

GSMA SAS Methodology for Subscription Manager Roles

Version 7.1

21 April 2021

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2021 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Scope 5
1.3 Intended Audience 5
1.4 Definitions 5
1.5 Abbreviations 7
1.6 References 8
2 Audit Process 8
2.1 Audit Setup 8
2.1.1 Audit Request 8
2.1.2 Confirmation of Audit Date 9
2.1.3 Contract 9
2.2 Audit Preparation (Off-Site) 9
2.2.1 Audit Agenda 9
2.2.2 Audit Pre-Requisites 9
2.3 Audit Process (On-Site) 9
2.3.1 Presentation and Documentation for the Audit Team 10
2.3.2 Audit Performance 10
2.3.3 Audit Report 10
2.3.4 Presentation of Results 10
2.4 Following the Audit 11
2.5 Appeals 11
2.6 Notification and Publication of Certification 11
2.7 Language 12
3 Provisional Certification 12
3.1 Provisional Certification Process 12
3.2 Provisional Certification Period 13
3.3 Duration of Provisional Certification 13
3.4 Duration of Provisional Certification Audits 13
4 Full Initial Certification and Certification Renewal 14
4.1 Certification Process 14
4.2 Certification Period 14
4.3 Duration of Certification 15
5 SAS-SM Participants 16
5.1 Auditee 17
5.2 Audit Team 17
5.2.1 Observing Auditor 17
5.3 SAS Subgroup 18
5.4 Audit Management 19
5.5 Participant Relationships 19
6 Audit Report Scoring and Assessment 19
6.1 Audit Result 20

7 Maintaining SAS Compliance 21
7.1 Notifiable Events for PKI certificate management 21
7.2 Examples of other Notifiable Events 22
7.2.1 What Should be Notified 22
7.2.2 What Would not Normally Require Notification: 22
8 Costs 23
8.1 First Dry Audit or Renewal Audit 23
8.2 Audit of Sites with Limited Scope 23
8.3 Audit of Central / Corporate Functions 23
8.4 Re-Audit 24
8.5 Off-Site Review of Improvements 24
8.6 Scope Extension Audits 25
8.7 Cancellation Policy 25
8.8 Appeals 25
9 Final Report 25
10 Auditing and Certification of Supporting Sites 25
10.1 Definition 26
10.2 Auditing and Certification Approach 26
10.3 Data Centres hosting SM Solutions 26
10.4 SM Backup Sites 27
10.5 Centralised or Outsourced IT Services 28
10.6 SM Remote Access Sites 29
10.7 Cloud Service Providers (CSP) 29
10.8 Audit Reports 30
10.9 SAS Certificates 31
11 SAS-SM Certification of Cloud Service Providers 31
11.1 Eligibility 32
11.1.1 CSPs as Support Sites 32
11.2 Application, Planning and Preparation 33
11.2.1 Audit Plan 33
11.2.2 Sampling Approach 34
11.2.3 Observed Inconsistencies Amongst Samples 35
11.2.4 Auditing of Centralised Controls 35
11.3 During the Audit 35
11.4 Changes Within Certified Cloud Regions 35
11.5 Renewal of Cloud Region Certification 36
11.6 SM Client Certification Dependency 36
11.7 Example Sampling Approach 37
11.7.1 Step 1: Certify First Cloud Region 37
11.7.2 Step 2: Certify Second Cloud Region 37
11.7.3 Step 3: Certify Third Cloud Region 38
11.7.4 Renewal of Certification 38
11.7.5 Step 4: Expand and Redefine Cloud Region 38
Annex A Final Audit Report Structure 39

A.1 First Page: 39
A.2 Subsequent Pages: 39
Annex B Standard Audit Agendas 42
B.1 First Dry and Renewal Audits 42
B.2 Wet Audits 47
Annex C Standard Document List 49
C.1 General Information Required 49
C.2 Documents List (per Requirements) 49
Annex D Subscription Management Processing Audit 53
D.1 Before the Audit 54
D.1.1 Preparation 54
D.1.2 Certificate Enrolment 54
D.1.3 Further Preparation for Audit (SM-SR) 54
D.1.4 During the Audit (SM-SR) 55
D.1.5 Further Preparation for Audit (SM-DP) 56
D.1.6 During the Audit (SM-DP) 57
D.1.7 Further Preparation for Audit (SM-DP+) 57
D.1.8 During the Audit (SM-DP+) 58
D.1.9 During the Audit (SM-DS) 59
D.2 After the Audit 59
Annex E Scope of Audit & Certification when using Cloud Service Provider 60
Annex F Document Management 61
F.1 Document History 61
F.2 Other Information 61

1 Introduction

1.1 Overview

The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which Subscription Manager – Secure Routing (SM-SR), Subscription Manager – Data Preparation (SM-DP), Subscription Manager – Data Preparation+ (SM-DP+) and Subscription Manager – Discovery Server (SM-DS) solution providers, and Data Centre Operations and Management (DCOM) providers hosting such solutions, subject their operational Sites and security control frameworks to an Audit. The purpose of the Audit is to ensure that these entities have implemented adequate security measures to protect the interests of mobile network operators (MNO).

Audits are conducted by specialist Auditing Companies over a number of days, typically in a single Site visit. The Auditors will check compliance against a the GSMA SAS Standard for Subscription Manager Roles [1] and its supporting documents ([2], [3]) by various methods such as document review, interviews and tests in specific areas.

Subscription Management entities that are found to be compliant with the requirements in the SAS-SM Standard are certified by the GSMA. This document describes the SAS-SM methodology and processes.

1.2 Scope

This scope of this document covers:

- SAS-SM participating stakeholders and their roles
- Processes for arrangement and conduct of SAS-SM Audit
- Audit scoring and Audit Report structure
- Certification and Provisional Certification Processes
- SAS-SM costs

1.3 Intended Audience

- Security professionals and others within supplier organisations seeking to obtain accreditation for Sites under SAS-SM.
- Security professionals and others within organisations seeking to procure subscription management services
- SAS Subgroup members
- Auditors

1.4 Definitions

Term	Description
Appeals Board	Two Auditors, one each from different GSMA selected Auditing Companies who consider and rule on appealed Audit Results. Auditors for the SAS-SM Appeals Board will be drawn from the SAS-UP Auditing Companies and vice versa.
Audit	The audit carried out by the Audit Team as part of the SAS-SM Auditing Services at the Auditee's Site

Term	Description
Audit Management	A GSMA team which: • Administers SAS-SM • Appoints the Auditing Companies • Monitors and assures the quality and consistency of the Audit Process and Auit Team • Issues Certificates to those Sites that the Audit Team assesses as compliant with the requirements.
Audit Process	As defined in section 2.
Audit Report, Audit Result, Audit Summary and Auditors' Comments	As defined in Annex A.
Audit Team	Two Auditors, one each from different GSMA-selected Auditing Companies, jointly carrying out the Audit on behalf of the GSMA.
Auditee	The supplier that is seeking SAS certification of its Site(s).
Auditing Companies	Companies appointed by the GSMA to provide Auditors.
Auditor	A person qualified to perform SAS-SM Audits
Certificate	Certificate issued by GSMA to Auditee following demonstration of compliance by the Site with the SAS requirements specified in [2].
Certification Process, Certification Period and Duration of Certification	As defined in section 4
Cloud Region	As defined in section 11.
Data Centre Operations and Management (DCOM)	Management and operation of IT infrastructure required for providing subscription management services. If provided by a third party, service model may vary and control/responsibility is shared and agreed between SM customer and DCOM provider. DCOM may include SM customer physical access to infrastructure or may also be provided as a cloud service (via a cloud service provider (CSP)) through network access only.
Dry Audit, and Wet Audit	As defined in section [3]
eUICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in a device, and enables the secure changing of profiles. Note: The term originates from "embedded UICC".
Full Certification	SAS certification of Site controls in live operation.
Primary Site, Secondary Site and Supporting Site	As defined in section 10.1.
Provisional Certification, Provisional Certification Process, Provisional Certification Period and Duration of Provisional Certification	As defined in section 3.

Term	Description
Renewal Audit	Audit performed towards the end of a period of SAS certification to check continued compliance by the Site with the SAS requirements and provide the basis for a decision to award further SAS certification.
Re-Audit	Audit performed to check if updated Auditee controls implemented following non-compliances found at the previous Audit are sufficient to satisfy the SAS requirements.
SAS Subgroup	A group of GSMA members and staff (including the Audit Management) that, together with the SAS Auditors, is responsible for maintenance and development of the SAS Standards, Methodologies, Consolidated Security Requirements and Consolidated Security Guidelines,
Scope Extension	Extension of the scope of certification of a Site that already holds some SAS-SM certification, as defined in 8.6.
Site	Auditee's physical facility and its relevant controls that are subject to the Audit.

See section 5 for more detailed explanations of each role.

1.5 Abbreviations

Term	Description
CSG	Consolidated Security Guidelines
CSP	Cloud Service Provider
CSR	Consolidated Security Requirements
DC	Data Centre
DCOM	Data Centre Operations and Management
eUICC	Embedded UICC
EUM	Embedded UICC Manufacturer
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group
GSMA	GSM Association
MNO	Mobile Network Operator
PKI	Public Key Infrastructure
PRD	Permanent Reference Document
RSP	Remote SIM Provisioning
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SAS-UP	Security Accreditation Scheme for UICC Production
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-DP+	Subscription Manager – Data Preparation (Enhanced compared to the SM-DP)
SM-DS	Subscription Manager – Discovery Service
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process

Term	Description
UICC	Universal Integrated Circuit Card (e.g. a SIM card)

1.6 References

Ref	Doc Number	Title
[1]	PRD FS.08	GSMA SAS Standard for Subscription Manager Roles
[2]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at www.gsma.com/sas
[3]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, available to participating Sites from sas@gsma.com
[4]	N/A	GSMA SAS-SM Standard Agreement (available from sas@gsma.com)

2 Audit Process

The Audit Process is described below.

2.1 Audit Setup

2.1.1 Audit Request

If an Auditee wants to be audited it must make a request to the Audit Management (GSMA) by completing and submitting an SAS application form. The Auditee shall specify on the application form the scope of activities being performed for which certification is being requested.

NOTE: It is possible for an Auditee to be audited for a subset of subscription management activities (e.g. data centre operations and management in the case of a cloud service provider). The scope of certification should be agreed with the Audit Management and Audit Team in advance (see Annex E for details). The agreed scope will be specified in the Audit Report and on the SAS-SM Certificate. See sections 8.2 and 8.3 for associated cost considerations.

The Auditee shall also specify the location of the Site to be audited (or multiple Site locations if processes are distributed across multiple Sites). On receipt of the request the Audit Management will log the details.

First SAS-SM audits of SM-SR, SM-DP, SM-DP+ and SM-DS services are always Dry Audits leading to Provisional Certification – see section 3 for details.

Audit applications should be submitted to GSMA several months in advance to increase the likelihood of the SAS Audit Teams being available to conduct an Audit on or near the dates requested by the Auditee. As a guide:

If SAS Audit application is submitted …	3 months before requested Audit dates,	**then GSMA will try to schedule Audit within …**	4 weeks of requested dates
	2 months before requested Audit dates		6 weeks of requested dates

	1 month before requested Audit dates		8 weeks of requested dates

Table 1 - Audit Scheduling Guidance

It is the responsibility of the Auditee to ensure that certification is in place to satisfy the requirements of any specific contract, customer or bid.

2.1.2 Confirmation of Audit Date

After logging the details of the Audit request, the information is sent to the Audit Team. The Audit Management team will liaise between the Auditee and Audit Team to agree Audit dates.

2.1.3 Contract

The Auditee enters into a standard agreement [4] with GSMA and pays GSMA in advance for the Audit.

2.2 Audit Preparation (Off-Site)

After Audit dates have been agreed the Audit Team and Auditee will liaise to agree arrangements for the Audit.

2.2.1 Audit Agenda

A provisional agenda will normally be agreed one week before the Audit Team travel to the Site to be audited. The agenda should include guidance for Auditees on information that should be prepared for each element of the Audit. A sample agenda is included in Annex B.

Changes to the agenda may need to be made during the Audit itself as agreed between the Audit Team and Auditee.

2.2.2 Audit Pre-Requisites

To assist in the auditing of processes and systems the Audit Team will make arrangements with the Auditee to prepare a eUICC and mobile network operator (MNO) data to be used during the Audit. The following options may be considered:

1. Use an existing eUICC and MNO data
2. Contract with a temporary eUICC and MNO data
3. Use a test tool (permitted for first Dry Audit and any associated Re-Audit(s) only) to simulate, eUICC, EUM and MNO

The Auditee is expected to prepare their systems to enable subscription management functionality within the scope of the Audit.

The Audit Team will liaise with the Auditee to ensure that pre-requisites are in place.

A more detailed guide to this process for Auditees is included in Annex D.

2.3 Audit Process (On-Site)

The audit is conducted on the Auditee’s Site(s) of operations and service.

It is possible that an SM service provider outsources data-center hosting to a SAS-SM cloud service provider (CSP), as described in sections 10.7 and 11. In such a case the CSP will need to be audited and certified as specified in those sections. An Audit of the SM service provider's Site(s) hosting and/or managing sensitive assets (on-site or remotely) will also be necessary.

2.3.1 Presentation and Documentation for the Audit Team

On the first day of the Audit the Auditee presents to the Audit Team the information and documentation specified in the Audit agenda. A list of the required documentation is included in Annex C. Documentation must be available to the Audit Team in English.

Having reviewed the documentation the Audit Team identifies the individuals to be interviewed during the Audit. It is the responsibility of the Auditee to ensure the availability of these individuals.

2.3.2 Audit Performance

The Audit Team assesses performance according to the agreed agenda, by various methods such as:

- Document review,
- Interviewing the key individuals
- Testing in the key areas based on a review of sample evidence of compliance.

