This document is classified as **Green**. Disclosure is limited, recipients can distribute this information to SEC Parties and SMIP stakeholders but must not be made publicly available.

SSC Guidance for Device Security Assurance & Triage

Part 3: Triage Security Controls Framework (TSCF):

Section 1: Triage Facility Security Assessment Methodology

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.6
Date	11 February 2026
Document Status	SSC Approved
Date of Next Review	TBD
Classification	Green

Change Record

Date	Author	Version	Change Reference
09/09/2022	User CIO	0.1	Initial draft for SSC review
15/09/2022	SECCo	0.2	Updated terminology to align with MP203
23/11/2022	SECCo	1.0	Updated to align with Parts 1 and 2 and approved by SSC
08/03/2023	SECCo	1.1	Updated with SSC clarifications on a) the scope of assurance of a Triage Facility and b) tamper-protection boundaries.
24/05/2023	SECCo	1.2	Updated with SSC clarifications on Certification of Triage Facility Provides, 'secure area' and personnel screening.
11/09/2024	User CIO	1.3	Updates to Section 2 only include lessons learned from the first triage assessments, including: • To provide clarity and ease of use for Users • Consideration of the differences in the baseline level of information security knowledge • Context around how Triage Facilities operate in practice. • A requirement to notify SSC of a material change. Provision of a fourth day on the Full User Security Assessment timetable (Appendix A), if required.
28/05/2025	SECCo	1.4	Updated following transfer of CPA Scheme from NCSC to SSC; updated references to DESNZ.
26/09/2025	SECAS	1.5	Updated versioning of Section 1 to align with changes made to Section 2 for ISO 27005:2011 & 2018 sections referenced in Appendix B (G5.14, G5.15) and Appendix F to reflect ISO 27001:2022 and 27005:2022.
11/02/2026	SECCo	1.6	Updated to include references to Part 4 (Use Case 005 TSCF) and to update references.

Table of Contents

Note: references to 'User' throughout this document should be read to apply to Triage Facility Providers for Use Case 004 (SEC G12.5) - applicable to GSME, ESME and SAPCs only.

1. Regulatory Context

The security controls and assurance arrangements for the end-to-end Smart Metering System are defined in the Smart Energy Code (SEC) and aim to provide confidence to all SEC Parties that the systems and Devices supporting smart metering are appropriately secure.

The SEC Section G7.19 places an obligation on the Security Sub-Committee (SSC): *"The Security Sub-Committee shall:*

(j) develop and maintain documents to be known as "SSC Guidance for Device Security Assurance and Triage" which shall set out the guidance of the Security Sub-Committee in respect of the requirements and processes to be followed in respect of Devices (including their triage and refurbishment) in order to:

(i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and

(ii) obtain and maintain CPA Certification."

The SSC Guidance for Device Security Assurance and Triage is in three parts:

- Part 1 provides the methodology, a process and a template for any party to raise a change to the Commercial Product Assurance (CPA) Security Characteristics (SCs) or to raise a Use Case for Device Triage.
- Part 2 provides details of the arrangements and the Security Requirements and Guidance to be applied to Use Cases that have been approved by the SSC.
- Part 3 provides details of the assurance arrangements for Triage Facilities in the form of a Triage Security Controls Framework (TSCF):
    - Section 1 of the TSCF describes the purpose and what the TSCF aims to achieve; the different types of Security Assessment and their frequency; and the role of the User CIO;
    - Section 2 of the TSCF provides greater detail at a practical level for the User Assessment lifecycle with information and logistical requirements for how a User should engage with the User CIO; the timeline for User Assessments; and the detailed questions the User CIO might ask, and the evidence it might expect to see from a User to support its assessment.
- Part 4 provides details of the of the assurance arrangements for Use Case 005 (4G CH & Later Factory Reset) Triage arrangements in the form of a Triage Security Controls Framework (4G CH TSCF) and provides detailed questions the DCC CIO might ask, and the evidence it might expect to see from the DCC and its Service Providers to support its assessment.

[Note that Manufacturer's (and DCC for 4G and later Communications Hubs) Triage Systems, Triage Tools and Triage System Interfaces are assured via an extension to the CPA Build Standard, as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC and CH SCs and CPA Build Standard Extensions"*.]

The SSC Guidance for Device Security Assurance and Triage forms part of the SEC Materials defined in SEC Section M5.1, and the document is regularly reviewed and updated by the SSC.

The Smart Metering Equipment Technical Specifications (SMETS2+) and Great Britain Companion Specifications (GBCS) are Schedules to the SEC that contain a minimum set of functional, technical and security requirements to enable SMETS2+ Devices to be installed and to operate efficiently and securely in consumer premises.

The SSC Guidance for Device Security Assurance and Triage has been created to support Device Triage for Use Cases approved by the SSC since the SMETS 2+ and GBCS do not contain requirements applicable after the Device has been removed from the consumer premises.

The documents comprising SSC Guidance for Device Security Assurance and Triage assume the reader has a high degree of familiarity with the SEC and the CPA SCs and is knowledgeable on security matters. As such, defined terms (where capitalised) have the same meaning as those defined in the SEC and CPA SCs and other capitalised terms are defined in this document.

Assurance of the Triage Facility Provider for 4G and later CHs is not in scope of this Triage Facility Security Controls Framework (TFSCF). Separate Security Assurance of CH Triage is managed via the DCC Security Controls Framework and the SSC Guidance on Device Security Assurance and Triage Part 4.

