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 2: Triage Facility Security Assessment Guidance

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 SEC G12.4(c) and Section 1 and approved by SSC
09/02/2023	User CIO	1.01	Updated following Triage Facility field visit
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	SECCo	1.5	ISO 27005:2011 & 2018 sections referenced in Appendix B (G5.14, G5.15) and Appendix F amended 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 generally 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. Introduction

Section 1 of the Triage Security Controls Framework (TSCF) explains that security and privacy are at the heart of the Smart Metering System and that 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, for the DCC, and for Users including 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 Triage Facility Provider must 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.

A Triage Facility Provider **(henceforth described as a 'User')**, which is a Party, shall, under SEC Sections G12.5 be treated for the purpose of SEC Sections G1, G3 to G5, G7, G8 as if it were a User and additional obligations are set out in SEC Section G12. References to Users in the Triage Security Controls Framework (TSCF) should therefore be taken to include Triage Facility Providers.

Section 1 of the TSCF explains the methodology for User Security Assessments including a description of assessment types, frequency and lifecycle of assessments and how the User CIO will approach the assessments.

Section 2 of the TSCF contains guidance for what to expect from an assessment and how a Triage Facility Provider can successfully prepare for one. It explains how to prepare for an assessment along with details of the timelines for an assessment and provides details of what the User CIO will be looking for during the assessment. It also explains how to prepare a User management response (known in the SEC as the User Security Assessment Response) to any observations raised by the User CIO; it provides details of what the Security Sub-Committee will be looking for in a User management response; and the potential steps and follow-up actions that might be required prior to the User being authorised to commence Triage Activities together with the arrangements for Certification of 'Triage Facility Assurance Status'.

As defined under G12.5 for the purposes of Sections G1, G3 to G5, G7, G8 and G12, 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 the organisation that is being assessed to provide a Triage Facility Provider.

The SSC is responsible for producing and maintaining the TSCF as part of the SSC Guidance for Device Security Assurance and Triage which is regularly reviewed and updated by the SSC.

It is important that Triage Facility Providers have read and are familiar with the TSCF in advance of a User Security Assessment and it will be assumed they have done this prior to any User Security Assessment.

This TFPSCF applies to specific Use Cases approved by the SSC and set out in the SSC Guidance for Device Security Assurance and Triage Part 2. **The Use Case approved for this TFPSCF is Use case 004.**

Assurance of the Triage Facility Provider for 4G and later CH 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 for Device Security Assurance and Triage Part 4.

2. Purpose

The purpose of Section 2 of the TSCF is to provide advice and guidance to Triage Facility Providers who will undertake a Security Assurance of Device Triage Facilities (aligned to a User Security Assessment). The information contained in the Section 2 Appendices should enable a Triage Facility Provider to fully prepare for a User Security Assessment by having all the relevant documentation available and to ensure that it is complete and contains evidence to demonstrate compliance with SEC security obligations.

The User CIO will scrutinise the evidence to ensure compliance with the SEC Security obligations in Section G of the SEC. Where there is no evidence or limited / partial evidence, the User CIO will raise an observation of non-compliance or potential non-compliance that will require a User management response. The rating scale used for these is detailed in Appendix I.

Obtaining the formal approval of an assurance status by the SSC (with responsibility now delegated from the SEC Panel) under SEC Section G8.36 is a necessary pre-cursor to commencing Triage Activities (SEC Section G12.7). Failure to obtain a Certificate of 'Triage Facility Assurance Status' confirming approval of the appropriate assurance status from the SSC will prevent approval to commence or continue Triage Activities. Further, where there are outstanding observations of non-compliance, approval to commence or continue Triage Activities is dependent on the SSC confirming satisfactory completion of a Remediation Plan to ensure that all the non-compliances or potential non-compliances have been satisfactorily addressed.

The SSC will continue to monitor compliance with the security obligations in Section G in subsequent User Security Assessments.

The guidance is focused specifically on assisting Triage Facility Providers and the User CIO to assess and achieve compliance with the security obligations in the SEC.

3. Structure of Guidance

The Guidance is set out in discrete Appendices for clarity:

- Appendix A explains the standard timelines for a typical Full User Security Assessment and a typical Optional Pre-Assessment.
- Appendix B describes the questions the User CIO might ask and the type of evidence the User CIO might consider and might expect to see to be able to confirm compliance with the SEC security obligations against which Triage Facility Providers will be assessed. Appendix B also contains an indication of the equivalent NIS / CAF requirements in case these are deemed useful by the Triage Facility. For the avoidance of doubt compliance with the NIS / CAF requirements is not mandated by the SEC, and they are included for reference only.
- Appendix C provides guidance on preparing the User management response that is required under SEC Section G8.26, G8.27, G8.28 and G12.6. SECAS security experts will validate the User management response on behalf of the SSC and will raise any potential problems with the User and seek to resolve them prior to the SSC review with an updated User management response as appropriate.
- Appendix D provides guidance for Triage Facility Providers on preparing for the review by the Security Sub Committee to ensure that the User management response fully addresses the User CIO observations and that all relevant information is available, and that SSC and User time is used as efficiently and effectively as possible.
- Appendix E explains what actions Triage Facility Providers are likely to be required to take prior to commencing Triage Activities depending on the assurance status that is set by the SSC.
- Appendix F provides a template of a User Security Verification Assessment which explains the SEC obligations against which the User CIO will assess compliance.
- Appendix G provides a template of a User Security Self-Assessment Return.
- Appendix H provides guidance to Triage Facility Providers with remaining non-compliances following SSC review of a second or subsequent User Security Assessment.

- Appendix I details the ratings allocated by the User CIO to any observations raised within a User Security Assessment Report.
- Appendix J provides a template of the Certificate of 'Triage Facility Assurance Status'.

4. Prior to an Assessment

This section sets out the steps to be taken prior to a security assessment being performed. The steps are common to all assessment types (except for the Follow-Up Security Assessment, where the steps to be taken may be unique to the nature of the follow-up required).

4.1 Engaging with the User CIO

Prior to any assessment, the Triage Facility Provider is required to engage with the User CIO:

- Engagement with the User CIO is managed via SECAS.
- Triage Facility Providers should seek to engage with the User CIO to schedule their User Assessment at least 12 weeks prior to their desired assessment date. Early engagement to schedule an initial and annual assessment is strongly recommended.
- It is the responsibility of the Triage Facility Provider to engage the User CIO in accordance with the review cycle. However, the User CIO will have regard to capacity and meeting the SEC schedule for User Security Assessments when scheduling the fieldwork for a second or subsequent User Security Assessment.
- Triage Facility Providers should seek to engage with the User CIO when they have system and process design stability and are confident that, for the initial or subsequent User Security Assessment, significant change or further significant change will not occur.
- Triage Facility Providers may wish to arrange an 'engagement day' meeting with the User CIO and SECAS prior to booking an initial assessment to understand how best to prepare for the assessment and to talk through the Triage Facility high-level design.
- For an additional cost, Triage Facility Providers may wish to book an 'Optional Pre—assessment' with the User CIO where existing design and controls can be assessed to provide the User with an understanding of what it needs to address prior to its initial assessment to achieve compliance.
- SECAS has developed a 'scheduling system' to enable Triage Facility Providers to book available slots for a User Assessment. It is recommended that Triage Facility Providers book slots as soon as possible to avoid disappointment if capacity subsequently affects availability and impacts planned dates. Currently, the booking system is held and maintained by SECAS. To understand availability, please contact SECAS.
- Triage Facility Providers wishing to change the dates of an assessment must inform the User CIO at least 4 weeks prior to the original assessment start date.
- A cancellation charge may be applicable if the Triage Facility Provider fails to comply with the appropriate cancellation period.

4.2 Information required by the User CIO

- Confirmation of whether an Optional Pre-Assessment is requested (Note that this will incur additional cost).
- The estimated total number of Smart Metering Systems for which the Triage Facility Provider intends to perform Triage Activities upon annually, this number should relate to the SEC defined Triage Activities which currently applies only to Use-case 004.
- A scope document including a physical and logical system and process architecture diagram explaining the Triage Activities, such as the physical locations of and interaction between the Triage Facility Provider, the Triage Tool(s) and the Triage System Interface(s). This might include a site map showing the security perimeter of the Facility with security controls such as CCTV and lock systems clearly labelled.
- The physical location(s) of the Triage Facility Provider at which the assessment will take place, including detail of how access will be provided to the User CIO.
- Any site specific health and safety or PPE requirements for the User CIO to be aware of.
- A nominated point of contact for the administration and planning of the assessment.

4.3 Information to be provided by the User CIO

- The scope of the assessment. The User CIO will engage with the Triage Facility Provider to determine the scope of the assessment as well as to determine the scale, length, and involvement of User Personnel.
- Where applicable, a preliminary schedule and assessment timetable.
- A list of key Triage Facility Personnel, by role, whom the User CIO may need to meet with during the assessment. This may include third party security personnel. Triage Facility Personnel likely to be required includes:
    - Chief Information Security Officer (CISO) / lead security consultants and architects
    - Site or floor managers
    - Security staff
    - ISMS officer / manager
    - System administrators
    - Solution designers
    - Human resources
    - Internal audit / Compliance resources
    - Senior management (where appropriate)
    - Third parties (where applicable)
- An indicative document request list
- An indicative list of responsibilities and requirements of the Triage Facility Provider to ensure an efficient assessment.
- A proposed assessment team with a User CIO key point of contact.

4.4 Compliance with standards defined in the SEC Section G

Triage Facility Providers will be assessed for compliance against the specific standards, procedures and guidelines set out in SEC Section G. When a standard, procedure or guideline is changed or updated, SEC G1.3 allows the SEC Panel to set a transitional period for compliance with a new or changed standard.

The SEC Panel has delegated this responsibility to the SSC and details of any standards that have changed since the version specified in the SEC, together with the SSC agreed transition period will be set out in the SMKI-PMA-and-SSC-Guidance-Standards-Procedures-and-Guidelines published on the SEC website.

The SSC have decided that a default period of three years will be allowed for compliance with a new or changed standard UNLESS a) the relevant governance body for the standard, procedure or guideline have set a different transitional period or, b) the SSC considers the change to be material in the context of smart metering and may then set a different period which will be publicised on the SEC website and accessible to SEC Parties.

For example, organisations will be expected to achieve compliance with ISO27005: 2022 by 2025. But may choose to be compliant with either the 2018 standard or the 2022 standard up until this date.

SECAS, on behalf of the SSC, will review the standards, procedures and guidelines specified in SEC Section G on a quarterly basis and will report any changes to the SSC

4.5 SSC Clarifications

Scope of assurance of a 'Triage Facility':

The SSC recognises that SEC Parties undertaking Triage Activities defined in SEC Section G12, may be undertaking other device triage activities in the same premises e.g. for other approved Use Cases or for SMETS1 or other Devices.

The SEC defines '**Triage Facility'** as:
"a premises where Triage Activities are undertaken."

The SEC defines '**Triage Activities'** as:

"any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances:

a) *the breach of the tamper-protection boundary;*
b) *any unlocking of internal non-operational ports;*
c) *any changes to the configuration of the Device Data;*
d) *confirmation of the firmware version on the Device when Triage has been completed; and*
e) *completion of Triage by replacing all internal non-operational port seals required pursuant to the CPA Security Characteristics and all tamper-protection boundary seals.*

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 in the a) to e) list above 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 considered whether a 'locked box' within a wider (non-Use case 004) triage facility which contains the Triage Tool and Triage System Interface accessible by authorised personnel will satisfy the security requirements. However, the SSC does not consider this arrangement will satisfy the requirement to prevent unauthorised access to the secure area where the Triage Activities take place since other personnel in the wider triage facility could gain access if the authorised Triage operator leaves the locked box unattended for any period e.g. for a toilet / comfort break. The use of a 'locked box' within the secure area is an added security measure if implemented but would not satisfy the Security Assessment on its own.

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.

Tamper-protection Seals:

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.

CPA Test Labs have confirmed that, for the purposes of meeting the CPA SCs, they are satisfied if any internal interfaces (including non-operational interfaces; additional interfaces; triage interfaces; or user interfaces) are protected by either an ESME terminal cover or a GSME battery cover.

To obtain CPA Certification, CPA Test Labs will have ensured compliance with the CPA Security Characteristics and will have:

- checked that non-operational interfaces have been a) disabled for normal operation, or b) cannot be used to undermine device security having examined the developer provided rationale;
- confirmed that the Device has satisfied the CPA SC requirements that internal non-operational interfaces have been adequately protected by a tamper-protection seal on the perimeter;
- checked that the Device has satisfied the CPA SC requirement for any breach of the tamper-protection boundary to have produced a tamper response and will record an entry in the Device Security Log;
- checked the very strong security controls implemented for Use Case 004 Triage and ensured that the Triage Interface can only be unlocked by a Manufacturer Signing Key.

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.

Personnel Security Screening:

The personnel security screening required by SEC Sections G4.2 and G4.3 applies to personnel who will work in the secure area used for Triage Activities. The SSC recognises that there will be other personnel who may need temporary access e.g. a Manufacturer of the Device being Triaged or a Supplier who will install a Triaged Device may require assurance of the process. In these circumstances, they do not need to be security screened but they do need to be escorted and monitored at all times within the secure area, preferably with a visible pass that indicates they are a visitor that needs to be escorted. The User is expected to have a clearly defined this process for visitors to its secure areas that aligns to the above guidance, but also to the User's own risk appetite.

4.6 Certificate of Triage Facility Assurance Status

The SSC will confirm an assurance status in line with SEC Section G12.7 and G12.8 and, 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 with the relevant details to the Triage Facility Provider. 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. A template of the Certificate of 'Triage Facility Assurance Status' is shown in Appendix J.

Appendix A - Full User Security Assessment (FUSA) Timetables

Outlined below is the standard assessment timetables submitted to a Triage Facility Provider in advance of their assessment. Full User Security Assessment (FUSA) timetables for assessments, which also act as a provisional timetable for an Optional Pre-Assessment (OPA) and supporting documentation lists are included. Please note the 'Personnel Required' is indicative and will depend on the roles and responsibilities of the relevant staff within each Triage Facility.

Week 1: Day 1 (SEC Party Site/)

Time	Activity	Objectives	Personnel Required
10:00–10:30	Introduction	To provide the User CIO with an understanding of the size and scale of the SEC Party's Triage operations.	Security Manager, Smart Metering Programme Director
10:30–12:30	Solution and Triage Facility scope walkthrough	To enable the User CIO to understand the SEC Party's Triage Facility size and scale, solution and scope.	CISO, Security Manager
12:30–13:30	Q&A	Opportunity for User CIO questions on the Triage Facility.	CISO, Security Manager
13:30–14:30	Governance and Risk Management overview	To discuss the approach taken by the SEC Party to security governance and risk management.	CISO, Security Manager
14:30–15:00	Document review	To allow the User CIO to read through documentation relating to the SEC Party in detail.	N/A
15:00–16:00	Overview of compliance with ISO27005 risk management practices	To discuss the risk assessment scope applied by the SEC Party and the methods applied to risk management.	Security Manager
16:00–17:30	Q&A	Opportunity for User CIO questions on the governance and risk management approach.	Security Manager

Week 1: Day 2 (SEC Party Site)

Time	Activity	Objectives	Personnel Required
09:00–10:00	Document Review	To allow the User CIO to rad through documentation relating to the SEC Party in detail.	N/A
10:00–11:00	Information Security Management System walkthrough	To allow the User CIO to assess the SEC Party's Information Security Management System (ISMS) processes and compliance with G12.4.	CISO, Security Manager
11:00–12:30	Document review	To allow the User CIO to read through documentation relating to the ISMS.	N/A

Time	Activity	Objectives	Personnel Required
12:30–13:45	Q&A	Opportunity for the User CIO to ask questions based on documentation reviewed.	Security Manager
13:45–14:30	Document review		
14:30–17:00	Assessment of SEC obligations	To allow the User CIO to assess the SEC Party's: • Major Security Incident Management procedures. • Evidence of how Personnel Screening processes are applied in practice. • Data retention and deletion procedures.	Security Manager
17:00– 17:30	Q&A	Opportunity for the User CIO to ask questions based on documentation reviewed.	Security Manager

Day	Activities	Location	Objectives
< Day 3 >	Assessment of SEC obligations	SEC Party site	To allow the User CIO to assess:: • any additional evidence provided by the SEC Party in relation to the observations noted. • Consolidate and document key observations from fieldwork. • Provide a view of the observations and discuss any outstanding points with the SEC Party.
< Day 4 (If Required)>	Assessment of SEC obligations	Virtual	To allow the User CIO to further assess: • any additional evidence provided by the SEC Party in relation to the observations noted. • Consolidate and document key observations from fieldwork. • Provide a view of the observations and discuss any outstanding points with the SEC Party. • Conduct a 'soft close' meeting.

