Systems Auditor (*CISA) **or** • Recognized Auditor / Lead Auditor course for Information Security management systems **and** • For auditors with less than 2 years experience working in cloud industry providing cloud service, the auditor shall attend course on cloud knowledge with the following content: i. Fundamental of Cloud computing: ○ Definition of cloud computing ○ Components of cloud infrastructure ○ Cloud computing model and operation ii. Cloud Computing Security ○ Infrastructure security for cloud computing ○ Assessment of the infrastructure security for cloud computing ○ Security basics of different cloud service models ○ Security of Cloud computing deployment models ○ Data protection and security for cloud computing ○ Security of cloud applications and users	

	iii. Manage cloud computing security and risk ○ Risk and governance ○ Legal and compliance ○ Audit ○ Portability and interoperability ○ Incident response	
Audit Experience	Performed a minimum of 4 Information Security Management System (ISMS) audits as a **qualified ISMS auditor within a 2-year period with a minimum of 10 auditor days on site. The 2-year period should be within immediate past 5 years.	Performed a minimum of 4 Information Security Management System (ISMS) audits as a **qualified ISMS auditor within a 2-year period with a minimum of 10 auditor days on site; **and** Performed an additional minimum of 3 audits as a Lead Auditor within a 2-year period. The 2-year period should be within immediate past 5 years.
Maintenance of qualification (once every 3 years)	Performed at least 5 ***MTCS or ISMS audits at the end of immediate past 3-year cycle	Performed at least 5 ***MTCS or ISMS audits at the end of immediate past 3-year; **and** At least 2 of these audits performed shall be in the capacity as the Lead Auditor.

Notes:

1) * CISA is awarded by Information Systems Audit and Control Association (ISACA). ISACA Singapore Chapter administers the certification for CISA

2) ***Qualification of MTCS auditor can be done internally by the certification body to perform third-party MTCS audit.*

3) ****MTCS audits include initial, surveillance or recertification audits. 2nd party audits (supplier / vendor audits) performed based on SS 584 can be considered as audit experience stated in this document. All audits have to include the critical processes.*