2. Introduction

Security and privacy are at the heart of the end-to-end Smart Metering System. Considerable effort has been invested by the energy industry in designing security protection into the end-to-end 'trust-based' security architecture. Security requirements have been developed for smart metering equipment, Users, the DCC and Triage Facility Providers with the purpose of designing proportionate security controls which are subsequently implemented and assured. The smart metering security obligations are set out in the Smart Energy Code (SEC) in Section G

As required by the Smart Energy Code (SEC), each Use Case 004 Triage Facility Provider with obligations set out in SEC Section G12 **(henceforth referred to as a 'User')** shall be a SEC Party and shall be independently assessed by the User Independent Security Assurance Service Provider also known as the User Competent Independent Organisation (User CIO) to a pre-defined assessment cycle set out in the SEC.

The purpose of these assessments is to provide confidence to SEC Parties (via the SEC Panel's responsibility, now delegated to the Security Sub-Committee (SSC), to set the assurance status as in SEC G12.7) on the compliance status of each Triage Facility Provider.

Following consideration of the User Security Assessment Report, the SSC will provide the Triage Facility Provider with confirmation of the assurance status and whether the next assessment (to be scheduled within 12 months) will be a Full User Security Assessment, a Verification User Security Assessment or a Self-Assessment.

To enable the SSC to set the assurance status, each Triage Facility Provider is to be assessed against SEC security obligations via a Triage Security Controls Framework (TSCF). The TSCF is intended to provide the basis for a consistent level of review across all Triage Facilities, and to provide a guide to the types of evidence which could be provided by a Triage Facility Provider to demonstrate compliance with its obligations.

The Security Sub-Committee (SSC) is responsible for producing and maintaining the TSCF as part of the SSC Guidance for Device Security Assurance and Triage and each version is approved by the SSC. The User CIO uses the latest version of the TSCF and the SEC. The TSCF forms part of the SEC Materials defined in SEC Section M5.1, and it is regularly reviewed and updated by the SSC.

As defined under G12.5 for the purposes of Sections G1, G3 to G5, G7 and G8, unless the "SSC Guidance for Device Security Assurance and Triage" otherwise requires, a Triage Facility Provider shall be treated as if it were a User, and reference to User relates to Triage Facility Provider that is being assessed to provide a Triage Facility.

3. Purpose

What the TSCF is intended to achieve

The TSCF is intended to provide support and guidance to all parties involved in the User Security Assessment Process. The Triage Security Controls Framework (TSCF) shall:

(i) set out the appropriate User Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G12 (Security Assurance of Device Triage Facilities); and

(ii) be designed to ensure that such security assurance assessments are proportionate, consistent and achieve appropriate levels of security assurance in respect of different Triage Facilities and their unique operational context.

Section 1 of the TSCF provides the methodology and high-level guidance to explain the approach, the types of assessment and the method that the User CIO will use to conduct the various types of User Security Assessment in line with the SEC obligations.

Section 2 of the TSCF provides more detailed and practical guidance for Triage Facility Providers to assist them through the assessment process and the review by the SSC and the potential steps required prior to commencing and continuing Triage Activities together with the arrangements for Certification of 'Triage Facility Assurance Status'. The Appendices in Section 2 describe the type of evidence the User CIO will expect to see, as well as providing guidance on formulating a management response to the User CIO observations, preparing for the review by the Security Sub-Committee (SSC) and the likely steps needed to be able to commence live operations together with a template of the Certificate of 'Triage Facility Assurance Status'.

What the TSCF (Sections 1 and 2) describe

The TSCF Section 1 describes the User Security Assessment methodology. It explains:

- the different types of User Security Assessment including the applicable assessment criteria and frequency of assessment.
- the high-level activities and requirements of each stage of the assessment lifecycle: prior to an assessment, during an assessment, and post-assessment.
- Frequently Asked Questions

The TSCF Section 2 provides greater detail at a practical level for the User Security Assessment lifecycle. It explains:

- information and logistical requirements for how a Triage Facility Provider engages with the User CIO along with the timeline for User Security Assessments;
- guidance on the transitional period allowed by the SSC for compliance with new or changed standards, procedures and guidelines that are specified in the SEC (with the responsibility in SEC G1.3 delegated to the SSC by the SEC Panel);
- the detailed questions the User CIO might ask, and the evidence it might expect to see from a User to support its assessment along with SSC clarifications where these seem appropriate**.** These are split between what the User CIO will expect for the design stage and for the implementation stage. **This is a 'must read' section for all Triage Facility Providers prior to undertaking a User Security Assessment.**
- guidance on preparing a User management response to User CIO observations and how to prepare for the SSC review.
- guidance on handling any follow-up actions from the SSC review, the setting of an assurance status and any follow up steps required prior to commencing live operations.
- arrangements for issuing and publishing the Certificate of 'Triage Facility Assurance Status'.

What the TSCF is not intended to achieve

The TSCF is not designed to be a prescriptive list of tests that a Triage Facility Provider must pass to be able to demonstrate compliance with its obligations. Similarly, it does not form part of a 'compliance checklist' exercise of controls that will be tested by the User CIO and the evidence that will be requested.

The TSCF is not exhaustive in its description of the questions that the User CIO may ask of Triage Facility Providers, and the evidence that the User CIO may need to gather to support its work.