Week 2

Day	Activities	Location	Objectives
Hard Close	Close-out call	Virtual	To allow the User CIO to: • Close-out and provide a view of the observations and discuss any outstanding points with the SEC Party.

Document Request List

The following list represents a consolidated list of documentation, which will assist the User CIO in performing the assessment. It should not be considered exhaustive, and the Triage Facility Provider should leverage the information provided within the Triage Security Controls Framework to support the identification of appropriate evidence in support of the assessment. This request list is subject to change once the assessment begins:

- Architecture diagram featuring the Triage Facility, Triage Tool(s) and Triage System Interface(s).
- Risk management scope (ISO27005); (G5.14)
- Triage Facility scope; Any ISMS documentation available, including governance;
- Smart metering related policies, processes, and procedures as applicable (based on SEC governance coverage);
- Risk assessment approach and output; (G5.14-G5.16)
- Risk treatment plan (Statement of applicability); (G5.15)
- Triage Facility asset register; (G5.21)
- Access control policy; (12.4(c))
- Incident management procedure; (G3.5)
- Data Retention Policy; (G3.10, G5.19)
- Information Classification Scheme; (G3.10, G5.19)
- Triage Facility Personnel screening policy; (G4.1 -G4.3)
- Record of Triage Activities (G12.4(f))

Full User Security Assessment timetable: After the User Assessment

Timing	Activity	Purpose
10 Working Days after the User Security Assessment hard close (described in the table above).	The User CIO will produce the User Security Assessment Report (SEC Section G8.22) with observations as appropriate and issue to the Triage Facility Provider and to SECAS via the secure storage platform (*Egress*).	The User Security Assessment Report is provided to the User: a. to enable the User to make report queries; and b. to enable the User to prepare the User Security Assessment Response (commonly known as the User management response). The Report is also provided to SECAS for the SSC (SEC Section G8.23).
Within 5 Working Days of receipt of the User Security Assessment Report.	The User: a. confirms to the User CIO (copied to SECAS) if the User has any report queries to raise; and b. starts to complete the User management response. The User CIO makes any necessary clarifications and amendments and provides an updated User Security	The report query stage aims to ensure that the User Security Assessment Report that is subsequently reviewed by the SSC is clearly understood by the User and factually accurate. The User may reach out directly to the User CIO to request clarification regarding the content of the report.

Timing	Activity	Purpose
	Assessment Report to the User and to SECAS on behalf of the SSC.	
Within 15 Working Days of receipt of the User Security Assessment Report (i.e. including the 5 days for factual accuracy checking).	The User provides a User Security Assessment Response to SECAS on behalf of the SSC setting out: a. whether the User accepts or rejects the observation; and b. the detailed steps that will be taken to address the observation (see Appendix C for guidance). The User should complete the spreadsheet template provided (the SECAS Validation Workbook).	The quality of the User management response is particularly important because its purpose is to provide the SSC with sufficient evidence to consider an assurance status. The SSC will consider the extent to which the response meets the observation in arriving at a recommendation.
Within 15 Working Days of receipt of the User management response.	SECAS will undertake an initial validation to assess the extent to which the response meets the observation. SECAS will provide the validation comments to the User and, where there appear to be weaknesses or a lack of detail, the User will (time permitted within the 10 days) have an opportunity to provide an updated Management Response.	The SECAS validation aims to ensure that SSC time is used to best effect by providing a view, based on experience and expertise, of whether the User management response or updated management response fully, partially or does not address the observation. This will often depend on the amount of detail in the response.
Within 5 Working Days of receipt of the SECAS Validation of User management response	Based on the feedback provided by SECAS the User may be required to provide an update to their management response giving more detail on specific aspects the validation team believe the User may have missed. The User will be time permitted to 5 Working Days	The updated management response allows the User to provide the Security Sub-Committee with a more comprehensive response. This will allow the User to provide the SSC with sufficient evidence before an assurance status is considered.
Within 5 Working Days of completion of the SECAS initial validation of the management response.	The User CIO will undertake a second stage validation to assess the SECAS validation and the extent to which the response meets the observation. SECAS will provide the validation comments to the User in advance of the SSC meeting	The User CIO validation also aims to ensure that SSC time is used to best effect by confirming whether the steps outlined in the User management response will address the observation. Where the SECAS and User CIO validations have indicated that the User management response fully satisfies the original observation, then the SSC is often likely to accept their validation without further discussion.

Timing	Activity	Purpose
5 Working Days before the scheduled SSC meeting.	SECAS will provide secure Egress access to SSC members to the documentation needed to review the User Security Assessment. This includes the User Security Assessment Report; the User management response; and the SECAS and User CIO validations on the SECAS Validation Workbook.	The purpose is to provide SSC members with the available evidence to support a review of the User Security Assessment.
5 Working Days after the SSC meeting.	SECAS will notify the User in writing of the assurance status set by the SSC [Note that the SEC Panel has delegated the responsibility for setting the assurance status as set out in G8.36 to the SSC.]	To provide the User with the information needed to: a. enable the Triage Facility Provider to undertake Triage Activities; b. take any steps that are considered necessary before starting Triage Activities.

Appendix B - What the User CIO will look for in a User Security Assessment

Overview

Appendix B is designed to help User's understand the Section G Obligations that apply to them and help them to understand what kind of questions that will be asked and what will need to be demonstrated to the User CIO during the assessment. Understanding the guidance in this appendix is the first step to achieving compliance. Appendix B explains the detail of what the User CIO might consider and what they might expect to see when applying the Triage Security Controls Framework (TSCF) and Agreed Interpretations in respect of SEC obligations G1, G3-G5, G7, G8 and G12. It aims to help Triage Facility Providers to prepare for a User Security Assessment by alerting them to the detail of the evidence the User CIO might expect to see when assessing compliance against a specific SEC obligation.

NOTE: A Triage Facility Provider which is a Party shall, under SEC Section G12.5, be treated for the purpose of SEC Sections G1, G3 to G5, G7, G8 and G12 as if it were a User and additional obligations are set out in SEC G12.5. References to Users in the Triage Security Controls Framework (TSCF) and Agreed Interpretations (AI) should therefore be taken to include Triage Facility Providers.

Note that 'Triage Facility' may in some cases refer to a secure area within a broader physical location. This could take the form, for example, of a secure area within a larger facility – see paragraph 4.5 of this document for the SSC clarification.

The SSC has confirmed that where there is a SEC requirement for an annual event, 'annual' should be interpreted as meaning taking place no more than 12 consecutive months after the previous event and does not mean once per calendar year.

SEC obligations are either considered in isolation or are combined with other obligations, where similar controls or themes exist. The table below illustrates how the obligations the obligations are set out in this Appendix:

SEC Obligation #	SEC Text
What the User CIO might consider	A list of questions the User CIO might ask and that a User should consider.
What the User CIO might expect to see	Examples of evidence that the User CIO might expect to be provided with during the fieldwork period. This is split between evidence applicable to the design phase, such as policies or contracts, and evidence applicable to the implementation phase, such as meeting minutes or training records. For the avoidance of doubt, once a Triage Facility has gone ahead with live operations following its initial FUSA, the User CIO will expect to see evidence of both design and implementation for each obligation detailed below. Before a Triage Facility has 'gone live' the User CIO will place greater emphasis on the design phase.

Consistent requirements

There are several consistent requirements that the User CIO is likely to request of a User to support the assessment of a particular obligation. These include:

- Documented policies and procedures.
- Evidence of how Triage Facility Providers ensure compliance and consistency of specific controls and policies.
- Asset register(s) including asset owners, locations, etc.
- Documented and communicated roles and responsibilities including who is responsible for engaging with third parties and the SSC / SEC Panel.
- Test evidence to demonstrate the testing and correct implementation of the Information Security Management System and encompassing procedures.

Networks and Information Systems (NIS) Directive and the Cyber Assessment Framework (CAF) Indicators of Good Practice (IGPs)

The CAF and IGP guidance is included at the request of Ofgem to provide additional context and guidance to the User. The CAF IGPs are, where appropriate, are reproduced in this Appendix B for ease of reference. Note however, that compliance with the CAF applies only to Operators of Essential Services (OES) and the User CIO only assesses compliance with the SEC security obligations and not compliance with the CAF IGPs.

Assessing compliance against SEC Security obligations

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.
What the User CIO might consider	• How do you define a 'Major Security Incident'? • How do you classify Security Incidents to determine which are Major Security Incidents? • Upon the occurrence of a Major Security Incident, what process do you follow for notifying the SEC Panel and the Security Sub-Committee, and within what timeframe do you aim to provide this notification? • What level of detail do you provide as part of that notification (e.g. does it include the incident type, number of affected Devices within your Triage Facility, etc.)?
What the User CIO might expect to see - Design	• A clear definition of a Major Security Incident that is relevant to the User's Triage Activities. • Security Incident Management policy and procedures, including the process through which incidents are identified, tracked, and classified to determine if they align to the User's definition of a Major Security Incident. Detailed roles and responsibilities including who is responsible for notifying the Panel and Security Sub-Committee in the event of a Major Security Incident. • Clear procedures for notifying the Panel and Security Sub-Committee of a Major Security Incident which includes any necessary contact details.
What the User CIO might expect to see - Implementation	• An information security incident log indicating any Major Security Incidents, with accurate application of the User's definition. • Evidence of notification to the Panel and Security Sub-Committee following the documented procedure upon any instance of a Major Security Incident.

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.	
What the User CIO might expect to see—Sampling Approach	Population • A list of all MSIs that have been identified since the User's last security assessment.	Sample • Note - The entire population of MSIs will be assessed.

Potentially equivalent CAF Principles	• C1.d: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response. • C1.e: Monitoring staff skills, tools and roles, including any that are out-sourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect.

SEC Obligation G3.9	Each User shall ensure that: (b) In respect of any new or materially changed component or functionality of its Triage Activities which comprises (or includes) a System that is being incorporated into its Triage Activities for the first time: (i) it notifies the Security Sub-Committee prior to that System becoming an operational part of its Triage Activities; (ii) together with that notification it provides to the Security Sub-Committee an adequate description of the System, of the purpose for which it will be used, and of the nature of its relationship to aspects of its of its end-to-end Triage Activities; and (iii) that System does not become an operational part of its Triage Activities unless and until the Security Sub-Committee has authorised the User to bring it into operation (for which purpose, following any such review or assessment as it may consider appropriate, the Security Sub-Committee shall be entitled to give or withhold authorisation by means of notice to the User) Note: part (a) is not in scope for Triage Facility Providers and thus have been removed from this obligation.
What the User CIO might consider	• How do you define a material change to your Triage Activities or Triage Facility? • What reporting mechanisms are in place to notify the SSC if you are planning to incorporate a second or subsequent Triage Facility or new secure area within an existing Triage Faciltiy? • What reporting mechanisms are in place to notify the SSC of a material change for any part of the Triage Activities? • What processes are in place to ensure that a material change to your Triage Activities or Triage Facility is not operational until you have been authorised by the SSC to bring it into operation?
What the User CIO might expect to see - Design	• A defined reporting mechanism for the notification of a Material Change in relation to your Triage Activities to the Security Sub-Committee. • Defined roles and responsibilities including who is responsible for providing the notification to the Security Sub-Committee.

	• Clear contact details and a process to notify the Security Sub Committee including the content of the notification.
What the User CIO might expect to see - Implementation	• Where applicable, evidence of a notification to the Security Sub-Committee via the defined reporting mechanism. • Where applicable, evidence that the User has included an adequate description of the System, the purpose for which it will be used, and of the nature of its relationship to the other aspects of its Triage Activities or Triage Facility as part of the notification to the SSC. • Evidence that Material Change did not come into operation prior to authorisation from the Security Sub-Committee.

SEC Obligation 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.
What the User CIO might consider	The SEC definition of a 'Data Retention Policy' means *"a document developed and maintained by a Party which sets out, in relation to Data held by that Party, the periods for which such Data will be held by it for the purpose of ensuring that it is able to satisfy its legal, contractual and commercial requirements in respect of the Data."* Therefore, the User CIO will expect to see evidence that the User has considered these legal, contractual and commercial requirements and is adhering to them. • What Data do you consider you develop, maintain and hold (including that which resides on Devices)? • Do you have a Data Retention Policy? • Is all Data that you use captured within this Data Retention Policy? • How was this policy developed and who was involved? Who approved it? • How do ensure this policy is consistently employed across the Triage Facility? • How do you identify how long Data should be retained for? • How long will you hold a Device at the Triage Facility before it is recommissioned or destroyed? • How do you identify when Data is to be deleted? • How do you ensure Data is securely deleted? • Under what circumstances do you deem a Device suitable for destruction? • How do you ensure the secure destruction of Devices where required? • Who is authorised to securely delete Data, to ensure that Data is not destroyed when it may still be required? • Is this captured within your Information Classification Scheme? • How do you manage Data retention and deletion where the data owner is a third party?
What the User CIO might expect to see - Design	• A User Data Retention Policy, detailing clear retention timeframes for all Data as either, as appropriate, a simple duration or a duration of time after an event i.e. decommissioning of a Device. • Evidence that those responsible for ensuring adherence are informed and aware of the policy and agree to comply.

	• An Information classification scheme, dictating how information and Data is to be securely deleted (including storage medium) • A process to securely remove and delete data (including Devices), as well as any contractual obligations with third parties i.e. contracted disposal services. • Documented roles and responsibilities identifying those responsible to destroy data. • A separate process for managing the deletion, reuse and destruction of data stored on Smart Metering Equipment, including any contractual obligations where a third party is engaged. • A defined timeframe that a Device will be stored at the Triage Facility before it is either recommissioned or destroyed. • A clear process for retaining and destroying Data where the data owner is a third party, including when the original data owner is no longer contactable.

What the User CIO might expect to see - Implementation	• Where applicable:
	  ○ Evidence of the ongoing tracking of Data in line with retention timeframes.
	  ○ Evidence of adherence to the process for managing the data stored on Smart Metering Equipment, including appropriate evidence where a third party is involved.

Potentially equivalent CAF Principles	• B3.a: You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function. This also applies to third parties storing or accessing data important to the operation of essential functions. B3.e: You appropriately sanitise media and equipment holding data important to the operation of the essential function. • B3.c. The CAF criteria for Stored data is more granular than the SEC and the criteria is reproduced below for ease of reference and clarity for Operators of Essential Services.

CAF – B3.c Stored Data

Not achieved	Partially achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You have no, or limited, knowledge of where data important to the operation of the essential function is stored. You have not protected vulnerable stored data important to the operation of the essential function in a suitable way. Backups are incomplete, untested, not adequately secured or could be inaccessible in a disaster recovery or business continuity situation.	All copies of data important to the operation of your essential function are necessary. Where this important data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used, you apply suitable technical and procedural means, but you have limited or no confidence in the robustness of the protection applied. You have suitable, secured backups of data to allow the operation of the essential function to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy. You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion. If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied. You have suitable, secured backups of data to allow the operation of the essential function to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies. Necessary historic or archive data is suitably secured in storage.

