

GSMA SAS Covid-19 Auditing and Certification Policy

Version 3.0

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 © 2020 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.

Antitrust Notice

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

Table of Contents

[1 Introduction 3](#_Toc53480808)

[1.1 Period of Validity 3](#_Toc53480809)

[1.2 Definitions 3](#_Toc53480810)

[1.3 References 3](#_Toc53480811)

[2 Overview 4](#_Toc53480812)

[3 SAS-UP 6](#_Toc53480813)

[3.1 Audit Process 6](#_Toc53480814)

[3.1.1 First or Dry Audit, Scope Extension 6](#_Toc53480815)

[3.1.2 Renewal and Wet Audits 6](#_Toc53480816)

[3.1.3 Temporary Extension 6](#_Toc53480817)

[3.1.4 Re-audits 7](#_Toc53480818)

[3.1.5 Major changes 7](#_Toc53480819)

[3.2 Applicable Audit methodology 7](#_Toc53480820)

[3.2.1 On-site Audit 7](#_Toc53480821)

[3.2.2 Hybrid audit 7](#_Toc53480822)

[3.2.3 Remote Audits 9](#_Toc53480823)

[4 SAS-SM 11](#_Toc53480824)

[4.1 First or Dry Audit, Scope Extension 11](#_Toc53480825)

[4.1.1 Remote Audit Considerations 11](#_Toc53480826)

[4.2 Renewal and Wet Audits 11](#_Toc53480827)

[4.2.1 Temporary Extension Assessment (TEA). 12](#_Toc53480828)

[4.2.2 Remote Audit 12](#_Toc53480829)

[4.3 Re-Audit 12](#_Toc53480830)

[4.4 Major Changes 12](#_Toc53480831)

[5 Next steps 12](#_Toc53480832)

[Annex A Document Management 13](#_Toc53480833)

[A.1 Document History 13](#_Toc53480834)

# Introduction

Audit travel and workplace attendance restrictions caused by the Covid-19 pandemic have made it impossible for SAS Audit Teams to visit and audit new and existing Sites participating in SAS. It is unclear how long these restrictions will last. In these circumstances, the GSMA, together with the SAS Auditing Companies, has introduced this temporary policy outlining alternative options, where possible, that sites can use to gain or maintain SAS certification. These include the option of conducting Remote Audits in certain circumstances where this can provide a sufficient level of assurance to enable SAS certification of those Sites.

This document is subject to change in accordance with the evolution of Covid-19-related controls and restrictions. Auditees are recommended to check with GSMA to ensure that they have the latest version.

## Period of Validity

This temporary policy applies while Covid-19 related disruption to normal on-site SAS Audits exists, at the sole discretion of the GSMA. Disruption may occur due to:

* GSMA, Auditee and Auditing Company travel and employee protection policies related to Covid-19.
* Travel and entry restrictions in the country of the Site to be audited that would apply to the SAS Auditors.
* Quarantine restrictions in the country of the Site to be audited and/or the Auditors (that would apply on return from the Audit).
* Onward international travel restrictions that may apply to Auditors following a visit to the country of a Site to be audited.
* Delays in performing a backlog of on-site SAS Audits after other restrictions are lifted.

The possibility of performing a normal on-site audit shall be evaluated separately for each audit request. An on-site audit shall remain as the preferred approach in SAS even while this policy exists, and shall be conducted if feasible, considering the factors above.

## Definitions

Definitions are as specified in [1], [2], [3], [4], and [5].

## References

| **Ref** | **Doc Number** | **Title** |
| --- | --- | --- |
|  | PRD FS.05 | GSMA SAS Methodology for UICC Production, latest version available at [www.gsma.com/sas](http://www.gsma.com/sas) |
|  | PRD FS.05C19 | SAS-UP Covid-19 Methodology Variations |
|  | PRD FS.09 | GSMA SAS Methodology for Subscription Manager Roles, latest version available at [www.gsma.com/sas](http://www.gsma.com/sas) |
|  | PRD FS.09C19 | SAS-SM Covid-19 Methodology Variations |
|  | SAS-UP Scope Definitions | SAS for UICC Production (SAS-UP) Scope Definitions, latest version available at [www.gsma.com/sas](http://www.gsma.com/sas) |

# Overview

Table 1 summarises the options available for different scenarios under SAS-UP and SAS-SM. The following sections provide more details on each option.