2.3.3 Audit Report

The Audit Team summarises the results in a report which is structured as follows:

- Audit Summary and overall assessment
- Actions required
- Auditors' Comments
- Scope of certification
- Detailed results

Detailed results are given in an annex in the Audit Report.

The Audit Report is completed during the Audit.

The Audit Report is restricted to the Auditors, Auditee and the Audit Management, save for the Auditee's right to release a copy to its customers. In case of an appeal (see below), the Audit Report will also be provided to the Appeals Board.

2.3.4 Presentation of Results

The final half day of the Audit is used to finalise the Audit Report. The Audit Team will present the Audit Results to the Auditee focussing on the key points identified in the Audit Report. It is not deemed necessary to have a slide presentation.

The Audit Results include the Audit Team's decision on certification of the Site, which is passed to the Audit Management.

2.4 Following the Audit

The Audit Management checks the report to confirm that the Audit has been carried out in accordance with this Methodology document and that the report meets GSMA quality requirements.

In the event of a successful Audit the Audit Management issues a Certificate to the Auditee within fifteen (15) business days of completion of the Audit.

2.5 Appeals

In the event that the certification decision and/or Duration of Certification are disputed, the Auditee may lodge a submission with the Audit Management within twenty (20) business days of completion of the Audit. The Audit Management will refer the appeal to the Appeals Board.

The Appeals Board is comprised of two Auditors, one each from different GSMA selected Auditing Companies and separate from the Auditing Companies that performed the Audit that is the subject of the appeal. For SAS-SM, the Appeals Board is comprised of representatives of the SAS-UP Auditing Companies, and vice versa. The individual Auditors from each auditing company that serve on the Appeals Board may be assigned by those Auditing Companies from a pool of suitably experienced Auditors pre-approved by GSMA, and may change per appeal.

The Appeals Board will consider and rule on appealed Audit Results. The process to be followed by the Appeals Board will include:

- Review of the Audit Report, focussing on the appealed assessment(s)
- Discussion with the Audit Team and the Auditee

The Appeals Board should not need to visit the Site.

The Auditee may request the members of the Appeals Board to sign an NDA prior to receiving a copy of the Audit Report and other information about the Site.

The Appeals Board will seek to rule on appeals within twenty (20) business days of lodgement of the appeal, subject to the availability of the Audit Team and the Auditee and the prompt provision of any information requested from either party.

The Auditee and the Audit Team agree to accept the decision of the Appeals Board as final.

See section 7 for a description of costs associated with the appeals process.

2.6 Notification and Publication of Certification

The GSMA will list certified and provisionally certified Sites (and Cloud Regions for CSPs) on the SAS website, with an explanation of Provisional Certification.

It is anticipated that interested parties may ask the GSMA to explicitly confirm certification/ Provisional Certification status of Sites and the GSMA is willing to support and respond to such requests.

2.7 Language

The language used in the course of the Audit for all SAS documentation and presentations is English.

The documents described in Annex C, or their equivalents, should be available to the Auditors in English.

Other documents may be in a language other than English but translation facilities should be available during the conduct of the Audit.

Where it is difficult to conduct Audit discussions with key personnel in English, Auditees should arrange for one or more translators to be available to the Audit Team.

3 Provisional Certification

Auditee Sites seeking SAS-SM certification for the first time for an SM service must undergo a two-stage Provisional Certification process for that SM service. This is required in order to satisfy the remote SIM provisioning (RSP) compliance process and gain eligibility to receive GSMA public key infrastructure (PKI) certificates. This Provisional Certification process will initially lead to Provisional Certification, and later lead to Full Certification.

Provisional Certification does not normally apply to CSPs or other Sites seeking independent SAS-SM certification with scope limited to data centre operations and management (DCOM) only. Such Auditees are normally already running live DCOM services prior to seeking SAS-SM certification. First Audits consider all in-scope controls in live operation, and compliance leads to immediate full certification

3.1 Provisional Certification Process

The Provisional Certification Process requires two audits to be conducted at the Site.

The first, referred to as a Dry Audit, takes place before live subscription management services using GSMA PKI certificates and live customer data commence at the Site. For a Dry Audit to take place, the Site must have a complete set of operational systems, processes and controls in place in all areas of the SAS-SM standard. The Site should be in a position to begin subscription management services for a customer immediately when a GSMA or customer (non-GSMA) PKI certificate and a customer order is received.
See Annex D for more details.

If the Site demonstrates compliance with the Standard [1] Provisional Certification is granted that remains valid for a period of nine months. A non-compliant result at a Dry Audit requires the Auditee to remedy identified non-compliances within three months. Successful Provisional Certification will be valid from the date of the repeat Dry Audit.

A follow up Wet Audit is required to upgrade the Provisional Certification to Full Certification. This Audit can only be undertaken if the Site has been in continuous live production using GSMA or customer (non-GSMA) PKI certificates for a minimum period of four to six weeks and it must be undertaken within nine months of the successful Dry Audit.

Successful completion of a Wet Audit leads to Full Certification. The period of Full Certification runs from the date of the successful Dry Audit. Provisional certification will be withdrawn if:

- The Wet Audit is not conducted within nine months of the successful Dry Audit
- The Wet Audit result is non-compliant, and a successful Re-Audit is not completed within three months
- Live Auditee services for a continuous period of four to six weeks cannot be demonstrated within nine months of the successful Dry Audit
- The Auditee chooses to withdraw from the certification process

3.2 Provisional Certification Period

The nine month Provisional Certification Period begins when the Site is first certified..

NOTE: The Provisional Certification Period extends from the date of the successful Dry Audit regardless of whether it is a first or repeat Dry Audit. This differs from the normal certification process, which backdates certification to the first Audit. An exception is made in the case of Provisional Certification because the three month period to make any improvements necessary after a first Dry Audit would reduce the window of opportunity within the nine month Provisional Certification Period to ramp-up subscription management services.

The Provisional Certification Period ends at the date specified on the Site's SAS-SM provisional Certificate or when the Site is fully certified following the successful completion of a Wet Audit.

3.3 Duration of Provisional Certification

The Duration of Provisional Certification is fixed at nine months. It is the responsibility of the Auditee to ensure the Wet Audit necessary to achieve Full Certification is undertaken within the nine month period of Provisional Certification.

If a Provisionally-Certified Site receives a non-compliant result at a Wet Audit, its Provisional Certification will not be withdrawn immediately and it will retain its Provisional Certification status until the end of the nine month Provisional Certification Period.

Full Certification will normally run for one year, in accordance with the provisions set out in section 4.3, and this will be back dated to the date on which the first Wet Audit was concluded. If the Wet Audit extends the scope of existing Full Certification for a Site, and there is significant overlap in controls between the existing and new scope elements, the Audit Team may extend the Full Certification expiry date for the new scope element to match the expiry date of the existing certification (if later).

3.4 Duration of Provisional Certification Audits

The first Dry Audit is conducted over a period as specified in Annex B depending on scope, and all controls will be audited. Auditee processes will also be examined but in the absence of live processes, the Audit Team will sample test controls. The duration of a repeat Dry Audit will depend on the areas to be re-audited. This are agreed with the Auditee in accordance with section 8.4 below.

The Wet Audit is normally conducted over a two day period to review the controls in operation. If the Wet Audit is conducted together with a Renewal Audit for other fully certified scope elements, some time savings on the total Audit duration may be possible.

4 Full Initial Certification and Certification Renewal

This section applies to:

- Sites eligible to achieve Full Certification following a successful first Audit, i.e. CSPs or other Sites already operating live services that are seeking independent SAS-SM certification with scope limited to DCOM)
- Sites seeking to renew SAS-SM Full Certification.

Sites seeking SAS-SM certification for the first time for a SM service should refer to the details of Provisional Certification contained in section 3 instead.

4.1 Certification Process

The initial Full Certification and Certification Renewal Process ("Certification Process") begins with the conduct of a first full Audit or a Renewal Audit at a Site.

The Certification Process ends when:

- A Certificate is issued based on the decision of the Audit Team.

  or

- The Site withdraws from the Certification Process by either:

  - Indicating that it does not intend to continue with the Certification Process

  or

  - Not complying with the Audit Team's requirements for continuing with the Certification Process following a non-compliant Audit Result. (Typically, the Audit Team requires the Site to arrange a Re-Audit or to provide evidence of improvement).

For an existing certified Site, the Certification Process can begin up to 3 months before the expiry of the current Certificate.

4.2 Certification Period

The Certification Period begins when a Certificate is issued based on the decision of the Audit Team.

The Certification Period ends at the date specified on the Site's SAS Certificate of compliance.

The Certification Period will be determined by the Audit Team based on the following criteria:

- If the Certification Process begins up to 3 months before the expiry of the existing Certificate

and

- the certification is awarded before the expiry of the existing Certificate

then

- the Certification Period will begin at the expiry of the existing Certificate

In all other cases the Certification Period will begin at the time that the Certificate is issued.



Figure 1 - Certification Renewal

For Sites eligible for initial Full Certification without an existing valid Certificate:

- the Certification Period will begin at the time that the Certificate is issued.

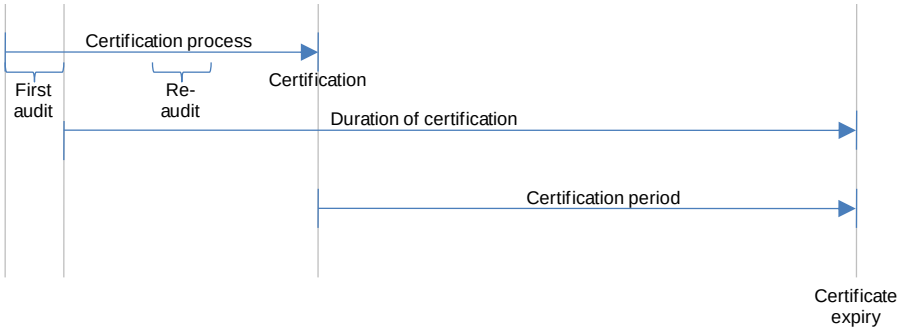


Figure 2 - Initial Full Certification of Sites

Under the terms of their contract with the GSMA, all Sites must be aware of their obligations relating to notification of significant changes at certified Sites within the Certification Period. See section 7 for more details.

4.3 Duration of Certification

The Duration of Certification is determined by the Audit Team.

The standard Duration of Certification for Sites eligible for initial Full Certification and without an existing valid Certificate (new Sites, Sites where certification has lapsed) is one year.

The standard Duration of Certification of Sites providing SM services that are renewing Full Certification is two years. This Duration of Certification will be applied in most cases.

The Audit Team may, at its discretion, decide that certification should be for a shorter duration, for reasons including:

- Significant planned changes at the Site related to security-critical processes or facilities
- Significant reliance on recently introduced processes or systems where there is little or no history of successful operation of similar or equivalent controls
- Repeated failure to maintain security controls at an appropriate level for the entire Certification Period (as evidenced by significant failure to meet the standard [1] at a Renewal Audit).

The Audit Team may also, at its discretion, decide that certification of Sites providing SM services should be for two years for Sites that perform exceptionally well at their Dry and Wet Audits.

The Audit Management will review decisions made on exceptional circumstances as part of its control of scheme quality and consistency.

The standard Duration of Certification for a Cloud Region is one year, starting from the date on which certification is awarded. See section 11.5 for more details.

Sites gaining Full Certification for the first time following one or more repeat Wet Audits shall, in all cases, be granted certification for a minimum of seven months from the month during which a Certificate is issued. This allowance reduces the likelihood that the next Renewal Audit at the Site resulting in 2-year certification is influenced by the most recent Wet Re-Audit rather than being an assessment of steady-state controls in operation at the Site.

The SAS-SM Methodology does not normally allow the GSMA to extend a Site's duration of certification. Sites with an existing Certificate that are planning or making major changes in advance of a Renewal Audit, which could affect the ability to demonstrate the necessary period of evidence, are encouraged to contact the GSMA as early as possible. On an exceptional basis, the GSMA may allow a short extension to the existing Certificate to accommodate the change process, ensuring that there is sufficient evidence of controls/operations available in their final form prior to the Renewal Audit. In such cases, the subsequent Certificate would be issued to the original renewal date; no advantage will be gained, beyond the Site's ability to schedule the SAS Renewal Audit effectively around the Site changes.

5 SAS-SM Participants

The following section describes the roles of the participants during the standard Audit Process. The role of the Appeals Board is not considered here (see section 2.5 for details instead).

5.1 Auditee

The Auditee is the service provider at the Site that is the subject of the Audit. The Auditee is responsible for supplying all necessary information at the beginning of the Audit. The Auditee must ensure that all key individuals are present when required. At the beginning of the Audit the Auditee makes a short presentation describing how it believes that it is compliant with the Standard [1] and the relevant documentation is made available to the Audit Team.

The Auditee is responsible to disclose to the Audit Team all areas of the Site where assets related to sensitive processes may be created, stored or processed. The Auditee may be required by the Audit Team to demonstrate that other areas of the Site are not being used to create, store or process relevant assets, and should honour any reasonable request to validate this.

5.2 Audit Team

The Audit Team consists of two independent Auditors, one from each of the Auditing Companies selected by GSMA following a competitive tender for the supply of SAS auditing services and in accordance with selection criteria defined by the GSMA. The Audit Team conducts the Audit by reviewing documentation, conducting interviews with key individuals and carrying out tests in specific areas. After the Audit is conducted, the Audit Team writes a report (see 2.3.3).

The independence of the Audit Team is of paramount importance to the integrity of SAS-SM. It is recognised that the chosen Audit companies are professional in the conduct of their business. Where the Audit Companies previously supplied consultancy services to an Auditee, the Audit Management should be informed of this fact prior to commencement of the Audit, and the Auditors performing the Audit should be different individuals to those who have provided the consultancy services.