SEC Obligation 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 Devices 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.
What the User CIO might consider	• How have you defined the roles and access allocated to individuals who are involved in Triage Activities? • Which individuals require access to the Triage Facility? • Are there any other roles that may indirectly have access to the Triage Facility (i.e. the management personnel who can grant someone access to a secure area or individuals with access to backup keys.) • What criteria have you used to determine the level of security clearance that User Personnel must have based on their role? • How have you ensured that these criteria are consistently applied to any newly developed roles at the Triage Facility? • What levels of security clearance have been applied to each different User Personnel role and what is being assessed within each level of clearance? E.g. criminal record check, financial background check, etc. • How have you ensured that these levels of clearance are appropriate given the criteria defined? • How do you ensure that this approach, the appropriateness of the chosen levels of clearance and the roles that they are applied to are reviewed annually? • How do you check that the level of screening held for each individual is still appropriate on at least an annual basis? • How do you track when the appropriateness of screening for each individual is next due for review? Note that: • G4.1 does not require that individuals are rescreened annually.
What the User CIO might expect to see - Design	• An assessment of the level of risk associated with each defined User Personnel role and consideration of the appropriate level of security clearance required for each role. • A documented approach which contains the clear criteria and rationale for determining what level of security clearance should be applied to User Personnel in different roles related to Triage Activities. • Management approval of the approach to selecting and mapping of selected appropriate levels of security clearance for User Personnel with access to the Secure Area within the Triage Facility. • Where Triage Activities takes place within a Secure Area in a larger premises, mapping of security clearance to the areas which personnel are able to access through technical or physical controls. • A register of User Personnel who fall within each identified role requiring security clearance and records demonstrating the appropriate levels of clearance having been obtained for the nominated User Personnel. • A methodology outlining the review process for the levels of security clearance applied, to ensure that they remain appropriate within a changing risk landscape, along with a process to renew and update security clearance levels if required.

SEC Obligation 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 Devices 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.
What the User CIO might expect to see - Implementation	• Evidence that the annual review has taken place to ensure the continued appropriateness of the security clearance held by each individual with access to Data held by the User. • A record of all User Personnel including their roles, security clearance held, and the date that the appropriateness of their security clearance based on their role was last reviewed. • Logs to demonstrate which individuals have accessed the Data held by the User mapped to the register of authorised individuals to ensure that only authorised individuals have been accessing Data held by the User.

Potentially equivalent CAF Principles	• B2.d: You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. • B2.a: You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential function.

SEC Obligation 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 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 standards referred to in Section G4.3(a); or (ii) any comparable national standard applying in the jurisdiction in which they are located. The Security Sub-Committee and the SEC Panel have confirmed that the obligations in G4.2 and G4.3 apply to all User Personnel including those working for any third parties where they are authorised to have access to the Triage Facility. For clarity, the BS7858/BPSS (or equivalent) screening does not necessarily apply to all staff in the wider triage facility. It is only appropriate to those who have physical access to the secure area where Triage Activities take place. Where the User screens personnel to the BS7858 Standard, the BSI standard specifies that any screening completed up to 31st March 2020 remains valid, where any screening that occurs after 31st March 2020 will be required to align to the BS7858:2019 standard.
What the User CIO might consider	• Which User Personnel including staff, contractors and third parties, are capable of accessing the secure area of the Triage Facility? • What process have you followed to identify these User Personnel (e.g. has this been informed by a risk assessment)? • Who will be performing the screening? (i.e. third party screening provider, in-house, etc.) • How will you ascertain that the individual(s) performing the screening are themselves compliant to the BS7858/BPSS or equivalent standard, and have been adequately trained to perform the screening? • What is your process for screening your UK-based User Personnel in a manner that is compliant with the latest standard of BS7858 or BPSS, or that the vetting regime used provides at least the same coverage as BS7858 or BPSS? How do you ensure this is applied to contractors and third parties? • If you are relying on screening undertaken prior to the employment of any of your User Personnel, what policies and procedures do you have in place to review the screening to confirm that it was conducted in accordance with BS7858 (or equivalent)? • If you are screening to BPSS rather than BS7858, how have you assessed that screening to this standard is deemed proportionate and aligns to the organisational risk appetite? • What additional controls are implemented to minimise the risk of the User Personnel accidentally, or maliciously, compromising the Triage Activities? • The BPSS/BS7858 standard does not impose a validity period on the screening conducted (i.e. there is no formal requirement to re-screen candidates on a periodic basis). However, it is expected that Triage Facility Providers will assess the risk of a change in personal circumstances and implement proportionate controls to manage that risk. Do you undertake periodic re-screening of your User Personnel? If so, on what frequency? If not, can you please present evidence to outline how you have assessed and managed this risk?
What the User CIO might expect to see - Design	• The output from a risk assessment detailing which Triage Facility Personnel could impact or are capable of compromising the Triage Activities. This might include, but is not limited to: Use-Case 004 operatives, Triage Facility security staff, administrators who assign access privileges, or third party staff. • Verification (e.g. on screen) that authorised Triage Facility Personnel have appropriate access permissions. • Where User Personnel are to be screened in accordance with the BS7858/BPSS or equivalent standard: ○ A procedure for screening User Personnel in line with the relevant standard.

	○ A procedure for reviewing the prior screening file of User Personnel received to ascertain whether the screening is in accordance with the relevant standard. ○ Evidence that the individual who would be conducting the screening has themselves been screened to the BS7858/BPSS or equivalent standard or a higher standard (such as HMG Security Check or Developed Vetting). ○ A record of authorised User Personnel who are authorised to carry out the activities listed in G4.2. ○ Records demonstrating that the appropriate levels of clearance had been obtained for the nominated User Personnel (including staff, contractors, and third parties). • Consideration as to the appropriate timeframe for which screening is valid, and, either: ○ A process to periodically renew and update the screening held by individuals if this is deemed necessary in accordance with the User's risk appetite; or ○ Evidence that the risk of a change in the personal circumstances related to User Personnel who have already been through screening has been risk assessed and managed in accordance with the User's risk appetite.	
T What the User CIO might expect to see - Implementation	• An up to date list detailing which User Personnel could impact or are capable of compromising Triage Activities with their associated security clearance (e.g. certificates from third parties, suppliers etc.). This list should include the date that this access was granted for each individual. • Verification that when an individual moves to a role that could impact or is capable of compromising the DCC Total System that they achieved BS7858/BPSS or equivalent standard before starting in that role. • Screening certificates for User Personnel who are deemed capable of compromising Triage Activities. • Evidence that BPSS, BS7858, or equivalent screening carried out by third parties or internally includes all required components of the current standard. • Where screening is carried out in-house, evidence that the individual who carried out the screening has themselves been screened.	
What the User CIO might expect to see—Sampling Approach	Population • A list of all new individuals who are authorised to carry out the activities identified in Section G4.2 since the User's last security assessment, including third party personnel.	Sample • One individual per unique organisation and/ or process.

Potentially equivalent CAF Principles	• Potentially equivalent CAF Indicators of Good Practice: • B2.d: You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. • B2.a: You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential function.

SEC Obligation G5.14, G5.15	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 for its Triage Activities. (d) any Smart Metering Systems held 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 Each User 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.
What the User CIO might consider	• What is your information risk management approach? • How do you identify risks (e.g. internal flagging of new issues, external threat sources, etc.)? • How have you defined the scope of your risk assessment, have you considered all elements of your broader smart metering infrastructure outside of the Triage Facility? • How do you identify and manage security risks relevant to your organisation? • How do you apply this to the scope of G5.14? • What governance mechanisms (i.e. boards, forums, sponsorship) are in place to challenge and corroborate the identification and management of risks? • What is your organisational risk appetite? How was this agreed at a suitably senior level, categorised and then explained to relevant personnel? • Who is involved in each key stage of the risk assessment (e.g. scoping, asset valuation and business impact assessment, threat and risk assessment, mitigating control selection, etc.)? • How do you select relevant controls? • How do you assess the effectiveness of the mitigating controls you have implemented? • Do you have clearly defined roles and responsibilities for accepting residual risks following the application of controls? How are individuals held accountable for risk acceptance decisions in the event of Compromise to the Triage Activities? • How do you communicate the outcome of risk assessment and risk management activities to those authorised to accept risk (i.e. top management)? • How have you determined that your risk management approach is compliant with the latest version of ISO 27005?

	• How have you considered the interaction between your security risk assessment and any health and safety or environmental risk assessments to ascertain if they include conflicting controls and how these conflicts are then managed. Note that: • The User CIO will carry out a detailed and in-depth review of risk assessments in the initial Full User Security Assessment (FUSA) to provide assurance for all SEC Parties that the systems supporting smart metering are appropriately secure because, all Triage Facility Providers, when implementing the specified functionality, become a source of security risk to the system as a whole. • Subsequent to the initial FUSA, the User CIO aims to take a proportionate approach and will focus on changes to risks arising e.g. from organisation changes such as changed company structures / mergers etc, changed governance arrangements, changes to Triage System design or operation, changes to any other technical components, changes to the threat landscape, changes in third party dependencies, supporting processes, any security incidents or vulnerabilities experienced or risk management methodology changes.
What the User CIO might expect to see – Design and Implementation	• Evidence of an embedded risk management process with appropriately defined roles and responsibilities, which includes any relevant third parties involved in the User's risk management activities (Section 6.3 of ISO 27005). • A statement detailing what is included within the scope of the risk assessment including any justifications and narratives. • A documented and approved risk management process, including a risk appetite statement and corresponding risk acceptance criteria, defined in terms that directly correspond to the output of the risk assessment process (Section 6.1 and 6.4 of ISO 27005). o For example, the organisational risk appetite could be defined as 'Cautious' and the User should then detail how this would map to accepting risks that are lower than a defined level based on how risks are scored. o Similarly, if a User's risk assessment methodology produces risk severity descriptors such as 'high', 'medium' and 'low', the risk acceptance criteria should state the level at which the User is content to accept the risk without the need for further mitigation • If a User relies on a third party to provide services that are within the scope of the User's risk assessment (such as parts of the Triage Facility, security systems, or asset tracking systems) the User will need to demonstrate what security requirements it has within a finalised contract between the User and the third party. • A risk management scope for the Triage Facility and the surrounding perimeter showing clear boundaries of what is considered to be in scope for risk management activities, including (but not limited to): o Triage Activities; o Any communications links between the Triage Facility, Triage Tool(s), and Triage System Interface(s); and o Any security functionality used for the purposes of compliance with Section G (e.g. communication link encryption, Intrusion Prevention System, CCTV cameras). o Any security functionality that facilitates the separation between the Triage Facility where Triage Activity takes place, and the rest of the premises (e.g. physical barriers, access controls systems, safety overrides)) • A documented approach to the assessment of information security risk that is comprehensive and produces a consistent, valid, and comparable set of results, which the User is able to justify when questioned (e.g. a rationale to justify the consequence scores assigned to different assets is applied consistently throughout the risk assessment, produces comparable results when representing

	equivalent levels of risk, and produces results that accord as closely as possible with reality) (Clause 6.1.2b of ISO 27001 and Section 6.5 of ISO 27005). • Where a User utilises an 'Asset-based' approach, evidence of an asset register containing all assets, at an appropriate level of granularity (e.g. through the identification of the different components used in Triage Activities , that have been identified to fall within the scope of risk management activities, should be produced. • Evidence that the assets have been assessed to determine any applicable risks by considering any threat and vulnerabilities that could compromise the confidentiality, integrity and/or availably of the asset, and classifying the consequence of the compromise experienced by the business using an appropriate set of criteria which take into account different consequences (e.g. regulatory, financial, health and safety, reputational etc.) (Section 7.2.1, and Annex A.2.5 of ISO 27005). • Evidence that the User has assessed specific compromises against the criteria above, considering the consequences that would result from, for example, in the compromise of any component of the Triage Activities for which they are responsible. • Where a User utilises an 'Event-based' approach, evidence of a list of strategic risk scenarios identified through an evaluation of events and consequences building on the experience of senior management and relevant individuals within the business who are responsible for a business process and any relationships with other organisations, such as third party IT developers or vendors, and onward to the risk source) (Section 7.2.1, and Annex A.2.4 of ISO 27005). • Evidence that a Business Impact Assessment has been performed in relation to assets. This assessment should determine what impact would be experienced by the business if each asset were to be compromised. It should consider different types of impact (e.g. regulatory, financial, health and safety, reputational etc.) (Section 7.2.1, Annex A2.2 and A2.5 of ISO 27005). • When conducting a Business Impact Assessment, a User should consider how the Compromise of a single asset might result in further Compromise. For example, Compromise of the Triage Facility would likely result in compromise of the Smart Metering Devices themselves. • A list of methods for identifying relevant risks and assigning appropriate risk ownership (Section 7.2.2 of ISO 27005) • A threat assessment that considers demonstrable, credible external sources of threat information proportionate to Triage Activities, which are appropriate to the risk profile of the individual User. This could be expected to take the form of a list of applicable threats and the sources of threat intelligence used to maintain an up-to-date view of the threat landscape, with a level of detail, and number of sources of information which is proportionate to the User's risk profile and encapsulate new threat sources, for example emerging technology such as artificial intelligence enabled risk. (e.g. number of Devices triaged etc.) (Section 10.5.2 of ISO 27005). • A clear methodology for identifying the risk likelihood that covers the predictably manageable range of anticipated event likelihoods. For a deliberate risk source, it considers the threat source capability and motivation, where a deliberate threat source is involved, with clear guidance on how the User performs a consistent assessment of the capability and motivation of threat sources. For an accidental risk source (e.g. environmental or technical) it identifies the probability of an events occurrence in a consistent and repeatable manner. (Section 7.3.3 of ISO 27005). • Where the threat source is a non-human threat actor (i.e. natural disaster), the User should have an alternative methodology for determining likelihood.

	• A complete assessment of all relevant risks aligned to the assets and events that form part of the risk management scope, ensuring the appropriate consideration of the different attack vectors that can lead to Compromise, including via malicious insiders, external hackers, physical intruders into offices/data centres and accidental Compromises (Section 7.2 of ISO 27005).
	• Risks being identified separately for Compromise to confidentiality, integrity and availability impacts of identified assets (ISO 27005 Section 7.3.2).
	• It is important to consider the confidentiality, integrity and availability aspects of each risk and asset (i.e. CCTV, Triage Tool, etc.) separately, because the impact of a confidentiality, integrity or availability risk being realised may be different and therefore the security controls required might be different.
	• For the likelihood, of a risk occurring different threat actors may prioritise the compromise of confidentiality, integrity or availability depending on their goals and objectives. The User CIO would expect to see that the risk register demonstrates that, for each risk, the confidentiality, integrity and availability aspects have been properly considered, assessed, scored and are being monitored. Note that it is not necessarily required that the User have a separate line in its risk register line for each of these elements.
	• A risk treatment plan which identifies the individual risk treatments that should be implemented for each risk in priority order and their timeframes, along with owners for risk treatment activities (Section 7.4 of ISO 27005).
	• Documentation of all relevant controls with a narrative summarising the key security-enforcing controls, a comparison of these against ISO 27001 Annex A, and a mapping to relevant policies and/or procedures containing further detail on their operation within a Statement of Applicability (Section 8.3, 8.4, and 8.5 of ISO 27005).
	• Consideration of how the User will gain assurance over the operational effectiveness of the controls put in place to mitigate the risks identified and adequate evidence to demonstrate that such assurance has been sought (Section 9.1 and 9.2 of ISO 27005).
	• Evidence demonstrating the acceptance of all risk treatment arrangements by risk owners/senior management and a process for managing any exceptions raised (e.g. regular reviews of the risk treatment arrangements for such risks) (Section 8.2.2,10.2 and 10.6 of ISO 27005).
	• Documented information and policies concerning the User's end to end risk management process (Section 10.4 of ISO 27005) including:
	  ○ Defined risk criteria (Section 6.4 of ISO 27005).
	  ○ Reasoning for the consistency of results (Section 6.4 of ISO 27005).
	  ○ A list of risk and risk owner identification methods (Section 7.2.2 of ISO 27005).
	  ○ Description of methods for analysing risks (Section 7.3 of ISO 27005).
	  ○ Description of comparing results with risk criteria. (Section 7.4.1 of ISO 27005).
	  ○ Method for selecting risk treatment options (Section 8.2 of ISO 27005).
	  ○ Method for determining controls (Section 8.3 of ISO 27005).
	  ○ How ISO 27001 Annex has been used (Section 8.5 of ISO 27005).
	  ○ How risk treatment plans have been produced (Section 8.6.1 of ISO 27005).
	  ○ How risk owner's approval has been obtained (Section 8.6.2 of ISO 27005).