| Site seeking | Policy & Approach | |
| --- | --- | --- |
| SAS for UICC Production (SAS-UP) | SAS for Subscription Management (SAS-SM) |
| First or Dry Audit, or Scope Extension | Certification based on a Remote Audit may be possible for some sites, depending on their activities, the Audit type, additional criteria and meeting certain pre-requisites, as indicated in section 3.1.  Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect.  Sites that are not eligible for a Remote Audit should register their interest with the GSMA, so that scheduling of an On-site Audit can take place once conditions allow. | Certification based on a Remote Audit is normally possible, as many of the controls relate to logical security and it is possible to assess them remotely.  Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect. |
| Renewal Audit or Wet Audit | Options:   * A Renewal Audit or Wet Audit performed remotely may be possible for some sites, depending on their activities, the Audit type, additional criteria and meeting certain pre-requisites, as indicated in section 3.1. Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect.   OR (Auditee choice),   * Temporary (6 month) extension of certification is possible following Temporary Extension Assessment (TEA). If Remote Audit is possible, then Site is limited to maximum one temporary extension.   OR (Auditee choice),   * (Renewal audit only): Hybrid renewal approach involving 2-step Audit process (Off-site review, On-site assessment). This option is available when an On-site Audit is possible now or forecast as possible within 4 months of the completion of the Off-site review.   Sites that are not eligible for a Remote Renewal Audit or Wet Audit should register their interest with the GSMA, so that scheduling of an On-site Audit can take place once conditions allow. | Options:   * Certification based on a Remote Audit is possible, on condition that an On-site Audit takes place to validate controls once this is possible. Certificate will have a note to this effect.   OR (Auditee choice),   * One Temporary (6 month) Extension of certification is possible following a Temporary Extension Assessment (TEA). |
| Re-Audit | Normal Off-site assessment remains valid if previously specified.  Where On-site Re-Audit was previously specified, a Remote Audit may be possible (see section 3.1) or a Hybrid audit involving a 2-step Audit Process (Off-site review, On-site assessment) can be used for Re-Audit. | Normal Off-site assessment remains valid if previously specified.  Where On-site Repeat Audit was previously specified, a Remote Audit approach may be possible, on condition that an On-site Audit takes place once possible to validate controls. Certificate will have a note to this effect |
| Major change at certified site | SAS certified Sites planning major changes to the certified controls should notify the GSMA as described in section 7 of FS.05 (for SAS-UP) and FS.09 (for SAS-SM), so that an Auditor assessment can be made regarding the need for auditing the planned changes and the options available for this. | |

1. - Summary of Auditing and Certification Options

# SAS-UP

For SAS-UP this document describes the types of Audit / audit interactions (the Audit Process in 3.1) and the applicable methodology(ies) (in 3.2).

## Audit Process

### First or Dry Audit, Scope Extension

A Site seeking initial certification via a first or Dry Audit, or a Scope Extension to existing certification, should submit an Audit application to the GSMA with details of:

* Its requested scope of certification.
* Any of the components (key management systems, data generation mechanisms, production asset control systems etc.) that form part of the activities for the Site for which certification is being sought that have previously been deployed and proven at other SAS-UP Sites.
* Its ability to comply with the requirements for an Off-site Audit as defined in FS.05C19 “SAS-UP Covid-19 Methodology Variations” [2]

The GSMA and the SAS-UP Auditors may request additional information, and will assess the Site’s eligibility for a Remote Audit in accordance with 3.2.3.

If the Site is not eligible for a Remote Audit, GSMA will record the request and monitor Covid-19-related restrictions, so that scheduling of an On-site Audit can take place once conditions allow.

### Renewal and Wet Audits

Sites seeking a Renewal or Wet Audit may apply for:

* A Temporary Extension.

Or

* A Remote Audit if this option is available to them (in accordance with 3.2.3 and following consultation with GSMA) and they are able to comply with the requirements defined in FS.05C19 [2].

Sites seeking a Renewal Audit may also request a Hybrid Renewal Audit.

### Temporary Extension

Temporary Extension of existing certification for 6 months, is available to Sites with existing SAS-UP Provisional or Full Certification.

* Sites ineligible for a Remote Audit may receive multiple Temporary Extensions.
* After 30 Sep 2020, sites eligible for a Remote Audit that have not previously received a Temporary Extension (TE) may receive one TE only. After that date, sites that have already received a TE may receive one additional TE only.

Each Temporary Extension is subject to a Temporary Extension Assessment (TEA). For details, see document FS.05C19 [2].

### Re-audits

In many cases and according to the SAS-UP Methodology [1], Re-Audits are performed via Off-site review of improvement evidence, with no On-site visit needed. This approach remains valid during the Covid-19 period of disruption.

In some cases, the outcome of a previous Audit may have specified that an On-site Audit should take place to assess the improvements made to Auditee controls judged as non-compliant, due to the nature and/or volume of the non-compliances. During the period of Covid-19 related disruption, it may be possible for such Re-Audits to be carried out Off-site (in accordance with 3.2.3 and following consultation with GSMA). In addition, a Hybrid Audit approach is available as an option to the Site, to reduce the On-site Re-Audit duration. For details, see document FS.05C19 [2].