5.2.1 Observing Auditor

On some audits, an additional observing SAS Auditor may accompany the Audit Team, in order to:

- Support the development of a common understanding of Audit schemes between the Audit Companies
- Ensure consistency in standards and the Audit Process
- Facilitate sharing of best practice in the Audit approach

Audit observation will be carried out at no additional cost to the Auditee, and subject to the following guidelines:

- A maximum of one observer will be present on any one Audit, except by the prior agreement with the Auditee. Auditees will be under no obligation to agree to any requests for participation of more than one observer.
- The observer will comply with all requirements of the Auditee:
    - Prior to the Audit (e.g. signing NDAs, providing personal information for visitor authorisation).
    - On-site (e.g. behaviour and supervision).

- The role of the observer is observe. The observation process should not interfere with the conduct of the Audit. Specifically, the observing Auditor:
    - Should not normally engage directly with the Auditee during the Audit Process to ask Audit questions.
    - Should only engage in discussion with the Auditee about the observer's own SAS scheme when such discussion will not interfere with the Audit Process.
    - Should not present or participate in any discussions during the closing meeting.
    - Should not contribute to the preparation of the Audit Report.

To maximise the benefits of the observation process the observer and Audit Team are expected to discuss elements of the Audit Process and approach. Such discussions:

- Should only take place outside of the Audit Process, and not in the presence of the Auditee.
- Should include an opportunity for the observer to read the Audit Report.
- May include a post-Audit discussion, either on- or off-site to discuss any questions or observations. The post-Audit discussion may be extended to include other Auditors if appropriate.

Members of the Audit Management may also seek to attend and observe Audits from time to time. They guidelines above will also apply to them.

5.3 SAS Subgroup

The SAS Subgroup is a committee comprised of GSMA staff (including the Audit Management) and members, and representatives of the Auditing Companies. It is responsible for maintenance of the following SAS-SM documentation:

- The Standard [1] which contains the security objectives for SAS-SM.
- The Consolidated Security Requirements (CSR) [2] which provide requirements for all sensitive processes (SPs) within the scope of the different SAS schemes. Many of the requirements are common across all schemes, however some requirements are specific to individual SPs, including subscription management. The requirements that apply to subscription management are indicated in that document. These are the requirements that the Auditee must satisfy in order to be certified.
- The Consolidated Security Guidelines [3] to guide interpretation and operational application of the CSR, and
- The Methodology (this document)

Updates will normally arise from an annual review meeting of the SAS Subgroup. Where acute issues are identified ad hoc meetings may be convened to discuss updates to the SAS-SM documentation.

The SAS Subgroup also contributes to the development of Auditing Company selection criteria when GSMA is procuring SAS auditing services from time to time. Operator members of the SAS Subgroup that do not offer any products or services within the scope of SAS will be invited by GSMA to participate in the review of tender responses and the selection of Auditing Companies.

5.4 Audit Management

The Audit Management comprises a team of GSMA staff members responsible for administering the scheme, including:

- Selecting suitably qualified Auditing Companies to carry out the audits, in conjunction with the SAS Subgroup as indicated in section 5.3, and ensuring that they provide a high-quality service.
- Ensuring that audits are conducted in accordance with the SAS-SM Methodology and that Audit Reports meet GSMA quality requirements.
- Managing Audit lifecycle tasks, pre and post Audit, for example maintenance of the Audit log and list of certified and provisionally certified Sites
- Contract and financial management between the GSMA and Auditees and the GSMA and Auditing Companies
- Distribution of SAS-SM documentation (this document, the Standard [1], the Consolidated Security Requirements [2], and the Consolidated Security Guidelines[3]) to Auditees and Auditors.
- Handling general queries about the scheme via sas@gsma.com.

5.5 Participant Relationships

The relationships between SAS-SM participants are indicated in Figure 3.

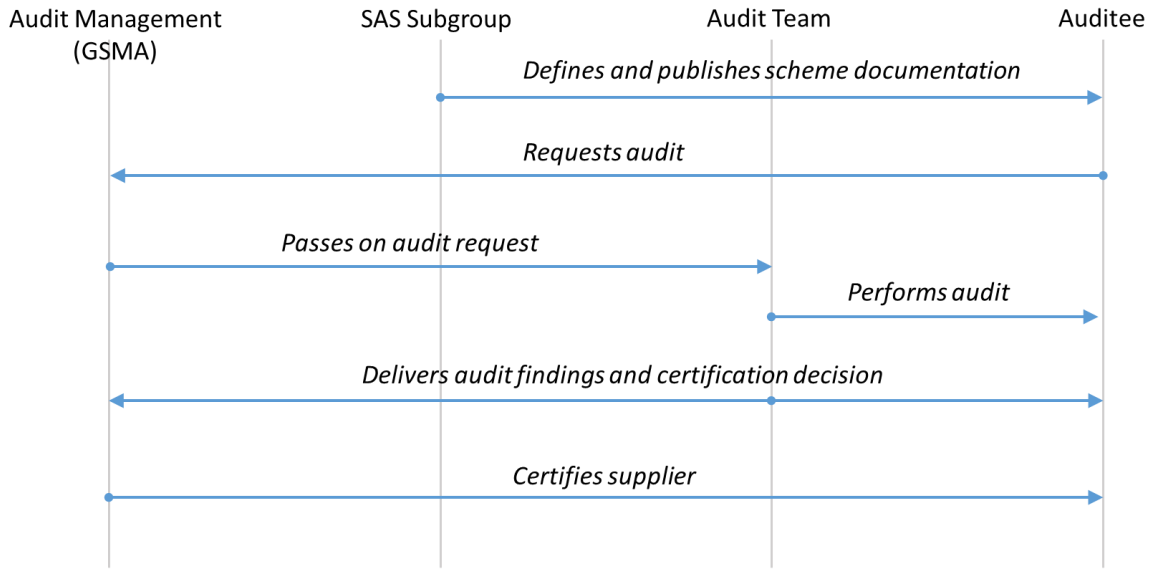


Figure 3 - SAS-SM Participant Relationships

6 Audit Report Scoring and Assessment

The Audit Report (see section 2.3.3) contains detailed Audit Results. An indexed matrix of requirements is used as a means to structure and standardise recording of compliance. Possible assessments are described in Table 2.

Compliant (C)	Indicates that the Auditors' assessment of the Site has found that a satisfactory level of compliance with the standard has been demonstrated during the Audit. To assist Auditees in assessing their Audit performance, and to plan improvements, the Auditors may, at their discretion, indicate the level of compliance as follows:	
	Compliant (C):	In the Auditors' assessment the Auditee has met the standard to an acceptable level. Comments for further improvement may be offered by Auditors.
	Substantially compliant (C-):	In the Auditors' assessment the Auditee has just met the standard, but additional improvement is thought appropriate to bring the Auditee to a level at which compliance can easily be maintained. An assessment of C- will be qualified with comments indicating the improvements required. Future audits will expect to see improvement in areas marked as C-.
Non-compliant (NC)	In the Auditors' assessment the Auditee has not achieved an acceptable level of compliance with the standard due to one or more issues identified. The issues identified require remedial action to be taken to ensure that an acceptable level of compliance is achieved. Remedial action is compulsory to ensure continued certification.	

Table 2 - Assessments Possible Under SAS-SM

Non-compliances and required actions will be summarised at the front of the Audit Report, and described further in the detailed findings.

Comments will normally be provided, marked as (**+**) and (**-**) in the *Auditor* remarks to indicate positive and negative implications of the comments. Comments with no symbol represent general comments. The number of (**+**) or (**-**) comments bears no relation to the section or sub-section score.

6.1 Audit Result

The Audit Result will be determined based on the level of compliance achieved in all sections of the Audit Report.

In the event that no sections of the Audit Report are assessed as non-compliant by the Auditors then the Audit Result will specify that certification will be awarded by GSMA without further improvement.

In the event that one or more sections of the Audit Report are assessed as non-compliant then the Auditee will be required to submit to further assessment in those areas. The assessment may be carried out:

- On-site during a Re-Audit
- Off-site through presentation of evidence

The re-assessment method will be determined by the number and nature of issues identified and will be indicated in the Audit Summary.

Certification will not be awarded where one or more areas of non-compliance are identified.

Once the Auditee has submitted to successful re-assessment of the issues identified an updated Audit Report will be issued specifying that certification will be awarded.

7 Maintaining SAS Compliance

SAS certification is awarded based on an assessment by the Audit Team that the Site met the requirements of the SAS Standard during the Audit, and that it demonstrated an ability and intent to sustain compliance during the Certification Period. Continued Site compliance with the SAS Standard during the Certification Period, including the implementation of SAS-compliant controls following any changes to the certified environment, is the responsibility of the Site.

Certified Sites are required, under their agreement with the GSMA, to notify the GSMA of any major change planned or proposed within the audited domain at the Auditee's Site, and to host within three months any audits deemed necessary by the GSMA to verify the continued compliance of the Site with the SAS Standard as a result of such change. Major changes to the Auditee's Site that require notification include but shall not be limited to significant production, process or relevant policy changes, and sale of the Auditee's Site.

7.1 Notifiable Events for PKI certificate management

Sites that perform PKI certificate management activities within the scope of their SAS-SM certification must notify the GSMA of some specific events that are directly related to that activity:

- Revocation of PKI certificate(s)

  If any live PKI certificate (whether issued as part of the GSMA or other PKI) within the scope of the Site's SAS-SM certification is revoked by the relevant certificate issuer, by the Site itself or by another party, this must be notified to the GSMA. Certificates used solely for test purposes that are revoked at end-of-life are excluded from this requirement.

- Security incidents

  Any security incident involving personnel, processes, physical locations, systems or sensitive materials related to management of PKI certificates or key pairs must be notified to the GSMA, even if the security incident itself does not relate to certificates or key pairs within the scope of SAS-SM certification.

- Transfer of GSMA PKI certificate private keys.

  Any activity involving the transfer of GSMA PKI certificate private keys to a new physical location (e.g. transfer between sites or relocation of key management systems or HSMs) or logical transfer or replication to a new key management system or HSM must be notified to the GSMA.

Transfer of GSMA PKI certificate private keys must always be carried out in accordance with the requirements of section 6.6 of [2].

7.2 Examples of other Notifiable Events

The following examples are provided to help Auditees understand what level of change should be notifiable. The list is provided to help guide Auditees only. Auditees are always encouraged to contact the GSMA in the event of any uncertainty about whether an event is notifiable.

7.2.1 What Should be Notified

- Revisions to policy or procedure that change controls audited within the scope of the SAS Audit, e.g.:
    - Removal of a procedure or control of sensitive assets
    - Removal of a security screening step for new employees.
    - Reduction in the frequency of a risk assessment process, security awareness training programme or IT vulnerability scan.
- Changes to the responsibility for physical security management, such as site security manager.
- Changes to the responsibility for logical security management, such as key manager, IT security manager.
- Changes to the physical environment where sensitive processes are located or housed, e.g.:
    - Relocation of sensitive processes to new premises or alternative locations within the existing certified Site.
    - Enlargement or other physical change to a room or workshop containing a sensitive process
    - Changes to the physical construction of areas of the Site where sensitive processes are carried out.
- Changes to the architecture of the networks used for sensitive processes, or to the security level of networks where sensitive processes take place.

7.2.2 What Would not Normally Require Notification:

- Replacement or implementation like-for-like of a data processing, production or infrastructure supporting system, e.g.:
    - Replacing a firewall with a new device implementing an identical policy
    - Implementing a new instance of an existing platform with a configuration that applies the same policies.
- Changes to layout of existing certified areas where CCTV visibility and other controls are maintained at an equivalent standard, e.g. changing the positions of:
    - Systems in a server room

8 Costs

The Audit fees for an Audit are determined by the Audit duration, which depends on the Audit type (e.g. first Dry Audit, Wet Audit, Renewal Audit, Re-Audit or Scope Extension Audit). Costs may also depend on the logistics involved in carrying out the Audit, that is, if more than one Site is included in each visit the presentations, document reviews and Audit performances may take longer than normal.

8.1 First Dry Audit or Renewal Audit

The Audit duration will depend on the Audit scope, as specified in Annex B. Costs guidance will be sent by the Audit Management to the Auditee in advance of the Audit. A daily auditing fee will be quoted in the GSMA SAS standard agreement [4] which is signed between GSMA and the Auditee.

Variable costs such as accommodation and travel will be incurred by the Auditors with a view to minimising costs while maintaining reasonable standards (see the agreement [4] for more information). The Auditors or the Auditee may book and pay for travel and accommodation as agreed between the parties on a case by case basis. Where audits are conducted at long haul destinations during consecutive weeks every effort will be made to minimise costs by conducting several audits during one trip and allocating the travel and accommodation costs proportionately between multiple Auditees where applicable.

8.2 Audit of Sites with Limited Scope

First audits for Sites with a very limited scope of certification (e.g. Sites only providing data centre operations and management) may be conducted over a period different to the standard Audit duration. Auditees should notify the Audit Management of the reduced scope at the time of application for first Audit. A proposed Audit duration will be agreed in advance of the first Audit. The proposed duration for subsequent Renewal Audits will be documented by the Auditors in the Audit Report.

8.3 Audit of Central / Corporate Functions

Subscription management entities may be group companies that have a number of Sites. In some cases some functions, knowledge or expertise may be centralised, with common solutions deployed at multiple Sites.

Auditees may request that common solutions are audited in detail, centrally. In such a case, successful audits will result in approval of such solutions for deployment across multiple SAS-SM certified Sites within the corporate group. Audits will be undertaken by the Audit Team to a scope agreed in advance between the Auditee, Audit Management and Audit Team. Approval will be granted via an Audit Report prepared by the Audit Team, issued to the Audit Management, and notified in writing to the Auditee.

Subsequent audits at Sites dependent on centralised functions deployed elsewhere will ensure that the centrally-approved solutions are deployed appropriately, but will not consider the detail of the solutions themselves.

