SAS-UP Covid-19 Methodology Variations
Version 1.1
18 April 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

As a global pandemic, Covid-19 has seen the introduction of unprecedented restrictions on national, regional and international travel along with periods of domestic 'lockdown' and quarantining requirements. These restrictions have a fundamental impact on the normal Security Accreditation Scheme for UICC Production (SAS-UP) Audit Process which is reliant on the Audit Team conducting on-site Audits at Auditee's Sites.

Due to the potential for different levels of restriction to be in effect for an unpredictable, extended period, alternative auditing arrangements must be considered to optimise the operation and integrity of SAS-UP. The solutions available for different certification scenarios are outlined in the GSMA SAS Covid-19 Auditing and Certification Policy [2].

This document ("Methodology Variation") describes variations to the GSMA's published Methodology FS.05 SAS UICC Production – Methodology v9.0 [1] for certification of Sites under SAS-UP, implemented to increase flexibility for the scheme during the period for which Covid-19 restrictions affect the Audit Process, Auditors and Auditees.

This document is intended to complement [1] by presenting variations to section 2 "Audit Process" of that document. Nothing in this document is intended to change the basic principles of the SAS-UP certification process. Certification of Sites will continue to be carried out in accordance with [1] where practically possible.

This document will be subject to periodic review by the GSMA and will be withdrawn from use when it is no longer considered to be necessary. Variations proposed within this document are not planned to be permanent changes to SAS-UP.

1.2 Scope

The scope of this document covers:

- A process for approval of the Temporary Extension of a SAS-UP certification for existing certified sites based on a review of key documents and indicators carried out by the Audit team – the Temporary Extension Assessment (TEA).
    - The process will be applied to any Temporary Extension to an SAS-UP certificate from the implementation date, whatever the scope of the site's certification.
- A process to conduct SAS-UP Renewal and Re-Audits using a hybrid approach involving review of some elements off-site remotely by the Audit Team as a precursor to completing the process at a shorter-duration on-site Audit – the Hybrid Audit (HA).
    - The process can be considered for Renewal or Repeat Audit (Re-Audit) of any SAS-UP Site from the implementation date of this variation, whatever the scope of the Site's certification.
- A process to conduct SAS-UP Audits of eligible Sites and activities (based on eligibility as specified in [2]) using a Remote Audit Process

1.3 Intended audience

- Participants in the SAS-UP certification scheme.
- SAS-UP Auditors
- SAS Subgroup members.

1.4 Definitions

Term	Description
Conventional Audit Process	Process for an Auditee to achieve certification based on an audit carried out on-site under the FS.05 Audit Methodology [1]
Hybrid Audit Process	As defined in section 4
Live	As defined in D.1.2
Off-line	As defined in D.1.2
Off-site	A process of compliance assessment carried out by the Audit Team without attending the Audit Site based on review of evidence. May be applied to an audit or to assessment of evidence. The review process may be carried out off-line, on-line or live.
On-line	As defined in D.1.2
On-site	A process of compliance assessment carried out by the Audit Team in person at the Audit Site. May be applied to an audit or to assessment of evidence.
Remote Audit Process	Process for an Auditee to achieve certification based on an initial off-site audit, as defined in section 5
Temporary Extension and TEA Process	As defined in section 2

Additional definitions are as specified in FS.05 [1].

2 Abbreviations

Abbreviations are as specified in FS.05 [1].

2.1 References

Ref	Doc Number	Title
[1]	PRD FS.05	GSMA SAS Methodology for UICC Production, latest version available at www.gsma.com/sas
[2]	N/A	GSMA SAS Covid-19 Auditing and Certification Policy
[3]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at www.gsma.com/sas

3 Temporary Extension Process

This Temporary Extension process allows Auditees to apply for an extension of an existing SAS-UP certificate for a period of 6 months where a conventional Renewal Audit cannot be executed due to Covid-19 restrictions. Temporary Extensions will be granted by the Audit Management, but be subject to a TEA process (TEA Process) carried out by the Audit Team.

3.1 Temporary Extension request

Auditees should formally request an extension from the Audit Management under the TEA Process for each period of extension required to the site's current SAS-UP certificate.

Each period of extension will be limited to 6 months from the date of expiry of the Site's current SAS-UP Certificate. The Audit management may issue a reminder to the Auditee as the expiry date of the current Certificate approaches; however the Auditee should not rely on this happening.

Requests should normally be made a minimum of 2 months before the expiry of the existing SAS-UP Certificate.

Requests will be logged by the Audit Management. Any necessary administrative processes (e.g. contract renewal) will be triggered under the control of the Audit Management on receipt of the request.

3.2 TEA Process

The TEA Process is normally expected to take approximately 6 hours of time per Auditor, split into 5 core phases:

3.2.1 Step 1 - TEA Preparation (0.5hrs)

Requests will be sent to the Audit Team by the Audit Management. The Audit Team will liaise directly with the Auditee's nominated contact person to conduct the TEA.

A schedule will be agreed between the Audit Team and Auditee for execution of the TEA. The Audit team will notify the Audit Management of the planned timescales for completion of the process.

An information request will be prepared by the Audit Team and submitted to the officially nominated Auditee representative. The information request will vary according to the scope of activities at the most recent Audit and the associated Audit Report. A sample information request is included in Annex A.

3.2.2 Step 2 - TEA Presentation (1hr)

The Auditee presents its response to the information request as part of an interactive video conference presentation.

3.2.3 Step 3 - TEA Review (2hrs)

The Audit Team will carry out a review of the information provided by the Auditee to identify any areas of potential concern or for further discussion.

In some cases the Audit Team may make one or more follow-up information requests where specific detail or evidence is required.

3.2.4 Step 4 - TEA Discussion (1.5hrs)

The Audit Team will schedule a discussion with the Auditee for the purpose of discussing the Audit Team's observations and any open points. The discussion will normally be carried out using an on-line video-conferencing facility to enable an interactive discussion and presentation of any materials relevant to the discussions. Where it is necessary to share any information considered commercially sensitive as part of the approval process this will be presented during the discussion.

3.2.5 Step 5 - TEA Reporting (1hr)

A formal report will not be prepared and submitted as part of the TEA Process. However, the Audit Team will prepare and submit a TEA approval statement to the Audit management, structured similarly to that in Annex B (TEA Approval Statement).

3.2.6 TEA Reassessment (varies)

If any areas of concern are identified during the TEA then the Audit Team may record this in a first version of the TEA Approval Statement as areas where the site has not demonstrated an appropriate level of compliance with the requirements of SAS-UP. Where non-compliant assessments are made, a Temporary Extension will not be issued until the Auditee provides evidence of appropriate improvements.

Evidence of improvements in the areas assessed as non-compliant must be submitted to, and reviewed by, the Audit Team following implementation of the improvements by the Auditee. The Audit team will prepare an updated version of the Approval Statement based on their review of the evidence provided and submit this to the Audit Management.

A Temporary Extension will only be issued once the TEA Approval Statement indicates that the auditors have accepted all of the improvements to the Site's controls made by the Auditee.

It is possible that the Audit team may determine during the TEA that major changes to SAS-UP certified controls at the Site have taken place at the site that have not previously been notified by the Auditee to the Audit Management . If such changes would normally require additional Auditing (beyond the scope and depth of the TEA process) prior to the Audit Management issuing a SAS-UP Certificate, the Temporary Extension may not be granted until such additional auditing takes place.

3.3 Temporary Extension Issue

Following submission of the TEA Approval Statement, the Audit Management checks the contents to confirm that the approval has been carried out in accordance with this Methodology Variation and meets GSMA quality requirements.

In the event of a satisfactory approval the Audit Management issues a Certificate to the Auditee within 10 business days of submission of the TEA Approval Statement.

3.4 Notification and Publication of Certification

The GSMA will publish Temporary Extension Certificates on the SAS website in accordance with section 2.6 of the FS.05 Methodology [1], with an explanation of the TEA Process.

3.5 Language

The language used in the course of the approval process for all SAS documentation and presentations is English. The TEA documentation requested, or their equivalents, should be available to the Auditors in English for the purpose of the approval review. Other documents may be in a language other than English but translation facilities should be available during the approval discussion. Where it is likely to be difficult to conduct approval discussions with personnel in English, Auditees should arrange for one or more translators to be available to the Audit Team.

3.6 TEA Fees

The TEA fees (“Fees”) for the TEA will normally be based on a fixed 0.75-day auditing duration, at the daily auditing rate specified in the SAS-UP Service Agreement between the GSMA and the Auditee The Fees will be payable by the Auditee to the GSMA. Save in the cases set out below, any expenses and additional costs are not expected to be incurred as part of the TEA process.

Where necessary, additional charges may be levied against the Auditee if:

- The process of obtaining information from the Auditee is unduly longer than normally expected due to, e.g.:
    - Delays due to language or translation
    - Failure to provide the requested information.
    - Significant changes at the site that have not previously been notified to the GSMA that necessitate additional effort to evaluate.
- Additional review time is required to review evidence of improvements identified as necessary during the initial review process.

4 Hybrid Audit Process

The Hybrid Audit Process allows an Audit to be carried out in two parts:

- An Off-site review of documentation and evidence carried out by the Audit Team remotely in conjunction with the Auditee through a number of pre-planned interactive video-conferencing sessions. The Off-site review will aim to address aspects of the Audit process normally conducted within a meeting room environment at the Site.
- An On-site validation of controls carried out by the Audit Team to complete the Audit Process. The On-site validation will aim to address aspects of the Audit Process normally conducted within the operational areas of the Site through a combination of:
    - Testing and validation of controls for those requirements initially assessed in the Off-site Audit Process.
    - Full auditing for parts of the Audit that cannot be assessed Off-site.

4.1 Hybrid Audit Request and Planning

4.1.1 Request

Auditees will continue to make requests to the Audit Management for the Audit, in accordance with the FS.05 Methodology [1].

Auditees will be required to confirm the scope of the SAS-UP certification required at the time of the request to facilitate planning.