Therefore, it should not be regarded as a replacement for the SEC. Placing reliance on the TSCF will not guarantee compliance with the SEC.

For the avoidance of doubt, Triage Facility Providers are required to comply with the SEC obligations; the TSCF provides guidance but does not contain compliance requirements or obligations.

4. The Role of the User CIO

The primary role of the User CIO is to conduct assessments of a User's compliance with SEC Sections G1, G3 to G5, G7, G8 and G12. The User CIO is also required, where requested, to consider the User's management response to this assessment and to advise the SEC Panel and its Security Sub-Committee on matters of non-compliance. The types of assessment that may be conducted are outlined below. The User CIO communicates impartial observations to Triage Facility Providers and the Security Sub-Committee. The User CIO is not responsible for making the decision regarding the assurance status or regarding sanctions that could be imposed should the User be deemed to be non-compliant with its obligations. The sanctions framework is specified in the SEC.

The role of the User CIO, as defined in SEC Section G8.3, is to:

(a) carry out User Security Assessments at such times and in such manner as is provided for in Section G12.6;

(b) produce User Security Assessment Reports in relation to Triage Facility Providers that have been the subject of a User Security Assessment;

(c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;

(d) otherwise, at the request of, and to an extent determined by, the Security Sub-Committee, carry out an assessment of the compliance of any User with its obligations under Sections G1, G3 to G5, G7, G8 and G12. where:
   (i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increases in the security risk relating to that Triage Facility Provider has been identified; or
   (ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;

(e) review the outcome of User Security Self-Assessments;

(f) at the request of the Security Sub-Committee, provide to it advice in relation to:
   (i) the compliance of any Triage Facility Provider with its obligations under Sections G1, G3 to G5, G7, G8 and G12; and
   (ii) changes in security risks relating to the Systems, Data, functionality and processes of any User which fall within Section G5.14 (Information Security: Obligations on Users) which also apply to Triage Facility Providers;

(g) at the request of the SEC Panel, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(h) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and

(i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G8.

5. User Security Assessments, Frequency and Roles

This section describes the types of User Security Assessment which a Triage Facility Provider may require and sets out the assessment frequency and lifecycle including what is expected of the Triage Facility Provider and User CIO prior to, during and after a User Security Assessment together with an explanation of User roles in relation to SEC security obligations.

Prior to go-live of a Triage Facility, any Triage Facility Provider must undertake an initial User Security Assessment.

Once this has been completed, as per G12.8 the SSC will make the determination of which of the four types of User Security Assessment the Triage Facility will undergo taking into account:

a) any security risks identified as part of the previous User Security Assessment, or any identified since the previous User Security Assessment

b) the volume of Devices for which Triage Activities are carried out.

5.1 Types of Assessment

Full User Security Assessments

A “Full User Security Assessment” is an assessment carried out by the User CIO to assess User compliance against the obligations specified in SEC Sections G1, G3 to G5, G7, G8 and G12 as required by SEC G12.6. It is typically performed on-site with the Triage Facility as agreed in advance.

The assessment itself typically takes between 3 and 8 days for the User CIO to review evidence to establish the extent of compliance, depending on the size, scale and nature of the User, and the scope of its Triage Activities.

The assessment involves:

- a review of relevant documentation, interviews with key stakeholders and the testing and evidence collection to demonstrate the effective operation of identified controls to demonstrate compliance with SEC Sections G1, G3 to G5, G7, G8 and G12. The User CIO will therefore require access to all key documentation and on-site access, as well as key stakeholders as agreed with the User, prior to commencing the assessment;
- a review of the outcome of any previous User CIO assessments and any risk assessments conducted and mitigations or changes implemented since;

At the request of the SSC, the User CIO has been asked to collect information on the number of Devices on which Triage Activities have been performed in the past twelve months and the volume awaiting Triage for each Triage Facility at the time of the assessment. This information is needed to assist the SSC in assessing the materiality and the degree of risk arising from any User CIO observations.

An outline of the assessment timetable for the Full User Security Assessment, together with the Optional Pre-Assessment timetable, is presented in TSCF Section 2 Appendix A.

All Triage Facility Providers are required to successfully complete an initial Full User Security Assessment as a condition of approval to undertake the Triage of Devices where SEC Section G12 applies.

Optional Pre-Assessment: High-level Scope and Governance Review

In advance of any User Security Assessment, a User may request an Optional Pre-Assessment. The purpose of this assessment is to assist a User to prepare for a User Security Assessment by performing a review against the TSCF document.

Such a Pre-Assessment may examine those areas that could be considered fundamental to a User's approach to achieving compliance, such as the interpretation of the Triage Activity definition. The high-level scope and governance review will typically include:

- a review of the scope of the User's Triage Activities.
- a review of the User's governance arrangements.
- A review of any other obligations the User wishes to discuss, within the scope of Section G.
- interviews with the following key stakeholders or equivalent, where applicable:
  - Chief Information Security Officer (CISO) - Opening Meeting.
  - Smart Metering ISMS Officer / Manager.
  - Key parties involved in defining the scope of the Triage Facility Systems.

The assessment is expected to take approximately 2 working days and Triage Facility Providers should be aware that the Optional Pre-Assessment does incur additional costs.

An outline of the assessment timetable for an Optional Pre-Assessment is presented in TSCF Section 2, Appendix A.