Certification of all Sites deploying such solutions will become dependent on renewal of approval of centralised solutions. Renewal will be required every two years.

Audits of centralised functions will be agreed on a case-by-case basis with Auditees. The duration of audits at individual Sites may be reduced where appropriate.

8.4 Re-Audit

The costs for a Re-Audit will depend on the required duration of the Re-Audit, which in turn depends on the number of areas assessed as non-compliant during the preceding Audit. The Re-Audit duration is agreed between the Audit Team and the Auditee at the end of the preceding Audit and the fixed cost is the daily rate quoted in the contract between GSMA and the Auditee, multiplied by the number of Auditor days required to conduct the Re-Audit.

Repeat audits must be conducted within three months of the original non-compliant Audit and the Auditee must certify that no significant changes have taken place to affect the Site security during the time period between the original and the Re-Audits.

8.5 Off-Site Review of Improvements

Where the Auditors' recommendation at Audit is non-compliant with an off-site reassessment method, it is likely that additional time will be required to review evidence of changes provided by Auditees. Such time may be chargeable to Auditees in addition to the cost of the Audit itself.

Where an off-site reassessment method is recommended by the Auditors, the Audit Report will include an estimate of the time required to review the evidence and update the Audit Report. This estimate will be used as the basis for charging.

The estimate will be based on the following structure:

Total units = Administration + Minor items + Major items

where:

Administration	1 unit	Applies to all off-site reassessment. Covers updates to report, general communication with Auditee and GSMA
Minor items	1 unit per item	Applies to each Audit Report sub-section assessed as NC where the scope of improvement is limited to: • Minor changes to individual documents • Changes to individual controls, where changes can be illustrated by simple photographs, plans or updated documents
Major items	4 units per item	Applies to each Audit Report sub-section assessed as NC where the scope of improvement is: • Significant changes to processes (new or existing) with multiple documents or elements to be reviewed • Changes to individual controls, where changes require detailed review or analysis of multiple documents, photographs, plans or video • Changes to multiple linked controls

Table 3 - Estimating Auditor Time for Off-Site Review of Improvements

For each Audit, charging will be based on the total applicable units:

- 0-3 units (one or two minor issues, plus admin) – no charge,
- 4-6 units (three or more minor items or one major item) – half-day charge per Auditor,
- >6 units – full day charge per Auditor.

8.6 Scope Extension Audits

If a Site is already certified for one or more SM services and wishes to extend certification to include other SM services, it needs to hold Dry and Wet Audits for the additional SM services for which SAS-SM certification is being sought. The duration of Scope Extension Dry and Wet Audits will normally be reduced compared to the audits that have previously taken place at the Site to gain initial SAS-SM certification. The duration will be agreed on a case-by-case basis with Auditees.

8.7 Cancellation Policy

An Audit cancellation fee shall be payable by the Auditee to each (of the two) Auditors for each scheduled Audit day where less than fourteen (14) business days' notice of cancellation, from the date that an Audit is due to commence, is given by the Auditee.

The Auditee shall also be liable for certain unavoidable and non-recoverable expenses (e.g. visa application fees) incurred by the Auditors where less than 60 days' notice of cancellation, from the date than an Audit is due to commence, is given by the Auditee, or where GSMA cancels the Audit as a result of non-compliance by the Auditee with the terms of the SAS-SM standard agreement. Such expenses shall be evidenced by receipts. More details are contained in the SAS-SM standard agreement [4].

8.8 Appeals

Charges for each appeal will be based on the same principles as for estimating charges for off-site review of improvements, as specified in section 8.5.

If an appeal results in a change to the certification decision for an Auditee Site, then no fee shall be payable by the Auditee and the Appeals Board cost will be borne by GSMA. If an appeal results in no change to the certification decision for an Auditee Site, then the costs of the appeal shall be payable by the Auditee.

9 Final Report

In the course of each Audit, the Auditors will make observations which will be recorded in the Audit Report. Various details will also be recorded in the course of the Audit that will result in the production of a final Audit Report, the content of which is described in Annex A.

10 Auditing and Certification of Supporting Sites

SAS provides auditing and certification on a Site-by-Site basis. However, Sites that participate in the scheme may use additional physical Sites owned and operated by themselves or by third party subcontractors to provide some supporting infrastructure or services within the scope of certification. This document specifies how Supporting Sites are formally handled within the scheme.

10.1 Definition

A Supporting Site is one that meets all of the following criteria:

- Provides supporting infrastructure and/or services within the scope of SAS certification to the Primary Site seeking certification.
- Does not wish to hold its own SAS certification, or is not eligible to do so.
    - To be eligible for SAS-SM certification as a Primary Site, a Site must operate, or be planning to operate, live and primary (not just backup) production or services that fulfil at least one of the primary SAS- SM scope elements.
        - Exceptional applications for SAS certification by Sites that do not meet these criteria will be considered by GSMA on a case-by-case basis.

In most cases the Supporting Site is primarily accountable (via internal or contractual agreements) to the Primary Site rather than to GSMA for its compliance with the SAS requirements. However, a Supporting Site must still be subject to the terms of SAS participation, and therefore must be named on an SAS agreement signed by the Primary Site or the Primary Site's parent company.

A Secondary Site is a Supporting Site that is included as part of the same Audit Process and Audit Report as the Primary Site.

10.2 Auditing and Certification Approach

The auditing and certification process to be followed is slightly different depending on the type of Supporting Site, as described in sections 10.3 to Table 7 below.

10.3 Data Centres hosting SM Solutions

Data centres hosting SM solutions typically provide the SM service provider with a secure room or cage within the data centre, electrical power, air conditioning, connectivity and building security controls. The focus of the SAS-SM Audit is the room or cage within which the SM platform is contained, which is under the control of the SM service provider. The data centre provider is responsible as a subcontractor to the SM service provider for the services that it provides within SAS-SM scope.

The Primary Site and the Supporting Site in this case are the same. On the SAS-SM Certificate, this will be represented by specifying the Auditee name, with a Site location as the data centre name and address. In practice, part of the SAS-SM Audit (documentation review, meetings, interviews) will be performed outside of the SM server room/cage. This may be in a different room, building, city or even a different country, depending on the corporate office facilities provided by the SM service provider and the locations of key personnel. If there are no sensitive processes within SAS-SM scope occurring at these corporate offices, the location(s) of these offices will usually not be specified on the SAS-SM Certificate. If sensitive processes are occurring at these locations, these will be specified as described (e.g. the location of remote administrative access would be specified as per section Table 6)

Item	Description
Application form	SAS-SM applicants should indicate on the SAS application form if an

Item	Description
	external data centre is being used.
Audit scheduling and duration	Although their focus is to provide supporting services, SM data centres (DCs) are considered as Primary Sites, given that they host SM servers and assets and are used for activities such as key ceremonies. The SAS-SM Audit duration is not affected solely by the use of a DC. However, in practice, if part of the SAS-SM Audit (e.g. documentation review, meetings, interviews) is performed outside of the DC, the distance between the DC and other Site(s) may affect the overall Audit duration. If the necessary transfer time between the DC and other Site(s) is significant and is expected to extend the overall Audit duration, this should be highlighting by the Auditee when the Audit is being scheduled.
SAS agreement and invoicing	SM data centres do not sign an SAS-SM participation agreement directly with GSMA. Their involvement in the scheme is indirect and through the SM service provider. However, the name and address of the DC should be specified in the agreement. The SM service provider is invoiced for the Audit.
Audit Report	A single Audit Report should be prepared covering the in-scope activities performed by the Auditee and/or relevant to the SM DC.
SAS Certificate and website listing	The SAS Certificate will contain specifying the Auditee name, with a Site location as the data centre name and address. A single certification expiry date applies and will be specified on the Certificate.

Table 4 – Supporting Site Auditing Approach – Data Centres

10.4 SM Backup Sites

Item	Description
Application form	If use of a backup Site is part of the business continuity plan for the Primary Site, then SAS-SM applicants should provide backup Site details on the SAS application form.
Audit scheduling and duration	SM backup Site audits may be conducted back-to-back or with some period between them, depending on Auditee preference. • Back-to-back audits of primary and backup Sites provides the fastest means to certification of the Primary Site, as there is no delay waiting for the backup Site Audit and outcome. It is likely to also result in lower overall Auditor travel expenses, and means that the Certification Periods for both Sites remain aligned. • Independent scheduling (Primary Site first) allows the participant to improve controls at the backup Site based on any non-compliances found during the Audit of the Primary Site, improving the chance of a compliant result at the first Audit of the backup Site and therefore avoiding the need for a Re-Audit. The standard Audit duration for SM backup Sites is 3 days, given the overlap in controls in many areas. For back-to-back audits, transfer time between primary and backup Sites will need to be considered when scheduling the audits and will determine whether the standard 1 day chargeable travel time applies to the Audit of the backup Site.

Item	Description
SAS agreement and invoicing	The backup Site (whether owned by Primary Site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The backup Site should be specified in the Primary Site's agreement. If the backup Site Audit request is received after the Primary Site's agreement has already been executed, then another instance of the agreement specifying the backup Site will need to be signed. The Primary Site applicant is invoiced for the Audit.
Audit Report	Controls and observations common to the primary and backup Sites made at a single point in time (i.e. back-to-back or closely scheduled audits) can be documented once only, but need to be highlighted as being common. The Audit Team can decide whether to report their findings in a single document (but clearly distinguishing which Site their observations refer to) or in two documents (with references in relevant sections to the observations and assessments on common controls described in the other report). If there is a significant time interval between primary and backup Site audits, separate reports are recommended.
SAS Certificate and website listing	The backup Site name and address are mentioned on the SAS Certificate of the Primary Site(s) to which they provide support.
Provisional certification	It may occur that the Primary Site holds Full Certification while the backup Site holds Provisional Certification. This will be highlighted on the SAS Certificate. If the certification of a backup Site lapses, GSMA may withdraw the SAS certification of the associated Primary Site(s).

Table 5 – Supporting Site Auditing Approach – SM Backup Sites

10.5 Centralised or Outsourced IT Services

Item	Description
Examples	Centralised IT administration, network operations centre, server farm, firewall management
Application form	The application form provides space to provide Supporting Site details and to outline the Site activities.
Audit scheduling and duration	Supporting Sites providing centralised or outsourced IT services may host initial audits scheduled back-to-back or closely scheduled with Primary Site audits. Audits of additional Primary Sites that depend on the Supporting Site's certification are scheduled independently. The Audit duration depends on the Supporting Site activities, and should be agreed on a case by case basis with the Audit Team. For back-to-back audits, transfer time between Sites should also be agreed.
SAS agreement and invoicing	The Supporting Site (whether owned by the Primary Site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The Site should be specified in the Primary Site's agreement. If the Supporting Site Audit request is received after the Primary Site's agreement has already been executed, then another instance of the agreement specifying the Supporting Site will need to be

Item	Description
	signed. The Primary Site applicant or its parent company is invoiced for the Audit.
Audit Report	Only the sections of the Audit Report relevant to the activities performed by the Site need to be completed by the Audit Team.
SAS Certificate and website listing	The Supporting Site name and address are mentioned on the SAS Certificate of the Primary Site(s) to which they provide support.

Table 6 – Supporting Site Auditing Approach – Centralised/Outsourced IT

10.6 SM Remote Access Sites

This applies to Sites that have remote access to networks, systems or information within the scope of SAS certification that require auditing, as specified in FS.17 [2] and FS.18 [3].

Item	Description
Application form	The application form provides space to provide Supporting Site details and to outline the Site activities.
Audit scheduling and duration	Flexible scheduling (scheduled independently of Primary Site Audit or conducted back-to-back). The Audit duration depends on the Supporting Site activities, and should be agreed on a case by case basis with the Audit Team. For back-to-back audits, transfer time between Sites should also be agreed.
SAS agreement and invoicing	The Supporting Site (whether owned by Primary Site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The Site should be specified in the Primary Site's agreement. If the remote access Site Audit request is received after the Primary Site's agreement has already been executed, then another instance of the agreement specifying the remote access Site will need to be signed. The Primary Site applicant is invoiced for the Audit.
Audit Report	Only the sections in the Audit Report relevant to the activities performed by the Site need to be completed. The Audit Team can decide whether to add their findings to the Primary Site Audit Report (but clearly distinguishing which Site their observations refer to) or produce a second report (with references in relevant sections to the observations and assessments on common controls described in the other report). If there is a significant time interval between primary and remote access Site audits, separate reports are recommended.
SAS Certificate and website listing	The Supporting Site name and address are mentioned on the SAS Certificate of the Primary Site(s) to which they provide support.
Provisional Certification	Not applicable. Certification type is determined by Primary Site only.

Table 7 – Supporting Site Auditing Approach – Remote Administrative Access Sites

10.7 Cloud Service Providers (CSP)

There are two options available to CSPs seeking to host SAS-SM certified services.

1. The CSP can seek its own independent SAS-SM certification (with scope DCOM) to allow multiple SM service providers to use its services. See section 11.
2. The CSP can be included within a SM service provider's certification as a subcontractor.

This section applies where a CSP is a subcontractor to an SM service provider, i.e.

- CSP does not hold its own SAS certification. It is listed as a Supporting Site on its client's SAS Certificate.
- It is only audited and certified for services that it provides to the specific client.
- It does not engage or contract directly with GSMA.

If a CSP applies directly to GSMA for its own SAS-SM certification with scope "Data Centre Operations and Management", then it should be handled as specified in section 11.