4.1.2 Scheduling

The Audit Management will maintain a register of Sites awaiting an Audit. The register will be reviewed periodically in conjunction with the Audit Team to consider:

- Feasibility of travel under Covid-19 restrictions in effect.
- Scheduling of Audits back-to-back wherever possible.

Audits will be scheduled in conjunction with Auditees based on this assessment of feasibility and optimisation of the scheduling process.

Audits may need to be rescheduled at relatively short notice where Covid-19 restrictions change.

Where Audits cannot be completed, Auditees will normally be offered the option of a Temporary Extension to certification, as described in section 4.5.

4.2 Planning

8-16 weeks before the scheduled Audit date the Audit Team will make contact with the Auditee to make:

- Detailed plans for the Off-site review.
- Initial plans for the On-site review.

As part of the planning process the Audit Team will confirm the planned duration for both elements.

Planning for the duration of the On-site and Off-site elements will be carried out based on the agreed scope of the Audit, as notified to the Audit Management in the Audit request. The durations of the two elements will normally be based on the sample agendas included in Annex C of this document, but may be varied for individual Audits based on the Audit Team's knowledge and experience of the Auditee and any initial discussions at the planning stage.

4.3 Hybrid Audit Preparation (Off-Site)

4.3.1 Audit Agenda

A sample agenda is included at Annex C for a Renewal Audit with typical scope (equivalent to a 4-day on-site Audit).

Agendas for:

- Renewal Audits with non-standard scope or duration
- Repeat Audits

Will be agreed on a case-by-case basis with each Auditee based on the appropriate scope.

4.3.2 Audit Performance

The objective of the Off-site review is to collect and analyse information to:

- Enable the Audit Team to understand key elements of the security management system.
- Perform an initial assessment of compliance in some areas.
- Identify specific validation / testing to be carried out during the On-site Audit to complete the assessment in all areas.

Some parts of the Audit Process will be strongly linked to operational activities (e.g. production processes; physical security) and will not normally be considered in detail as part of the Off-site review.

The Audit Team assesses performance according to the agreed agenda by 3 main methods:

- Independent document review
- Interactive discussions via video conference with key personnel
- Presentation of specific items of requested evidence via video conference with key personnel.

4.3.3 Interim Report

The Auditors will prepare an interim version of the Audit Report as part of the process of completing the Off-site review. The Interim Report will be a working document for the Audit Team that:

- Provides detailed comments to support the preparation of the final Audit Report for those requirements where the Audit Process is largely or wholly complete at the end of the Off-site review.

- Provides a summary of information captured during the Off-site stage for internal use by the Audit Team.
- Notes specific checks or controls that should be carried out or validated On-site based on findings or observations made during the Off-site review.

Where the Auditors' assessment is that sufficient understanding of controls has been achieved to make an initial assessment of compliance, and that assessment is that an appropriate level of compliance has not been achieved then the Auditors may communicate improvement statements to the Auditee with a view to assessing any improvements made at the time of the On-site Audit.

Where the number and/or severity of improvements is such that the Auditors do not believe that it will be possible to complete the review of the improvement within the planned duration of the On-site Audit, the Auditors and Auditee may discuss extending the duration, subject to this being possible within the Audit schedule.

4.4 Hybrid Audit Process (On-Site)

A sample agenda is included at Annex C for a Renewal Audit with typical scope (equivalent to a 4-day on-site Audit).

Agendas for:

- Renewal Audits with non-standard scope or duration
- Repeat Audits

Will be agreed on a case-by-case basis with each Auditee based on the appropriate scope.

4.4.1 Audit Agenda

The objective of the On-site review is to collect and analyse information to:

- Undertake detailed operational review and testing of controls based on information collected during the Off-site part of the Audit Process.
- Enable the Audit Team to conduct full auditing of operational activities that cannot be audited Off-site (e.g. production process; physical security).

The On-site Audit will be conducted according to the agreed agenda. The On-site Audit can only take place where the Off-site Audit Process has been completed satisfactorily. If the Off-site Audit has not been completed, the On-site Audit Process must be rescheduled.

4.4.2 Audit Performance

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

- Additional and follow-up document review
- Additional and follow-up interviews with key individuals where necessary
- On-site review and testing of operational activities based on a review of sample evidence of compliance.

On-site review and testing is expected to be carried out for all main sections of the SAS requirements within the scope of activities at the Site. This testing may be based on information collected during the off-site review or directly during the On-site Audit.

4.4.3 Final Audit Report

The final Audit Report will be prepared On-site following the standard report template. The final Audit Report will summarise the Auditors' assessment of both the Off-site and On-site elements.

The final Audit Report is structured consistent with the Audit Report prepared as part of a conventional on-site Renewal Audit, as defined in the FS.05 Methodology [1].

Where the Auditee submits revised controls for items assessed as non-compliant at the initial Audit and it is the Auditors' assessment that these represent appropriate improvement then the assessment may be updated accordingly.

4.4.4 Presentation of the Results

The Audit Team will present the Audit Results to the Auditee at the end of the On-site element of the Audit, focussing on the key points identified in the Audit Report. It is not deemed necessary to have a slide presentation.

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

4.4.5 Audit Result and Certification

The certification process described in the FS.05 Methodology [1] is unaffected by the proposed variations in this document.

Where the level of compliance is assessed to be insufficient for SAS-UP certification, the requirement for evidence of improvement to be assessed through Off-site review or an On-site Re-Audit will continue to be assessed by the Audit Team and recorded in the Audit Report. The process for completing the certification process will be as described in the FS.05 Methodology [1].

4.4.6 Appeals

The appeals process described in the FS.05 Methodology [1] is unaffected by the proposed variations in this document.

4.4.7 Notification and Publication of Certification

Renewals carried out through a Hybrid Audit will not normally result in any change to the process for publication of the SAS-UP Certificate on the GSMA SAS website. Certificates awarded following a Hybrid Audit Process for renewals will be considered directly equivalent to Certificates awarded following a conventional on-site Renewal Audit.

4.5 Delay of On-site Audit

The On-site Audit should normally:

- Be completed prior to expiry of the Site's existing SAS-UP Certificate.

- Be scheduled to occur within 4 months of the completion of the Off-site review.

Where the On-site review is delayed (e.g. to Covid-19 travel restrictions or local lockdowns):

- Auditees should apply to the Audit Management for a Temporary Extension to the existing SAS-UP Certificate to avoid expiry of the Site's current SAS-UP certification.
- The Auditors will conduct a Temporary Extension Assessment (TEA) as part of the process, allowing a further review and re-validation of controls and changes, including those already reviewed as part of the Off-site Audit Process.
- The On-site Audit will be conducted at the earliest possible date agreed by all parties.
- Final review of controls and the certification decision will be made based on the on-site Audit as soon as this is completed.

4.6 Language

The language used in the course of the approval process for all SAS documentation and presentations is English. The documentation requested, or their equivalents, should be available to the Auditors in English for the purpose of the approval review. Other documents may be in a language other than English but translation facilities should be available during the approval discussion. Where it is likely to be difficult to conduct approval discussions with personnel in English, Auditees should arrange for one or more translators to be available to the Audit Team.

4.7 Hybrid Audit Costs

The costs of the Hybrid Audit will include Audit fees and expenses. Audit fees will be calculated based on the Audit duration and the daily auditing rate specified in the SAS-UP Service Agreement between the GSMA and the Auditee. The Audit duration will be based on the scope of activities at the Site and any previously-noted requirement to vary or extend the Audit duration – consistent with section 8 of the FS.05 Methodology [1].

Auditees will continue to be responsible to pay the Auditors' reasonable expenses incurred during the On-site Audit. Some savings are likely due to the shorter duration of the On-site Audit period. Expenses are not normally expected to be incurred as part of the Off-site review.

5 Remote Audit Process

The Remote Audit Process for an SAS-UP Audit to be carried out Off-site is intended to replicate as closely as possible the Conventional Audit Process carried out on-site. Inevitably, there are some variations in the approach taken, and these will have some impact on the overall effectiveness of the Audit Process, however this section of the Methodology Variation has been defined with the objectives of:

- Achieving a practical balance between the needs of Auditees and end-user stakeholders to maintain and operate a Certification Process that ensures an appropriate baseline security standard across certified Sites.
- Employing a variety of techniques, utilising a mix of commonly-available business technologies to allow the auditors to:
    - Understand the controls in place and assess their compliance with the requirements of SAS-UP.
    - Confirm the consistency of understanding and application of the documented controls amongst responsible personnel.
    - Validate the effectiveness of the controls in the live environment at the Site.
- Ensuring transparency for end-users in understanding the Audit Process and limitations for Certificates issued under this process.

This section of the Methodology Variation acts as a guide for Auditees, describing how the Remote Audit Process will be carried out, including the pre-requisites and other requirements for Sites considering this certification option.

For context, with the addition of this Remote Audit Process, SAS-UP supports:

- A Conventional Audit Process that:
    - Will always begin with an **On-site Audit** that may be **Full, Dry** or a **Scope Extension.**
        - That may result in non-compliances requiring evidence of improvement to be reviewed:
            - **On-site.**
            - **Off-site.**
    - May require a follow-on **On-site Audit** that is **Wet.**
        - That may result in non-compliances requiring evidence of improvement to be reviewed:
            - **On-site.**
            - **Off-site.**
- A **Remote Audit Process** that:
    - Will always begin with an **Off-site Audit** that may be **Full** or **Dry** or a **Scope Extension.**
        - That may result in non-compliances requiring evidence of improvement to be reviewed **Off-site.**

- Normally requires a follow-on **On-site Audit** when possible, to physically validate controls audited **Off-site.**
  - That may result in non-compliances requiring evidence of improvement to be reviewed:
    - **On-site.**
    - **Off-site.**

The remote audit process is divided into 5 phases:

Phase 0	Audit setup
Phase 1	Audit preparation (off-site) • Preparation and planning • Acknowledgement and acceptance of pre-requisites • Agreement on the use of techniques and testing of tools • Agreement of audit agenda and session schedule
Phase 2	Off-site Audit • Completion of the Audit Process in accordance with the agreed agenda / schedule.
Phase 3	Conclusion and initial certification • Preparation of Audit Report by Audit Team • Closing meeting with Auditee representatives • Submission of Audit Report to Audit Management • Issue of initial Certificate
Phase 4	On-site audit • On-site review of activities to re-validate in live environment once travel to Site becomes feasible. • Issue of updated Certificate.