Verification User Security Assessment

A "Verification User Security Assessment" is an assessment carried out by the User CIO to identify any material increase in the security risk since the last Full or Verification User Security Assessment, in accordance with the obligations in SEC Section G5.14. The scope of this assessment focuses on those areas exposed to any material increase in security risks. It is anticipated that the assessment will take between 2 and 3 days depending on the size, scale and nature of the Triage Facility, the scope of its Triage Facility systems and processes and the degree of any change to the risk profile. The User CIO will require access to key documentation and locations as well as key stakeholders as agreed with the User prior to the assessment, as part of the pre-assessment communication. Triage Facility Providers are referred to TSCF Section 2 Appendix F for further information on what information is typically sought for this type of review.

User Security Self-Assessment

A User Security Self-Assessment is carried out by the User to identify any material increase in the security risk since the last occasion on which a Full or Verification User Security Assessment was carried out. The scope of this assessment focuses on those areas exposed to any material increase in security risks as indicated by a Triage Facility's obligation to identify and manage risk (in accordance with SEC Section G5.14).

The User is responsible for conducting the Self-Assessment using internal resources and under their own timescales and is responsible for producing a response to be presented to the User CIO for review within a pre-agreed timescale prior to the results being provided to the SSC (with responsibility delegated by the SEC Panel).

The User will be required to provide evidence to support some of the assertions made in the Self-Assessment and this will be considered by the User CIO. The information that the User CIO would expect to find enclosed within this report is contained within TSCF Section 2 Appendix G.

Follow-up Security Assessment

A Follow-Up Security Assessment is an assessment carried out by the User CIO at the request of the SSC. The User Security Assessment Response (generally known as the User management response), where relevant, sets out the steps the User commits to take to address any instances of non-compliance or partial

compliance observed by the User CIO. Under SEC Section G8.29, the SSC may request the User CIO to perform a Follow-Up Security Assessment of a User to:

a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

The scope and duration of the Follow-Up Security Assessment is dependent on the requirements set by the SSC who will provide details to the Triage Facility Provider and the User CIO.

5.2 The Security Assessment Lifecycle

Prior to any assessment, the User will have a period between informing the User CIO (via SECAS) of their requirement to be reviewed and the assessment taking place. Upon initiation of the cycle, the User CIO will provide the User with sufficient information with which to prepare for the assessment. This may include an assessment timetable, key stakeholders for interviews, and a documentation request list.

During the assessment, the User CIO will work with the User to refine the schedule to ensure all the necessary SEC obligations are covered whilst limiting disruption to Triage Facility business operations.

Post assessment, the User CIO will provide the User with a draft report. The User will have adequate time to respond to any findings before the User Assessment is reviewed by the SSC.

5.3 Timings of Second and Subsequent Assessments

Second User Security Assessment

Triage Facility Providers are obliged in SEC Section G8.40 to schedule their second Security Assessment within twelve months of the SSC (with delegated responsibility from the SEC Panel) setting an assurance status to either '***approved***' or '***approved, subject to the Party taking steps ...***'' the start of this second User Security Assessment then locks in the User's annual fieldwork start deadline.

For clarity, the second Full or Verification User Security Assessment or Security Self-Assessment is not required to take place within twelve months of the assurance status being set, just for the User Security Assessment to be scheduled and then started within 12 weeks. This allows for some flexibility in the timing of the User Security Assessment taking place, to cater for capacity in the User CIO resources to undertake multiple User Security Assessments, for capacity in the SECAS resources to undertake validation of the User management response and in the capacity of the SSC to review multiple User Security Assessments.

An example of this is if an organisation was granted its assurance status on 8th November 2022, they will be required to have their next assessment booked 12 months later, by 8th November 2023, and started no later than 12 weeks later, by 31st January 2024. This date then becomes the annual fieldwork start deadline that all future Assessments must start by.

Subsequent User Security Assessments

The SSC expects that all Full or Verification User Security Assessments or Security Self Assessments following the second-year assessment should be scheduled to ensure they are started on or before the User's annual fieldwork start deadline. The User's annual fieldwork start deadline is fixed, and will not be reset if, due to extenuating circumstances, a User were to gain exceptional approval from the SSC to miss their deadline in one year.

For example:

A second year User Security Assessment started by 31 January 2024 must have the next assessment commenced by the annual fieldwork start deadline of 31 January 2024;

If the next Assessment occurs in March 2025, due to extenuating circumstances approved by the SSC, then the subsequent assessment is still due by 31 January 2026 (not March 2026);

As outlined above, any Assessment that is requested to take place after the set annual fieldwork start deadline can only occur with the approval of the SSC. The User must make a formal request to the SSC, including sufficient rationale, for their Security Assessment to take place later than required, including the date on which they wish their assessment fieldwork to start. This would be on an exception basis and would not reset the annual fieldwork start deadline and the User's next Security Assessment would be expected to occur within the original timeframe.

Scheduling

SECAS will maintain an overview of the second and subsequent User Security Assessments that are becoming due and will contact Users at least six months before their annual fieldwork start deadline with suggested dates for their assessment.

It ultimately remains the responsibility of the User to make sure their User Security Assessments take place when required and Triage Facility Providers should look to book these in as soon as possible to obtain a preferred date.