Item	Description
Application form	The application form should specify all CSP Sites where SM service provider data may be held, via multiple application forms if necessary.
Audit scheduling and duration	Although their focus is to provide supporting services, CSP data centres (DCs) may be considered and treated as Primary Sites as described in section 10.2, given that they host SM servers and assets. Scheduling is flexible (scheduled independently of Primary Site Audit or conducted back-to-back). Audit duration depends on the number of CSP Sites to be audited, the activities performed and the consistency of controls at each Site, and should be agreed on a case by case basis with the Audit Team. For back-to-back audits, transfer time between Sites should also be agreed.
SAS agreement and invoicing	The CSP Sites must be subject to the terms of the SAS participation agreement. The Sites should be specified in the Primary Site's agreement.
Audit Report	Usually a separate report to Primary Site, but will depend on services provided. Only the sections in the Audit Report relevant to the activities performed by the Site need to be completed.
SAS Certificate and website listing	The CSP Site name(s) and address(es) are specified on the SAS Certificate of the SM service provider to which they provide support. If multiple CSP Sites provide support, a customised SAS Certificate may be created to list these. CSP Cloud Regions that have gained independent certification (see section 11) receive their own Certificates.
Provisional Certification	Not applicable to CSPs, as their activities are already live. First audits of these Sites lead to Full Certification.

Table 8 – Supporting Site Auditing Approach – Cloud Service Providers

10.8 Audit Reports

Relevant contextual information about the Audit should be provided within all Audit Reports (within "Auditors' Comments" section or other standardised tables/subsections within template). This is especially important if a Supporting Site is being audited. The information

provided should include Site location(s), dates and duration, Audit type and approach, summary of activities performed at each Site, any relevant Audit history, and explanatory notes in relation to how the report has been prepared and any deviations from standard Audit practice if necessary.

10.9 SAS Certificates

If the certification expiry dates of a Primary Site and a backup Site are different, GSMA will include both expiry dates on the Certificate. Note that this approach will trigger reissue of Certificates to Primary Site(s) by GSMA each time a Supporting Site renews certification.

If the certification of a Supporting Site lapses, GSMA may withdraw the SAS certification of the associated Primary Site(s).

11 SAS-SM Certification of Cloud Service Providers

The growth and development of SM deployments has led to the use of cloud service providers (CSPs) services for SM solution hosting. The standard individual Site-based approach to SAS-SM certification does not align with the physical and logical data centre-based architecture of CSPs and their use of consistently deployed and managed data centres (DCs).

Virtually all public cloud physical architectures revolve around the notion of a region. A region is a geographical location mapped to a collection of physical DCs and/or server rooms in that region. Every region is physically and logically isolated and independent from all other regions (power, cooling, network, update cycles, etc.).

Within a region, resources can be shared. While details vary from CSP to CSP, security processes, policies, tools and network assets are typically shared across a whole region and managed region-wide, normally from a separate centralised facility. In addition, it is common for a region to spread its network, compute and storage resources across multiple server rooms or DCs in a dynamic way, often transparently to the tenant, or to add new server rooms or DCs as the demand grows. It is also common for CSPs to deploy and operate DCs in a highly consistent manner, both physically and logically.

With such architectures, seeking to audit and certify DCs individually and independently is not practical or efficient and it can be difficult to define the physical and logical boundaries of a certified site in the context of SAS-SM. This section therefore introduces the concept of a **Cloud Region** for the purposes of SAS-SM certification, defined as a collection of data centers (including server rooms providing DC functions within other non-DC facilities of the auditee) that are part of the same logical cloud deployment and cloud management unit. A Cloud Region is not defined by a the number of DCs in the region, or by a geographical location or jurisdiction, but is a flexible definition associated with the overall population of DCs for which SAS-SM certification is being sought. The definition of a Cloud Region for the purposes of SAS-SM auditing and certification may be agreed between GSMA, Auditors and CSPs if necessary to adapt to the physical and logical architectures used by different CSPs, but should align with the principles specified here.

A Cloud Region could be made up of several different physical sites and buildings separated by varying distances, typically measured in kilometers. It is not practical for an Audit Team to

visit each DC during a single Audit. However, most CSPs maintain the same security standards and controls on all DCs within the same cloud region.

If a CSP is seeking SAS-SM certification for a Cloud Region, it therefore may be possible to physically visit and audit a subset of DCs in order to certify a larger population of Sites comprising a Cloud Region. The sections below specify the conditions in which such a sampling approach can be used, and the approach to be taken.

Note: The term “sampling” refers to the normal auditing practice used in SAS-SM audits of checking a subset of systems, services or records in order to develop an opinion on overall compliance. However, unless otherwise indicated, use of the term “sampling” in this section refers specifically to the practice of auditing a subset of DCs in order to certify a larger population of Sites comprising a Cloud Region. For the avoidance of doubt, it does not permit Auditees to only be audited for a sample of the SAS-SM requirements, or to only apply the necessary controls to a sample of the DCs.

It is assumed that SAS-SM Audits will only ever occur at live operational DCs, so the concepts of Dry and Wet Audits and Provisional Certification do not apply. Successfully auditing of DCs within a Cloud Region will therefore always lead to Full Certification for the Cloud Region.

11.1 Eligibility

A sampling approach to audit and certify DCs hosting SM solutions that exist as part of a Cloud Region may be considered under the following conditions:

3. There is a very high level of consistency between the controls within SAS-SM scope deployed at all sites within the Cloud Region.
    - A high level of consistency does not mean that all systems and controls must be identical, but the controls in use must satisfy the SAS requirements to the same extent and using the same approach, to a level that would allow an Audit Team to have assurance that a control assessed at one DC is representative of the controls at all of the other DCs within the Cloud Region.
4. A significant proportion of the controls within SAS-SM scope that apply to all of the DCs within the Cloud Region are managed centrally, and can be audited centrally.
5. The CSP is seeking SAS-SM certification for the Cloud Region independently of any client (as distinct from as a support site as described in section 11.1.1 below).

11.1.1 CSPs as Support Sites

Scenarios may arise where an SM solution provider agrees with a CSP to deploy its solution at a single specified DC or a small number of DCs owned by the CSP. The CSP may be only seeking to support the certification of this single customer for the services within SAS-SM scope that it provides to that customer. In this case, the CSP is considered as a subcontractor of the SM service provider, and the CSP’s DC would not receive its own certification following successful audit. Instead, the SAS-SM certificate for the SM service provider’s Site would specify that that the CSP’s DC has been audited and satisfied the

SAS-SM requirements for only the services within audit scope that it has provided to its customer.

Due to the limited number of DCs involved and the role of the SM service provider as the entity ultimately response for SAS-SM compliance, the concept of Cloud Region certification and the use of sampling described below is not normally possible for this Support Site deployment model. SAS-SM auditing and certification of such DCs, in support of the SM service providers using them, will take place in accordance with the approach described in section 10.7.

11.2 Application, Planning and Preparation

On its SAS-SM application form, the CSP (referred to below as the Auditee) will need to specify the Cloud Region for which SAS-SM certification is sought, and all DCs within the Cloud Region. If seeking to be audited and certified using a DC sampling approach, the Auditee should indicate which DCs, in its view, would satisfy the eligibility criteria for this.

The GSMA and the Auditing Companies will consider the Auditee's application and engage in case-by-case discovery discussions with the Auditee to learn more about its certification objectives, the overall scope and complexity of the assessed environment, and at a high level, the Cloud Region's physical and logical architecture. These planning and preparation discussions will be more extensive than for other types of SAS-SM Audits due to the bespoke nature of the Audit approach needed for each CSP. The confidentiality of Auditee information exchanged during this discovery period will be protected by the SAS agreement signed between the Auditee and GSMA.

If SAS-SM certification of a Cloud Region is being renewed or extended, the planning and preparation activities are normally less extensive, and focus on changes since the previous Audit and a review and update of the audit plan. In particular, the sampling approach and rationale must be reviewed and updated for each certification renewal or extension.

11.2.1 Audit Plan

Based on the application information submitted, other information that may be requested, and discussions with the Auditee, the Audit Team will prepare an audit plan. The audit plan will specify the following:

- Locations of DCs seeking SAS-SM certification in order to physically host SM solutions, including DCs where SM sensitive assets are replicated. Locations of Support Sites (e.g. remote access, management and/or administration) for these DCs that have access to sensitive data or perform sensitive activities within SAS-SM Audit scope, and an outline of their functions.
- Location of facilities where the document review and interview portions of the SAS-SM Audit will take place, if separate from the facilities already listed.
- Names and contact details of the assigned SAS-SM Auditors in the Audit Team.
- Name(s) and contact details of primary contact(s) at the Auditee
- A list of the Auditee's cloud services for which SAS-SM certification is sought.
- Whether one or more standardised control models is/are in place across the Cloud Region.

- An initial assessment of the SAS requirements that apply to the CSP, with reference to the embedded spreadsheet in Annex E of this document.
- Whether use of a sampling approach is considered feasible to enable certification of some DCs (specified) or all of the DCs within the Cloud Region.
- If a sampling approach is to be used:
    - The number of DCs to be sampled within the Cloud Region
    - The rationale used for selecting the number of DCs to be audited (sample size).
    - The sample DCs that will be audited; the justification behind the chosen sample and why this is appropriate and representative of the overall population
    - The SAS-SM requirements (sections of FS.17) that will be audited using a sampling approach at the selected DCs.
    - The SAS-SM requirements (sections of FS.17) that cover controls managed centrally by the Auditee, that will be be audited centrally.
    - The audit procedures that will be followed at the sampled DC(s) in order to achieve the audit objective.
- Proposed audit schedule

The audit plan is an important document setting the context for the certification of the Cloud Region, and shall be referenced from all Audit Reports based upon it.

11.2.2 Sampling Approach

This SAS-SM Methodology document does not specify the sampling rate, i.e. the proportion of samples that should be audited from within the population of DCs within a Cloud Region. This is decided by the Audit Team, in consultation with the Auditee and the GSMA. However, the sampling approach and rate will be influenced by the following factors:

- Information provided by the Auditee about the types of control and the level of consistency of controls at the DCs within the Cloud Region.
    - This may include the DC ownership model e.g. DC owned and operated directly by the Auditee, or operated by a third-party landlord in a single-tenant or multi-tenant arrangement.
- The professional judgement of the Auditors in designing an approach where samples can be assumed to be representative of all types and locations of business facilities and be sufficiently large enough to provide the Audit Team with the assurance that all relevant controls are being implemented as expected.
- The history of the Auditee’s participation in the scheme. Specifically:
    - The level of compliance and consistency previously observed at these (for Certification Renewal) or other DCs or Cloud Regions already SAS-SM certified that use the same control framework.
    - Audit team statements in past Audit Reports of DCs within the Cloud Region relating to how a sampling approach should be implemented in future.
- The number of standardised control models that are in place within the Cloud Region. If more than one standardised control model is in place, sufficient samples must be chosen to achieve the audit objectives for all DCs using each control model.

If there are no standardized or centralised GSMA SAS-SM processes/controls in place then all DCs and Support Sites must be audited to ensure controls are being met individually.

11.2.3 Observed Inconsistencies Amongst Samples

If during an Audit, the Audit Team observes that one or more sampled DCs do not implement the expected standardised procedures and controls, then the Audit Team will highlight this in the Audit Report. The Auditee will need to either:

- Acknowledge the different control framework in use at the noted DC(s) and have it/them audited separately (either individually or via a sampling approach under a separate control framework within the Cloud Region)
- Align the controls at the noted DC(s) with the standard framework, and submit them for Re-Audit.

The Audit Team may require that additional sample DCs be audited before the Cloud Region can be certified.

11.2.4 Auditing of Centralised Controls

When planning to audit a Cloud Region by using a sampling approach, the Audit Team should first work with the Auditee to identify all possible Auditee centralised policies, procedures and controls that are applicable within the DCOM scope of the CSP and that can be centrally audited once, and plan a time and location to perform this portion of the Audit. For example:

- Auditing corporate policies and procedures within an Auditee-provided meeting room at any location that is convenient for the Audit Team and necessary Auditee staff.
- Visiting the location(s) from where remote support services are provided to multiple DCs in order to audit the services within SAS-SM scope.

This approach reduces the proportion of requirements that need to be audited using a sampling approach.

11.3 During the Audit

When auditing SAS-SM requirements at a sample DC, the Audit Team needs to assess and report on:

6. The compliance of the controls in use with the SAS-SM requirements; and
7. The level of consistency of the controls with the standardised control framework.

(2) may be achieved through comparison with other sample DCs and/or the standardised control framework documentation that is audited centrally.

11.4 Changes Within Certified Cloud Regions

As outlined above, the basis for CSP certification is a Cloud Region. Major changes within a Cloud Region may occur during the period of certification. For example:

- Commissioning a new DC within the Cloud Region.
- Decommissing an existing DC within the Cloud Region
- Planned deviation of the controls within a DC from the standardised control model.

- Change to ownership model of a DC.
- Major changes to the physical or logical infrastructure within one or more DCs
- Significant changes to the standardised control model used within the Cloud Region
- Significant changes at Support Sites included within the scope of certification that are used by the certified Cloud Region.

If major changes affect SAS-SM certified services, they should be notified to GSMA as described in section 7. Changes will be reviewed by GSMA and the Auditing Companies, and may trigger the need for additional auditing to validate continued compliance of the Cloud Region with the SAS-SM requirements.

11.5 Renewal of Cloud Region Certification

The standard Duration of Certification for a Cloud Region is one year, starting from the date on which certification is awarded. In order to maintain SAS-SM certification, each Cloud Region must undergo a Renewal Audit process prior to the expiry of its existing certification. Planning for the Renewal Audit process involves:

- Consideration by the Audit Team of the previous Audit Report(s) with special attention to recommendations for future auditing and sampling approach contained in that/those Audit Report(s)
- Discussions between the Audit Team and the CSP on any major changes within the certified Cloud Region during the Certification Period.
- A decision by the Audit Team on how many and which DC(s) within the Cloud Region to sample, and which CSP services to sample.
    - The Audit Team should select sample DCs to audit in a non-predictable way.
- A review and update of the previous audit plan and sampling approach by the Audit Team following discussions with the CSP.