5.1 Phase 0 – Remote Audit setup

5.1.1 Audit request

Auditees will continue to make requests to the Audit Management for the Audit, in accordance with the FS.05 Methodology [1].

Auditees will be required to confirm the scope of the SAS-UP certification required at the time of the request to facilitate planning.

5.1.2 Eligibility

Each request will be evaluated by the Audit Management in conjunction with the Audit Team against the criteria defined in the GSMA SAS Covid-19 Policy [2]. Auditees will be advised whether their request qualifies for the Remote Audit Process.

5.1.3 Scheduling

Scheduling of phases 1-3 will be carried out by the Audit Management in conjunction with the Audit Team.

As part of the scheduling process the Audit Team will provide proposed durations for both the Off-site audit (phases 1-3) and On-site (phase 4) elements. Proposals for the duration of each part will be based on the agreed scope of the Audit, as notified to the Audit Management in the Audit request. The durations of the two parts will normally be based on the sample agendas included in Annex D of this document, but may be varied for individual Audits based on the Audit Team's knowledge and experience of the Auditee and any initial discussions at the planning stage. The duration of phase 4 will be reviewed as part of the conclusion of phases 1-3 and updated where necessary.

5.2 Phase 1 – Remote Audit preparation (Off-site audit)

5.2.1 Preparation and planning

4-6 weeks before the scheduled date for commencement of phases 1-3, the Audit Team will make contact with the Auditee to:

- Ensure that Auditee has the latest documentation regarding the requirements for the Off-site audit (based on this Methodology Variation, but including any subsequent updates or any considerations specific to the site or audit scope)
- Make plans for the phases 1-3 of the Remote Audit Process (the Off-site Audit), leading to initial certification of Sites that have demonstrated an appropriate level of compliance.

Planning for phase 4 of the Remote Audit Process will only take place once there is a reasonable likelihood of travel to the site being possible.

5.2.2 Audit pre-requisites

Due to the specific requirements of the Remote Audit Process, the Auditee will be required to confirm that they have reviewed and understood the documents included at Annex D.

As described in the GSMA SAS Covid-19 policy [2], sites unable or unwilling to meet these requirements will be ineligible for the Remote Audit Process and will need to revert to the Conventional Audit Process.

5.2.3 Agreement and testing of tools

As part of the preparation, the Auditee will be asked to confirm the details of the tools and techniques to be used to facilitate the:

- Off-line review of information.
- On-line interactive audit sessions.
- Live Audit process.

The Auditors will conduct a basic functionality test with the Auditee to confirm that the tools are working and appear to be capable of fulfilling the requirements defined in D.1.2.

Where encryption keys need to be set-up or exchanged, this will be carried out in parallel with the agreement and testing of tools.

5.2.4 Agreement of Off-site Audit agenda and session schedule

A sample agenda for the Off-site Audit as part of the Remote Audit Process is included at D.1.3, reflecting a site with typical scope (equivalent to a 4-day conventional Audit).

Agendas for each Audit will be agreed on a case-by-case basis with each Auditee.

The agenda will normally be planned around a number of sessions, with each session expected to take 2-3 hours to complete. As part of the planning process the Auditors and Auditee will agree the initial schedule for these sessions to be completed. Scheduling of sessions will consider:

- The overall schedule for the Off-site Audit.
- Any local restrictions on the availability of Auditee personnel or activities.
- Accommodating time zone differences between the Site and Audit Team as far as is practically possible.

Progress with the sessions will be reviewed periodically throughout the Audit to determine any changes to the agenda that are required. In the event that the Audit duration needs to be changed (lengthened) this will be subject to the process described in 5.4.4.

5.3 Phase 2 – Remote Audit process (Off-site Audit)

The Off-site Audit will be conducted according to the Remote Audit Process documents included at Annex D.

5.4 Phase 3 - Conclusion and initial certification

5.4.1 Initial Audit Report

The initial Audit Report will be prepared at the end of the Off-site Audit process to summarise the Auditors' initial assessment of compliance with SAS-UP requirements.

The initial Audit Report will be structured consistent with the structure of the final Audit Report defined in the FS.05 Methodology [1].

5.4.2 Presentation of results

The Audit Team will present the Audit Results to the Auditee at the end of the Off-site Audit, focussing on the key points identified in the Audit Report. As with the core FS.05 Methodology [1], it is not deemed necessary to have a slide presentation.

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

5.4.3 Audit result and initial certification

The Certification Process described in the FS.05 Methodology [1] is unaffected by the proposed variations in this document.

Certification will be awarded only where no sections of the initial Audit Report are assessed as non-compliant (NC) by the Audit Team.

In the event that one or more sections of the Audit Report are assessed as non-compliant:

- The Auditee will be required to submit to further assessment in those areas. The re-assessment method will be determined by the number and nature of the issues identified and will be indicated in the Audit Summary.
- Certification will not be awarded until the Auditee has submitted to successful re-assessment of the issues identified, allowing an updated Audit Report to be issued specifying that certification will be awarded.
    - The reassessment process must be completed within the normal timescales defined in the FS.05 Methodology [1].

As described in the GSMA SAS Covid19 Policy [2] the SAS-UP certificate issued will be awarded:

- On condition that an On-site Audit takes place once possible to ensure all controls have been validated.
- With notes to the effect that the Audit:
    - Has been carried out Off-site due to Covid-19 travel restrictions.
    - Will be validated with the On-site Audit once possible.

5.4.4 Changes to Off-site Audit process

The Audit Team will plan and execute the Off-site Audit process based on an understanding that the Auditee:

- Has provided accurate information about the scope of the Audit and certification.
- Has carried out reasonable preparations for the Audit based on the process documents included in Annex D.
- Will make available the information and technical tools to allow the Audit to be carried out.

Where the Remote Audit Process itself is adversely affected by:

- The Auditee’s failure to ensure the above.
- The ability to conclude the Audit within the agreed timescales due to other unforeseen factors (including, but not limited to, difficulties in obtaining clear explanations or evidence from Auditee during the Audit).

…then the Audit Team will:

- Highlight concerns to the Auditee as soon as they become clear.
- Work with the Auditee to consider possible ways forward.
- Propose adjustments to change (lengthen) the duration of the Audit where:

  - Necessary to ensure that the Audit can be completed in appropriate detail.
  - Possible for the Audit Team.

- Provide notice to the Audit Management of any changes made.

Any changes that result in the Audit duration being lengthened will be included within the overall costs in section 5.7.

In the exceptional event that the Audit Team believes that it is not possible to complete the Audit then, through consultation with Audit Management, the process will be temporarily suspended pending agreement of a way forward; typically:

- Closure of the Off-site Audit, either immediately or following completion of additional Off-site Audit sessions as agreed between the Audit Team, Auditee and Audit Management.
  - An initial Audit report will be completed by the Audit Team based on the completed parts of the Off-site Audit.
- Followed by either:
  - Completion of the Remote Audit Process through an extended phase 4 On-site audit.

  Or

- Conducting an On-site Re-audit or first Audit according to the SAS-UP Methodology [1] for the Conventional Audit Process.

Sites will not receive SAS-UP certification until the Audit Process has been completed.

5.5 Phase 4 – Remote Audit process (On-site Audit)

The Remote Audit Process will normally be completed with an On-site Audit. The On-site Audit will take place once travel restrictions have been lifted.

The objective of the On-site Audit is to collect and analyse information to:

- Undertake additional live review and testing of controls at the Site.
- Validate the initial assessment of compliance carried out as part of the Off-site Audit.

If the Audit Team is satisfied that the Off-site Audit has provided sufficient assurance of Site compliance with all of the requirements, it may decide to waive the On-site Audit, or defer this to be part of the next scheduled Audit (e.g. Wet Audit, Renewal Audit). Where applicable, this conclusion will be highlighted on the issued Certificate.

5.5.1 Audit agenda

A sample agenda for the On-site Audit as part of the Remote Audit Process is included at D.2.1. The agenda reflects a Site with typical scope (equivalent to a Site requiring a 4-day conventional Audit for certification).

Agendas for each Audit will be agreed on a case-by-case basis with each Auditee, using the Audit Team's knowledge of the Site acquired during the Off-site audit. The agenda will consider any local restrictions on the availability of Auditee personnel or activities where possible, but the short duration of the On-site audit may limit the amount of flexibility that can be shown.

Progress will be reviewed periodically throughout the Audit to determine any changes that are required.

The On-site Audit will normally only take place where the Off-site Audit has been completed satisfactorily and the site is certified. If the Off-site audit has been completed but has not resulted in certification, the Auditee may choose to request that the certification process changes from the Remote Audit Process to the Conventional Audit Process, replacing the On-site Audit with an On-site Re-audit. Scheduling of the On-site Re-audit will be subject to travel to the Site being possible.

5.5.2 Audit performance

The On-site Audit will allow the Audit Team to assess performance according to the agreed agenda, by various methods such as:

- Additional and follow-up document review
- Additional and follow-up interviews with key individuals where necessary
- On-site review and testing of operational activities based on a review of sample evidence of compliance.

On-site review and testing is expected to be carried out for all main sections of the SAS requirements within the scope of activities at the Site. This testing may be based on information collected during the Off-site Audit or directly during the On-site Audit.

5.5.3 Final Audit Report

The final Audit Report will be prepared at the end of the On-site Audit process. The report will be based on the initial Audit Report prepared after the Off-site Audit and will continue to be structured as defined in the FS.05 Methodology [1].