The exact timing of the User Security Assessment will normally be allocated no later than 12 weeks prior to the annual fieldwork start deadline by SECAS to depending on the capacity of the User CIO, SECAS and the SSC to manage the volume of User Assessments.

SECAS will contact the User to confirm the total number of Devices on which is performs Triage Activities annually (in the preceding 12 months).

5.4 Post Assessment

More detail is provided in TSCF Section 2, but the methodology requires that, following the completion of a Full User Security Assessment, a Verification User Security Assessment or a Follow-Up Security Assessment, the User CIO will produce a written report which shall:

a) set out the findings of the User CIO on all the matters within the scope of the User Security Assessment;

b) in the case of a Full User Security Assessment:

   (i) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G1, G3 to G5, G7, G8 and G12 which have been identified by the User CIO; and

   (ii) set out the evidence which, in the opinion of the User CIO, establishes each of the instances of actual or potential non-compliance which it has identified; and, in the case of a Verification User Security Assessment:

   (iii) specify any material increase in the security risk relating to that User which the User CIO has identified since the last occasion on which a Full User Security Assessment was carried out in respect of that User; and

   (iv) set out the evidence which, in the opinion of the User CIO, establishes the increase in security risk which it has identified.

The User CIO will submit a draft copy of the User Security Assessment Report to the User for review of factual accuracy checking and also to enable the User to start to draft a User management response. The User shall have 5 working days to review the report and respond to the User CIO with changes of factual accuracy for consideration but will continue to draft the User management response.

The User CIO will then have up to 5 working days to accept, explain or reject factual accuracy changes submitted for considerations by the User. The User Security Assessment Report will be updated as applicable where the change is accepted by the User CIO and re-issued to the User.

From the point at which the User receives the original draft copy of the User Security Assessment Report, the User will have 15 working days to compile the User management responses to the identified observations and submit these to SECAS. The User management responses are intended to satisfy the requirements of the User Security Assessment Response (set out in SEC G8.24 and G8.26).

SECAS will undertake a validation of the User management response on behalf of the SSC and will advise the SSC of the extent to which the response meets the User CIO observation. Where SECAS considers that the User management response is inadequate or requires clarification, SECAS will advise the User and provide an opportunity for an improved response to be submitted. The User CIO will then have 5 working days to consider the User management response (updated as appropriate following SECAS advice) and the SECAS validation and to provide comments to the SSC. The SSC will consider whether, based on the User CIO observations, the User management response and the comments from SECAS and the User CIO, whether to confirm an assurance status in line with SEC Section G12.7 and G12.8. If the assurance status is approved, the SSC will issue a Certificate of 'Triage Facility Assurance Status' that records the date of the relevant SSC meeting and shows the start date of the approval and the date the next approval is due. If the assurance status is 'approved subject to the Party taking steps….' e.g. to remediate any observations of non-compliance by a certain date or if the SSC wishes the Triage Facility Provider to note any conditions attached to the approval, then the SSC will provide a letter to the Triage Facility Provider. Where the status is 'approved' the SSC will publish the Certificate on the SEC website for visibility by Manufacturers, Suppliers and any parties who have an interest in the assurance of the Triage Facility Provider.

6. Changes of Company Ownership

The situation may arise where there is a change in company ownership after the assurance status has been set by the SSC (having had the responsibility delegated by the SEC Panel) to:

- 'approved'; or
- 'approved subject to steps' and those steps have been completed to the satisfaction of the SSC; or
- 'approved subject to steps and both taking such steps and being subject to a Follow-up Security Assessment by such date as the SEC Panel (delegated to the SSC) may specify' and the SSC, is satisfied on the evidence of the Follow-up Assessment that the steps have been completed; or
- 'provisionally approved subject to taking steps and having a Follow-up Assessment' and the SSC, is satisfied on the evidence of the Follow-up Assessment that the steps have been completed.

In these circumstances, the SSC has agreed it would not normally expect to require any further security assessment to be carried out on a company taking ownership of an existing company, either when it is bought off the shelf or when ownership changes by any other legitimate means.

However, the SSC reserves its right under G8.3(d)(ii) to instruct a security assessment in any case in which it has a legitimate concern arising from the change of ownership, or in which the circumstances of the company otherwise justify it.

Unless the SSC instructs a security assessment under G8.3(d)(ii), then the next User Security Assessment would be the next, scheduled, annual User Security Assessment.

Appendix A – Frequently Asked Questions

(Note that greater detail is provided in TSCF Section 2 that will address many of the FAQs)

List of FAQs

How do I engage with the User CIO

Triage Facility Providers should engage with the User CIO through SECAS who will act as the intermediary and can be contacted through email at: SSC@talan.com.

When should I engage with the User CIO?

Triage Facility Providers should engage with the User CIO through SECAS at least 12 weeks prior to their requested assessment date. Triage Facility Providers are responsible for engaging with the User CIO.

When will I get my assessment report?

Unless otherwise agreed, a draft User Security Assessment report will be released to the User for review 10 working days after the final day of the fieldwork (sometimes referred to as the 'hard close' meeting). The User will then have 15 working days to compile the User management responses to the identified observations and submit these to SECAS. This will be considered as the User Security Assessment Response, as mandated by G8.22. In the interim, the User will have 5 working days to provide the User CIO with comments with regards to factual accuracy checking. The User CIO will then have 5 working days to respond to the User to accept, explain or reject and make updates to the report, which will be sent back to the User.