The standard Duration of Certification for initial certification for support sites used by the certified Cloud Region is one year. The standard Duration of Certification for Support Sites renewing certification is two years.

The standard Duration of Certification for Cloud Regions and Support Sites specified above will be applied in most cases. The Audit Team may, at its discretion, decide that certification should be for a shorter or a longer duration, as specified in section 4.3

11.6 SM Client Certification Dependency

If an SM service provider is using a CSP to host its solution, then end-to-end responsibility for SAS-SM compliance will be divided between the SM service provider and the CSP. Each Auditee will be audited against the requirements relevant to the activities that it performs. An example of the Audit scope for each Auditee type is provided in Annex E.

If a CSP is independently certified as described in this section 11, it may have multiple SM service providers as clients, fully and/or provisionally certified, using all or a subset of its SAS-SM certified services. Certification of each of these SM service providers will be dependent on continued certification of the CSP. The SAS-SM Audit of each SM service

provider will check that the CSP services within SAS-SM scope that are in use by that SM service provider are within the certified scope of the CSP.

A CSP may hold full SAS-SM certification while some of its SM service provider clients hold provisional SAS-SM certification for their scope of activities. The certification status of each Auditee will be specified on its SAS-SM certificate.

11.7 Example Sampling Approach

The following example is provided to aid understanding of the approach and processes described above. In practice, the approach that will be taken will vary depending on many factors, and be decided based on consultation between the Auditee, the Audit Team and the GSMA.

A CSP has 20 Cloud Regions worldwide, each with 10 DCs. Within each Cloud Region, the DCs use a standardised control model and there is a very high level of consistency between the controls deployed at all DCs within each Cloud Region. Between Cloud Regions, there is still a high level of consistency, but greater and varying levels of deviation from the standardised control model compared to within a Cloud Region due to various environmental factors (political, economic, social, legal).

The CSP wishes to host customer SM solutions within 3 Cloud Regions (e.g. Paris, New York, Berlin). The CSP wants to be able to host a specific SM solution within any DC within a specific certified Cloud Region (but not across regions), and manage its DC infrastructure from a single centralised remote management facility in Chicago.

11.7.1 Step 1: Certify First Cloud Region

The CSP initially applies for SAS-SM certification for the Paris Cloud Region. A sampling approach is used. Three out of ten DCs in the Cloud Region are successfully audited. The support services provided by the centralised remote management facility in Chicago are also successfully audited. The CSP's centralised corporate policies and procedures that specify the standardised control model and apply globally are also audited by the audit team while in Chicago. This leads to SAS-SM certification for the Paris Cloud Region.

The Paris Cloud Region SAS-SM certificate is issued, listing all DCs covered by the certification. The centralised remote management facility in Chicago is also specified as a support site for the Paris Cloud Region's certification.

11.7.2 Step 2: Certify Second Cloud Region

The CSP next applies for SAS-SM certification for the Berlin Cloud Region. The Audit Team considers that a sampling approach is also appropriate for this Cloud Region. The Berlin region's DCs use the same control framework as the Paris Cloud Region. Remote management is provided from the facility in Chicago in the same way as for the Paris Cloud Region. Based on this, and on the high level of SAS-SM compliance and consistency seen between sampled DCs during the Paris DC audits, the Audit Team is satisfied that auditing a sample of two out of ten DCs in the Berlin Cloud Region is sufficient to certify that Region.

The centralised remote management facility in Chicago is still within its Period of Certification, so it does not need to be audited again. The centralised remote management

facility in Chicago is also specified as a support site for the Berlin Cloud Region's certification.

11.7.3 Step 3: Certify Third Cloud Region

The CSP next applies for SAS-SM certification for the New York Cloud Region. A different control framework is in use compared to the Paris and Berlin Regions. Six of the DCs are owned and operated directly by the CSP. The remaining four DCs are owned and operated by a third-party landlord under a service agreement with the CSP.

The Audit Team decides to audit a sample of two DCs from each group (four in total). The Audit Team also visits the centralised remote management facility in Chicago to audit additional services that it provides to the New York Cloud Region. Additional control framework policies and procedures that apply for North American DCs are audited as part of one of the DC audits.

Significant inconsistencies in controls observed within one of the DC groups during the Audits leads to a non-compliant overall Audit Result. A subsequent Re-Audit of both DCs in the group takes place following re-alignment of controls. To provide increased assurance for the sampling approach within this group, the Audit Team requests that another sample DC within that group is audited. Following successful Audit Results, the New York Cloud Region gains SAS-SM certification.

11.7.4 Renewal of Certification

Annually thereafter, each Cloud Region hosts Renewal Audits at a sample of the DCs within each Region. The number of sampled DCs, and the DCs selected, are chosen by the Audit Team. Over time, a continued high level of SAS controls compliance and consistency leads to a reduction in the number of sample DCs that need to be audited annually to maintain certification for each Cloud Region.

A Renewal Audit of the CSP's centralised corporate policies and procedures is performed annually as part of one of the DC Audits. An Audit of the support services provided from Chicago is performed every two years.

11.7.5 Step 4: Expand and Redefine Cloud Region

Over time, the CSP seeks to expand its SAS-SM certification to cover all DCs in Europe. An approach similar to the above is followed per Cloud Region. A high level of consistency with a single control framework is applied by the CSP across all of the certified Cloud Regions, and validated by the SAS-SM audit teams throughout European DCs. By agreement between the CSP, audit teams and GSMA, the auditing, sampling and certification approach evolves and is optimised to define Europe as a single Cloud Region for the CSP.

Annex A Final Audit Report Structure

A.1 First Page:

- Headline: Security Accreditation Scheme for Subscription Manager Roles Qualification Report
- Scope of Audit:
  - SM-SR only
  - SM-DP only
  - SM-DP+ only
  - SM-DS only
  - Multiple SM roles (specify)
  - Data Centre Operations and Management
- Type of Audit (within SAS certification lifecycle):
  - “First-Audit” for the first Audit at the Site
  - “Renewal Audit” in the following years after a first Audit
  - “Re-Audit” because the result of the “First Audit” or the “Renewal Audit” was unsatisfactory
  - Dry Audit / Wet Audit, if applicable
  - Scope Extension Audit
- Type of Audit (if a provisional Audit):
  - Dry Audit
  - Wet Audit
- Name of the Auditee and location of the audited Site
- Date of the Audit
- Audit number
- Audit Team participants

A.2 Subsequent Pages:

- Audit Result and summary
- Auditors’ comments
- Actions required
- Appendix A – Detailed Results

Section	Result of Sub-Section	Auditor Remarks
Policy, Strategy and Documentation Result		
Strategy	C	**+** comment
Documentation	C	
Business continuity planning	NC	**-** comment

Section		Result of Sub-Section	Auditor Remarks
	Internal audit and control	C	
Organisation and Responsibility Result			
	Organisation	C	
	Responsibility	NC	
	Incident response and reporting	C	+ comment
	Contracts and Liabilities	NC	
Information Result			
	Classification	NC	- comment - comment
	Data and media handling	C-	
Personnel Security Result			
	Security in job description	C	Comment
	Recruitment screening	C	+ comment
	Acceptance of security rules	C	
	Incident response and reporting	C	
	Contract termination	C-	
Physical Security Result			
	Security plan	C	
	Physical protection	NC	
	Access control	NC	- comment
	Security staff	NC	
	Internal audit and control	C	+ comment
Certificate and Key Management Result			
	Classification	C	+ comment
	Roles and Responsibilities	C	
	Cryptographic key specification	C	
	Cryptographic key management	C	- comment
	Audit and accountability	NC	
	GSMA PKI Certificates	NC	- comment
Sensitive Process Data Management Result			
	Data transfer	C	
	Sensitive data access, storage and retention	C	
	Data Generation	C-	- comment
	Auditability and accountability	C	+ comment - comment
	Duplicate production	C	+ comment

Section	Result of Sub-Section	Auditor Remarks
Data integrity	C	+ comment
Internal audit and control	C	
SM-DP, SM-SR, SM-DP+ and SM-DS Service Management Result		
SM-DP, SM-SR, SM-DP+ and SM-DS service	NC	
Remote entity authentication	C	
Audit trails	C	
Computer and Network Management Result		
Policy	C	
Segregation of roles and responsibilities	NC	
Access control	C	
Network security	C	
Systems security	C	
Audit and monitoring	C	
External facilities management	C	- comment
Internal audit and control	C-	- comment
Software Development	C	

Table 9 – Final Audit Report Structure

- Appendix B: SAS Scoring Mechanism (that is, a copy of Table 2 of this document)
- Appendix C: Document Management

Annex B Standard Audit Agendas

Note This section assumes that DCOM is part of the scope of an SM service provider audit. If DCOM is not within audit scope (e.g. if the Auditee is using a CSP), a shorter audit duration and agenda may apply, and will be agreed with the Audit Team based on the in-scope activities that it performs.

B.1 First Dry and Renewal Audits

The standard durations of first Dry and Renewal Audits at Sites operating different services are as follows:

Services within Audit scope	Audit Duration (days)	Notes
Single function in-scope (e.g. M2M or Consumer)	4.5	M2M = SM-SR or SM-DP or both. Consumer = SM-DP+
Both functions in-scope (e.g. M2M and Consumer)	5	
Discovery Services (SM-DS), as standalone service.	4	Where SM-DS is included in an Audit of M2M and/or Consumer functions, the Dry Audit duration will be as specified for the M2M and/or Consumer functions (i.e. SM-DS additional review will not materially increase the Audit duration).

Table 10 – Standard Dry Audit Durations

The following agenda is proposed for first Dry and Renewal audits as a guide for Auditees. Non-standard dry and Renewal Audits (Re-Audits, Scope Extension audits, audits at Supporting Sites) may have shorter durations and a specific agenda will be developed by the Audit Team.

- The Dry Audit purpose is to determine the design of the governance and control environments;
- The Renewal Audit purpose is to:
    - Conduct a full review of all areas of the SAS-SM requirements, as it may be 1-2 years since the last Audit at the Site.
    - Identify and reassess areas where the design of controls has changed. Both the design and effectiveness will be reviewed.
    - Review the ongoing effectiveness of the governance and control identified during previous audits. During the Renewal Audits, a deep-dive approach is adopted.

Auditees should ensure that appropriate information has been prepared to facilitate the Audit Process.

For each part of the Audit the Auditors will normally expect to:

- Discuss the controls in place (documentation, processes, systems) with responsible personnel to understand the security management system. Discussions will typically take place within a meeting room environment.
- Review and validate controls on-site where the sensitive processes are carried out.

The standard Audit agenda for a Dry or Renewal Audit is split into half-day segments, which will normally be carried out in the sequence set out below.

Half-day Segment	Outline Agenda	Suggested Auditee Preparation
1	Company introduction and overview	Preparation of introductory presentation to include: • Company/corporate background and overview • Site introduction/overview • Production and audit scope
	Roles and responsibilities (FS.17 section 2) • Organisation • Responsibilities • Incident response and reporting • Contract liabilities	Organisation documentation and evidences: • Organisational chart/structure for the SAS-SM environment, covering security responsibilities. • Cross-functional security forum (security steering committee) meeting minutes and evidences of action items being tracked. • Incident response process • Details of the contractual liabilities and insurance cover for commercial partners
	Policy, strategy, and documentation (FS.17 section 1) • Policy • Strategy • Business continuity planning • Internal audit and control	Policy documentation and evidences: • Information security policy with confirmation of review on an annual basis • Employee acknowledgements of security policies and updates • Risk management policy and procedures • Risk assessments relating to SAS-SM • Risk registers • Business continuity policy and procedures • Business continuity plan relating to SAS-SM • Business continuity testing results • Internal audit methodology/policy • Internal audit and control annual plan • Audit reports • Recommendation action plans, progress tracking and reporting to management
2	Personnel security (FS.17 section 4) • Security in job description • Recruitment screening	• Security roles and responsibilities matrix and job descriptions • Human resources policy and procedures,

Half-day Segment	Outline Agenda	Suggested Auditee Preparation
	• Acceptance of security rules • Incident response and reporting • Contract termination	covering recruitment and pre-employment screening • Sample HR files • Completed confidentiality agreements • Information security training plan, training materials and records • Incident response and reporting including whistleblowing policy and procedures • Human resources policy and procedures, covering role changes and termination of employment
	Information (FS.17 section 3) • Classification • Data and media handling	• Information classification policy and procedures • Asset classification policy and procedures • Data access management policy and procedures • Media management policy and procedures
3	Physical Security (FS.17 section 5) • Security plan • Physical protection • Access control • Security staff • Internal audit and control	• Security plan, defining the layers of physical security and their classification level, together with the security controls in place and attack and escalation times • Floor plan of each building, in scope for the SAS-SM Audit, detailing the security controls in place • Physical access management policy and procedures including access right matrix • Visitor procedures and audit trails • Physical key procedures and audit trails • Physical security policy and procedures • Physical security staff training records Physical tour: • The Auditors will need to physically inspect the high security area (HSA) (as defined by the security plan), which hosts the SAS-SM infrastructure • The Auditors will need to physically inspect other areas supporting the Site's certification, such as: operations room, security control room, etc. • The Auditors will to need to see the configurations of the badge access system and CCTV system
4	Certificate and key management (FS.17 section 6)	• Information classification policy and procedures, which incorporates the