Additional comments will be made in each section where further testing or validation is carried out during the On-site Audit. In sections where the Audit team's understanding and assessment is unchanged, the comments from the initial Audit Report will continue to apply.

5.5.4 Presentation of results

The Audit Team will present the Audit Results to the Auditee at the end of the Off-site Audit, focussing on the key points identified in the Audit Report. As with the core FS.05 Methodology [1], it is not deemed necessary to have a slide presentation.

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

5.5.5 Audit result and final certification

The Certification Process described in the FS.05 Methodology [1] is unaffected by the proposed variations in this document.

Certification will be maintained only where no sections of the final Audit Report are assessed as non-compliant (NC) by the Audit Team.

In the event that one or more sections of the Audit Report are assessed as non-compliant:

- The Auditee will be required to submit to further assessment in those areas. The re-assessment method will be determined by the number and nature of the issues identified and will be indicated in the Audit Summary.
- 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.
- Certification may be withdrawn if a successful re-assessment of the issues identified has not been completed by the Audit Team within the agreed timescales.

Notes to the SAS-UP Certificate will be updated to reflect the successful completion of the On-site Audit.

5.5.6 Appeals

The appeals process described in the FS.05 Methodology [1] is unaffected by the proposed variations in this document.

5.5.7 Notification and publication of certification

Certification resulting from the remote audit process will be published according to the standard process described in the FS.05 Methodology [1].

Certificates will carry notes to the effect that they are the result of a remote audit process, as described in sections 5.4.3 and 5.5.5.

5.6 Language

The language used in the course of the Remote Audit Process is English. The documentation requested, or their equivalents, should be available to the Auditors in English for the purpose of the Off-site and On-site reviews. Other documents may be in a language other than English but translation facilities should be available during the Audit Process discussion. Where it is likely to be difficult to conduct Audit discussions with personnel in English, Auditees should arrange for one or more translators to be available to the Audit Team.

Auditees should note:

- The additional difficulties in communication that will arise where the Audit is conducted remotely.
- That availability of documentation in English wherever possible (rather than relying on translation during the audit) will be a significant advantage.
- The comments in D.1.2 about the importance of the quality of audio for the on-line audit sessions.

5.7 Remote Audit Process Costs

The costs of the Remote Audit Process will include Audit fees and expenses. Audit fees will be calculated based on the audit duration and the daily auditing rate specified in the SAS-UP Service Agreement between the GSMA and the Auditee. The Audit duration will be based on the scope of activities at the Site and any previously-noted requirement to vary or extend the Audit duration – consistent with section 8 of the FS.05 Methodology [1]. The total fees will include time for all phases (0-4) described in this variation document. Fees for phase 4 will be invoiced separately from fees for phases 0-3, and around the time when the On-site Audit takes place.

Auditees will continue to be responsible to pay the Auditors' reasonable expenses incurred during the On-site Audit. Some expenses savings compared to the Conventional Audit Process are likely due to the shorter duration of the On-site Audit. Expenses are not normally expected to be incurred as part of the Off-site audit.

Annex A TEA Sample Information Request

This template is provided as a sample structure that will be adapted for each use and submitted to the Auditee by the Audit Team.

As part of the Temporary Extension process for SAS-UP certification the GSMA requires the Auditors to carry out a high-level off-site Temporary Extension Assessment (TEA) to validate key areas of the security management system.

To help us to complete this process we anticipate a number of steps:

1. We make this request for some initial information to understand any significant changes at the site since the last renewal audit, and to ask for some specific evidence of security controls, effectiveness and incidents.
2. We have an initial video conference call (expected to take around one hour) where you present your response to this request.
3. We spend some time reviewing the information off-site, and may ask for additional specific information if necessary.
4. We schedule a follow-up video conference call (typically of around 1 hour) to discuss any questions and observations.

At the end of the process we will confirm the to the GSMA that we are happy to approve the site's Temporary Extension request.

This process is not intended to replace a full Renewal Audit, but to provide some evidence that controls are still in operation and are consistent with those reviewed as part of the most recent SAS-UP certification at the site.

Based on this request, we would like to:

1. Provisionally schedule dates and times for the video conference calls. We would suggest <around 2 weeks and 4 weeks from date of request>.
2. Confirm that the details contained in the "Summary of Certification" from the last SAS-UP audit report remain correct.
3. Request initial information based on the list below.

Please provide the following:

a. A summary document or PowerPoint presentation describing details of any major changes to processes or security controls at the site since the last renewal audit. Examples of changes could include:
    i. Changes to primary security management system documents (security policies, security manuals etc.).
    ii. Changes to the physical security zoning concept, physical site layout or physical security controls (CCTV, access control, alarm systems etc.)
    iii. Changes to key members of the security organisation
    iv. Changes to members of the key management team.
    v. Changes to key management systems (installation of new HSMs or KMS for UICC or eUICC activities at the site).
    vi. Changes to mechanisms for customer key exchange.

vii. Changes to data generation mechanisms in use.
viii. Modifications to the production asset control process (e.g. changing incoming or outgoing counts, changes to remake procedures, changes to destruction activities).
ix. Changes to IT security controls at the site (particularly relating to the requirements for access control, network security and system security).

b. A status of actions taken to:
   i. Maintain the status of improvements to NC areas from the last certification audit.
   ii. Implement improvements in areas assessed as C- at the last certification audit.
c. Details of the date(s) of the most recent update to the site's security risk assessment and any improvement actions identified as part of the process.
d. A summary of any security incidents identified, investigated and reported as part of the site's security incident reporting procedure(s) within the last 6 months, comprising:
   i. Date of incident.
   ii. Internal reference for incident (if any).
   iii. High level name/description of incident.
   iv. Date of closure of incident.
e. Dates of internal audit checks (operational checks and independent controls) carried out for physical security, key management, data processing, production and IT security within the past 3 months.
f. Details of any EUM certificate key pairs generated at the site and/or for which EUM certificates have been issued.
g. Dates, times and quantities for destruction of UICCs (and/or eUICCs as appropriate) within the last 2 months for each form-factor within the scope of SAS-UP.
h. Dates for completion of vulnerability scans and penetration tests for systems/servers within the scope of SAS-UP certification within the past year for systems and networks used for:
   i. External data exchange (e.g. customers, data generation sites, production sites).
   ii. Operational key management.
   iii. UICC/eUICC data generation.
   iv. UICC/eUICC personalisation.

If you believe that the requested timescales will not be possible then please provide an indication of when you think you will be in a position to proceed.

Auditor PGP keys are attached to this request and may be used to encrypt any information considered confidential. We are not expecting sensitive information (e.g. details of security incidents; details of risk assessments) to be provided at this point. The auditors may request specific examples to be provided during the video conference call.

If you have any questions about the approval process or the information requested above then please do not hesitate to contact us.

Annex B TEA Approval Statement

Audit site	{Site name}, {Location}		
Date of approval	01 June 2020	**SAS-UP Standard**	V9.0
		Consolidated Security Requirements (CSR)	V3.0

Result

Following an off-site assessment by the Auditors of evidence provided by the Auditee:

The Auditors approve Temporary Extension of this site's SAS-UP Certificate for a period of 6 months	Immediately	**Following improvement**

The assessment considered a number of key indicators of the ongoing operation and effectiveness of the Site's security management system, including:

- {Update as appropriate}
- Discussion of any significant changes made at the Site.
- Implementation and maintenance of improvements based on the last SAS-UP audit process.
- Changes to the security management organisation and security management system documentation.
- Updates to the Site security risk assessment and completion of appropriate improvement actions.
- Review of security incidents.
- Review of the internal audit programme, sample internal audits and completion of improvement actions.
- Review of sample events related to sensitive processes in:
  - Key management
  - Customer data processing
  - UICC personalisation
- Maintenance of appropriate IT security controls.

A full Renewal Audit of the controls in place will be carried out on-site at a future date as agreed between the Auditee, Auditors and GSMA.

Signatures

For FML (James Messham)	**For ChaseWaterford (Vernon Quinn)**

Actions required

Improvements are required to the Security Management System in the areas described below.

5.3	Physical protection	
	Evidence of improvement...	Confirmation of improvement and review of evidence.

Summary of certification

The contents of this section have been re-confirmed as correct with the Auditee as part of the approval process and will be used to create the SAS Certificate that will be issued to the Auditee's Site and published on the GSMA SAS website.

Scope of certification

Successful assessment of compliance with the requirements of SAS-UP during this Audit Process will result in the following scope of certification for the Site:

Generation of data for personalisation	**R**	UICC	**W**	eUICC		
Management of PKI certificates	**W**	GSMA	-	Non-GSMA		
Personalisation	**R**	Card	**R**	Embedded	-	Wafer
Post-personalisation packaging	**R**	Card	-	Embedded	-	Wafer

For each activity within scope: **P** provisional certification; **W** full certification following wet audit;
N new full certification; **R** renewal of full certification.

Sites

Certification of one Site may have a number of dependencies on other Sites, as defined below*[1].

Primary Audit Site

Audit site			
Address			
Date of audit			
SAS UP Standard	V9.0	**Methodology**	V7.0
Consolidated Security Requirements (CSR)			V3.0

[1] The Primary Audit Site is the main Audit Site for which the SAS-UP Certificate will be issued.

Secondary Site(s) will include any locations directly supporting the activities of the Primary Site and included as part of the same Audit Process and Audit Report. Secondary sites will not be issued with SAS-UP Certificates, but will be noted as part of the certification of the Primary Site.

Supporting Audit Sites are independent locations that are subject to separate certification Audits. Audit findings will be documented separately in another SAS-UP Audit Report. Dependence of the Primary Site on the Supporting Audit Site(s) will be noted as part of the certification of the Primary Site.

