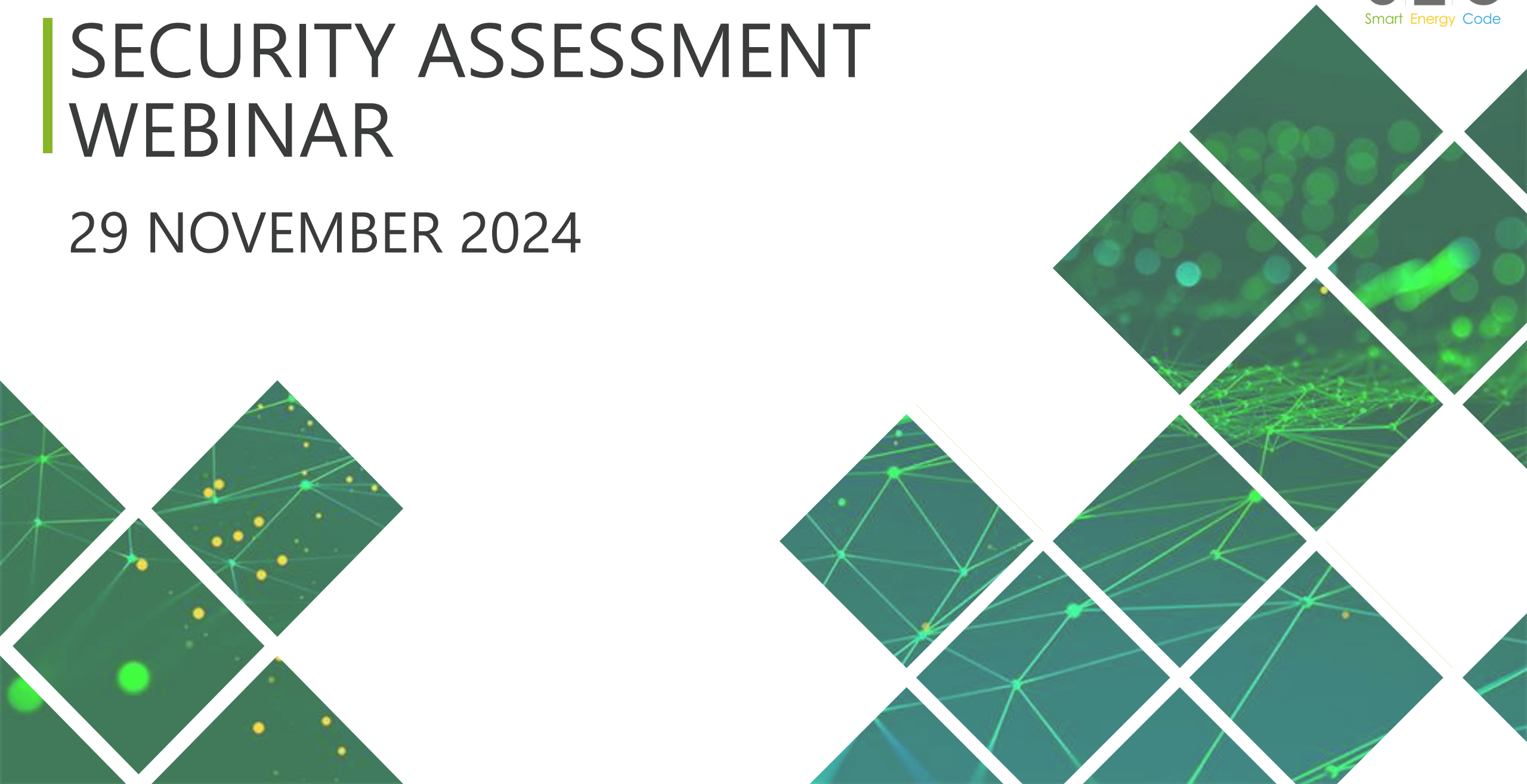
# SECURITY ASSESSMENT WEBINAR

## 29 NOVEMBER 2024



# AGENDA

1. Introduction
2. SECAS Security Team
   - Introduction to SECAS Privacy Team
   - Overview of SECAS Team Role
   - Assessment Booking Information
   - Party Communications & Engagement
   - Reminder of User Obligation
3. User CIO
   - Introduction to User CIO
   - Overview of CIO role
   - Security Risks, SEC G Obligations and the Assessment Approach
   - Small Suppliers, Triage Facility providers, and understanding the ISO27005 risk assessment approach
   - Q&A
4. SECAS Security Experts
   - Security Expert Team
   - Security Expert Roles
   - FUSA/VUSA Validation Process
   - Setting the Assurance Status
   - Material Change Notification
   - Incident and Vulnerabilities Management
   - Key Obligations - Common Issues
   - Validation Top Tips
   - Guidance Links
5. Q&A