	• Where a User has an automated risk management tool the User CIO will require appropriate access to review the User's risk assessment, for example:
	  ○ The User CIO can be provided with 'view only' or 'auditor' access to the automated tool interface.
	  ○ The User can walk through its risk assessment with the User CIO via 'screen sharing'.
	  ○ The User can export its risk assessment data to a readable excel file for the User CIO to review.

Potentially equivalent CAF Principles	• A1.a You have effective organisational security management led at board level and articulated clearly in corresponding policies. • A1.b Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks. • A1.c: You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of essential functions are considered in the context of other organisational risks. • C1.c: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts. • A2.a: Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities. • "A3.a Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling)." • A2.b: You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential functions. • A1.c: You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of essential functions are considered in the context of other organisational risks.

SEC Obligation G5.16	Each User 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;
	  (i) any other Data, Systems, or processes on which it relies upon for its Triage Activities.
	  (ii) 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.

What the User CIO might consider	• At what frequency do you conduct assessments for identifying and managing risk? • What are the triggers for a full risk assessment? • How do you define a material change to your Triage Activities? • What mechanisms are in place to ensure an assessment is conducted following a material change to components confined within the scope of the Risk Assessment or the occurrence of any Major Security Incident in relation to its Triage System? • Who is responsible for carrying out the assessment of the process for identifying and managing risk in (a), (b), and (c)? • Which other Systems outside of your Triage Activities, are you reliant upon to triage smart Devices? (i.e. wider warehouse perimeter security controls, etc.)
What the User CIO might expect to see - Design	• Evidence of risk management artefacts including assessments, and treatment plans. • Evidence of business and system owner engagement as well as appropriate levels of senior management engagement. • Evidence of threat and vulnerability input into the risk management process. • Evidence of inherent and residual risk analysis and mitigating control selection analysis. • Evidence of the reassessment of risks, where they have previously been identified through prior assessments. • Evidence of changes to the Triage System scope triggering a risk assessment.
What the User CIO might expect to see - Implementation	• An information security incident log indicating any Major Security Incidents, with accurate application of the User's definition. • Evidence outlining if the Triage Activities have undergone any material changes since the previous assessment, with accurate application of the User's definition. • A risk assessment which has been re-assessed prior to a material change, following a Major Security Incident or if a year has passed since the previous assessment. • Evidence that any risks where a mitigating control is the responsibility of a third party, have been reviewed on an annual basis. *Note: The SSC has confirmed that where there is a SEC requirement for an annual event, 'annual' should be interpreted as meaning taking place no more than 12 consecutive months after the previous event and does not mean once per calendar year.*

Potentially equivalent CAF Principles	• C1.d: You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response. • D2.b: Your organisation uses lessons learned from incidents to improve your security measures. • A2.a: Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated 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. Note: to demonstrate full compliance with G5.18 the User is also required to demonstrate compliance with the other obligations referenced in parts (b) (i), (ii) and (iii). Where the User CIO identifies non-compliance with those other obligations this will be reported under the relevant part of the SEC. Whilst technically also a non-compliance with G5.18, these observations will not be listed again under this obligation to avoid any duplication.
What the User CIO might consider	• How have you obtained Management commitment to developing and embedding an ISMS, including appropriate levels of governance, within the organisation? • If reliance is placed on the ISMS of a service provider, how do you gain assurance that this ISMS is appropriate and acceptable to your organisation (considering elements such as the scope and risk appetite, etc.)?How have you designed and documented your ISMS? • How are the requirements and scope of the ISMS defined? • How has the risk assessment process been used to assist the design of the ISMS? • Have you obtained ISO27001 certification for any or all of your Triage Activities? Is the certification from a UKAS accredited organisation? • How do you ensure the Statement of Applicability is appropriate for your organisation? • What review mechanisms are in place for individual components, policies and procedures of the ISMS as well as the ISMS itself? • Who is responsible for establishing, complying, maintaining, reviewing and improving the ISMS? • Where you are using a third party to provide elements of your ISMS, evidence that the ISMS has been shared, reviewed and agreed on an annual basis?

What the User CIO might expect to see – Design and Implementation	• A defined scope and policy framework for an ISMS in line with ISO 27001. • A documented Statement of Applicability of controls to identify the applicability of controls (including rationale as to why any controls have been excluded). • Demonstration of compliance with ISO 27001 (which may include an ISO 27001 certificate covering the Triage Activities). • Evidence of the effectiveness of the ISMS including evidence of the 'Plan Do Check Act' model. • Demonstrative evidence of the implementation of the mandatory sections of ISO 27001. • Documented impact levels / scenarios of compromise with evidence of business engagement. • Documented review mechanisms for scheduled reviews of individual policies and procedures, as well as the ISMS. • Documented reviews of any elements of the ISMS provided by third parties.

Potentially equivalent CAF Principles	• B1.a: You have developed and continue to improve a set of cyber security and resilience policies and processes that manage and mitigate the risk of adverse impact on the essential function. • B1.b: You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved. • B5.b: You design the network and information systems supporting your essential function to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated. • D2.b: Your organisation uses lessons learned from incidents to improve your security measures.

SEC Obligation G5.19	Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of: (b) the establishment and maintenance of an Information Classification Scheme in relation to the Triage Facility; and (d) the education, training and awareness of those with access to the Triage Facility. Note: parts (a) and (c) are not in scope for Triage Facility Providers and thus have been removed from this obligation.

What the User CIO might consider	• What are the main sections of your information security policy and what do they seek to achieve?
	• How was the policy created? What scope and Systems does it apply to, and who approved it?
	• Who is required to comply with this policy? Have they been informed and how is compliance assessed?
	• How does your information security policy address:
	  ○ Education, training and awareness regarding information security.
	  ○ Information Classification Scheme (are the levels well-defined, with clear and sensible criteria for data classification and proportionate controls for data processing, storage, transfer and deletion implemented to protect data at each level?).

What the User CIO might expect to see - Design	• A documented information security policy which is embedded within the business practices of User Personnel. • Evidence of senior management endorsement of the policy.

	• Communications to those this policy applies to and receipt and/or compliance acknowledgements. • The establishment of an Information Classification Scheme detailing the different levels of classification that Data is assigned, and how it should then be handled based on its classification. • A process detailing the Information Security education, training and awareness of those with access to the Triage Facility must undertake, including the frequency and format of the education, training and awareness.
What the User CIO might expect to see - Implementation	• Evidence of ongoing compliance with the education, training, awareness requirements in respect to information security, including training records of User Personnel and any third parties with access to the Triage Facility. Industry good practice generally dictates that such testing should be undertaken at least annually. In exceptional circumstances a User may wish to present a case for undertaking such training less frequently (up to a maximum of every two years), but this would only be acceptable in the event that the training is demonstrably robust and fit for purpose. • Communications to those to whom the information security policy applies and receipt and/or compliance acknowledgements.

Potentially equivalent CAF Principles	• B6.b: The people who support the operation of your essential function are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed. • B6.a: You develop and pursue a positive cyber security culture.

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 User.
What the User CIO might consider	• What is your approach to information security (e.g. do you have a security strategy)? • How is your approach to information security reflected within the structure of your ISMS? • Within your ISMS what is the approach to: • Human resources security; • Physical and environmental security; • Managing third parties whom you are reliant upon for your Triage Activities. • Do you have specific policies for each of these key areas? How have you developed, implemented and regularly reviewed these? • How do you ensure the physical security of the Triage Facility and the Devices on which Triage Activities are performed? • What is in place to limit access into the Triage Facility?

	• What is in place to control access between the Triage Facility and the broader premises?
	• As part of your physical access arrangement, how have you:
	  ○ Considered who is authorised to access the Triage Facility?
	  ○ Ensured that the principle of least privilege is adhered to?
	  ○ Ensured that review processes assess the continued requirement and appropriateness of access to the Triage Facility?
	  ○ Considered the access controls required to ensure that only authorised User Personnel are able to access the Triage Facility?
	  ○ Considered the processes and controls required to grant, amend, review and revoke access? Is there a separate or enhanced process regarding privileged accounts?
	  ○ Considered the separation of the Triage Facility such that the impact of compromised credentials can be reduced?
	  ○ Considered how these differ based on those requiring only temporary access?
	• If a third party provides or manages elements of the Triage Facility, how has the third party demonstrated they conform to recognised security standards?
	• What audit data does your third party provide to you, and how have you considered whether it is sufficient to meet your needs?

What the User CIO might expect to see - Design	• A documented security strategy with appropriate senior management sponsorship.
	• A documented information security policy which is embedded within the business practices of the enterprise, specifically drawing on mandatory controls:
	  ○ Information security;
	  ○ Human resources security;
	  ○ Physical and environmental security, including physical access;
	  ○ Third party compliance.
	• Documented risk management procedures embedded within the ISMS and information security policy including:
	  ○ Management of risk and risk governance arrangements with third parties;
	  ○ Processes for setting risk appetite with third parties;
	  ○ Process for setting the scope of the ISMS with third parties;
	  ○ Any identified risks around shared systems;
	  ○ How this is enforced in contract and what mechanism is in place to ensure this is implemented, including the provision of suitable audit data.
	• Evidence that the policies are implemented and adhered to (e.g. by inspecting system configurations, physical entry barriers to the Triage Facility, or by engaging with end users within a User organisation).
	• A physical access control solution which includes User provisioning, escalation of privileges, User recertification, and revocation and the processes by which this engages with the joiner mover leaver process.

What the User CIO might expect to see - Implementation	• Evidence of the implementation of required controls, such as physical and environmental security control reviews. • Demonstration of the physical security controls in place used to limit access and monitor the Triage Facility. • Demonstration of the physical security controls facilitating separation between the Triage Facility and the broader premises. • Evidence of adherence with the physical security access control procedures, including a review of physical access privileges granted to User Personnel. • Evidence that changes in physical access rights, such as starters, movers and leavers, are handled in compliance with policies.

Potentially equivalent CAF Principles	• A3.a Everything required to deliver, maintain or support networks and information systems necessary for the operation for essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling)." • B1.b: You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.

SEC Obligation 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.
What the User CIO might consider	• How have you compiled your asset register and what process is in place to maintain and ensure compliance to the asset management procedure, for all assets in scope of the Triage Facility, including the Smart Metering Systems held there? • What processes do you have in place to make sure this asset register is kept up to date? • Where you are reliant on a third party for the disposal of assets, what arrangements there are in place to demonstrate they are disposing of assets in line with your requirements?
What the User CIO might expect to see - Design	• A documented Asset Management Policy and Procedure including appropriate measures to keep the asset register up to date. • An asset register containing both physical and information assets in scope of the Triage Facility, Triage Tool(s) and the Smart Metering Systems held there including onsite review to confirm its accuracy. • Note that the Smart Metering Systems themselves that would undergo Triage Activities and the assets that make up the Triage Facility can be held on separate asset registers.
What the User CIO might expect to see - Implementation	• An up to date asset register containing both physical and information assets for in scope of the Triage Facility, Triage Tool(s) and the Smart Metering Systems held there. • Onsite evidence including testing a sample of assets held on site against the register, a sample of assets on the register to the site, to identify these are being accurately accounted for. • Evidence that an asset has been handled in line with the Asset Management Policy and Procedure (e.g. during updates or decommission).

What the User CIO might expect to see—Sampling Approach	Population • All Triage Facility asset registers	Sample • One per asset register.

Potentially equivalent CAF Principles	A.3.a Asset management: Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

Assessing Compliance against SEC Security Obligations

Additional Obligations on Triage Facility Providers

SEC Obligation G12.4(a)	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); *Note: This obligation relates only to "the tamper-protection boundary required by CPA Security Characteristics (taking into account any allowable beaches necessary for Device maintenance and/or the decommissioning process)", This does NOT include the metrology seal or the terminal cover or battery cover seal. See paragraph 4.5 of this document for the SSC clarification that these fall under the category of 'Device maintenance and/or decommissioning'.*
What the User CIO might consider	• Have you established a definition of the expected tamper protection boundary required by the CPA Security Characteristics for each type of Device to be Triaged within the Triage Facility? • How have you defined a 'breach' of the tamper-protection boundary for the purpose of determining if it is allowable or appropriate to carry out Triage Activities? • How do you determine the perimeter of the Triage Facility to establish when a Device has entered? • What process is in place to ensure that you have not attempted to undertake Triage Activities on any Device where the expected tamper-protection boundary has been breached? • What is your process to manage Devices where the tamper-protection boundary has been breached inappropriately?
What the User CIO might expect to see - Design	• A documented process, including a definition of an inappropriate tamper-protection boundary breach, of the appropriate measures in place to ensure that no Triage Activities are carried out on Devices with breached tamper-protection boundaries that are not allowable.

What the User CIO might expect to see - Implementation	• Evidence that prior to any Triage Activities, Devices are checked to make sure the tamper-protection boundary was not breached where it is not allowable or appropriate prior to it entering the Triage Facility.

SEC Obligation G12.4(b)	G12.4 Each Triage Facility Provider shall: (b) only use the Triage Tool and Triage System Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;
What the User CIO might consider	• What Triage Tool(s) and Triage System Interface(s), provided by the manufacturer(s), is/are being used to access the Triage System(s)? • How have you gained assurances that the Triage Tool and Triage System Interface has confirmed compliance with the requirements of the Commercial Product Assurance (CPA) Scheme Build Standard as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC and CH SCs and CPA Build Standard Extensions"*.
What the User CIO might expect to see - Design	• An architecture diagram detailing how the Triage Facility links in with the Triage Tool and the Triage System Interface • A documented policy requiring the Device Manufacturer who provides the Triage Tool and the Triage System Interface to have demonstrated compliance with the requirements of the Commercial Product Assurance (CPA) Scheme Build Standard Extensions.
What the User CIO might expect to see - Implementation	• Evidence of how the Device Manufacturer's provided Triage Tool and Triage System Interface has demonstrated it meets the requirements of the Commercial Product Assurance (CPA) Scheme Build Standard Extensions.

SEC Obligation G12.4(c)	G12.4 Each Triage Facility Provider shall: (c) 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 System Interface; Note that SEC Section G12.9 defines the Triage System Interface as: "*a secure virtual private network (VPN), encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a remote Triage Facility, which provides mutual authentication, confidentiality and integrity of communications. The Triage System Interface:* *• Must use either TLS or IPsec, and* *• If using TLS then must include client authentication."*
What the User CIO might consider	• How do you control access to the GUI of all Triage Tool(s)? • How do you control access to the Triage System Interface(s)? • If you are using TLS for your Triage System Interface, how will you implement client authentication?

	• How have you implemented multi-factor authentication on the GUI of all Triage Tool(s) and on the Triage System Interfaces?
	• How have you ensured that the Triage Tool will only be utilised where multi-factor authentication is in place?
	• As part of your access control policy, how have you:
	  ○ Considered who is authorised to access the different components of the GUI and the Interface?
	  ○ Ensured that the principle of least privilege is adhered to?
	  ○ Ensured that review processes assess the continued requirement and appropriateness of access to Data?
	  ○ Considered the access controls required to ensure that only authorised personnel are able to access Data?
	  ○ Considered the processes and controls required to grant, amend, review and revoke access? Is there a separate or enhanced process regarding administrative and service accounts?