Secondary Audit Site(s)

Audit site	Not applicable
Address	
Function(s)	

Supporting Audit Site(s)

Audit site	Not applicable	
Address		
Function(s)		

Notes and Exclusions

None

Next Renewal

Audit duration*	6 days	**Standard**	Non-standard
Comments	-		

Annex C Hybrid Audit / Sample Agenda

The sample agenda below presents a typical structure for the On-site and Off-site elements of a Hybrid Audit based on a 4-day On-site Renewal Audit.

Agendas for Renewal Audits with different scope/agenda or for Re-Audits will be agreed on a case-by-case basis.

Agendas are split into:

- Sessions for the Off-site review. Each session will typically be 2-3hrs duration.
- Half-day segments for the On-site review.

Agendas will normally be carried out in the sequence set out below for the Off-site and On-site elements. Auditees should ensure that appropriate information has been prepared to facilitate the Audit Process by preparing the requested information and documents.

The Auditors will normally expect to:

- Review primary documents defining aspects of the security management system (as described in Annex C of the FS.05 Methodology [1])
- Discuss the controls in place (documentation, processes, systems) with responsible personnel to understand the security management system. Discussions will typically take place:
    - Interactively during Off-site sessions.
    - Within a meeting room environment during the On-site Audit.
- Review and validate controls:
    - By the presentation of appropriate evidence during interactive Off-site sessions or the On-site Audit.
    - By direct review On-site where the sensitive processes are carried out.

The agendas may be adjusted based on production schedules or availability of key personnel. The Auditors may also wish to change the amount of time spent on different aspects during the On-site or Off-site Audits based on progress during the Audit itself.

C.1 Off-site Audit Sample Agenda

The Off-site review will be carried out over a number of sessions at times and dates agreed between the Audit Team and Auditee.

The majority of sessions will require interactive involvement between the Audit Team and Auditee representatives via video-conference or similar environment. Some sessions may involve the Audit Team working to review documents or information without the need for interactive involvement by the Auditee.

Sessions will normally be planned to take 2-3 hours.

Session	Outline agenda	Format	Suggested Auditee preparation	Auditee personnel
1	• Company / Site introduction and overview. • Overview of changes to Site and security management system. • Description of security management system.	Auditee presentation	Preparation of introductory presentations to include: • Company/corporate background and overview. • Site introduction/overview. • Confirmation of Audit scope and sensitive processes carried out at the Site. • Security management organisation, responsibility and system. • IT and information security overview.	Key members of security organisation
	• Review of security policy and organisation. • Detailed review of security management system documentation.	Auditee presentation Off-line review by Audit Team Question and answer (Q+A)	Preparation of printed copies of security management system documents, as described in FS.05 Methodology Annex C.	Key members of security organisation
2	• Security awareness training	Q+A	• Copies of employee security awareness training materials.	Security manager / HR / training as appropriate

Session	Outline agenda	Format	Suggested Auditee preparation	Auditee personnel
			• Employee security awareness training records for the past 2 years.	
	• Risk assessment • Business Continuity Plan	Q+A	Preparation of copies of documents for review by the Auditors (see also document list). Evidence of the most recent security risk assessment completed. Business continuity training and testing records.	Risk assessment responsible representative BCP responsible representative
	• Human resources	Q+A Presentation of requested samples	Description of processes for: • Security screening as part of on-boarding process. • Regular re-screening of personnel. • Defining security responsibilities within job description. • Security and confidentiality within legal documentation (e.g. employment contracts). • Security incident reporting and whistleblowing. • Disciplinary action. • Off-boarding at end of employment. • Sample employee files to provide evidence of controls being applied (Audit Team will specify the requested files for the HR team to present).	HR representative Security manager

Session	Outline agenda	Format	Suggested Auditee preparation	Auditee personnel
3	• IT security policy	Q+A	Preparation of copies of appropriate documents for review by the Auditors during the Audit, including: • IT security policy.	IT security business owner
	• IT network security	Q+A Presentation of requested samples	• Overall network layout. • Production network layout. • Firewall configuration policy and rules. • Penetration test and vulnerability scan results.	Network security team representative System administrator(s)
	• IT systems security	Q+A Presentation of requested samples	• System hardening checklists. • Patch and virus management records. • User authorisation / account creation process and example records.	Systems security team representative System administrator(s)
4	• IT systems security (continued)			

	• Key management.
	  • Overview of key storage mechanisms in use for UICC production activities.
	  • Processes for secure generation and exchange of keys with other entities in the production chain.
	  • Processes for secure generation and management of
		Q+A
		Presentation of samples
			Preparation of key management process documentation and supporting evidence, including:
			• Process documentation.
			• Roles and responsibilities.
			• Key management activity records.
			• Technical details of key storage mechanisms.
			The Auditors may request completion of a demonstration key ceremony during the Audit using test/dummy keys.
				Security manager
				Key manager
				Key administrator(s)
				Technical system architect / developer representative

Session	Outline agenda	Format	Suggested Auditee preparation	Auditee personnel
	keys for internal protection of data.			

5	• Data generation
	  • Development and management of data generation profiles
	  • Secure exchange of data (input files, output files, production data etc.)
	  • Generation of sensitive data
	  • Authentication and other keys
	  • Device certificates
	• Protection of sensitive data (encryption and access control)
	• Prevention of duplicate production
	• Production audit trails
		Q+A	Preparation of detailed data flow diagrams and supporting information to show end-to-end lifecycle of production data, to include:
			• Exchange of:
			  • Input files / data.
			  • Personalisation data.
			  • Response / output data.
			With other entities in the production chain.
			• Generation / processing of data for:
			  • Electrical personalisation.
			  • Graphical personalisation.
			  • Customer response/output.
			• Management of personalisation data and UICC status during and after the personalisation process.
			Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.
			Preparation of detailed description of data generation mechanism used for sensitive personalisation data (e.g. individual subscriber keys).
				Security manager
				Data processing team representative
				Technical system architect / developer representative

	• Production data management
	  • Receipt and transfer of personalisation data into the production network
	  • Protection of sensitive data (encryption and access control)
	  • Control of personalisation
	  • Repersonalisation flow
	  • Prevention of duplicate production
	  • Production audit trails
		Q+A		Security manager
				Data processing team representative
				Production data management representative
				Technical system architect / developer representative

Session	Outline agenda	Format	Suggested Auditee preparation	Auditee personnel
			Overview of controls in place to prevent duplicate production occurring. The Auditors may arrange for exchange of test data files with the Site as part of the Audit preparation (as described in the SAS-UP Methodology).	
6	• Internal audit system	Q+A Presentation of requested samples	Overall plan for internal audits/operational controls covering physical security, production, data processing and IT security controls. Internal audit checklists used at operational, supervisory and independent audit levels for each area. Access to samples of completed checklists and tracking mechanisms for remediation actions as requested.	
	• Closing meeting	Audit Team summary presentation of findings.		Auditee representatives.

C.2 On-site Audit Sample Agenda

Half-day segment	Outline agenda	Suggested Auditee preparation
1	• Introductions • Agreement of agenda • Overview of changes to Site and security management system since Off-site Audit	Preparation of any necessary introductory presentations (not normally expected/required except where significant changes have occurred).
	• Testing of IT security controls	On-site visit to data/server rooms and IT management suites. Sample checks of system configuration to validate consistency against processes described.
	• Testing of key management controls	On-site review of key management systems and records. The Auditors may request completion of a demonstration key ceremony during the Audit using test/dummy keys.
2	• On-site review of data flow	Site visit to data processing room. Review of processes, systems and records (system-based logs and manual records).
	• Logistics and production. • Process and asset control	Site walk-through of production processes and asset control measures including testing and validation of controls.
3	• Physical security concept • Physical security • External inspection	Preparation of printed copies of Site plans and layouts of security systems for use by the Auditors. Plans will be used as working documents for annotation by the Auditors during the physical security review. Plans will only be used during the Audit and will not be removed from the Site at any time.

4	• Physical security
	  • Internal inspection
	  • Security control room	

5	• Internal audit system • Finalise report, present findings	

Annex D Remote audit process documents

This annex contains documentation intended to assist Auditees in preparing for the Remote Audit Process. The annex includes:

- An overview of the assessment process

  The overview describes the basis for assessment, how information will be collected and provides an overview of the requirements for tools to be provided (by the Auditee) to facilitate the process.

- A sample agenda

  The sample agenda presents a typical structure for an SAS-UP Audit to be carried out Off-site. The agenda is based on a standard 4-day Audit equivalent to that described in the FS.05 Methodology [1] for an Audit Site with typical scope of activities.

  Agendas for all Audits will be agreed on a case-by-case basis as part of phase 1 of the Remote Audit Process. The sample Agenda will, however, provide a common framework for the vast majority of Audits conducted remotely.

  The agenda may be adjusted based on production schedules or availability of key personnel. The Auditors may also wish to change the amount of time spent on different aspects during the Audit process based on progress during the Audit itself.

  The agenda is split into sessions for the Off-site review. Each session will typically be 2-3hrs duration.

- A detailed mapping of the collection process and tools required for each part of the Audit is provided for reference.

D.1 Remote audit: Off-site Audit process

D.1.1 Audit assessment and compliance

The Audit (whether On-site or Off-site) seeks to utilise a number of different sources to allow the Auditors to assess compliance, consistency and confidence of the controls in place. As described in FS.05 SAS-UP Methodology, the Auditee must receive a C or C- assessment in each section of the Audit Report for certification to be granted - reflecting an appropriate level of conformity across all applicable sections of the FS.17 SAS Consolidated Security Requirements [3].

For the Off-site Audit to demonstrate operation of SAS-UP compliant controls, the Auditee must provide appropriate access to relevant information to enable the Audit Team to assess compliance, consistency and certification. Assessment will normally consider the information sources documented below. For reference, an indication of what might be considered poor conformity (resulting in an NC assessment) and good conformity (resulting in a C assessment) is also included.