slido

Please download and install the Slido app on all computers you use

# Join at slido.com
# #2831997

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

# How well do you understand the Security Assessment processes?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

# How well do you understand the roles of User CIO and the SECAS Security Experts?

ⓘ Start presenting to display the poll results on this slide.


# THE SECAS PRIVACY TEAM

# YOUR SECAS SECURITY & PRIVACY TEAM

**Fiona Bond -** Security & Privacy Delivery Manager

**Graham Hall -** Smart Energy Consultant

**James Hosen -** Security & Privacy Consultant

**Alex Scott** - Governance and Operations Analyst

**Annie Da Costa -** Senior Governance Administrator

**Rachael Jones -** Senior Governance Administrator

SEC
Smart Energy Code

# OVERVIEW OF THE SECAS TEAM ROLE

# OVERVIEW OF THE SECAS TEAM ROLE



**Meeting Management**



**Assessments & User CIO**



**Projects and Procurement**

# MEETING MANAGEMENT (SSC)

- Annual Terms of Reference (ToR) reviews for Security Sub-Committee
- Calendar invites, agendas, papers, actions, headlines, minutes, rooms/facilities, Independent Chair liaison
- Elections/ member management co-ordination of scheduled and ad-hoc elections for committees (advertising/shortlisting/voting)
- Management of SSC Risks Registers
- Monitoring Modification Proposals
- Maintaining distribution lists (MS Teams, Outlook)
- Maintaining Website Information (Terms of Reference, Meeting Dates, Membership List, Finalised Minutes)

SEC
Smart Energy Code

# ASSESSMENT BOOKING INFORMATION

# ASSESSMENT BOOKING INFORMATION

To book your Security Assessment parties should visit our **Assessment Management System (AMS)**

AMS is an **online booking solution** allowing SEC Parties, SECAS and the User CIO to fully manage the booking process

Requested assessment dates are required to be **at least twelve weeks** after the date your request is submitted

Indicative costs for Security Assessments can be found on the **Security Rate Card 2023 – 2024**

Most Security Assessments fall into the **lower banding for Security** indicated on the Rate Card

The Security Validation Workbook v1.5 will be used for the Management Response and Validation stages of the Assessments and will be provided to Users via the secure sharing platform **Egress**

SEC
Smart Energy Code

# PARTY COMMUNICATIONS & ENGAGEMENT

# PARTY COMMUNICATIONS & ENGAGEMENT

- SSC@gemserv.com is a dedicated Security Subcommittee inbox
- Created to supplement the SSC and all Security Assessment related activity
- The inbox is monitored by the SECAS Security & Privacy team
- It is the best place to raise queries, seek guidance and gain information on the assessment process
- The SSC inbox acts as the central point of external communications to Users, such as updates on assessment progress, updates to the SCF and requests from the SECAS validations team

SEC
Smart Energy Code

# REMINDER OF USER OBLIGATION

# REMINDER OF USER OBLIGATION

Section G of the SEC details the security arrangements required for DCC Users to interact with the DCC. These are designed to ensure that there is no single point of vulnerability.

To become eligible to use the DCC Systems, SEC Parties must pass a User Security Assessment conducted by the User Competent Independent Organisation (User CIO). After this, assessments are annual. The specific type of User Security Assessment required depends on the number of Smart Meter Systems a User interacts with (see following slide).

The SEC highlights three areas of security obligations for the DCC and Users:
System Security, Organisational Security, and Information Security

Users are expected to co-operate during the assessment process, ensuring they review the SCF (Security Controls Framework) and engage with SECAS if they have any queries ahead of their assessment.