Half-day Segment	Outline Agenda	Suggested Auditee Preparation
	• Classification • Roles and responsibilities • Cryptographic key specifications • Cryptographic key management • Auditability and accountability • GSMA public key infrastructure (PKI) certificates	classification for keys. Roles and responsibilities documentation and evidences: • Key management organisation chart • Appointment forms/letters for key management personnel • Key management policy and procedures including : ○ HSM commissioning/decommissioning ○ HSM initialisation ○ Key lifecycles (key generation, exchange and storage, backup, destruction, key compromise) • Validation of HSM FIPS certification • Key management logs • Certificate management policy and procedures
5 and 6	Computer and network management (FS.17 section 10) • Policy • Segregation of roles and responsibilities • Access control • Network security • Systems security • Audit and monitoring • External facilities management • Internal audit and control • Software development	Policy documentation and evidences: • IT security policy and supporting procedures • Matrix of IT security roles and where segregation of roles is not possible details of the deployed compensating controls • Access control policy and procedures • Password policy • Remote access policy and procedures • Network topology and diagrams (physical, rack, logical, data flows) • Hardening standards and configuration settings for all systems and network devices • Change management policy and procedures • Vulnerability scanning and patch management policy and procedures plus report • Anti-virus policy and procedures • Unattended terminal / session timeout policy and procedures • Decommissioning/decertification policy and procedures for assets. • Backup, retention, and destruction policy and procedures. • Contracts for service providers, specifically governance (steering committees), SLAs

Half-day Segment	Outline Agenda	Suggested Auditee Preparation
		and KPIs • Supplier assurance policy and procedures and evidences from reviews • Secure software development lifecycle policy and methodology • eSIM platform development overview
7 and 8	SM-DP, SM-SR, SM-DP+ and SM-DS service management (FS.17 section 8): • SM-DP, SM-SR, SM-DP+ and SM-DS service • Remote entity authentication • Audit trails Sensitive process data management (FS.17 section 7) • Data transfer • Sensitive data access, storage and retention • Auditability and accountability • Duplicate production • Data integrity • Internal audit and control	• Platform documentation, including data flow diagrams detailing the end-to-end lifecycle of profile management and data transfers externally and between modules • Data backup, retention, and destruction policy and procedures. • Customer onboarding policy and procedures, including certificate enrolment. • Audit logs

Table 11– Standard SAS-SM Dry Audit Agenda

The Audit agenda may be adjusted based on production schedules or availability of personnel. The Auditors may also wish to change the amount of time spent on different aspects during the Audit itself. The typical Audit schedule for a Dry Audit is:

<table>
<tr><th></th><th colspan="5">Outline Agenda</th></tr>
<tr><th>Time</th><th>Day 1</th><th>Day 2</th><th>Day 3</th><th>Day 4</th><th>Day 5</th></tr>
<tr><td>09:00:09:30</td><td>Company Introduction and Overview</td><td rowspan="3">Physical Security (5)</td><td rowspan="8">Computer and Network Management (10)</td><td rowspan="5">SM-DP, SM-SR, SM-DP+, SM-DS Service Management (8) / Sensitive Data Management (7)
(M2M)</td><td rowspan="5">Report Preparation</td></tr>
<tr><td>09:30-10:00</td><td rowspan="2">Organisation and Responsibility (2)</td></tr>
<tr><td>10:00-10:30</td></tr>
<tr><td>10:30-11:00</td><td rowspan="3">Policy Strategy and Documentation (1)</td><td rowspan="2">Physical Tour (5)</td></tr>
<tr><td>11:00-11:30</td></tr>
<tr><td>11:30-12:00</td><td rowspan="2">Lunch</td><td rowspan="2">Lunch</td><td rowspan="2">Lunch</td><td rowspan="2">Lunch</td></tr>
<tr><td>12:00-12:30</td></tr>
<tr><td>12:30-13:00</td><td rowspan="3">Personnel Security (4)</td><td rowspan="3">Certificate and Key Management (6)</td><td rowspan="2">Lunch</td><td rowspan="5">SM-DP, SM-SR, SM-DP+, SM-DS Service Management (8) / Sensitive Data Management (7)
(Consumer)</td><td rowspan="3">Report Preparation</td></tr>
<tr><td>13:00-13:30</td></tr>
<tr><td>13:30-14:00</td><td rowspan="4">Logical Tour (10)</td></tr>
<tr><td>14:00-14:30</td><td rowspan="2">Information (3)</td><td rowspan="2">Dummy Key Ceremony (6)</td><td rowspan="2">Close Out Meeting</td></tr>
<tr><td>14:30-15:00</td></tr>
<tr><td>15:00-15:30</td><td rowspan="2">1st Day Verbal Feedback</td><td rowspan="2">2nd Day Verbal Feedback</td><td rowspan="2">3rd Day Verbal Feedback</td><td rowspan="2">4th Day Verbal Feedback</td><td rowspan="2">Signing Audit Report</td></tr>
<tr><td>15:30-16:00</td></tr>
<tr><td>16:00-16:30</td><td colspan="5">Administration time | Requirements review | Auditor time</td></tr>
</table>

Table 12 – Typical SAS-SM Dry Audit Schedule

B.2 Wet Audits

The typical duration of a Wet Audit is 2-days and should be regarded as a continuation of the Dry Audit, where:

- The Dry Audit purpose is to determine the design of the governance and control environments.
- The Wet Audit purpose is to determine the effectiveness of the controls over live production data.

In preparation for the Wet Audit, the Auditee should collate the following information:

- Details of any changes since the time of the Dry Audit:
    - Overview of customers and level of traffic
    - Changes to personnel
    - Other significant changes

The Wet Audit agenda is based on a review of live provisioning activities. The typical Audit agenda for a Wet Audit is:

Section	Outline Agenda
Introductory Session	• Review of remediation of N/Cs from Dry Audit • Changes to personnel • Major changes to policies and procedures • Major changes to network and systems • Major changes to the Site's physical security
6 – Certificate and key management	• Changes to key management documentation • Key management training evidences (if due, or if personnel have changed) • Evidence of re-screening of key management personnel (if due, or if personnel have changed) • Key ceremony evidence review (using updated keys imported since Dry Audit)
7 - Sensitive process data management	• Data transfer • Sensitive data access, storage and retention. • Data generation • Auditability and accountability • Duplicate production • Data integrity • Internal audit and control
8 - SM-DP, SM-SR, SM-DP+ and SM-DS Service Management	• SM-DP, SM-SR, SM-DP+ and SM-DS Service • Remote Entity Authentication • Audit trails
10 - Computer and network management	• 10.4.4 Network vulnerability management • 10.5.1.iv Change control • 10.5.1.v System vulnerability management

Section	Outline Agenda
	• 10.6 Audit and monitoring
Reporting	• Report preparation • Presentation of Audit Result

Table 13 – Wet Audit Outline Agenda

To enable the Wet Audit to be undertaken effectively and efficiently, Auditees should ensure that they have the following documents or evidence available for the start of the Audit:

- Previous GSMA SAS-SM Audit Report
- Evidence of any remediation arising from the previous GSMA SAS-SM Audit
- Records of changes to personnel
- Details of the major changes to policies and procedures
- Details of the major changes to network and systems
- Details of the major changes to the Site's physical security
- Key/certificate management procedures
- Key/certificate audit trails
- Key management personnel records
- Key and certificate architecture and lifecycle details
- HSM FIPS certificate and configuration settings
- Data transfers and protections (linked to data flows)
- Data retention and destruction procedures and audit trails
- List of computer and network management changes made
- Copies of vulnerability scanning and pen testing reports

The afternoon of day 2 will be reserved for the collation and presentation of the Wet Audit Result and Report.

Annex C Standard Document List

The Auditors will normally require access to the documents listed below during the Audit, where such documents are used by the Auditee and where the documents are relevant to the audit scope. Access to the current version of these documents must be available in to the Audit Team (hard copy, soft copy, or projected on screen).

Where such documents are not available in English translation services must be provided by the Auditee. Verbal translation in real time may be utilized where it is not practical to deploy an automated document translation tool.

C.1 General Information Required

- Subscription Management system description

  This should specify which subscription management roles that the entity provides at the Site. It shall include a high-level network diagram of the entity's networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should summarize all locations and key systems, and the boundaries between them and should include the following.

  - Connections into and out of the network including demarcation points between the subscription management environment and other networks/zones
  - Critical components within the subscription management environment, including systems, databases, firewalls, HSM and web servers, as applicable
  - Clear and separate identification of respective components for separate systems if the Site is operating multiple processes (e.g. SM-SR and SM-DP). Description of associated processes and responsibilities.

C.2 Documents List (per Requirements)

It is accepted that in some cases not all of these documents will be used by Auditees, or that one document may fulfil multiple functions.

Document	Requirement Refs.	Comment
Security policy	1.1.1	
Information security management system (ISMS) (typically those listed below, but this is not a definitive list)	1.1.2	
• Risk management policy	1.2.1, 5.1.1	
• Security strategy	1.2.1, 5.1.1	
• Business continuity policy	1.3.1	
• Asset management policy	2.2.3, 7.2.1	
• Incident management policy	2.3.1	
• Data classification policy	3.1.1	

Document	Requirement Refs.	Comment
• Access management policy	3.2.1, 5.3.1, 10.2.1, 10.4.2	
• Human resources policy	4.2.2, 4.3.3	
• Physical security policy	Section 5	Including Site classification and controls
• Cryptographic policy	Section 6	
• IT security policy	10.1.1	
• Password policy	10.3.3	
• Change management policy	10.4.3, 10.5.1	
• Vulnerability & patch management policy	10.4.4	
• Backup and recovery policy	10.5.2	
• 3rd Party management policy	2.4.1, 10.7.1	
• Secure software development life cycle SDLC policy	10.9.1	
Clear desk policy	3.2.2	
Whistleblowing policy	4.4.1	
Disciplinary policy	4.4.2	
Data retention & destruction policy	7.2.3, 7.4.1, 7.4.2	
Employees' declarations of acceptance of the information security policy	1.1.2, 4.3.1	Contract of employment; NDAs; declaration form (manual or electronic)
Risk management methodology / procedures	1.2.1	
Risk assessments	1.2.1, 5.1.1	
Risk registers	1.2.1	Relating to SAS-SM
Business continuity plan and disaster recovery plan	1.3.1	
Business impact assessments	1.3.1	
Business continuity planning and disaster recovery test plans and evidence of testing	1.3.1	
Internal checks and audit programme	1.4.1, 5.5.1, 7.7.1, 10.8.1	
List of key controls	1.4.1, 5.5.1, 7.7.1, 10.8.1	
Internal checks and audit methodology / procedures	1.4.1, 5.5.1, 7.7.1, 10.8.1	Detailing how each check/audit is performed, reporting requirements, and action tracking
Organisational Chart for SAS-SM, including security responsibilities	2.1.1	

Document	Requirement Refs.	Comment
Cross-function security forum meeting minutes / action tracking	2.1.2	Security steering committee
Defined security responsibilities (job descriptions)	2.2.1, 2.2.2, 4.1.1	List of duties
Asset inventories and audit trails	2.2.3, 7.2.1	Hardware, software, data
Incident response plans	2.3.1	
List of reported incidents	2.3.1	
Customer and supplier contracts	2.4.1	Liability clauses
Supplier insurance certificates	2.4.1	
Data classification and handling procedures	3.1.1	
Business processes relating to SAS-SM	3.1.1	
Network diagrams and data flow diagrams	3.1.1, 10.4.2	
Access management procedures	3.2.1, 5.3.1, 10.2.1, 10.3.2, 10.3.3, 10.3.4	Grant / amend / remove access Remote access Passwords
Roles and responsibilities matrices	3.2.1, 10.2.1, 10.3.2	Physical access, logical access.
Pre-employment / ongoing screening procedures and checklists	4.2.1	
Evidences of pre-employment and ongoing screening	4.2.1	
Human resources procedures and checklists	4.2.2, 4.3.3, 4.5.1	Appointments, change of jobs, terminations
Evidences of completed checklists	4.2.2, 4.3.3, 4.5.1	
Security awareness training procedures	4.3.3	
Evidence of security awareness training and course material	4.3.3	eLearning reports, attendance registers, etc.
Whistleblowing procedures	4.4.1	
Disciplinary procedures	4.4.2	
Grievance procedures	4.4.2	
Physical security procedures and operations manual	Section 5	
Site map with security controls	5.2.1, 5.2.2	
Visitor registration and logbooks	5.3.1	
Badge access system logs/audit trails	5.3.2, 10.3.1	
Key/certificate management procedures	6.1.1, 6.2.2, 6.4.2, 6.5.1, 6.6.1	

Document	Requirement Refs.	Comment
Key/certificate audit trails	6.1.1, 6.2.2, 6.4.2, 6.5.1, 6.6.1	Key management system /HSM logs, key/certificate inventories, key ceremony forms, safe inventories and in/out logbooks, etc.
Key management personnel records	6.2.1	Appointments, re-appointments, roles and responsibilities, declarations, training.
Key and certificate architecture and lifecycle details	6.3.1	
HSM FIPS certificate and configuration settings	6.4.3	FIPS 140-2 level 3 and configured to meet this level
Data transfers and protections (linked to data flows)	7.1.1	Protocols in use, encryption applied, etc.
Data retention and destruction procedures and audit trails	3.1.1, 7.2.3, 7.4.1, 7.4.2	
IT procedures and evidences	Section 10	
• Network device hardening and configurations	10.4.1, 10.4.3	Firewalls, IDS/IPS, switches
• System hardening and configurations	10.5.1	
• Vulnerability Management	10.4.4	Vulnerability scanning, penetration testing, anti-virus
• Change Management	10.4.3, 10.5.1	
• Backup and Restoration	10.5.2	
• Supplier management	10.7.1	Key external dependences
• Secure SDLC procedures	10.9.1	

All documents shall be used on-site during the Audit only; the Auditors shall not remove documents from the Site during the Audit and shall return all materials at the end of each Audit day.

Annex D Subscription Management Processing Audit

As part of the Audit of the Site's Subscription Management system and supporting processes it is preferred that Auditees prepare a SM-SR, SM-DP, SM-DP+ or SM-DS SAS-specific Audit scenario in advance of the Audit date. The Audit scenario may use test data (for a Dry Audit) or live data (for a full or Wet Audit). This document provides a suggested approach; the Auditee and Audit Team will agree the precise approach for each Audit.

This section is not applicable for Auditees being audited for DCOM only.