Assess	Target	Assessed through		Poor conformity	Good conformity
Compliance	The Auditee has defined and implemented policy, procedures and operational controls that meet the requirements of SAS-UP.	[D]	**Documentation review.**	Controls appear to be new and/or untested. Documentation is missing or incomplete, or shows a very high level of inconsistency at the same level (e.g. policies are inconsistent) or across levels (e.g. work instructions are not consistent with procedures; processes do not comply with policies).	Controls are well-established and documented and have been in regular operation for an extended period. There is a high level of stability, with major changes happening infrequently. Where changes do occur, their introduction is carefully managed through training and monitoring to ensure effectiveness.
		[S]	**Stakeholder interview.**		

Assess	Target	Assessed through		Poor conformity	Good conformity
Consistency	Controls are clearly understood by personnel at all levels and are operated consistent with those defined and documented.	[S]	**Stakeholder interview.**	Personnel do not appear to clearly understand the controls that should be in place through a lack of training and/or familiarity. General discipline appears poor.	Personnel understand the controls and their responsibilities clearly and are able to explain and demonstrate them when asked. The need for sustained compliance is understood, based on personnel having a clear recognition of the importance of the controls to the business and certification and their personal accountability for maintaining the appropriate level of control.
		[P]	**Operational personnel interview and activity review.**		Personnel are disciplined and demonstrate a clear culture of security and compliance as core to their actions. Personnel embrace their individual and collective accountability.
		[O]	**Live observation of activities and behaviour.**	Appropriate records are not maintained or cannot be provided. Records that are available are incorrect or incomplete.	Complete, comprehensive and accurate records exist. Records are reliable and genuine. Different sources are consistent and can readily be validated through cross cross-correlation to validate them.
		[C]	**System configuration review.**	There is little or no evidence available that live activities are being carried out following the defined processes. Quality, consistency and accuracy of record taking is consistently poor.	Sampling checks of live operational activities, inventories, records and system configurations show no significant errors or discrepancies.

Assess	Target	Assessed through		Poor conformity	Good conformity
		[T]	**Operational sampling and testing.**	Samples taken during the audit are often incorrect or unclear, showing a high level of deviations or discrepancies.	
Confidence	Reliable evidence exists of appropriate operation of controls over an extended period, with an effective system of internal audits acting to ensure the level of effectiveness is maintained.	[L]	**Written records.**	Records are not available to demonstrate that controls have been applied prior to the Audit. Where records do exist, they are incomplete or inconsistent or do not show that controls have been applied consistent with those described or presented.	Sampling checks of operational activities carried out over an extended period prior to the Audit show a sustained level of performance with very few errors or discrepancies. Where errors or deviations have occurred, these have been identified quickly and handled appropriately to resolve them and prevent recurrence. A comprehensive system of internal audits is in place at a number of levels. Clear evidence exists of audits being carried out based on well-defined checklists. Details of samples are recorded. Personnel conducting audits are trained and experienced. Where improvements and non-compliances are identified these are reported through a clear escalation process to ensure appropriate action is taken to address them quickly and effectively.
		[L]	**Notifications and reports.**		
		[L]	**System audit logs and trails.**		
		[I]	**Internal audit reports and findings.**		
		[R]	**CCTV recordings.**	The internal audit system is poorly defined, infrequent and carried out by personnel without a clear understanding of the requirements.	

D.1.2 Collection of information

The level of conformity in D.1.1 will be assessed based on the information collected during the audit. Due to the specific challenges of conducting the Off-site Audit remotely, the Auditors have defined three levels of information collection. For each level the Auditee must ensure that it is able to fulfil the stated requirement with due consideration to the comments made.

Sites that are not able to confirm their ability to meet these requirements prior to the Off-site Audit will be required to revert to a Conventional Audit Process, as described in FS.05 Methodology [1].

Sites that are not able to meet these requirements once the Off-site Audit is underway will be subject to the process described in 5.4.4.

Collection		Requirement	Considerations
Off-line	Off-line review by Auditors using information / evidence provided by Auditee.	A mechanism for requested information to be shared with the Audit Team to enable it to be reviewed independently without the need for direct/real-time involvement of the Auditee's representative(s). Options may include providing the Audit Team with access to: • Download requested files through a file sharing repository or service. • View files directly through an on-line file sharing service that prohibits downloading/copying. • Individual copies of documents / files via encrypted email.	Auditees must balance the requirements of the Audit Process with their internal policies for protection of sensitive information. Information requested for review off-line is intended to enable the assessment of the security management system controls. Some of the information requested is likely to be security sensitive and carry internal information security classifications due to the details of security controls it contains. The Audit Process will not normally require commercially sensitive information to be shared for the purpose of assessment of security controls. Any documentation that the Auditee needs to provide that does contain commercially sensitive information (e.g. details of specific customers, pricing, risks, security incidents etc.) should be discussed with the Audit Team to determine the appropriate way forwards (partial redaction, review on-line etc.). Any information received by the Audit Team will be protected consistent with the classification and used solely by the members of the Audit Team for the duration of the Audit Process for the purpose of completing the Audit. Confidentiality of Auditee information is covered by

			confidentiality/non-disclosure agreements between the Auditee and GSMA and GSMA and Audit companies, however Auditees may wish to propose additional NDAs or undertakings provided that these are appropriate and proportionate.

On-line	On-line interactive session between Auditors and Auditee in real-time from a meeting room or similar environment	A mechanism for an on-line video conference to be established with a fixed location (e.g. a meeting room) at the Auditee site from which the Auditee can make available presentations, personnel, documentation and other evidence to meet the Audit Team's requests.
		Appropriate hardware should be available at the Auditee end to support the participation of small groups in the Audit Process.
		The objective will be to replicate as closely as possible on-site auditing of activities from a meeting room (as distinct from the live environment).
			Auditees should ensure that the solution can support:
			• Audio and video conferencing
			  • Presentation by Auditees.
			  • Interactive Q+A between the Audit Team and Auditee representatives.
			• Screen and file sharing:
			  • Delivery of formal presentations by Auditee (as defined in D.1.3).
			  • Real-time sharing of documents for discussion.
			  • Real-time sharing of electronic and printed evidence of controls.
			  • Live view of system configuration.
			• Shared whiteboarding
			  • Facilitation of discussions.
			For simplicity, an integrated solution that can also support the inclusion of live video where required (as below) is encouraged.
			
			Particular emphasis should be placed on ensuring the quality of audio for the interactive sessions. Low-quality speakers and microphones (including those integrated into laptops) typically do not provide an appropriate level of quality for use in meeting room environments. Dedicated conference speakers/phones positioned specifically for small groups of participants are normally the minimum requirement, but Auditees should still test to confirm that the audio quality is

			appropriate in both directions. Use of individual conference speakers/phones in the centre of large meeting rooms with many participants is typically a poor solution. Attempting to use 2 (or more) different audio connections within the same meeting room will often result in a disrupting delayed "echo" effect. The Audit language remains English. The use of remote audit mechanisms can make communication significantly more difficult where an intermediary is acting as a translator when compared to Audits carried out on-site. The Auditee remains responsible for ensuring that appropriate resource is available to facilitate the Audit Process where English is not the first language of the personnel involved.
Live	On-line interactive session in the live environment	A facility to enable the Audit Team to conduct direct audits of activities within the live operational environment (e.g. data processing rooms, production workshops, IT server rooms, security control rooms, internal and external physical security inspections) using an interactive approach that allows the Auditee to allow live/real-time: • 2-way audio between the Audit Team and Auditee representative(s) in the live environment. • Streamed video to be transmitted from the live environment to the Audit Team. • Relay of screen images from within the live environment (via the video link or other mechanism).	Use of a mobile phone is normally sufficient to provide the video link. Auditees should ensure that the solution: • Has been tested to ensure sufficient signal quality throughout the site to support video transfer at an appropriate resolution to facilitate the audit process. Is supported by a dedicated local Wi-Fi connection where 3G/4G/5G signal is not sufficiently strong or reliable. • Includes sufficient external power packs to support 3-4 hours continuous operation of the video link. Auditees are strongly encouraged to consider: • Carrying out their own internal trial audit with use of the camera in the different environments to ensure familiarity with the process and tools and to optimise camera positions for key parts of the audit process. • Using a stabilisation gimbal for the Live Audit Process.

- Using a tripod where the camera is to be used for relay of screen images or to relay images of documents or other evidence samples.

D.1.3 Off-site Audit sample agenda

The Off-site Audit will be carried out over a number of sessions at times and dates agreed between the Audit Team and Auditee.

Sessions will normally be planned to take 2-3 hours.

As described in D.1.2, the majority of sessions will require **On-line** interactive involvement between the Audit Team and Auditee representatives via video-conference or similar environment. Some sessions may involve the Audit Team working **Off-line** to review documents or information without the need for interactive involvement by the Auditee. Sessions carried out in the **Live** Audit environment to include testing and sampling will require the using of interactive audit tools.

A detailed mapping of the FS.17 Requirements [3], the corresponding assessment sources and whether these will be carried out Off-line, On-line or Live is included in D.1.4.