### Major changes

SAS certified Sites planning major changes to their certified controls, including Sites that want / need to transfer certified activities to a new physical location, should notify the GSMA in advance as described in section 7 of the applicable SAS Methodology (FS.05/FS.09), so that an Auditor assessment can be made regarding the need for auditing the planned changes and the options available for this. Sites should particularly avoid making changes during the Covid-19 disruption period without notifying the GSMA in advance as this may limit their eligibility to receive a Temporary Extension of Certification.

## Applicable Audit methodology

### On-site Audit

**Applies to:** All audit types

On-site Audits remain the preferred option for certification. Where possible, Auditees will be offered the option for an On-site audit in-line with the SAS-UP Methodology document. The ability to conduct an Off-site Audit will, however, be affected by the issues described in 1.1 and may result in a delay to the certification process.

### Hybrid audit

**Applies to:** Renewal audits  
Re-audits

A hybrid approach allows Sites the opportunity to complete a review of documentation and evidence during an Off-site phase. An On-site validation of controls will still be required to complete certification renewal, however the duration of this period on-site will be reduced compared with the Conventional Audit Process. This Hybrid Audit option for Renewal Audits should be pursued when the interval between the Off-site and On-site stages is not expected to exceed 4 months. This approach has the following benefits:

* Minimises time spent on-site by Audit Team, reducing site effort and risk in complying with Covid-19 workplace restrictions.
* Provides a period between Off-site and On-site phases during which the Site may resolve non-compliances highlighted during the Off-site phase.
* Allows audit teams to conduct the anticipated backlog of SAS Audits more quickly once travel restrictions are lifted.

For details, see document FS.05C19 [2].

### Remote Audits

**Applies to:** Eligibility for remote audits will be determined based on Site type and activity as specified in Table 2, with reference to the colour coding in Table 3. Activity definitions are provided in [5].

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Activity** | | |  |  |
|  |  |  | **UICC data gen & perso only1** | **eUICC perso2** | **eUICC data gen + PKI3** | **Notes** | |
| **Site type** | A (New Site) | (i) New activity |  |  |  | Brand new Sites with no track record / history of certification | |
| (ii) Activity certified elsewhere |  |  |  |
| B (Scope Extension) | (i) New activity |  |  |  | Existing certified Sites with track record / history of certification for some activities, but wish to extend the scope of certification to include new ones | |
| (ii) Activity certified elsewhere |  |  |  |
| C (Site Relocation) | N/A |  |  |  | Existing certified Sites that want / need to transfer certified activities to a new physical location | |
| D (Major change) |  |  |  | Existing certified Sites undergoing a major change to how existing activities are performed or controlled | |
| E (Re-audit) |  |  |  | Previously assessed (pre-Covid-19) as needing an On-site Re-audit to demonstrate improved controls. | |
| F (Renewal / wet) |  |  |  | Sites requiring a Renewal or Wet Audit (no changes to how activities are performed or controlled) | |
| 1 Generation of data for UICC personalisation and/or UICC personalisation only  2 eUICC personalisation  3 Generation of data for eUICC personalisation; Management of PKI certificates |  |  |  |  |  | (i) | Activity completely new to Auditee and unproven within SAS-UP. |
|  |  |  |  |  |  | (ii) | Activity utilising existing components (equipment, procedures etc.) previously deployed and proven at other SAS-UP Sites. |

1. – SAS-UP Remote Audit Eligibility

|  |  |
| --- | --- |
| **Colour** | **Remote Audit Eligibility** |
|  | Off-site audit process not considered acceptable. Certification only possible with On-site Audit. |
|  | Off-site Audit process and certification (with caveats clarifying lack of On-site Audit) may be possible, subject to agreement of GSMA and SAS-UP Auditors, considering:  - Level of certified component/activity re-use  - Scope of activities, and   - History of Audit performance at Auditee Site and/or at other certified Sites using components planned for re-use at Auditee Site. Prerequisites below must also be satisfied. |
|  | Off-site Audit process and certification (with caveats clarifying lack of On-site Audit) normally possible, subject to agreement of GSMA and SAS-UP Auditors. Site must satisfy Off-site audit prerequisites e.g.:  - Additional application information (for new sites) & pre-audit planning call(s) as necessary to allow assessment of whether off-site audit is feasible  - Provision of tools to facilitate off-site audit (video conference service, secure document sharing repository, live streaming for physical evidence review, translation if needed etc.). Full details in FS.05C19 [2]. |

1. – Key to Remote Audit Eligibility Matrix

The Remote Audit considerations in section 4.1.1 are applicable to SAS-UP. More details are available in document FS.05C19 [2].