What the User CIO might expect to see - Design	• A documented approach to the implementation of multi-factor authentication across both the GUI and the Interface. • A documented approach to applying controls appropriate to the Triage System Interface. • Consideration of relevant sources of good practice in this area (e.g. from NCSC) around securely implementing multi-factor authentication on these systems. • An access control policy and procedure for all in-scope personnel. • A documented and embedded joiner, mover, leaver process. • An access control solution which includes user provisioning, escalation of privileges, user access reviews, user recertification, and revocation and the processes by which this engages with the joiner, mover, leaver process.
What the User CIO might expect to see - Implementation	• Evidence that multi-factor authentication has been implemented across both the GUI and the Interface (e.g. by a system demonstration of the log-in process to the User CIO). • Evidence of adherence with the access control policy, procedures, including a review of the ongoing relevance of the access privileges granted to personnel in line with the 'need to know' principle. • A review of access privilege requests and approvals. • Evidence to demonstrate that joiners, movers and leavers are handled in compliance with policies.

SEC Obligation G12.4(d)	G12.4 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; *Note that the SSC accepts that the Triage Facility Provider will use 'reasonable endeavours' to ensure the physical security of the Triage Tool and Devices being triaged.*
What the User CIO might consider	• How to you prevent unauthorised access to the Triage Tool(s), Triage System Interface(s), and any Devices that are subject to Triage Activities within the Triage Facility? • How do you track access to the Triage Tool(s), Triage System Interface(s) and any Devices to prevent unauthorised use? • How is/are the Triage Tool(s) physically secured when not in use and what is the process to enable them for use? Where this location is not where the Triage Activities take place, how has this been considered as secure?

	• What process do you have to make sure that the Triage Tool(s) within the Triage Facility is only used by an authorised user only when the Device Manufacturer has securely authorised such use? How is this authorisation provided? • How do you ensure the physical security of the Triage Tool(s), Triage System Interface(s), and any Devices that are subject to Triage Activities within the Triage Facility? • Where you have considered Health and Safety controls (For example, emergency fire exits or entrance overrides) while implementing security controls how have you managed any conflicts?
What the User CIO might expect to see - Design	• A documented process which details the controls in place to prevent unauthorised use and ensure the physical security of the Triage Tool(s), Triage System Interface(s) and any Devices within the Triage Facility in which Triage Activities take place. • A documented process detailing how the Triage Tool(s) within the Triage Facility is unlocked to allow its use, and how authorisation is securely provided for this to take place.
What the User CIO might expect to see - Implementation	• Evidence that the User has implemented sufficient controls to prevent unauthorized use and ensure the physical security of the Triage Tool(s), Triage System Interface(s) and any Devices within the Triage Facility. • Evidence that the Triage Tool(s) within the Triage Facility has only been unlocked for use on receipt of authorisation by the manufacturer, and has only been used by an authorised user.

SEC Obligation G12.4(e)	G12.4 Each Triage Facility Provider shall: (e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities; *Note: The SSC has provided clarification of which tamper-protection seals are affected for the purpose of G12.4 a) and these apply to G12.4 (e)*
What the User CIO might consider	• How do you determine when Triage Activities on a Device have been completed? • How have you determined which tamper-protection seals are required for each Device? • How do you ensure that following the completion of Triage Activities a Device has been secured with the required replacement of its tamper protection boundary? • How are the tamper protection seals required for the tamper protection boundary provided by the manufacturer? • How are the tamper protection seals required for the tamper protection boundary that are provided by the manufacture secured for use only as part of completing Triage Activities? How do you demonstrate compliance with CPA requirements for seals to be replaced following Triage Activities?
What the User CIO might expect to see – Design	• A documented process which set out the steps taken following the completion of Triage Activities, including the replacement of tamper protection seals required for the tamper protection boundary and how this activity is tracked. • A tracker showing how Device tamper-protection seals have been inspected, removed, and replaced for all Smart Meter Devices that pass through the Triage Facility. • A process for protecting tamper-protection seals provided by the Device Manufacturer until they are required.

What the User CIO might expect to see - Implementation	• Evidence that all Devices, once Triage Activities have been completed, have had appropriate tamper protection seals required for the tamper protection boundary, and details of this documented within a tracker. • Evidence that manufacturer tamper protection seals required for the tamper protection boundary are appropriately protected.

SEC Obligation G12.4(f)	G12.4 Each Triage Facility Provider shall: (f) 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; (v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;	
What the User CIO might consider	• How do you define and record the Triage Activities that take place and what information is recorded? • How do you make sure that all Triage Activities are monitored and recorded? • How do you make sure that your record of Triage Activities is appropriately kept up to date and protected e.g. from unauthorised modification?	
What the User CIO might expect to see - Design	• A documented process for the recording of Triage Activities undertaken within the Triage Facility. • A system which includes details of the Triage Activities undertaken, including details such as: ○ The requestor of any change to a configuration of a Device, ○ The model and serial number of Devices for which the Triage Activity has been attempted or completed, and if the tamper-protection boundary has been breached ○ details of the Triage Activities attempted or completed; and ○ details of any failed attempts to complete Triage Activities, including what if any changes have been made to the Device. • Details of how the system makes sure all Triage Activities are accurately recorded, and how it is prevented from being tampered with.	
What the User CIO might expect to see - Implementation	• Evidence demonstrating that the Triage Facility has recorded all attempted Triage Activities with all required details	
What the User CIO might expect to	Population • All Devices on which Triage Activities have been carried out	Sample • One device per unique process

see—Sampling Approach		

Assessing obligations without complete supporting evidence

A single observation is raised for 'obligations without complete supporting evidence' where 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 required by the obligation(s) at this stage of the system development lifecycle, but where the User CIO has reviewed plans and design documentation relating to the proposals for compliance which have been approved through the relevant User's internal smart metering governance group.

The following observations have been identified as obligations, where evidence of compliance may not be available until the Triage Activities are fully operational, or are only applicable when triggered by an event (such as a major security incident) and as such may be raised as part of an observation in respect to 'obligations without supporting evidence' where no other observation of non-compliance has been raised for the obligation in question:

G3.5	G5.19
G3.9	G5.21
G3.10	G5.22
G4.3	G12.4

Due to the iterative nature of the approach to adding Obligations to this category, not all of these obligations may have been highlighted as 'obligations without supporting evidence' within the User's Full User Security Assessment report.

Appendix C – Preparing a User Management Response

Appendix C provides guidance on preparing the User management response that is required under SEC Section G8.26, G8.27, G8.28 and G12.6.
The User management response should be made on the standard template (SECAS Validation Workbook) provided by SECAS that will also contain the 'locked down' User CIO observations. The User management response should be as clear and comprehensive as possible because the SSC will use this as a key input to inform their recommendation on setting the assurance status.

The User management response will be reviewed and validated by SECAS in advance of being sent to the SSC to confirm that all mandatory elements are included. If the User management response is deficient, then SECAS, acting on the direction of the SSC, may reject the User management response and request that further detail be provided in an updated User management response.

If a User management response is not considered to have addressed the User CIO observations, then the User will not be prepared for their Security Sub-Committee review and will be invited to re-submit an updated User management response with the requisite information. The SEC requires that a User management response that is not considered to have addressed the findings in the report should have the assurance status set as 'deferred' (SEC Section G8.36 (d)). A 'deferred' status will not enable Triage Activities to be approved.

There are some mandatory elements that are required by the SEC and the SSC has established best practice that it is advisable to follow. These are explained below:

Mandatory content

The User management response must:

SEC G8.26 (a): indicate whether the User accepts the findings of the User CIO and, where it does not, must explain clearly why this is the case.

The SSC will expect to see the logic and any supporting evidence / grounds for not accepting the User CIO findings and to provide authorised Director level[1] sign-off of this position.

SEC G8.26 (b): set out any steps that the User has or will take to remedy and / or mitigate the actual or potential non-compliance or the increase in security risks.

[1] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".

The SSC will expect to see a clear explanation with an adequate level of detail of any proposed changes e.g. to the design or scope of the Triage Facility; also any process changes; documentary changes; contractual changes with third parties etc. and to provide the titles and ID numbers of any updated documents as appropriate; together with any updated risk assessment and risk treatment plan as a consequence of these changes; an implementation plan and timetable for any changes; and details of the internal governance arrangements for sign-off and approval. It isn't sufficient to say e.g. 'we will put this right'. It needs a clear and detailed explanation of what exactly will be done to put it right.

SEC G8.26 (c): identifies a timetable within which the User proposes to take any such steps that have not already been taken.

The SSC will be looking for a date commitment when the remediation / mitigation actions will be complete. The date should be realistic and achievable to ensure that all the necessary actions are complete and that any changes, documentation etc. have been signed-off through the User's appropriate internal governance processes.

The SSC strongly advises Triage Facility Providers to avoid committing to an early date that may not subsequently be achieved because this is likely to result in re-scheduling the SSC review and could incur delays to the approval of Triage Activities .

SECAS Initial Validation of the User management response

At the direction of the SSC, SECAS will have 10 days to conduct an initial validation of the User management response prior to presentation to the SSC to ensure that it corresponds to the mandatory SEC requirements. In addition, SECAS will check that the User management response:

- addresses every part of the observations in the User CIO report; and
- will provide the SSC with a commentary on the adequacy, in the context of the materiality of any observations, of the User management response, based on the extent and comprehensiveness of the description of the steps already taken or being taken by the User.

This validation exercise will aim to identify any weaknesses or a lack of detail in a User management response that the SSC will be likely to find insufficient, leading to a status of Deferred[2]. Some common examples are below:

- Poor – An undertaking by a User to re-assess, re-analyse or otherwise re-evaluate an approach – when described in such broad terms, this neither identifies the detail of the action to be taken nor commits the User to implementing a particular or specific course of action(s).
- Good – A specific set of detailed steps that are clearly and comprehensively described and will evidently address all aspects of the User CIO observation.
- Poor - A non-specific statement committing a User to complete an action(s) recommended by the User CIO observation – this is unlikely to be sufficiently detailed as the User CIO observation is unlikely to specifically list what action(s) need to be taken – just the lack of compliance with the SEC obligation.
- Good – A thorough and detailed description of the precise steps that the User is committing to take to address all aspects of the User CIO observation.

- Poor - An unrealistic timeline is given for a course of action(s) that typically requires significant effort, such as the re-running of a risk assessment, changes to HR policies for personnel screening or re-scoping the Triage Activities – depending on the context of the organisation and the observation this is likely to require many weeks to complete and to obtain sign-off through internal governance.
- Good – An explicit and precise timeline(s) is provided that takes realistic account of the complexity and magnitude of the effort required to re-run a task in the context of the criticality of the User CIO observation and which describes the intermediate steps with timings.

User CIO validation

For Full and Follow-Up User Security Assessments, following the SECAS validation of the User management response and any follow-up with the User which may result in a revised and updated User management response to address any perceived deficiencies, the User CIO will have 5 days to confirm that the User management response now fully addresses the User CIO observation or explains for SSC attention what is still outstanding.

The importance of a high quality, detailed User management response cannot be overstated. Triage Facility Providers should carefully consider the content of their User management response to ensure comprehensive information and detail is provided that addresses every aspect of the User CIO observations, including logic, rationale, governance sign-off and implementation plans with document reference IDs where documents have been changed since this will be the basis for the SSC to set an assurance status.

Standard Template to be used

The User CIO and SECAS have developed a template (SECAS Validation Workbook) that will be provided to the User with the User CIO observations displayed but locked down. The template will have a provision for the User to provide their User management response to each observation. The same template will be used by SECAS and the User CIO for their subsequent validation of the User management response and will also be provided to the SSC for their review of the User Assessment. This template will be made available to a User at the same time as their User Security Assessment Report is provided by the User CIO and will also be used by the SSC when they review the User Assessment.

The SECAS Validation Workbook will be used throughout the assessment cycle process. The template will contain separate worksheets for the initial Full User Security Assessment (FUSA), User Security Follow-Up Assessment, Director Letter Action Plan and Verification User Security Assessment (VUSA).

Triage Facility Providers are requested to use the template as this is a standard and familiar format that is used by the User CIO, SECAS and SSC for consistency.

[1] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".
[2] As per Section G8.36 of the SEC .

Appendix D – Preparing for the Security Sub-Committee (SSC) Review

Appendix D provides guidance to Users on preparing for the SSC review of the User CIO Assessment and the associated User management response.

Conflict of Interest: When a User CIO Assessment is to be considered at an SSC meeting, the SSC Chair will remind SSC members of the provisions of SEC Section C5.24 et seq which requires members to declare a conflict of interest if one exists. The SSC Chair will also set the confidentiality status of the discussion at Traffic Light Protocol (TLP) RED which limits any information and discussion on the subject to SSC participants and the SEC Panel.

User Representatives: The SSC has agreed that Users may bring up to two representatives to the SSC meeting that will consider their User Assessment. The representatives should include a technical professional who has a thorough understanding of the Triage Facility and Triage Activities, the overall architecture and the physical and technical security controls and their operation; and a security professional who understands and has experience of operating under ISO27001, ISO27005 and a working knowledge of the ISMS and other relevant documentation.

New Users are always asked to attend, but for any subsequent SSC meetings Users will be requested to attend on an exception basis.

User management response: In advance of the SSC meeting, SECAS and the User CIO, operating at the direction of the SSC, will have prepared an analysis of the extent to which the User management response addresses the User CIO observation. To maximise the effectiveness of the User management response at the SSC review, SECAS may seek further clarification of points from Triage Facility Providers prior to the SSC review and may provide an opportunity for the User to improve the User management response as suggested by SECAS to assist the SSC to better assess the extent to which the User management response meets the User CIO observation.

Conduct of the meeting: The SSC Chair will have reviewed the documentation and the SECAS and User CIO validation and will have developed a structure for SSC consideration of the observations and the User management responses to ensure the most efficient and effective use of time at the meeting. The User representatives are expected to fit in with the structure set by the SSC Chair and to answer any questions that SSC Members may raise. SECAS will have provided SSC members with the User CIO observation, the User management response and the SECAS and User CIO validations in a single document for ease of reference.

The SSC aims to meet its obligations under G8.27 / 28 et seq and enable the User to demonstrate that they have secure systems and processes that are compliant with the SEC. This will provide assurance to the SSC and SEC Panel and confidence to all SEC Parties that the systems supporting smart metering are appropriately secure. The SSC will be focussed on ensuring that the User CIO observations have been or will be satisfactorily addressed and that there is evidence and User and Shared Resource (where appropriate) internal governance sign-off to substantiate the completion of the actions.

Where, following discussion, the SSC considers that the User management response does not sufficiently address the observation by the User CIO there will be opportunity at the meeting for the User and the SSC to agree an updated or alternative set of steps for the User to take as allowed in SEC Section G8.27. Where this is the case or where the SSC requests or proposes that the User re-consider certain aspects, the agreed follow-up list of actions will be communicated to the User within the week following the SSC. Where it is not possible to agree an updated or alternative set of steps, the SSC is likely to set a status of ‘deferred’.

Architecture diagram: At the SSC meeting, new Users will be asked to commence the review by presenting a brief overview of the scale and nature of business operations and a diagram and explanation of the Triage Facility and should show functional, physical and network components and all connectivity into and out of the Triage Activities and explain where management controls reside to clarify.

The diagram should clearly identify the Triage Activities and distinguish this from other back-end or contributory or other corporate systems etc. and the User should explain any third-party involvement in provision of services or support This enables the SSC to get an understanding at the outset of how the Triage Facility is separated to meet the SEC obligations and to gain assurance that risk assessments have been properly and proportionately applied to individual components and that adequate controls and mitigations are in place.

Consideration of User CIO observations: The structure for the review is set by the SSC Chair. Where the SECAS and User CIO validations have indicated that the User management response satisfies the original observation, then the SSC is likely to accept their validation without further discussion.