Assessment source (from D.1.1 and D.1.4)					
D	Documentation review	O	Live observation of activities/behaviourT	L	Records, logs and reports
S	Stakeholder interview	C	System configuration review	I	Internal audit reports and findings
P	Operational personnel interview and activity review	T	Operational sampling and testing	R	CCTV recordings

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
1	• Company / Site introduction and overview. • Overview of changes to Site and security management system. • Description of security management system.	Auditee presentation [D, S]	Preparation of introductory presentations to include: • Company/corporate background and overview. • Site introduction/overview. • Confirmation of Audit scope and sensitive processes carried out at the Site. • Security management organisation, responsibility and system. • IT and information security overview.	Key members of security organisation

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
	• Review of security policy and organisation. • Detailed review of security management system documentation.	Auditee presentation Off-line review by Audit Team Question and answer [D,S,P,L]	Preparation of printed copies of security management system documents, as described in FS.05 Methodology Annex C.	Key members of security organisation
2	• Security awareness training	Q+A [D,S,P,L]	• Copies of employee security awareness training materials. • Employee security awareness training records for the past 2 years.	Security manager / HR / training as appropriate
	• Risk assessment • Business Continuity Plan	Q+A [D,S,L]	Preparation of copies of documents for review by the Auditors (see also document list). Evidence of the most recent security risk assessment completed. Business continuity training and testing records.	Risk assessment responsible representative BCP responsible representative
	• Human resources	Q+A Presentation of requested samples [D,S,L]	Description of processes for: • Security screening as part of on-boarding process. • Regular re-screening of personnel. • Defining security responsibilities within job description. • Security and confidentiality within legal documentation (e.g. employment contracts). • Security incident reporting and whistleblowing. • Disciplinary action.	HR representative Security manager

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• Off-boarding at end of employment. • Sample employee files to provide evidence of controls being applied (Audit Team will specify the requested files for the HR team to present).	
3	• IT security policy	Q+A [D,S,P]	Preparation of copies of appropriate documents for review by the Auditors during the Audit, including: • IT security policy.	IT security business owner/representative

	• IT network security	Q+A
		Presentation of requested samples
		[D,S,P,C,T,L,R]
			• Overall network layout.
			• Production network layout.
			• Firewall configuration policy and rules.
			  • Samples of documentation for recent firewall rule change.
			  • Samples of documentation for recent firewall rule review.
			• Penetration test and vulnerability scan results.
				Network security team representative
				System administrator(s)

	• IT systems security	Q+A Presentation of requested samples [D,S,P,C,T,L,R]	• System hardening checklists. • Patch and virus management records. • User authorisation / account creation process and example records. • System backup process and example records. • Component destruction records.	Systems security team representative System administrator(s)

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• System event log review records.	
4	• IT systems security (continued)			

	• IT systems security	Live audit
		[P,O,C,T,L]
			Copies of layout plans for areas where sensitive activities are carried out including:
			• Server rooms.
			• IT administration rooms.
			Plans should clearly show the locations of:
			• Systems and servers are installed / used / stored.
			• All physical security hardware within the environments including:
			  • CCTV cameras.
			  • Alarm system sensors.
			  • Points of entry / exit (personnel access, materials transfer, emergency exits).
			  • Access control hardware (access card readers, biometric sensors etc.).
			Components should be clearly labelled (e.g. with reference numbers) to facilitate communication between the Audit Team and Auditee team.
				Network security team representative
				Systems security team representative
				System administrator(s)

5	• Key management.	Q+A Presentation of samples [D,S,P,C,T,L,R]	Preparation of key management process documentation and supporting evidence, including: • Process documentation.	Security manager Key manager Key administrator(s)

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
	• Overview of key storage mechanisms in use for UICC production activities. • Processes for secure generation and exchange of keys with other entities in the production chain. • Processes for secure generation and management of keys for internal protection of data. • Examination of physical storage facilities for keys/key components (key safes or similar). • Examination of key management system / HSM configuration. • Review and reconciliation of sample keys.		• Roles and responsibilities. • Training records. • Key management activity records. • Technical details of key storage mechanisms. The Auditors may request completion of a demonstration key ceremony during the Audit using test/dummy keys.	Technical system architect / developer representative

		Live audit
		[P,O,C,T,L]
			Copies of layout plans for areas where sensitive activities are carried out including:
			• Physical storage facilities for key management materials.
			• Locations where key management systems and HSM are installed.
			• Key ceremonies are conducted.
			Plans should clearly show the locations of:
			• Equipment and assets are installed / used / stored.
			• All physical security hardware within the environments including:
			  • CCTV cameras.
			  • Alarm system sensors.
			  • Points of entry / exit (personnel access, materials transfer, emergency exits).
				Security manager
				Key manager
				Key administrator(s)
				Key custodian(s)

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• Access control hardware (access card readers, biometric sensors etc.). Components should be clearly labelled (e.g. with reference numbers) to facilitate communication between the Audit Team and Auditee team.	

6	• Data generation
	  • Development and management of data generation profiles.
	  • Secure exchange of data (input files, output files, production data etc.).
	  • Generation of sensitive data.
	  • Authentication and other keys.
	  • Device certificates.
	• Protection of sensitive data (encryption and access control).
	• Prevention of duplicate production.
	• Production audit trails.
		Q+A
		[D,S,P,C,T,L,R]
			Preparation of detailed data flow diagrams and supporting information to show end-to-end lifecycle of production data, to include:
			• Exchange of:
			  • Input files / data.
			  • Personalisation data.
			  • Response / output data.
			With other entities in the production chain.
			• Generation / processing of data for:
			  • Electrical personalisation.
			  • Graphical personalisation.
			  • Customer response/output.
			• Management of personalisation data and UICC status during and after the personalisation process.
			Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.
				Security manager
				Data processing team representative
				Technical system architect / developer representative

	• Production data management.
	  • Receipt and transfer of personalisation data into the production network.
	  • Protection of sensitive data (encryption and access control).
	  • Control of personalisation.
		Q+A
		[D,S,P,C,T,L,R]
				Security manager
				Data processing team representative
				Production data management representative
				Technical system architect / developer representative

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
	• Repersonalisation flow. • Prevention of duplicate production. • Production audit trails.		Preparation of detailed description of data generation mechanism used for sensitive personalisation data (e.g. individual subscriber keys). Overview of controls in place to prevent duplicate production occurring. The Auditors may arrange for exchange of test data files with the Site as part of the Audit preparation (as described in the SAS-UP Methodology).	

[7]		Live audit
		[P,O,C,T,L]
			Typically carried out as part of production live audit process.
			Copies of layout plans for areas where sensitive activities are carried out including:
			• Input/output file handling.
			• Operational data processing.
			• Server rooms.
			Plans should clearly show the locations of:
			• Equipment and assets are installed / used / stored.
			• All physical security hardware within the environments including:
			  • CCTV cameras.
			  • Alarm system sensors.
			  • Points of entry / exit (personnel access, materials transfer, emergency exits).
				Data processing team representative
				Production data management representative

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• Access control hardware (access card readers, biometric sensors etc.). Components should be clearly labelled (e.g. with reference numbers) to facilitate communication between the Audit Team and Auditee team.	

7	• Production process.
	  • Storage of materials.
	  • Asset control within the personalisation process.
	  • Repersonalisation.
	  • Post-personalisation packaging.
	  • Finished goods storage.
	  • Reject handling and destruction.
		Q+A
		[D,S,T,L,R]
			Presentation of the production process flow describing controls in place for the personalisation process, including:
			  • Incoming materials flow for devices prior to personalisation, including storage and stock control.
			  • Control of quantity of devices entering environment where the personalisation process is carried out.
			  • Embedded cards or embedded form-factor devices for dedicated personalisation workshops.
			  • White or printed card bodies for combined card body / personalisation workshops.
			  • Control of quantity of good, reject and unused devices at end of personalisation process.
			  • Control of quantity of good, reject and unused devices at end of any post-personalisation packaging process.
				Logistics manager
				Logistics supervisor(s)
				Production manager
				Production supervisor(s)

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel

			• Confirmation of point of final control and sealing of finished, personalised UICCs.
			• Materials flows for:
			  • Finished, sealed personalised UICCs.
			  • Surplus unused devices from the personalisation process.
			  • Rejects from the personalisation and/or post-personalisation packaging processes.
			• Remake processes for devices:
			  • Rejected during the personalisation process.
			  • Rejected after the personalisation process.	

		Live audit [P,O,T,L]	Copies of layout plans for areas where sensitive processes are carried out including: • Materials storage. • Asset counting. • Personalisation. • Re-personalisation / remake. • Post-personalisation packaging. • Finished goods storage. • Finished goods shipping. • Reject storage and reconciliation. • Destruction.	

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel

			Plans should clearly show the locations of:
			• Production equipment.
			• All points of asset control (counting).
			• All physical security hardware within the environments including:
			  • CCTV cameras.
			  • Alarm system sensors.
			  • Points of entry / exit (personnel access, materials transfer, emergency exits).
			  • Access control hardware (access card readers, biometric sensors etc.).
			Components should be clearly labelled (e.g. with reference numbers) to facilitate communication between the Audit Team and Auditee team.	

8	• Physical security	For physical security, the scope of the Audit will be based around the activities at the Site within the scope of SAS-UP certification (UICC/eUICC data generation, personalisation and post-personalisation packaging, and any key and certificate management related to those activities)
		The Audit will consider all areas involved in:
		• The storage and processing of relevant assets:
		  • Information (including production data)
		  • IT
		  • Production
		  • Cryptographic keys
		• Operational management of systems and components related to:		

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
		• Activities within the scope of SAS-UP certification • The management of logical and physical security controls for activities within the scope if SAS-UP certification. Specifically, this will include the: • Overall site perimeter. • Building perimeter for each building housing activities or assets within the scope of SAS-UP certification. • Floors or areas within each building housing activities or assets within the scope of SAS-UP certification. • The areas of normal or potential access between the site perimeter and building perimeter. • The points of normal or potential access between the building perimeter and relevant floors or areas. • Activities within areas where site security is managed, monitored or administered, including: • Security control rooms. • Access / badge administration offices. • Security reception desks.		
	• Physical security concept	Q+A [D,S,P,C,T,L,R]	Detailed plans showing: • The mapping of security levels onto the Site's physical layout. • The location of all physical security hardware within the environments including: • CCTV cameras. • Alarm system sensors. • Points of entry / exit (personnel access, vehicle access, materials transfer, emergency exits).	Security manager Physical security supervisor and/or technical systems representative

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• Access control hardware (access card readers, biometric sensors etc.). In all cases components should be clearly labelled (e.g. with reference numbers) to facilitate communication between the Audit Team and Auditee team. Documentation of the physical security concept: • Security levels: • Level definitions. • Baseline security controls (for access control, CCTV, alarm systems) applied at each security level. Presentation of the implementation of the concept for areas within the scope of the SAS-UP audit (as described below). Presentation of management controls for physical security elements: • CCTV: • CCTV layout concept. • Recording and retention policies. • Operational system checks. • Preventative and reactive maintenance. • Alarm system: • Alarm system concept. • Arming and disarming policies.	