Sites requesting an Off-site Audit will be required to confirm their ability to satisfy the requirements defined in FS.05C19 for facilitation of the audit process. Sites unable or unwilling to meet these requirements will be ineligible for the Off-site Audit process and will need to revert to a conventional on-site audit.

# SAS-SM

Core controls for SAS-SM Audits relate to the logical security of the environment and SM platforms. GSMA and SAS-SM Auditing Companies therefore consider it possible to carry out Remote Audits to achieve a minimum satisfactory level of SAS-SM assurance, as a temporary measure while the current restrictions are in place, and subject to a case-by-case- assessment.

Remote Audits will provide less assurance than on-site Audits, therefore:

* Their availability is not planned as a permanent change to SAS-SM.
* This option of remote auditing will be withdrawn by GSMA when no longer considered to be necessary.
* SAS-SM certificates issued based on Remote Audits will always contain a note to indicate that an on-site Audit has not been completed.

## First or Dry Audit, Scope Extension

Sites seeking initial SAS-SM certification via a first or Dry Audit, or a Scope Extension to existing certification may request a Remote Audit, subject to their confirmation that they can satisfy the Remote Audit mandatory pre-requisites specified in document “FS.09C19 SAS-SM Covid-19 Methodology Variations”.

### Remote Audit Considerations

There are several differences in approach between a standard Audit and a Remote Audit:

* A Remote Audit may take longer than a standard Audit, and therefore have higher Audit fees compared to an on-site Audit. This chargeable duration and cost will be determined during the pre-audit planning and preparation.
* A Remote Audit will require Audit planning and preparation sessions between the Auditee and the Audit Team to exchange preliminary information about the Site to be Audited, the Audit scope, duration, schedule and costs, Audit Team expectations etc.
* A Remote Audit requires the advance sharing of documentation within Audit scope with the Audit Team for assessment.
* A Remote Audit will normally require a further chargeable on-site follow-up visit after the Covid-19 restrictions have been lifted to confirm compliance against certain requirements.
* Following a compliant Remote Audit outcome, the resulting Certificate will be marked to differentiate to interested parties that this Certificate was not awarded following a standard on-site Audit (until after the on-site follow-up visit).
* A number of other logistical challenges related with remote meetings will need to be agreed between the Auditee and Auditors.

More details are available in document “FS.09C19 SAS-SM Covid-19 Methodology Variations” [4].

## Renewal and Wet Audits

Sites seeking a Renewal or Wet audit may avail of one or both of the options below.

### Temporary Extension Assessment (TEA).

A single Temporary Extension of Certification for 6 months is available to Sites with existing SAS-SM Provisional or Full Certification that either:

* Would normally require a Renewal Audit to maintain existing certification
* Would normally require a Wet Audit to move from Provisional to Full Certification

The Temporary Extension is subject to a Temporary Extension Assessment (TEA). For details, see FS.09C19 [4]. Prior to the end of the Temporary Extension period, the site must undergo a successful Remote Audit in order to maintain certification.

### Remote Audit

As per section 4.1.

## Re-Audit

In many cases and according to the SAS-SM Methodology [3], Re-Audits are performed via off-site review of improvement evidence, with no on-site visit needed. This approach remains valid during the Covid-19 period of disruption.

In some cases, the outcome of a previous (pre-Covid-19) Audit may have recommended that an on-site Re-Audit should take place to assess the improvements made to sections judged as non-compliant, due to the nature and/or volume of the non-compliances. In light of the Covid-19 travel restrictions, it may be possible to perform the Re-Audit remotely to gain a level of assurance enabling certification to be awarded, on condition of a follow-up on-site visit when possible. More details are available in FS.09C19 [4].

## Major Changes

As per section 3.1.5.

# Next steps

Please contact [sas@gsma.com](mailto:sas@gsma.com) with any questions or to discuss or apply for any of the auditing and/or certification options described above.

1. Document Management
   1. Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Brief Description of Change | Editor |
| 1.0 | 27 May 2020 | First released version as remote audit policy and process only. | GSMA, SRC & NCC Group |
| 2.0 | 23 Jun 2020 | Extended to cover all options available per audit type for SAS-UP and SAS-SM. Moved processes into separate documents. | David Maxwell, GSMA |
| 2.1 | 1 Jul 2020 | Updates following legal review | David Maxwell, GSMA |
| 3.0 | 9 Oct 2020 | Introduced SAS-UP remote audits.  Updated SAS-UP references to point to a single SAS-UP methodology variation. Introduced limitation on SAS-UP temporary extension availability. | David Maxwell, GSMA |