Assurance status options: After considering the User CIO observations and the User management responses, supplemented by information that may be provided at the SSC meeting, the User representatives will be asked to withdraw whilst the SSC considers what assurance status to set (with responsibility to set the assurance status as in G12.6.

The options under the SEC are (where the with the term 'Panel' should be read as 'Security Sub-Committee'):

G12.7
On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:

(a) where the assurance status is set to 'approved' under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;

(b) where the assurance status is set to 'approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and

(c) where the assurance status is 'deferred' or 'rejected' under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

A lack of suitable evidence, for whatever reason, will increase the probability that a 'deferred' status is set or a Follow-up Security Assessment by the User CIO will be required.

Where the User management response indicates that the User has committed to taking steps to address the User CIO observation, the SSC may accept the steps that the User proposes to take and the timetable or may seek to agree alternative steps and / or timetable that would, in the opinion of the SSC, be more appropriate (SEC G8.27). Where alternative steps are to be agreed and/or further clarification as to the steps being taken by the User is provided then this information will be considered to be part of the User management response.

The SSC setting of the assurance status: The SSC voting members will be asked to vote on the assurance status to be set and the outcome will be recorded in the confidential minutes. The vote will be based on the User management response, together with any additional information provided to the SSC in advance or at the SSC meeting, including any alternative steps proposed by the SSC to be agreed with the User in accordance with G8.27.

The SSC Chair will offer a verbal communication of the SSC decision on the assurance status to the User representatives after the SSC meeting. SECAS will subsequently notify the User in writing of the assurance status.

Within this notification SECAS, on behalf of the SSC, will detail any alternative steps agreed with the User in accordance with G8.27. At that point, subject to no formal request to the SSC for a change to be made, these alternative steps will be considered to be part of the User Security Assessment Response.

On behalf of the SSC, SECAS will confirm with the User that, prior to commencing Triage Activities, one of the alternative steps will be to return to the SSC with a Director's letter [2] and a detailed explanation of how the steps have been taken and the actions completed.

Prior to the commencement of Triage Activities by the User, the SSC will schedule a review of the Director's letter and the detailed explanation to confirm that all the necessary steps have been completed to the SSC's satisfaction and there are no remaining security non-compliances. Prior to the SSC meeting and at the direction of the SSC, SECAS will undertake a validation of the Director's letter and the accompanying detailed explanation. If there are any aspects that, in the opinion of the SECAS Security Expert, would not satisfy the SSC, they will communicate with the User to offer the opportunity to improve the evidence.

At the SSC meeting, the SSC will consider the evidence in the Director's letter and the accompanying detailed explanation of the actions and steps taken and will consider any other available evidence and the SECAS validation. Once the SSC is satisfied, the User will be notified that there are no further actions to prevent the start of Triage Activities.

This will ensure that the User is able to commence Triage Activities by providing the necessary confirmation to the SSC that there are no outstanding security non-compliances or potential non-compliances.

[2] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".

A Summary of the SSC Decision-making Process on a Recommendation to the SEC Panel

Step	Action
1)	In advance of the SSC meeting, SSC Members will have reviewed the User Security Assessment Report, the User management response, the SECAS initial validation, any updated User management response and the User CIO validation to consider whether the User management response, if implemented as described, will lead to a compliant solution and whether there are any remaining actual or potential non-compliances.
2)	At the start of the SSC review, the SSC Chair will remind attendees of the obligations in SEC C5.24, C5.25 and C5.26 and ask if any SSC member wishes to declare a conflict of interest. The SSC Chair will also remind SSC members that the discussion will be held at TLP – RED and that all SSC Members have signed a Non-Disclosure Agreement.
3)	SSC Members will review the architecture diagram that has been requested from Users to understand the User topography, security controls, any third-party support, roles and responsibilities etc. This will enable SSC Members to understand the context of any User CIO observations.
a)	If no actual or potential non-compliance has been observed by the User CIO, the SSC should decide upon an assurance status of 'Approved' and the User will have satisfied the security obligations that will enable the start of Triage Activities and no further action on the Initial User Security Assessment is required.
b)	If any actual or potential non-compliance has been observed by the User CIO, SSC Members should assess whether the User management response potentially addresses the actual or potential non-compliances in the User Security Assessment Report. The potential of a User management response to address actual or potential non-compliances will depend on the volume and / or the severity of the observations and the time proposed to address them which will influence the level of confidence the SSC can take from the quality of the response. For example, responses should contain a management commitment to fully resolve the observation with a detailed explanation of how the observation will be addressed and a plan showing the timescales for mitigation activity and an explanation of the governance arrangements for oversight and sign-off. If SSC members believe that the response is satisfactory, they may accept the response as set out or may request a Director-level letter with an accompanying action plan to confirm when the actions have been completed for SSC review prior to the User starting Triage Activities.
c)	If SSC Members do not believe the User management response and any subsequent follow-up has the potential to address the actual or potential non-compliances identified in the User Security Assessment Report, they can request additional details and justification from the User at a later SSC meeting in accordance with the SEC (G8.28). Alternatively, SSC Members can vote to set a 'Deferred' assurance status and the User will not be able to start Triage Activities.
d)	If SSC Members are content that the User management response and any subsequent follow-up addresses the actual or potential non-compliances identified in the User Security Assessment Report, SSC Members should consider the materiality of actual or potential non-compliances and the level of confidence in the User to address them. Depending on the views of the SSC, an assurance status may be set to: a) 'approved…. subject to steps' (to be taken by the User) as in G12.7 (b); b) 'approved…. subject to steps (being taken by the User) and also being subject to a Follow-up Security Assessment by the User CIO by a specific date'; as in G8.36 (b) (ii). The User will not be able to start Triage Activities until completion of the relevant steps has been agreed with the SSC and a further review by the SSC of any Director's letter and accompanying detailed action plan.

Step	Action
e)	If SSC Members, having considered the User management response and any subsequent follow-up and the materiality of actual or potential non-compliances and have concerns about the User's capability to address them appropriately, then the SSC should consider setting the assurance status to 'deferred' as in G12.7 (c) subject to the Party first taking the steps proposed in the Response and being subject to a Follow-up Security Assessment by the User CIO.
f)	If, after considering the User Security Assessment Response and any subsequent follow-up evidence available including a Follow-up Security Assessment Report, SSC members require confirmation of any specific aspect of the observations, they may request the User CIO to review the specific evidence and report back to the SSC as provided for in SEC G8.3 (d) (ii).
4)	In considering the assurance status, SSC Members will have regard a) to the observation type ('Inadequate' or 'Requires Improvement') for each actual or potential non-compliance and b) to the potential likelihood and business impact of each actual or potential non-compliance.
5)	After User representatives have left the meeting, SSC Members will discuss and consider the User Security Assessment Report, the User management response and any validation and follow-up from SECAS, the User and the User CIO alongside the assurance status options having regard to factors relating to the Triage Activities and the significance and severity of the observations.
6)	Where the User management response indicates that the User has committed to taking steps to address the User CIO observation, the SSC may accept the steps that the User proposes to take and the timetable or may seek to agree alternative steps and / or timetable that would, in the opinion of the SSC, be more appropriate (SEC G8.27).
7)	The SSC Chair will then ask voting SSC Members to vote on a proposed assurance status, having regard to all the factors. The resulting assurance status will be communicated verbally to the User following the SSC meeting.
8)	SECAS will subsequently confirm the decision of the SSC to the User. On behalf of the SSC, SECAS will seek confirmation from the User that, prior to commencing Triage Activities, one of the alternative steps will be to return to the SSC with a Director's letter and a detailed explanation of how the steps have been taken and the actions completed. Prior to the commencement of Triage Activities by the User, the SSC will schedule a review of the Director's letter and the detailed explanation to confirm that all the necessary steps have been completed to the SSC's satisfaction. This will ensure that the User is able to commence Triage Activities by providing the necessary confirmation to the SSC that there are no outstanding security non-compliances or potential non-compliances.

Appendix E – Follow-up action prior to commencing Triage Activities

Appendix E provides guidance to Triage Facility Providers on any follow-up action required after the SSC has set the assurance status in line with SEC Section G12.7 (see Appendix D for details of the assurance status options). Where the User has agreed to taking steps to address an observation, the User should update the User management response to provide a detailed explanation of how the steps have been taken and the actions completed together with a timetable, by continuing to use the standard template spreadsheet provided by SECAS as described in Appendix C that was reviewed by the SSC and to add details of the updated evidence.

The updated spreadsheet should be submitted to SECAS for validation when all the actions have been completed accompanied by an authorised Director's[3] letter to allow for a SECAS validation prior to an SSC review of the Director's letter and the detailed actions. If, during the SECAS validation, it is considered that the User management response will not satisfy the SSC requirements, SECAS will provide the User with comments and an opportunity to further update the User management response. In some cases, SECAS may ask for sight of evidence e.g. updated documentation or contract clauses to confirm that the relevant action has been taken correctly.

Approved

If the SSC has set the assurance status as 'Approved' then there is no further User Security Assessment action for the User to carry out prior to commencing Triage Activities. The SSC will issue a Triage Facility Assurance Status Certificate to enable the Triage Facility Provider to confirm to relevant manufacturers that the assurance status allows Triage Activities to take place and this will be published on the SEC website.

Approved … subject to taking steps G12.7(b)

If the SSC has set the assurance status as in G12.7 (b)to 'Approved, subject to the Party taking such steps as it proposes to take in its User Security Assessment Response', then the SSC will provide details of the steps to be taken prior to commencing Triage Activities as required by G8.27. The SSC will issue a Triage Facility Assurance Status Certificate to confirm the assurance status.

Usually, the steps the SSC specify may require an authorised Director's letter and a detailed explanation of how the steps have been taken and the actions completed and for this to be provided to SECAS for validation prior to review by the SSC to confirm that the steps have been completed and approved through the appropriate internal governance processes. In some cases, the SSC may ask for specific evidence to be provided (usually to SECAS or to the User CIO) in the form of an extract from updated documents or reports.

As required by G8.28 (b), the User should report to the SSC on progress in taking the steps required; on completion of the steps in line with the timetable; and any failure to complete the steps with reasons.

This status will require completion of some further actions that the SSC will review prior to commencement of Triage Activities.

Approved … subject to taking steps and being subject to a Follow-up Security Assessment G8.36 (b) (ii)

If the SSC has set the assurance status as in G8.36 (b) (ii) to 'Approved, subject to the Party both taking such steps as are identified by the SSC and then being subject to a Follow-up Security Assessment by such date as the SSC may specify', then the SSC will provide details of the steps to be taken as in G8.36 (b) (i) above and of the scope of the Follow-up Security Assessment. The SSC will issue a Triage Facility Assurance Status Certificate to confirm the assurance status.

[3] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".

It will be necessary for the User to liaise with SECAS and the User CIO to arrange a Follow-up Security Assessment by the User CIO.

As required by G8.28 (b), the User should report to the SSC on progress in taking the steps required; on completion of the steps in line with the timetable; and any failure to complete the steps with reasons.

It is not intended that, in undertaking the Follow-up Security Assessment, the User CIO will revisit aspects of security compliance that did not result in an observation on the initial Assessment unless e.g. an updated Risk Assessment identifies new or changed risks that require changes to existing security controls that were previously assessed.

The SSC will provide the User CIO and the User with details of the observations and areas that need to be assessed and the SSC may ask the User CIO to also review any Director's Letter and a detailed explanation of how the steps have been taken and the actions completed or may require the User to make this available to the SSC for review.

On completion of the Follow-up Security Assessment, the process that is described in Clause 5.1(Types of Assessment) of the Triage Security Controls Framework Section 1 (Methodology) will apply i.e. 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 Follow-up User Security Assessment;

b) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G3 to G6 which have been identified by the User CIO; and

c) 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;

d) 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

e) 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 Follow-up User Security Assessment Report to the User for review for the purpose of factual accuracy checking prior to providing the final report to the User and to SECAS. The User then has an opportunity to provide a User management response which SECAS will validate as for a first Full User Security Assessment.

When the post-assessment steps are completed for SSC review, then the User should arrange with SECAS for the item to be included on the agenda for the next available SSC meeting.

The SSC will consider whether, on the balance of risk, this status will satisfy the criteria to enable Triage Activities to commence or whether it will require completion of some further actions specified by the SSC and a Follow-up Security Assessment by the User CIO to be undertaken and the outcome to be reviewed by the SSC prior to commencement of Triage Activities. Also, if any material security vulnerabilities have been identified prior to completing the User Security Assessment Process, these will need to be reported to the SSC prior to commencing Triage Activities.

Deferred … subject to taking steps G12.7 (c)

If the SSC has set the assurance status as in G8.36 (c) to 'Deferred, subject to the Party having first taken such steps as it proposes to take in its User Security Assessment Response in accordance with Section G12.7(b) and been subject to a Follow-up Security Assessment; and the SSC having determined that it is satisfied, on the evidence of the Follow-up Security Assessment, that such steps have been taken'.

In this situation, the SSC will provide details of the steps to be taken as required by G8.27. The SSC will issue a Triage Facility Assurance Status Certificate to confirm the assurance status.

It is possible that some of the steps may be met by an authorised Director's letter providing confirmation that certain actions have been completed and documentation updated and signed-off through internal governance.

However, it will be necessary for the User to liaise with SECAS and the User CIO to arrange a Follow-up Security Assessment by the User CIO as in G8.29 for when the actions have been completed.

As required by G8.28 (b), the User should report to the SSC on progress in taking the steps required; on completion of the steps in line with the timetable; and any failure to complete the steps with reasons.

The SSC will provide the User CIO and the User with details of the specific observations and areas that need to be assessed as part of the Follow-up Security Assessment.

On completion of the Follow-up Security Assessment, the process that is described in Clause 5.1(Types of Assessment) of the Triage Security Controls Framework Section 1 (Methodology) will apply. When the post-assessment steps are completed for SSC review, then the User should arrange with SECAS for the item to be included on the agenda for the next available SSC meeting.

After reviewing the Follow-up Security Assessment, the SSC voting members will be asked to vote on the assurance status. The SSC Chair will offer an informal communication of the SSC decision to the User representatives after the vote. SECAS will subsequently notify the User in writing of the assurance status set by the SSC.

The Follow-up Security Assessment by the User CIO will be reviewed by the SSC. Triage Activities cannot be commenced until the SSC has confirmed that the steps set in G12.7 (b) have been taken.

Rejected … subject to the Party having a second Full User Security Assessment G8.36 (c)

If the SSC has set the assurance status as in G8.36 (c) to 'rejected subject to the Party having a second Full User Security Assessment to address any issues identified by the SSC as being, in the opinion of the SSC, not adequately addressed in that response; and the SSC reconsidering the assurance status in accordance with Section G8.35 in the light of such amendments to the User Security Assessment Response. The SSC will issue a Triage Facility Assurance Status Certificate to confirm the assurance status.

In this situation, it is likely that the Management Response is considered by the SSC to be inadequate for consideration of one of the 'Approved' or 'Approved .... subject to steps' or 'Deferred.

The User is expected to revise the management response and re-submit for a further SSC review.

The User is NOT approved for Triage Activities. Further consideration will be given to the status when a revised management response is submitted for review.

Director's[4] Letter

Triage Facility Providers should seek to engage with SECAS to schedule when they believe they would like to have their Director's Letter reviewed by SECAS at least 8 weeks prior to their desired Go Live date. Early engagement is strongly recommended, as the validation of the Director Letter is a minimum of 10 WDs since the validation will seek to engage the User back and forth depending on the quality of the response and number of observations raised by the User CIO. The early engagement will enable SECAS to ensure that the adequate resource can be allocated.