The purpose of these Audit scenarios is to allow the Audit to be carried out in a consistent way to consider:

For SM-SR

- SM-SR interaction with other roles in the embedded SIM ecosystem (ES1, ES3, ES4, ES5, ES7)
- Profile download and installation with SM-DP
- Platform and eUICC management operations
- Data protection
- Log files

For SM-DP

- SM-DP interaction with other roles in the embedded SIM ecosystem (ES2, ES3, ES8)
- Profile creation, download and installation with SM-SR
- Profile management operations
- Data protection
- Log files

For SM-DP+

- SM-DP+ interaction with other roles in the embedded SIM ecosystem (ES2+, ES8+/ES9+, ES12)
- Profile creation, download and installation
- Local profile management notification
- Data protection
- Log files

For SM-DS

- SM-DS interaction with other roles in the embedded SIM ecosystem (ES11, ES12, ES15)
- Event Registration
- Event Deletion
- Event Retrieval
- Data protection
- Log files

The Audit scenarios are intended to be transparent and will not deliberately involve any form of system intrusion.

Note: For the performance of an Audit scenario in a Dry Audit, interactions between entities can be simulated. For a wet or full Audit, evidence of interactions with other production entities must be available.

D.1 Before the Audit

D.1.1 Preparation

The Auditee should make arrangements to prepare the relevant other roles (e.g. EUM, MNO, SM-DP, SM-SR, SM-DP+, SM-DS, eUICC) that will needed by the Auditee to demonstrate its compliance with the Standard. The roles may be set up for simulation only (for Dry Audits). Existing connected entities used in production must be used for wet or full audits.

It is recognised that different configurations may be used for different roles. One should be selected that is representative of the current scope of activities at the Site. The Audit will focus on those security processes that are typically practiced and/or recommended by the Auditee to mobile operator customers. It is the Auditee*'s* responsibility to select appropriate, representative processes.

If more than one SM-SR, SM-DP, SM-DP+ or SM-DS solution is offered to customers (excluding any customer-specific solutions) then the number of different solutions and the nature of the differences should be confirmed with the Audit Team before setting up the Audit scenarios.

D.1.2 Certificate Enrolment

The Auditee should initiate its process for certificate enrolment, to include:

- Exchange of certificates

If the Certificate Issuer (CI) does not exist at the time of an Audit, the Auditee will need to self-certify or utilise the GSMA's test certificates.

D.1.3 Further Preparation for Audit (SM-SR)

D.1.3.1 eUICC Registration

Two input eUICC information files (eUICC-1 and eUICC-2) will be prepared by the Auditee and supplied to the Audit Team in advance of the Audit. See below for a description of how these files will be used. Test data will be used for a Dry Audit, and live data will be used for a wet or full Audit. The input eUICC information will be submitted electronically by the Auditee*'s* nominated mechanism or an alternative mechanism if set-up cost is implied.

The Auditee will prepare the input file which will include test data and structure to be used in the Audit and supply this in advance to the Audit Team.

D.1.3.2 Processing of eUICC Registration eUICC-1

Auditees should carry out eUICC registration for the first eUICC in advance of the Audit.

NOTE: Registration for eUICC-2 should not be processed before the Audit

D.1.3.3 Profiles

Personalised profiles for the targeted eUICCs will normally be created by the Auditee and made available to the Audit Team in advance of the Audit. The personalised profile will be submitted electronically by the Auditee's nominated SM-DP in the profile download and installation procedure or an alternative mechanism (for example, using test data) in the case of a Dry Audit.

D.1.3.4 Processing of Profile Download and Installation for eUICC-1

Auditees should carry out profile installation and download for a personalised profile for the first eUICC in advance of the Audit.

NOTE: Profile download and installation for eUICC-2 should not be processed before the Audit

D.1.3.5 Timescales

Exact timescales for the process will be agreed between the Audit Team and Auditee, but would typically involve:

Time before Audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-SR Audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	Auditee to maintain eUICC information available for review by the Audit Team Auditee to process first eUICC Registration and Profile Installation and Download Auditee to maintain output responses for first eUICC for review by the Audit Team.

D.1.4 During the Audit (SM-SR)

D.1.4.1 Review of Certificate Enrolment and Verification

The Audit Team will discuss and review the certificate enrolment and verification process with the Auditee, including reference to relevant logs and records.

D.1.4.2 Review of eUICC Registration Processing

The Audit Team will discuss and review the processing of registration of eUICC-1 with the Auditee, including reference to relevant logs and records.

D.1.4.3 Demonstration of Input eUICC 2 Processing

The Audit Team shall request that Auditees use input information for eUICC-2 to provide a live demonstration of the eUICC registration processing flow.

D.1.4.4 Review of Profile Download and Installation Processing

The Audit Team will discuss and review the processing of profile download for eUICC-1 with the Auditee, including reference to relevant logs and records.

D.1.4.5 Demonstration of Profile Download and Installation Processing

The Audit Team shall request that Auditees provide a live demonstration of the profile download and installation processing flow using a personalised profile for eUICC-2.

D.1.4.6 Demonstration of Enabling, Disabling and Deletion of Profile

The Audit Team shall request that Auditees provide a live demonstration of the profile enabling, disabling and deletion processing flow using a personalised profile for eUICC-1 or eUICC-2.

D.1.4.7 Demonstration of SM-SR Change

The Audit Team shall request that Auditees provide a detailed plan of the process to perform an SM-SR change.

D.1.5 Further Preparation for Audit (SM-DP)

D.1.5.1 Unpersonalised Profile Creation

The unpersonalised profile is created by the Auditee taking into account the MNO's profile description and the eUICC type. For the Dry Audit, a sample profile description and sample eUICC type chosen by the Auditee may be used.

D.1.5.2 Profile Ordering and Personalisation

Two operator input files (IF-1 and IF-2) containing for example, IMSI, ICCID, POL1, will be prepared by the Auditee and supplied to the Audit Team in advance of the Audit. See below for a description of how these files will be used. Test data (may be generated by the Audit Team in a format agreed with the Auditee) will be used for a Dry Audit, and live data will be used for a wet or full Audit. The input files will be submitted electronically by the Auditee*'s* nominated mechanism or an alternative mechanism if set up cost is implied.

The Auditee will prepare the input file which will include test data and structure to be used in the Audit and supply this in advance to the Audit Team*.*

The Auditee will use the input file IF-1 to personalise profiles in advance of the Audit, including generation of the operator keys (Ki), and use IF-2 to personalise profiles and generate operator keys (Ki) during the Audit.

D.1.5.3 Profile Download and Installation

The Auditee will ensure that there is a personalised profile ready to be downloaded and install.

D.1.5.4 Timescales

Exact timescales for the process will be agreed between the Audit Team and Auditee, but would typically involve:

Time Before Audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-DP Audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	Auditee to maintain profile ordering information available for review by the Audit Team Auditee to process the IF-1, profile creation and profile download and Installation. Auditee to maintain output responses for first IF-1 for review by the Audit Team.

D.1.6 During the Audit (SM-DP)

D.1.6.1 Review of Certificate Enrolment and Verification

The Audit Team will discuss and review the certificate enrolment and verification process with the Auditee, including reference to relevant logs and records.

D.1.6.2 Demonstration of Input IF-1 Processing

The Audit Team will review the data flow of the input file (IF-1) that has been received and processed and it will check the protection of the sensitive assets and logs involved in this process.

D.1.6.3 Review of Profile Download and Installation Processing

The Audit Team will discuss and review the processing of profile download for IF-1 with the Auditee, including reference to relevant logs and records.

D.1.6.4 Demonstration of Profile Download and Installation Processing

The Auditee may provide a live demonstration of the profile download and installation processing flow using a personalised profile for IF-2.

D.1.6.5 Demonstration of Enabling, Disabling and Deletion of Profile

The Auditee may provide a live demonstration of the profile enabling, disabling and deletion processing flow using a loaded profile.

D.1.7 Further Preparation for Audit (SM-DP+)

D.1.7.1 Unpersonalised Profile Creation

The unpersonalised profile is created by the Auditee taking into account the MNO's profile description and the eUICC type. For the Dry Audit, a sample profile description and sample eUICC type chosen by the Auditee may be used.

Note: this current process if done for SM-DP is to be applicable for SM-DP+.

D.1.7.2 Profile Ordering and Personalisation

Two operator input files (IF-1 and IF-2) containing for example, IMSI, ICCID will be prepared by the Auditee and supplied to the Audit Team in advance of the Audit. See below for a description of how these files will be used. Test data (may be generated by the Audit Team in a format agreed with the Auditee) will be used for a Dry Audit, and live data will be used for a wet or full Audit. The input files will be submitted electronically by the Auditee*'s* nominated mechanism or an alternative mechanism if set up cost is implied.

The Auditee will prepare the input file which will include test data and structure to be used in the Audit and supply this in advance to the Audit Team.

The Auditee will use the input file IF-1 to personalise profiles in advance of the Audit, including generation of the operator keys (Ki), and use IF-2 to personalise profiles and generate operator keys (Ki) during the Audit.

Note: this current process if done for SM-DP is to be applicable for SM-DP+.

D.1.7.3 Profile Download and Installation

The Auditee will ensure that there is a personalised profile ready to be downloaded and install.

D.1.7.4 Timescales

Exact timescales for the process will be agreed between the Audit Team and Auditee, but would typically involve:

Time Before Audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-DP+ Audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	Auditee to maintain profile ordering information available for review by the Audit Team Auditee to process the IF-1, profile creation and profile download and Installation. Auditee to maintain output responses for first IF-1 for review by the Audit Team.

D.1.8 During the Audit (SM-DP+)

D.1.8.1 Review of Certificate Enrolment and Verification

The Audit Team will discuss and review the certificate enrolment and verification process with the Auditee, including reference to relevant logs and records.

D.1.8.2 Demonstration of Input IF-1 Processing

The Audit Team will review the data flow of the input file (IF-1) that has been received and processed and it will check the protection of the sensitive assets and logs involved in this process.

D.1.8.3 Review of Profile Download and Installation Processing

The Audit Team will discuss and review the processing of profile download for IF-1 with the Auditee, including reference to relevant logs and records.

D.1.8.4 Demonstration of Profile Download and Installation Processing

The Auditee may provide a live demonstration of the profile download and installation processing flow using a personalised profile for IF-2.

The Auditee must demonstrate the download and installation on all 3 modes from the specification: (activation code, default SM-DP+, service discovery).

D.1.8.5 Demonstration of Enabling, Disabling and Deletion of Profile

The Auditee may provide a live demonstration of the profile enabling, disabling and deletion processing flow using a loaded profile via LPA and ensure the SM-DP+ gets the proper notification.

D.1.9 During the Audit (SM-DS)

D.1.9.1 Review of Certificate Enrolment and Verification

The Audit Team will discuss and review the certificate enrolment and verification process with the Auditee, including reference to relevant logs and records.

D.1.9.2 Demonstration of event registration and retrieval

The Auditee must demonstrate the download and installation in a service discovery mode including event registration, retrieval and deletion.

Note: the operation can use simulation for SM-DP+ and LPA.

D.2 After the Audit

Following the Audit the Audit Team will confirm that requests and records are no longer required and can be removed/archived as appropriate by the Auditee and deleted by the Audit Team.

Annex E Scope of Audit & Certification when using Cloud Service Provider

As described in section 11, it is possible that a SM service provider may outsource DCOM to a CSP. To provide assurance to other parties in the remote provisioning ecosystem that the overall solution is secure, the CSP Site or Cloud Region hosting the solution and the SM service provider managing the solution must be SAS-SM certified for the activities that they perform within the scope of the scheme.

The table embedded below indicates what is likely to be in scope for SAS-SM Audits at the CSP and the SM service provider. It should be considered as a starting point for discussion. The final scope of such Audits will depend on the activities performed by each Auditee, and shall be agreed between the Auditee, the Audit Team and the GSMA in advance of an Audit.



SAS_SM scope CSP v2.xlsx

NOTE Readers of the PDF version of this document can request this spreadsheet from sas@gsma.com

Annex F Document Management

F.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	13 October 2014	PSMC approved, first release	Arnaud Danree, Oberthur
2.0	13 May 2015	Transferred ownership to FASG	Arnaud Danree, Oberthur
2.1	16 May 2016	Clarify Dry Audit prerequisites. Update Provisional Certification duration to 9 months. Specify minimum certification duration for new Sites.	David Maxwell, GSMA
3.0	31 Mar 2017	Updated to reflect use of Consolidated Security Requirements (CSR) and Consolidated Security Guidelines (CSG) for SAS-SM, and extension of SAS-SM to support Audit and certification of SM-DP+ and SM-DS solution providers, plus associated cloud service providers.	RSPSAS Subgroup
4.0	16 Feb 2018	Remove Certification Body. Specify that Audit Team makes certification decision. Introduce Appeals Body. Revise cancellation policy. New section on maintaining SAS compliance.	David Maxwell, GSMA
4.1	18 Feb 2019	Clarify that Provisional Certification is a necessary step towards full SAS-SM certification. Minor general updates in other sections.	David Maxwell, GSMA
5.0	25 Jul 2019	Added process for auditing and certifying Supporting Sites	David Maxwell, GSMA
6.0	3 Apr 2020	Additions and changes to SM standard Audit agendas and required documents.	Neil Shepherd & Kent Quinlan, NCC Group David Maxwell, GSMA
6.1	1 Jul 2020	Editorial changes adding defined terms to support legal framework for SAS-SM.	David Maxwell, GSMA
7.0	20 Nov 2020	Introduce process for certification of Cloud Service Providers	David Maxwell, GSMA
7.1	21 Apr 2021	Added notifiable events for PKI certificate management.	David Maxwell, GSMA

F.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Group
Editor / Company	David Maxwell, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at sas@gsma.com. Your comments or suggestions and questions are always welcome.