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel

			• Alarm review and response process.
			• Operational system checks.
			• Preventative and reactive maintenance.
			• Access control:
			  • Operational system checks
			  • Preventative and reactive maintenance.
			  • Lifecycle management of access for permanent and temporary employees, contractors, visitors etc., to include:
			  • Policies for granting access.
			  • Processes for application, approval, granting, modification, revocation and removal of access.
			  • Management of physical access tokens (access cards / badges).
			  • Control of unauthorised use.
			  • Processes for periodic review and re-approval of access rights.
			  • Monitoring and response for access control events.
			  • Forced opening.
			  • Denied access.	

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
			• Door open too long. • Anti-passback.	

9	• Physical security
	  • External inspection
	  • Physical protection at the site boundary.
	  • Control of authorised and unauthorised access.
	  • Deployment of physical security systems (CCTV, alarms, access control).
	  • Internal inspection
	  • Physical protection within the areas of the site linked to the scope of SAS-UP certification.
	  • Control of authorised and unauthorised access.
	  • Deployment of physical security systems (CCTV, alarms, access control).
	  • Security control room operations
	  • Validation of physical security system operation.
	  • Evaluation of control room operating procedures and discipline of personnel.
		Live audit
		[P, O, C, T, L, R]
			Plans (as above).
			Preparation of appropriate test equipment to enable physical security system components (e.g. alarm sensors, emergency exits) to be tested during the live audit.
			The ability to simultaneously view video from the live audit location with streams from the alarm console(s) may allow significant time to be saved if this can be achieved reliably.
				Security manager
				Physical security supervisor

10	• Internal audit system	Q+A Presentation of requested samples	Overall plan for internal audits/operational controls covering	Internal audit lead Internal auditors

Session	Outline agenda	Assessment source	Suggested Auditee preparation	Auditee personnel
		[D,S,P,L,I]	physical security, production, data processing and IT security controls. Internal audit checklists used at operational, supervisory and independent audit levels for each area. Access to samples of completed checklists and tracking mechanisms for remediation actions as requested.	
	• Closing meeting	Audit Team summary presentation of findings.		Auditee representatives

D.1.4 Off-site assessment methodology mapping

The table below provides a detailed mapping of how the Audit Team will normally expect to collect information to assess each requirement. The mapping identifies whether the indicated assessment is:

E Essential	Considered to be mandatory for the Off-site Audit to be completed in sufficient detail to enable an SAS-UP certificate to be issued. Auditees are required to indicate in advance (as part of phase 1) if any Audit Process marked as Essential cannot be completed using the approach. Although the Auditors and GSMA will make reasonable efforts to agree alternative approaches, Auditees may be required to revert to a Conventional On-site Audit Process.
H Highly recommended	Considered to be highly beneficial for the Off-site Audit to be completed in sufficient detail without significant inconvenience for the Auditee or Audit Team. Where assessment by "Highly recommended" Audit Processes is not possible, the Auditors may need to adjust (lengthen) the Audit duration to ensure that evidence can be assessed in sufficient detail. Such changes will be handled in accordance with the process described in 5.4.4.
B Beneficial	Considered to simplify the Audit Process for Auditee and Audit Team but not normally considered essential. An inability to support these Audit Processes should not normally affect or delay the Off-site Audit.

CSR section	Assessed through (See explanations in Audit tools reference)																							
	Document review D			Stakeholder interview S			Operational personnel interview P			Live observation O			System configuration review C			Sampling and testing T			Logs, reports and records L			Internal audit reports I			CCTV recordings R		
Policy, Strategy and Documentation	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live
1.1 Policy	E[1]				E																						
1.2 Strategy	E[1]				E															E							
1.3 Business continuity planning	E[1]				E															E							
1.4 Internal audit and control	E[1]				E																	H	E				

CSR section	Assessed through (See explanations in Audit tools reference)																							
	Document review D			Stakeholder interview S			Operational personnel interview P			Live observation O			System configuration review C			Sampling and testing T			Logs, reports and records L			Internal audit reports I			CCTV recordings R		
	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live
Organisation and Responsibility																											
2.1 Organisation		E[1]			E			H												E							
2.2 Responsibility		E[1]			E			H																			
2.3 Incident response and reporting		E[1]			E			H												E							
2.4 Contracts and liabilities		E[1]			H																						
Information																											
3.1 Classification		E[1]			E															E							
3.2 Data and media handling		E[1]			E															E							
Personnel Security																											
4.1 Security in job description		E[1]			E															E							
4.2 Recruitment screening		E[1]			E															E							
4.3 Acceptance of security rules		E[1]			E															E							
4.4 Incident response and reporting		E[1]			E															E							
4.5 Contract termination		E[1]			E															E							
Physical Security																											
5.1 Security plan		E[1]			E			H				E															
5.2 Physical protection		E[1]			E			H				E		E	H		E	E		E	H					E[2]	H
5.3 Access control		E[1]			E			H				E		E	H		E	E		E	H					E[2]	H
5.4 Security staff		E[1]			E			H	E			E								E	H					E[2]	H
5.5 Internal audit and control		E[1]			E			E														H	E				

CSR section	Assessed through (See explanations in Audit tools reference)																							
	Document review D			Stakeholder interview S			Operational personnel interview P			Live observation O			System configuration review C			Sampling and testing T			Logs, reports and records L			Internal audit reports I			CCTV recordings R		
	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live
Certificate and Key Management																											
6.1 Classification		E[1]			E															E							
6.2 Roles and Responsibilities		E[1]			E															E							
6.3 Cryptographic key specification		E[1]			E									E				H		E	H						
6.4 Cryptographic key management		E[1]			E				E			E		E	H		E	H		E	H					E		B
6.5 Audit and accountability		E[1]			E									E						E	H					E		B
6.6 GSMA PKI Certificates		E[1]			E							E		E						E								
Sensitive process data management																											
7.1 Data transfer		E[1]			E			H						E			E	H		E						H		B
7.2 Sensitive data access, storage, retention		E[1]			E			H				H		E	H		E	H		E								
7.3 Data generation		E[1]			E			H				E		E	H		E	H		E						H		B
7.4 Auditability and accountability		E[1]			E			H				H		E	H		E	H		E	H					H		B
7.5 Duplicate production		E[1]			E			H				E		E	H		E	H		E								
7.6 Data integrity		E[1]			E			H				H		E			E	H		E								
7.7 Internal audit and control		E[1]			E			E												E		H	E					

CSR section	Assessed through (See explanations in Audit tools reference)																										
	Document review D			Stakeholder interview S			Operational personnel interview P			Live observation O			System configuration review C			Sampling and testing T			Logs, reports and records L			Internal audit reports I			CCTV recordings R		
	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live	Off	On	Live
Logistics and production management																											
8.1 Order management	E[1]			E					E																		
8.2 Raw materials	E[1]			E					E			E					E	E		E							
8.3 Control, audit and monitoring	E[1]			E					E			E					E	E		E	S					E[2]		S
8.4 Destruction	E[1]			E					E			E					E	E		E	S					E[2]		S
8.5 Storage	E[1]			E					E			S					E	E									
8.6 Packaging and delivery	E[1]			E					E			E					S	S									
8.7 Internal audit and control	E[1]			E				E												E		S	E				
Computer and network management																											
10.1 Policy	E[1]			E				S	E																		
10.2 Segregation of roles and responsibilities	E[1]			E				S	E			E		E	S					E	S						
10.3 Access control	E[1]			E				S	E			E		E	S					E	S					S	
10.4 Remote access	E[1]			E				S	E			E		E	S					E	S						
10.5 Network security	E[1]			E				S	E			E		E	S		E	S		E	S					D	
10.6 Systems security	E[1]			E				S	E			E		E	S		E	S		E	S					D	
10.7 Audit and monitoring	E[1]			E				S				E		E	S		E	S		E	S						
10.8 External facilities management	E[1]			E				S												E	S						
10.9 Internal audit and control	E[1]			E				S												E		S	E				

For entries marked as E^n it is essential that the Audit Team can access the information during the Audit, either through Off-site review or as part of an On-site interactive session.
For E^1 it should normally be possible to provide most information to the Audit Team for Off-site review, but the Auditee may indicate its preference to provide some specific parts only through an interactive audit session where there are legitimate concerns about commercial sensitivity.
For E^2 it should always be possible to provide the information through an interactive audit session, but there may be benefits in making it available for review by the Audi Team Off-site.

D.2 Remote audit: On-site assessment process

D.2.1 On-site Audit Sample Agenda

Half-day segment	Outline agenda	Suggested Auditee preparation
1	• Introductions • Agreement of agenda • Overview of changes to Site and security management system since off-site Audit	Preparation of any necessary introductory presentations (not normally expected/required except where significant changes have occurred).
	• Testing of IT security controls	On-site visit to data/server rooms and IT management suites. Sample checks of system configuration to validate consistency against processes described. Testing of physical security controls within the IT environment(s).
	• Testing of key management controls	On-site review of key management systems and records. The Auditors may request completion of a demonstration key ceremony during the Audit using test/dummy keys. Testing of physical security controls within the key management environment.
2	• Testing of production security controls	On-site review of production security controls. Testing of physical security controls within the production environment.
	• Physical security external and internal inspection and testing	Site and building perimeter inspection. Testing of physical security controls around the site exterior/perimeter Testing of physical security controls applied internally at the site.
3	• Security control room inspection and testing	Review of control room live operations. Testing of physical security systems.
4	• Internal audit system • Finalise report, present findings	

Annex E Document Management

E.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	9 Oct 2020	Merged existing methodology variations for temporary extension assessments and hybrid audits and new methodology variation for remote audits into a single document.	James Messham, FML Vernon Quinn, ChaseWaterford David Maxwell, GSMA
1.1	18 Apr 2023	Updated GSMA logo.	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 & questions are always welcome.