What do I need to do if I wish to change or cancel my assessment?

Triage Facility Providers are requested to inform the User CIO at the earliest opportunity if the dates of an assessment are required to be changed.

The User CIO will also be entitled to recover any sunk costs associated with work undertaken in advance of an assessment, regardless of notice provided.

The following cancellation fees also apply:

- 0% of the estimated assessment fees will be charged if you provide greater than 4 weeks' notice, or if the User CIO is able to redeploy its allocated resource to other projects at no additional cost to them.
- 25% of the estimated assessment fees if you provide the User CIO with less than or equal to 4 weeks' notice.

How do I ensure an efficient assessment?

There are a number of key factors which contribute to ensuring an efficient review. It is recommended that Triage Facility Providers:

- Have a clearly articulated scope and definition for the systems and processes that are under assessment along with identification and explanations of interdependencies.
- Have a physical and logical system and process architecture diagram that clearly demonstrates the scope of the Triage Facility, how 'separation' has been achieved between the Triage Facility and adjacent physical areas and identifies the security controls to treat the risks identified in the risk assessment.
- Ensure that risks have been thoroughly assessed from the perspective of Confidentiality, Integrity and Availability in line with ISO27005.
- Have a clearly defined traceability matrix linking the SEC obligations a User is required to meet to the security controls implemented which the User deems supports their compliance.
- Provide the User CIO with the required documentation including hard and soft copies in a timely manner when requested. The User should consider existing certifications which could be relied upon by the User CIO, e.g. ISO 27001 certificates for an appropriate scope.
- Be prepared to show the User CIO evidence, to support the obligations under assessment.
- For assessments at the Triage Facility site, provide meeting locations including a permanent 'base' location for the User CIO onsite team to be located throughout assessment.
- In the case of assessments at a Triage Facility site, organise in advance the appropriate access for the User CIO onsite team to the Triage Facility.

- Have the appropriate staff or suitable alternates available throughout the assessment and inform the User CIO in advance if any key staff are unavailable.
- Remain transparent and cooperate with the User CIO throughout the assessment.
- With respect to a User Security Self-Assessment, provide concise evidence and be prepared to show it to the User CIO, (whether on-screen or through submitting documents) to support some of the assertions made in the template provided in TSCF part 2 Appendix G.

Whom might the User CIO need to meet with?

- Chief Information Security Officer (CISO) / lead security consultants and architects
- System administrators
- Solution designers
- Human Resources representatives
- Internal audit / Compliance
- Third parties (where applicable)

Is there a process for dealing with a disagreement?

Yes. The User CIO report is intended to be a factual account of what has been discovered and provide the SSC with impartial findings and recommendations. Should the User consider the report to contain factual inaccuracies, this matter will be resolved initially between the User CIO and the User. The role of the SSC is to set a User's assurance status and to establish whether there are any security non-compliances. Where a Party disagrees with any decision made by the SSC, it may refer the matter to the Panel. Where a Party disagrees with any decision by the Panel, it may appeal to the Authority and the determination of the Authority shall be final and binding (SEC G8.39).

Will my documentation and information be handled confidentially by the User CIO?

Yes. SECAS provide Triage Facility Providers and the User CIO access to a secure and encrypted platform for the sharing of any User documentation and the provision of the User Security Assessment Report and any Management Responses.

Triage Facility Providers may also make use of their own file sharing platform if they so wish as long as access can be granted to the User CIO for the duration of the User Security Assessment.

Any hard copy information provided by the User will not be taken off-site by the User CIO and any electronic records received will, as required, be temporarily stored on laptops with full disk encryption, before being deleted or transferred to encrypted server infrastructure and only retained to comply with legal, regulatory and professional record keeping obligations.

What approach will the User CIO take towards sampling evidence?

The fieldwork will be principally interview-based, supported with document reviews and observing controls (e.g. on screen). Evidence sampling will take the form of 'review' level assurance, whereby the User CIO will seek to obtain evidence as required to support the assertions of a User, however formal statistical based audit level assurance (e.g. to demonstrate rigorous control effectiveness) will not be employed.

It is recognised that for some Triage Facility Providers some information and evidence may not be available for presentation to the User CIO, simply as a result of the lack of occurrence of a particular event such as replacing a tamper protection seal (where required) following Triage Activities, prior to live running. Another example is that a security incident may not yet have occurred within the Triage Facility System to demonstrate the correct operation of the User's incident management policy. In these situations, where an event is yet to occur, the User CIO may consider the policy and evidence recorded during the User's design, development and testing phases and the detailed future plans to assess the correct functioning of certain controls.

During the assessment, the User CIO will present its understanding to the User in the form of daily review meetings (usually known as a 'wash up' sessions) to clarify evidence received and share provisional

observations based on gaps identified to reduce the risk of factual inaccuracies being identified following delivery of the report.

A 'soft close' meeting will be held upon completion of the fieldwork stage to confirm the accuracy of the observations identified. Following the 'soft close' meeting, there may be an additional evidence upload period, where the User can provide additional evidence in an attempt to address observations raised, lasting up to 5 working days prior to the 'hard close' meeting to formally end the assessment. There should therefore be no surprises for the User when the report is received.

Note: in the case of scenarios where a User is assessed by the User CIO prior to the User's go-live and associated supporting evidence (e.g. replacement of tamper-protection seal (where required) etc) is not available for review at the time of the User CIO's assessment, the User CIO will note this obligation to which the evidence would relate within the "Obligations without complete supporting evidence" category.