A Director's letter should be signed either by an Officer of the Company or by a Director stated to be authorised to make commitments on behalf of the Company. The Director's Letter should confirm that the steps set out in the User management response, together with any additional or alternative steps set out by the SSC, have been completed and signed off through internal governance. The Director's Letter should be accompanied by the spreadsheet (as described in Appendix C) that has been used since the provision of the User Assessment CIO Report and should be updated with a detailed explanation of the steps that have been taken and the

[4] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".

actions that have been completed since the SSC review and details of any documentary evidence that has been updated.

In some cases, it may not be possible to complete all the actions prior to seeking SSC confirmation that the steps have been met Triage Activities. In these cases, the Director's letter should confirm that these steps will be completed with a planned date, together with explanatory details.

Appendix F – Verification User Security Assessment (VUSA)

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 areas exposed to any material increase in security risks, areas that have changed since the previous User Security Assessment, and to identify if a User has remediated any outstanding non-compliances raised from a previous User Security Assessment.

It is anticipated that the assessment will take between 2 and 3 days depending on the size, scale and nature of the User, and the degree of any change to the risk profile. The first day will be carried out on site at the Triage Facility premises, the following days may be carried out either on site or virtually as required or requested by the User. The User CIO will require access to key documentation as well as key stakeholders as agreed with the User prior to the assessment, as part of the pre-assessment communication.

Engaging with SECAS prior to an Assessment

Prior to any assessment, the User is required to engage with the User CIO:

- Engagement with the User CIO is managed via SECAS.
- Triage Facility Providers should seek to engage with the User CIO to schedule their User Assessment **at least 12 weeks** prior to their desired assessment date. Early engagement to schedule an initial and annual assessment is strongly recommended.
- It is the responsibility of the User to engage the User CIO in accordance with the Security Assessment Life Cycle (located in Section 1 of the TSCF). However, the User CIO will have regard to capacity and meeting the SEC schedule for User Security Assessments when scheduling the fieldwork for a second or subsequent User Security Assessment.
- SECAS has developed a 'scheduling system' to enable Triage Facility Providers to book available slots for a User Assessment. It is recommended that Triage Facility Providers book slots as soon as possible to avoid disappointment if capacity subsequently affects availability and impacts planned dates. Currently, the booking system is held and maintained by SECAS. To understand availability, please contact SECAS.
- Triage Facility Providers wishing to change the dates of an assessment must inform the User CIO at least 4 weeks prior to the original assessment start date.
- A cancellation charge may be applicable if the User fails to comply with the appropriate cancellation period.

Information to be provided by the User CIO

- The scope of the assessment. The User CIO will engage with the User to determine the scope of the assessment as well as to determine the scale, length, and involvement of User Personnel.
- Where applicable, a preliminary schedule and assessment timetable.
- A list of key User Personnel, by role, whom the User CIO may need to meet with during the assessment. This may include third party suppliers. User Personnel likely to be required includes:
    - Chief Information Security Officer (CISO) / lead security consultants and architects
    - ISMS officer / manager
    - System administrators
    - Solution designers
    - Human resources
    - Internal audit / Compliance resources
    - Third parties (where applicable)
    - An indicative document request list.
    - A list of responsibilities and requirements of the User to ensure an efficient assessment.
    - A proposed assessment team with a User CIO key point of contact.

The below table provides a list of the in-scope obligations that each User will be assessed against as part of a VUSA. It provides guidance regarding how each obligation will be considered by the User CIO. For avoidance of doubt, User's should still refer to Appendix B for detailed guidance on how to comply with each obligation.

Incident and Vulnerabilities Review

#	SEC Obligation Reference	Guidance
1	G3.5	*[As part of the Verification User Security Assessment, the User CIO will check to verify that all Major Security Incidents that have occurred since the last User Security Assessment have been reported to the Security Sub-Committee within an appropriate timescale.]*
2	G3.9	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User has ensured that any material change has been notified to the SSC prior to implementation.]*

Risk Identification and Management Review of Changes

#	SEC Obligation Reference	Provisional Observation
3	G5.14	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User adequately maintains its processes for the identification and management of the risk of Compromise to the Triage Facility.]*
4	G5.15	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User remains compliant to the latest version of ISO 27005 as a result of any changes since the last User Security Assessment.]*
5	G5.16	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User adequately carries out assessments for the identification and management of risk, annually, upon a material change to processes or components within the risk management scope and on the occurrence of any Major Security Incident in relation to its Triage Activities.*

Information Security Management System (ISMS) Review of Changes

#	SEC Obligation Reference	Provisional Observation
6	G5.17	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User remains compliant to latest version of ISO 27001 as a result of any changes since the last User Security Assessment.]*
7	G5.18	*[As part of the Verification Assessment, the User CIO will check to verify that the User's Information Security Management System continues to provide for security controls which are proportionate to the potential impact of each part of its Triage Activities being Compromised.]*

Additional Obligations on Triage Facility Providers (G12.4)

#	SEC Obligation Reference	Provisional Observation
8	G12.4(a)	*[As part of the Verification User Security Assessment, the User CIO will check to verify that the User adequately maintains its processes for the intake of Devices including inspection of tamper-protection boundary prior to undertaking Triage Activities.]*
9	G12.4(d)	*[As part of the Verification User Security Assessment, the User CIO will check to verify the controls in place to prevent unauthorised use of the Triage Tool and*

#	SEC Obligation Reference	Provisional Observation
		Triage System Interface and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities.]
10	**G12.4(f)**	***[As part of the Verification User Security Assessment, the User CIO will review the User's asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility and observe a record of the Triage Activities undertaken since the previous User Security Assessment.***

Obligations without complete supporting evidence

#	SEC Obligation Reference	Provisional Observation
11	**Obligations without complete supporting evidence***	***[As part of the Verification Assessment, the User CIO will check to verify that for any obligations without complete supporting evidence that were outlined in the User's previous Full User Security Assessment can be observed to be implemented.***
12	**Prior year observations**	***As part of the Verification Assessment, the User CIO will identify if a User has remediated any outstanding non-compliances raised from the previous User Security Assessment.***

***The User CIO will review implementation of all obligations where complete supporting evidence would not have been available at the time of the User Security Assessment. Please refer to Appendix B for guidance on and a list of obligations without complete supporting evidence.**

Post Assessment

The User management response should be made on the SECAS Validation Workbook (on the VUSA tab) provided by SECAS that will also contain the 'locked down' User CIO observations. The User management response should be as clear and comprehensive as possible because the SSC will use this as a key input to inform their recommendation on setting the assurance status. The User will have 15 WDs from the day the Assessment Report is provided to produce the User Management Response and submit it to SECAS.

The User management response will be reviewed and validated by SECAS in advance of being sent to the SSC to confirm that all mandatory elements are included. If the User management response is deficient, then SECAS, acting on the direction of the SSC, may reject the User management response and request that further detail be provided in an updated User management response. If the management response is not considered to have addressed any User CIO observations by the Final SECAS validation, the User management response will still be presented to the SSC for review. This is to make the SSC aware of the period of non-compliance and to ensure that they are aware of any residual risk from the outstanding observations. The SSC will then determine the remedial actions required from the User.

SECAS Initial Validation of the User Management Response

At the direction of the SSC, SECAS will have 10 WDs days to conduct an initial validation of the User management response prior to presentation to the SSC to ensure that it corresponds to the mandatory SEC requirements. In addition, SECAS will check that the User management response:

- addresses every part of the observations in the User CIO report; and
- will provide the SSC with a commentary on the adequacy, in the context of the materiality of any observations, of the User management response, based on the extent and comprehensiveness of the description of the steps already taken or being taken by the User.

This validation exercise will aim to identify any weaknesses or a lack of detail in a User management response that the SSC will likely find insufficient, leading to a finding on non-compliance with the SEC security obligations and, if not remediated quickly within an agreed remediation plan, a report to the SEC Panel to consider an Event of Default[5]. Some common examples are below:

- Poor – An undertaking by a User to re-assess, re-analyse or otherwise re-evaluate an approach – when described in such broad terms, this neither identifies the detail of the action to be taken nor commits the User to implementing a particular or specific course of action(s).
- Good – A specific set of detailed steps that are clearly and comprehensively described and will evidently address all aspects of the User CIO observation.

- Poor – A non-specific statement committing a User to complete an action(s) recommended by the User CIO observation – this is unlikely to be sufficiently detailed as the User CIO observation is unlikely to specifically list what action(s) need to be taken – just the lack of compliance with the SEC obligation.
- Good – A thorough and detailed description of the precise steps that the User is committing to take to address all aspects of the User CIO observation.

- Poor – An unrealistic timeline is given for a course of action(s) that typically requires significant effort, such as the re-running of a risk assessment, changes to HR policies for personnel screening or re-scoping the Triage Activities – depending on the context of the organisation and the observation this is likely to require many weeks to complete and to obtain sign-off through internal governance.
- Good – An explicit and precise timeline(s) is provided that takes realistic account of the complexity and magnitude of the effort required to re-run a task in the context of the criticality of the User CIO observation and which describes the intermediate steps with timings.

Updated User Management Response

Following the SECAS validation of the User management response and any follow-up with the User which may result in a revised and updated User management response to address any perceived deficiencies, The User will have 5 WDs to confirm that the User management response now fully addresses the User CIO observation or explains for SSC attention what is still outstanding. The Validation of the updated management response will be conducted by SECAS and once this is complete, final comments will be provided to the User in advanced of the SSC meeting, which will then be presented to the committee for their approval.

The importance of a high quality, detailed User management response cannot be overstated. Triage Facility Providers should carefully consider the content of their User management response to ensure comprehensive information and detail is provided that addresses every aspect of the User CIO observations, including logic, rationale, governance sign-off and implementation plans with document reference IDs where documents have been changed since this will be the basis for the SSC to confirm whether there are any non-compliances with SEC security obligations.

Verification User Assessment Timetable

Verification User Assessment timetable template (typical duration is two to three working days). *Please note that this timetable may be subject to change.* Please note the 'Personnel Required' will depend on the roles and responsibilities of the relevant staff within each Triage Facility.

Week 1: Day 1 (SEC Party Site)

Time	Activity	Objectives	Personnel Required
10:00 – 10:30	Introduction	To provide the SEC Party with an overview of the objectives and scope of the VUSA. To provide the User CIO with the progress overview with regards to actions committed to as part of the Director Letter. To agree on the type of evidence that SEC Party will be providing for obligations without complete supporting evidence that were observed as part of the last Full User Security Assessment. To provide the User CIO with a high-level overview of any material changes that SEC Party has made since the previous FUSA.	Security Manager, Smart Metering Programme Director
10:30 – 12:30	Solution and Triage Facility scope walkthrough	To provide the User CIO with an understanding of the any changes to the Triage Facility.	CISO, Security Manager
12:30 – 13:30	Q&A	Opportunity for User CIO questions on the Triage Facility.	CISO, Security Manager
13:30 – 15:30	Governance and Risk Management overview Overview of compliance with ISO27005 risk management practices	To discuss the approach taken by the SEC Party to security governance and risk management. To discuss the risk assessment scope applied by the SEC Party and the methods applied to risk management.	CISO, Security Manager
15:30 – 16:00	Document review	To allow the User CIO to read through documentation relating to the SEC Party in detail.	N/A
16:00 – 17:30	Q&A	Opportunity for User CIO questions on the governance and risk management approach.	Security Manager

Day 2 (Virtual/ SEC Party site/ User CIO site)

Time	Activity	Objectives	Personnel Required
9:00 – 10:00	Document Review	To allow the User CIO to read through documentation relating to the SEC Party in detail.	N/A
10:00 – 11:00	Information Security Management System walkthrough	To allow the User CIO to assess the SEC Party's evidence of how ISMS and G12.4 processes are applied in practice.	CISO, Security Manager

Time	Activity	Objectives	Personnel Required
11:00 – 12:30	Document review	To allow the User CIO to read through documentation relating to the ISMS	N/A
12:30 – 13:45	Q&A	Opportunity for the User CIO to ask questions based on documentation reviewed.	Security Manager
13:45 – 14:30	Document review		
14:30 – 17:00	Obligations without complete supporting evidence	Review evidence for obligations without complete supporting evidence that were observed as part of the last Full User Security Assessment	Security Manager
17:00 – 17:30	Q&A	Opportunity for the User CIO to ask questions based on documentation reviewed.	Security Manager

Day	Activities	Location	Objectives
< Day 3 >	• Assessment of SEC obligations • Close-out meeting	Virtual/ SEC Party site/ User CIO site	To allow the User CIO to Assess the SEC Party's: • Further assess any additional evidence provided by the SEC Party in relation to the observations noted. • Consolidate and document key observations from fieldwork. • Provide a view of the observations and discuss any outstanding points with the SEC Party.

Document Request List

The following list represents a consolidated list of documentation, which will assist the User CIO in performing the assessment. It should not be considered exhaustive, and the Triage Facility Provider should leverage the information provided within the Triage Security Controls Framework to support the identification of appropriate evidence in support of the assessment. This request list is subject to change once the assessment begins:

- Architecture diagram featuring the Triage Facility, Triage Tool(s) and Triage System Interface(s).
- Risk management scope (ISO27005); (G5.14)
- Triage Facility scope; Any ISMS documentation available, including governance;
- Smart metering related policies, processes, and procedures as applicable (based on SEC governance coverage);
- Risk assessment approach and output; (G5.14-G5.16)
- Risk treatment plan (Statement of applicability); (G5.15)
- Triage Facility asset register; (G5.21)
- Access control policy; (12.4(c))
- Incident management procedure; (G3.5)
- Data Retention Policy; (G3.10, G5.19)
- Information Classification Scheme; (G3.10, G5.19)
- Triage Facility Personnel screening policy; (G4.1 -G4.3)
- Record of Triage Activities (G12.4(f))

Appendix G – User Security Self-Assessment Return (SSA)

Introduction

A User Security Self-Assessment is carried out by the User with the results being reviewed by the User CIO and the SSC. The aim of the self-assessment is to identify whether there may have been any material increase in the security risk relating to the Triage Activities since the last User Security Assessment was conducted.

The SSC has approved the SECAS Validation Workbook, which contains an excel worksheet with the Self-Assessment Template. This will enable the User to provide the relevant information and supporting evidence for the User CIO to determine compliance with the SEC security obligations. The time-period of completion of the Security Self-Assessment is limited to 10 working days from the commencement date of the assessment.

Questions

All the following questions should be answered in relation to the changes which have been made since the date on which the previous User Security Assessment report was released. The User is expected to use the SECAS Validation Workbook to complete the answers to the questions below (the questions are replicated in the SECAS Validation Workbook). The User will be required to provide evidence to support the assertions made in the Self-Assessment. The evidence required will be confirmed 4 weeks in advance of the assessment commencement date by SECAS.

Once completed, the User is also expected to upload the updated workbook to Egress and alert SECAS (via SSC@talan.com) that this has been completed. SECAS will then inform the User CIO that the updated Validation Workbook has been uploaded to Egress and the User CIO will then begin to review the information provided.

If the User CIO has any questions relating to the answers provided by the User, then these will be raised directly with the User to try to clarify and resolve any uncertainties or potential non-compliances. The User will have the opportunity to update their responses on the SECAS validation workbook

After the clarification process between the User CIO and the User, the User CIO will seek to identify whether there may have been any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Triage Facility Providers) since the previous User Security Assessment as set out in SEC G8.18. If this is the case, the User CIO will notify the SSC on the SECAS Validation Workbook that this area may require special attention from the SSC as part of completing its review.

Following a review of the User's completed SECAS Validation Workbook and any User CIO comments, the SSC may:

- consider that the User responses are proportionate and satisfactory and do not reflect any security non-compliances and SECAS will notify the User accordingly; or
- may request the User to undertake actions and to provide further evidence and/or a plan to clarify the nature of any material increase in the security risk identified by the User CIO or to remediate any potential non-compliance indicated by the User CIO comments and report to the SSC as required in G8.28(b); or
- may request the User CIO to formally carry out an assessment of compliance as allowed in G8.3(d).

Please refer to the Self-Assessment timetable for duration of this process.