How will the User CIO take account of existing security certifications, such as ISO 27001?

The User CIO will take account of existing security certifications and assess whether reliance can be placed upon them during the course of the review. For example, if a User holds ISO 27001 certification for the scope of the Triage Facility System, there is a likelihood that the User CIO will be able to place reliance upon this, subject to being able to confirm the exact scope of certification, the level of testing performed, and whether any material changes had occurred since certification was awarded. In this instance, it is considered that the User CIO would be able to progress more swiftly through certain aspects of the TSCF, such as those pertaining to security governance, risk management, policies and standards, and incident management.

How can a User obtain a threat assessment to inform the risk assessment?

The SSC has provided the following advice on threat identification and assessment:

"A key input to a Party's risk assessment process is the identification of threats to the organisation's assets. A process for identifying threats is outlined in Section 7.3.3, 10.5.2 and Annex A2 of ISO27005, the risk management standard which must be complied with by all DCC Users. Annex C of the standard provides examples of the types of threats that an organisation may be subject to and these may be considered within the context of the business to determine to what extent each of these threats may be in scope.

Understanding the capability and motivation of threat actors that might seek to compromise a system is an important part of this process. Information that may inform this assessment may arise from within (e.g. operational staff, information security specialists etc) or outside your organisation (e.g. threat catalogues, industry bodies, commercial threat assessment providers etc).

The National Cyber Security Centre (NCSC) may be one source of external advice and guidance on threat:

- alerts, advisories and reports on some of the latest threats and this can be found here.
- guidance on how to collect, analyse and evaluate threat intelligence can be found here.

What approach is taken by the User CIO to assess material changes to a User's Triage Activities after a Security Assessment?

The User CIO will assess a User based on the functionality of the User's Triage Activities at the time of the assessment. If a User introduces new functionality (e.g. due to managing a change in risk or to support the development of business processes) that could be considered to be a material change there is no expectation for the User to inform the User CIO of this change. Therefore, and irrespective of whether a User introduces a material change to the functionality of the User's Triage Activities, assessments will be performed as per the timescales outlined in the TSCF such that the next assessment will review material changes to the User's Triage Facility system functionality.

Where there is a predictable material change on the horizon, such as the movement or expansion of a Triage Facility, the User CIO may review designs (subject to them being in a mature and approved state, e.g. by a Design Authority) however it is considered likely that the User CIO will need to raise observations owing to insufficient evidence being available to demonstrate the security controls operating effectively.

How will the User CIO account for evidence that cannot be provided because systems are not operational at the time of the assessment?

The User CIO has agreed with the Security Sub-Committee that an additional category of observation will be included in the User Security Assessment Report known as "Obligations without complete supporting evidence" (colloquially known as the 'Bucket List') to account for the scenario where a User cannot yet provide supporting evidence as systems are not operational at the time of the assessment. These obligations will be assessed at the next User Security Assessment.

This category is to include a list of obligations against which the User CIO has been unable to observe evidence to demonstrate that compliance has been achieved, because the User has not yet implemented the controls at this stage of the system development lifecycle.

Obligations are aligned to this category on the basis that the User CIO has reviewed plans and design documentation relating to the proposals for compliance which have been approved through the relevant internal smart metering governance group. This documentary evidence, supported by discussions with User personnel, has not resulted in any specific observations relating to the obligations being raised within the main body of the report (covering sections G1, G3 to G5, G7, G8 and G12).

How will the User CIO assess a Triage Facility that is undertaking Triage of Use Case 004 Devices as well as other Devices (e.g. other approved Use Cases or SMETS1 or other devices)?

The SSC recognises that there are a number of steps to receive Use Case 004 Devices into the (non-Use Case 004) triage facility premises that can take place without needing to be subject to the same security controls that must apply to the area where the unlocking of internal non-operational ports and changes to configuration of Device Data occurs. These include e.g. reading barcodes and logging the asset details, checking for Devices that are damaged or do not qualify for Use Case 004 Triage etc.

It is specifically the Triage Activities specified in the SEC Section G12.4 a) to e) that should be conducted in a secure area such as a room or cage inside the wider (non-Use Case 004) triage premises and the User Security Assessment should focus on the processes and personnel specifically engaged in Triage Activities.

The SSC has clarified that it is not the intention that the (non-Use Case 004) wider triage facility premises undertaking triage should be subject to User CIO assurance.

Which tamper-protection seals are subject to the User CIO assessment of compliance with SEC Section G12.4(a)?

Devices undergoing Triage Activities are likely to have multiple tamper-protection seals and the provisions of SEC Section G12 only relate to those covered by CPA Security Characteristics (SCs), including the Triage Security Characteristics Document. SEC Section G12.4 states:

G12.4 Each Triage Facility Provider shall:

(a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);

The SSC has clarified that metrology seals should never be broken during Triage Activities but are not covered by the CPA Security Characteristics.

It is likely that most Devices received into a Triage Facility will have had the tamper-protection of the terminal cover of an ESME and/or the battery cover of a GSME breached during essential maintenance or decommissioning.

The SSC has clarified that breach of tamper-protection of an ESME terminal cover or GSME battery cover falls within the SEC Section G12 a) description of 'essential Device maintenance and/or the decommissioning process' and does not prevent Triage Activities for that Device.

Appendix B – Security Obligations Applicable to Triage Facility Providers

List of SEC Obligations

G3.5	19
G3.10	19
G4.1	19
G4.2	19
G4.3	19
G5.14	20
G5.15	20
G5.16	20
G5.17	21
G5.18	21
G5.19	21
G5.20	22
G5.21	22
G12.4(a)	22
G12.4(b)	22
G12.4(c)	22
G12.4(d)	22
G12.4(e)	22
G12.4(f)	23
G12.4(g)	23

SEC Obligation	
G3.5	Each User shall, on the occurrence of a Major Security Incident in relation to its Triage Activities, ensure that the Panel and the Security Sub-Committee are promptly notified.
G3.10	Each User shall: (a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and (b) when any Data held by it cease to be retained in accordance with User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.
G4.1	Each User shall: (a) ensure that each member of its User Personnel who is authorised to access Data held as part of Its Triage Activities, including access to Smart Metering Systems themselves, holds a security clearance which is appropriate to the role performed by that individual and to the Data which he or she is authorised to access; and (b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data which he or she is authorised to access.
G4.2 *G4.3*	G4.2 Each User shall comply with Section G4.3 in respect of any of its User Personnel who are authorised to carry out activities which: (a) involve access to resources, or Data held, for Triage Activities; and (b) are capable of compromising any Triage Activities, or any Device in a manner that could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises. G4.3 Each User shall ensure that any of its User Personnel who are authorised to carry out the activities identified in Section G4.2: (a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with: (i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or (ii) At a minimum where deemed appropriate and justified through a risk assessment, BPSS (Baseline Personnel Security Standard); or (iii) any equivalent to that British Standard which updates or replaces them from time to time; and (b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with: (i) the British Standards referred to in Section G4.3(a); or (ii) any comparable national standard applying in the jurisdiction in which they are located.

SEC Obligation	
G5.14	G5.14 Each User shall establish, maintain and implement processes for the identification and management of the risk of Compromise to: (a) its Triage Activities; (b) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its Triage Activities; (c) any other Data, systems, or processes on which it relies upon for its Triage Activities. (d) any Devices processed within the Triage Facility. (e) any communications links established between any of its Systems and the Triage Activities; and any security functionality used in respect of those communications links or the communications made over them.
G5.15	G5.15 Each Triage Facility shall ensure that such processes for the identification and management of risk comply with: (a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Management Systems); or (b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.
G5.16	Each Triage Facility shall carry out an assessment of such processes for the identification and management of risk: (a) on at least an annual basis; (b) on any occasion on which it implements a material change to: (i) its Triage Activities; (ii) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its Triage Activities; (iii) any other Data, Systems, or processes on which it relies upon for its Triage Activities. (iv) any Smart Metering Systems held within the Triage Facility; and (c) on the occurrence of any Major Security Incident in relation to its Triage Activities.

SEC Obligation	
G5.17 *G5.18*	G5.17 Each User shall comply with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its Triage Activities: (a) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or (b) any equivalent to that standard which updates or replaces it from time to time. G5.18 Each User shall: (a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as its User Information Security Management System; (b) ensure that its User Information Security Management System: (i) is so designed as to ensure that it complies with its obligations under Sections G3 and G4; (ii) is compliant with the standard referred at Section G5.17; (iii) meets the requirements of Sections G5.19 to G5.21; and (iv) provides for security controls which are proportionate to the potential impact of each part of its Triage Activities being Compromised, as determined by means of processes for the management of information risk; and (c) review its User Information Security Management System on at least an annual basis and make any changes to it following such a review in order to ensure that it remains fit for purpose.
G5.19	Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of: (a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the User Systems, including measures relating to Data handling, retention and protection; (Out of Scope) (b) the establishment and maintenance of an Information Classification Scheme in relation to the User Systems; (c) the management of business continuity; (Out of Scope) and (d) the education, training and awareness of those with access to the Triage Facility. Note: (a) and (c) are not in scope for Triage Facility Providers.

SEC Obligation	
G5.20	Each User Information Security Management System shall specify the approach of the User to: (a) information security, including its arrangements to review that approach at planned intervals; (b) human resources security; (c) physical and environmental security; and (d) ensuring that any person who provides services to the User for the purpose of ensuring that the User is able to comply with its obligations under this Code must establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the Triage Facility.
G5.21	Each User Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the User to establish and maintain a register of the physical and information assets on which it relies for the purposes of complying with its obligations under this Code.
G12.4(a)	Each Triage Facility Provider shall not attempt to undertake "Triage Activities" on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);
G12.4(b)	Each Triage Facility Provider shall only use a Triage Tool and Triage System Interface that is provided by a manufacturer to access the manufacturer's "Triage System" that has confirmed compliance with the requirements of the Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
G12.4(c)	Each Triage Facility Provider shall ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage Interface;
G12.4(d)	Each Triage Facility Provider shall at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;
G12.4(e)	Each Triage Facility Provider shall ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;

SEC Obligation	
G12.4(f)	Each Triage Facility Provider shall maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of: (i) the Requestor of any change to the configuration of a Device; (ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities; (iii) details of Triage Activities successfully undertaken; (iv) details of any failed attempts to complete Triage Activities; and (v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;
G12.4(g)	Each Triage Facility Provider shall when requested by the Security Sub-Committee to do so, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.4(f)