Reference	Question
A. Introductory Information *Please answer in relation to changes which have taken place since your last User Security Assessment*	
A.1	How many Devices have you conducted Triage Activities on in the past 12 months?
A.2	Have there been any changes to your contractual or operational arrangements with third party suppliers that provide services in relation to any part of your Triage Activities (whether these are suppliers of services or resources)? *E.g. The new arrangement with XYZ Vendor for the provision of security hardware within our Triage Facility replaced the previous arrangement with ABC Vendor for provision of XXX services effective from DD/MM/YYYY.*
A.3	Have there been any changes to your contractual or operational arrangements with any third-party suppliers that provide services to the relevant 'backend systems' within the scope of the risk management activities mandated by SEC G5.14 (whether these are suppliers of hardware, software and/or resources)? *E.g. The organisation providing 24/7 monitoring our CCTV operations changed on DD/MM/YYYY. The new contract is in place with XYZ Vendor. It replaced previous arrangement with ABC Vendor.*
B. How has the scope or method of operation of your Triage Facility changed, if at all since your last User Security Assessment? *Please answer in relation to changes which have taken place since your last Triage Facility Security Assessment*	
B.1	Have there been any material changes to your Triage Facility? *E.g. We have expanded out the Triage Facility with the addition of three new rooms which occurred on DD/MM/YYYY.*
B.2	Have there been any changes to the in-scope 'backend systems' supporting Triage Activities, as defined within SEC G5.14 part (c)? *E.g. New external CCTV system was implemented on DD/MM/YYYY which replaced our old external CCTV system.*
B.3	Have there been any changes to the communications links and the method used to secure these communications between the Systems included in the scope of your risk management activities per SEC G5.14 (i.e. your Triage Facilities and in-scope Triage Activities? *E.g. The VPN used to connect with manufacturer ABC was changed on DD/MM?YYYY.*
C. How do you consider the risks you face have changed, if at all, since your last User Security Assessment? *Please answer in relation to changes which have taken place since your last User Security Assessment*	
C.1	Have there been any changes to your Risk Management methodology? *E.g. We've moved from using the IS1 methodology to using IRAM2*
C.2	Have there been any changes to the mechanisms (boards, forums, sponsorship) used to govern your Risk Management processes? *E.g. We used to have monthly Information Security Forum meetings, now we are conducting quarterly ISF meetings*
C.3	Have there been any material changes within the business impact assessment included as part of your risk assessment? If yes, was a risk assessment against the material changes performed in line with your policies?

	E.g. We have increased the potential impact of compromise to our Triage Activities from 4 to 5 on account of the fact that we have acquired a significant number of new customers since our last User Security Assessment.
C.4	Have there been any changes to the threat intelligence sources you use to formulate your threat assessments? *E.g. We now have an additional source of threat intelligence via membership of the NCSC Smart Energy Information Exchange (SEIE).*
C.5	Do you consider the threat landscape has changed, and if so, how are the changes reflected in your risk assessment? *E.g. Intelligence indicates that smart meter exploits are being sold on the criminal market. We now see criminal gangs as the largest threat actor. We reassessed and increased the Capability and Motivation rating for this threat actor.*
C.6	Have there been any changes to your definitions of Material Change and Major Security Incident? If so, please explain how and why these changes have been made. *E.g.. Financial and reputational damage has now been added to the definition of a Major Security Incident.*
D. How has your approach to risk mitigation changed, if at all since your last User Security Assessment? *Please answer in relation to changes which have taken place since your last User Security Assessment*	
D.1	Have there been any changes in risk appetite for your Smart Metering Programme? If so, please explain how and why these changes have been made. *E.g. Since DD/MM/YYYY the Smart Metering Programme risk appetite was reviewed by the ISF and changed to "Cautious" from "Open" as per the Treasury Orange Book classification. This impacted the Risk Acceptance criteria for inherent risks and new controls were implemented for risks that were now outside the "Cautious" range.*
D.2	How has your control environment changed, e.g. via introducing new controls that are now required, or phasing out controls that are no longer required? If so, please explain how and why these changes have been made. *E.g. Due to the changes in risk appetite, existing and new controls were identified for risks outside the risk appetite range* *- Due to the changes in risk rating, ABC new controls were implemented.* *- Due to the new vulnerabilities identified in ABC, we have now implemented XYZ new controls.* *- With replacement of XYZ system and communication links, the respective controls of XXX and YYY were phased out.*
D.3 (Evidence Required)	Have you added any new risks since your last User Security Assessment? If so, please provide an extract of your risk assessment detailing the new risks, their risk ratings and whether the risks have been assessed as being within your risk appetite. *E.g. Yes, as a part of our quarterly review, we have identified [number] of new risks which have been added to our risk assessment. Please see the attached extract of our risk tracker which evidences the new risks, their risk ratings and the fact that all of them are within our risk appetite.*
E. How have you managed the screening of individuals since your last User Security Assessment? *Please answer in relation to changes which have taken place since your last User Security Assessment*	
E.1	How many individuals within your organisation fall within the scope of G4.2, and therefore require screening in accordance with G4.3? *E.g. There are 15 individuals who require screening in accordance with BS7858: 2019 or BPSS (where appropriate).*

E.2	Of the individuals identified in your response to E.1, how many have successfully completed the personnel screening process? *E.g. Of the 15 individuals who require screening, 12 have successfully been screened in accordance with BS7858: 2019 and 2 have successfully been screened to BPSS following a risk assessment to determine that the BPSS level is appropriate for those individuals.*
E.3	Where the individuals identified in E.2 have not completed the personnel screening process, please explain whether the screening process has begun including the date it was initiated and an estimated completion date. *E.g. One individual's screening is currently in progress as they have only recently joined us on DD/MM/YY and their screening was initiated on DD/MM/YY. Screening is due to be completed by DD/MM/YY.*
E.4	Do any individuals who have yet to be successfully screened have access to the Triage Facility, in contravention of G4.3? If yes, please explain whether any mitigating controls have been implemented and what the nature of these are. *E.g. No, the one individual who is awaiting completion of their personnel screening does not have access to any part of our Triage Facility.* *E.g. Yes, one individual who is awaiting completion of their personnel screening has been granted access to elements of the Triage Facility however, we have a protective monitoring solution in place designed to detect any unauthorised activity.*
E.5 (Evidence Required)	Please provide evidence of your compliance with SEC sections G4.2 and G4.3. Different Triage Facilities may choose to provide different forms of evidence to achieve this objective, but as a minimum the User CIO would typically expect to see your personnel screening tracker containing: • the names of individuals requiring screening • the level of screening required • the completion date of the required screening. • the date access to the Triage Facility was granted. *E.g. Please provide a tracker in table format containing the level of screening required, when the screening was performed and when access to the User Facility was granted to evidence compliance with sections G4.2 and G4.3.*
F. How have you managed the education, training and awareness of User Personnel in relation to information security since your last User Security Assessment? *Please answer in relation to changes which have taken place since your last User Security Assessment*	
F.1	In relation to your obligation to deliver information security training and awareness (G5.19), how many of your personnel have been identified as requiring information security training? *E.g. There are 15 individuals who require annual information security training.*
F.2	Of the individuals identified in your response to F.1, how many have now received information security training? *E.g. Of the 15 individuals who require training, 14 have received it.*
F.3	In any instance where any individuals identified above have not received information security training, please explain whether training has begun or is scheduled and provide a scheduled completion date. *E.g. The individual who requires training is currently on maternity leave and will receive the training when they return to work. This is scheduled to be completed by DD/MM/YY.*
F.4	Do any individuals who have yet to receive information security training have access to your Triage Facility? If yes, please explain whether any mitigating controls have been implemented and what the nature of these are.

	E.g. No, all individuals with access to the Triage Facility have had information security training. *E.g. Yes, our Information Security Manager has access to the Triage Facility without having received information security training this year however, this individual has 15 years of information security experience and oversees the delivery of information security training to other individuals.*
G. How have you managed any security related incidents? Please answer in relation to changes which have taken place since your last User Security Assessment.	
G.1	Have you experienced any security incidents in relation to your Triage operations and if so, did these meet your definition of a Major Security Incident? *E.g. On DD/MM/YY we experienced a security incident where an unauthorised attempt to access our shared resource provider business orchestration layer was detected. The incident did not meet our definition of a Major Security Incident and the incident has been dealt with in line with our incident management procedures.*
G.2	If the incident met your definition of a Major Security Incident, was the Security Sub Committee notified and was the notification given within your established timeframe? If the notification fell outside of the established timeframe, what were the reasons for this? *E.g. Yes, the SSC was notified within 24 hours of the incident which falls within the 72 hour timeframe which forms part of our incident management procedures.*

Self-Assessment Timetable

User Security Self-Assessment timetable template (typical duration is five working days). *Please note that this timetable may be subject to change.*

Week 1 – <Date of Week 1 Day 1> to < Date of Week 1 Day 5>

Day	Activities	Location	Objectives
<Day 1>	Review self-assessment	User CIO	To allow the User CIO to: Review the self-assessment Document any questions to be discussed on the teleconference with the User
<Day 2>	Q&A Status review meeting Compile updates	Teleconference (AM)	To allow the User CIO to: Ask the SEC Party questions based on the documentation review Request additional information from the SEC Party To allow the SEC Party to: Respond to questions from the User CIO Compile any additional information required by the User CIO to complete the self-assessment
<Day 3>	Compile updates	SEC Party	To allow the SEC Party to compile any additional information required by the User CIO to complete the self-assessment
<Day 4>	Document review	User CIO	To allow the User CIO to review any updated responses the SEC Party has provided.
<Day 5>	Assessment of SEC obligations Close-out meeting (as required)	Teleconference (PM)	To allow the User CIO to: Ask any final questions and/or inform the SEC Party that their Self-Assessment return is ready for submission to SECAS

Evidence Required

Evidence is required to support some of the assertions as a part of Self-Assessment, as specified in the template. The following list represents a consolidated list of evidence required, which will assist the User CIO in performing the assessment. It should not be considered exhaustive, and the User should leverage the information provided within the Security Controls Framework to support the identification of appropriate evidence in support of the assessment.

This evidence list is subject to change once the assessment begins:

- **D.3 –** extract of your risk tracker
- **E.5 –** evidence of your tracker that details:
    - the names of individuals requiring screening
    - the level of screening required.
    - the completion date of the required screening.
    - The date access to the Triage Facility was granted.

Appendix H – Remaining non-compliances following SSC review of a second or subsequent User Security Assessment

User Security Assessments after the initial Full User Security Assessment

For the Full, Verification and Self-Assessments that take place after the initial Full User Security Assessment, the SSC is not required to set an assurance status, but is required to identify and act on any security non-compliances that have been identified by the User CIO. Appendix H provides guidance to Triage Facility Providers on any follow-up action required after the SSC has reviewed a second or subsequent User Security Assessment.

Remediation Plan and Director-signed Cover Letter

Where the User has remaining observations following SSC review of a second or subsequent User Security Assessment, the SSC will aim to agree a remediation plan with the User to be implemented within an agreed timescale.

The User should initially update its SECAS Validation Workbook template provided by SECAS (as described in Appendix C) to provide a timeline of remedial action to be validated by SECAS. The User shall subsequently provide a detailed explanation of its remedial action for each observation along with any supporting evidence. If, during the SECAS validation, it is considered that the remedial action outlined by the User will not satisfy the SSC requirements, SECAS will provide the User with comments and an opportunity to further update the remediation plan.

Once all remedial action is complete, each User shall provide an authorised signed Director's[6] letter to confirm all outstanding actions have been completed. This allows for SECAS validation prior to an SSC review of the Director's letter and remediation plan.

Recommendations to the SEC Panel

SEC Section G8.57 requires the SSC to consider the materiality of any security non-compliance and refer the matter to the Panel to consider whether that non-compliance represents an Event of Default. The SSC will recommend an Event of Default to be considered by the Panel in cases:

- where the User refuses to produce a Remediation Plan, or the proposed Remediation Plan timetable is unacceptable, or
- if the User fails to remediate the observations and/or the remediation timetables, are not being met as was agreed with the SSC, or
- where the SSC concludes that the User has breached the SEC.

[6] The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".

Appendix I – Observation scoring catalogue

The ratings assigned to any observation within User Assessment Reports are defined as follows:

Area	Identifier	Description
Rating	Inadequate	• Significant non-compliance was observed by the User CIO against the SEC relevant obligation, or • Insufficient evidence was presented such that an effective assessment of compliance could not be performed, or • The User CIO identified a matter that should be discussed by the SSC to assign the appropriate Assurance Status for the SEC Party.
	Requires Improvement	• Non-compliance or potential non-compliance was observed by the User CIO against the relevant Obligation, or • Incomplete evidence was presented such that only a limited assessment of compliance could be performed, or • The User CIO identified a matter that the SSC may wish to consider discussing to assign the appropriate Assurance Status for the SEC Party.
	Adequate	• Non-compliance was not observed by the User CIO against the relevant obligation, and • Sufficient evidence was presented to the User CIO such that an effective compliance assessment could be performed, and • The User CIO did not identify any matters that should be raised to the SSC for discussion.
	For Information	• Non-compliance was not observed by the User CIO against the relevant obligation, but the User CIO identified a matter that the User may wish to consider taking action on or updating as not rectifying this could lead to future non-compliance. • The identified matter is not one that the SSC should consider discussing to assign the appropriate Assurance Status for the SEC Party.
	Remediated	• Initial non-compliance, limited to a documentation issue, was observed by the User CIO against the relevant obligation, and • Evidence was presented to the User CIO such that the non-compliance has been addressed and no management response is required. • The User CIO identified a matter that the SSC may wish to consider discussing to assign the appropriate Assurance Status for the SEC Party however no further User action is required.
Scale	Isolated	• The non-compliance observed by the User CIO occurred in two or fewer instances of the control operation to comply with the relevant obligation; and • This non-compliance did not represent a substantial or total failure to operate the control throughout the assessment period (e.g. failing to perform an annual review of a process which, whilst being a single instance of non-compliance, would be considered as Systemic, per the definition below).
	Systemic	• The non-compliance observed by the User CIO occurred in three instances or more of the control operation to comply with the relevant obligation; or • The non-compliance observed by the User CIO represented a substantial or total failure to operate the control throughout the assessment period (e.g. failing to perform an annual review of a process).
Type of observation	Documentation Issue	• Non-compliance, limited to a documentation issue, was observed by the User CIO against the effective design of controls used to comply with the relevant obligation.
	Deficient Evidence	• No evidence was presented to demonstrate compliance with the relevant obligation, or

Area	Identifier	Description
		• The evidence presented was deficient such that an effective assessment of compliance could not be performed.
	Observed Non-Compliance	• Non-compliance was observed by the User CIO against the effective design and/or implementation of controls used to comply with the relevant obligation.
Immediate non-compliance addressed		• Evidence was presented to the User CIO such that remedial action against the immediate non-compliance identified was taken at the time or has been taken during the assessment. However, the User is requested to provide a Management Response to this observation which demonstrates how the User plans to prevent a re-occurrence of the same issue.

Appendix J: Template of the Certificate of 'Triage Facility Assurance Status'

SEC
Smart Energy Code

Triage Facility Provider Certificate

This is to certify that

[Name of Triage Facility Provider]

has undertaken a User Security Assessment as required by the Smart Energy Code (SEC) Section G12. The Security Sub-Committee has set the assurance status to

'Approved'

In line with SEC Section G12.7

Authorised by the SEC Security Sub-Committee (SSC) at SSC Meeting: [Meeting number] [Meeting date]	Approved From: [Date of start of approval] Next Approval Due: [Date next assessment to be scheduled by]

Conditions that apply to this assurance status:
Any conditions set by the SSC e.g.

The Triage facility Provider must ensure that the Triage Tool and Triage System Interface used for triage Activities have been assured under the CPA Build Standard as required by the *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC and CH SCs and CPA Build Standard Extensions"*.