# REMINDER OF USER OBLIGATION

As the lead Government Department for Smart Metering, DESNZ are responsible for any potential impacts Smart Metering could cause to Critical National Infrastructure (CNI) and the wider energy system. Therefore, the assurance of organisations participating in Smart Metering is a fundamental part of the assurance of the end-to-end smart metering security architecture.

This is due to the remote connection of smart metering gas and electricity meters in consumer premises to energy Suppliers, Network Operators and Other Users. Security requirements have been developed for smart metering equipment, the DCC and Users with the purpose of designing proportionate security controls which are subsequently implemented and assured to ensure the risk to CNI is minimised.

Security and privacy are at the heart of the Smart Metering System and considerable effort has been invested by Government and the energy industry in designing security protection into the end-to-end security architecture. Within this, User Security Assessments provide assurance to all Users that security controls are being maintained.

# SECURITY ASSESSMENT CATEGORIES

SEC
Smart Energy Code

| User Security Assessments | | |
|---|---|---|
| **Full User Security Assessment (FUSA)** | **Verification User Security Assessment (VUSA)** | **Security Self-Assessment (SSA)** |

| | # of Domestic Premises supplied with electricity or gas | User Entry / Year One | Year Two | Year Three |
|---|---|---|---|---|
| **Supplier Parties** | More than 250,000 Domestic Premises | Full Assessment | Full Assessment | Full Assessment |
| | More than 50,000 Non-domestic Premises | Full Assessment | Full Assessment | Full Assessment |
| | (5N) + D > 250,000* | Full Assessment | Full Assessment | Full Assessment |
| | 250,000 or less | Full Assessment | Verification Assessment | Self-Assessment |
| **Network Parties** | More than 250,000 | Full Assessment | Verification Assessment | Verification Assessment |
| | 250,000 or less | Full Assessment | Verification Assessment | Self-Assessment |
| **Other Users** | n/a | Full Assessment | Verification Assessment | Self-Assessment |

# REMINDER OF USER OBLIGATION

## Assessment timelines – CIO, SECAS and User obligations

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 12 weeks prior to assessment | | | 10 working days | 5 working days | | 10 working days | 5 working days | |
| Submit application to SECAS | Cancellation fee Incurred | Fieldwork Assessment | User Assessment Report | Factual Accuracy Challenge | User Management Response | SECAS validation | User CIO Validation | SSC Review |
| | Final 4 weeks | Up to 10 working days | | <<<<15 working days>>>> | | | | Occur every 2nd and 4th Wednesday of the month |
| Users can book their assessment as early as they wish but will be reminded to book if they have not done so within 12 weeks of their assurance window. | | | | The 15 working days encompasses both the Factual Accuracy Challenge (which needs to be submitted within the initial 5 days) and the User Management Response stages. | | If SECAS require more evidence from the User, this stage can be repeated. | | SSC will review the assessment and set a Compliance Status. All Users are sent an extract of the SSC minutes. |

SEC
Smart Energy Code

# THE USER COMPETENT INDEPENDENT ORGANISATION

# THE USER CIO

CHRIS GANDHI

**User CIO Team Lead**

LINDSEY FLAGLER

**Security Assessment Lead**

# SECURITY

- The energy industry has invested significantly to design and maintain a secure end-to-end Smart Metering Infrastructure
- Smart Meters control the flow of energy in the UK
- We are here to make sure that DCC Users are operating in a secure manner to preserve the integrity of the end-to-end infrastructure
- Governed by the Smart Energy Code (SEC)

# ASSURANCE

- The User CIO provides assurance that User Smart Metering operations are carried out securely by performing security assessments.
- The Security Sub Committee utilises User CIO reports to set each SEC Party assurance status to enable them to ‘go live’ and determine their ongoing compliance status each year.
- The overall goal is to provide confidence to all SEC Parties that the Systems supporting Smart Metering are appropriately secure.

# SEC RISK DEEP DIVE

G5.14 – The Risk Scope

Defines the what

G5.15 – The Risk Process

Defines the how

G5.16 – The Risk Assessment triggers

Defines the when

# G5.14: RISK SCOPE

*Each User shall establish, maintain and implement processes for the identification and management of the risk of*

*Compromise to:*

*(a) its User Systems;*

*(b) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;*

*(c) any other Data, Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface;*

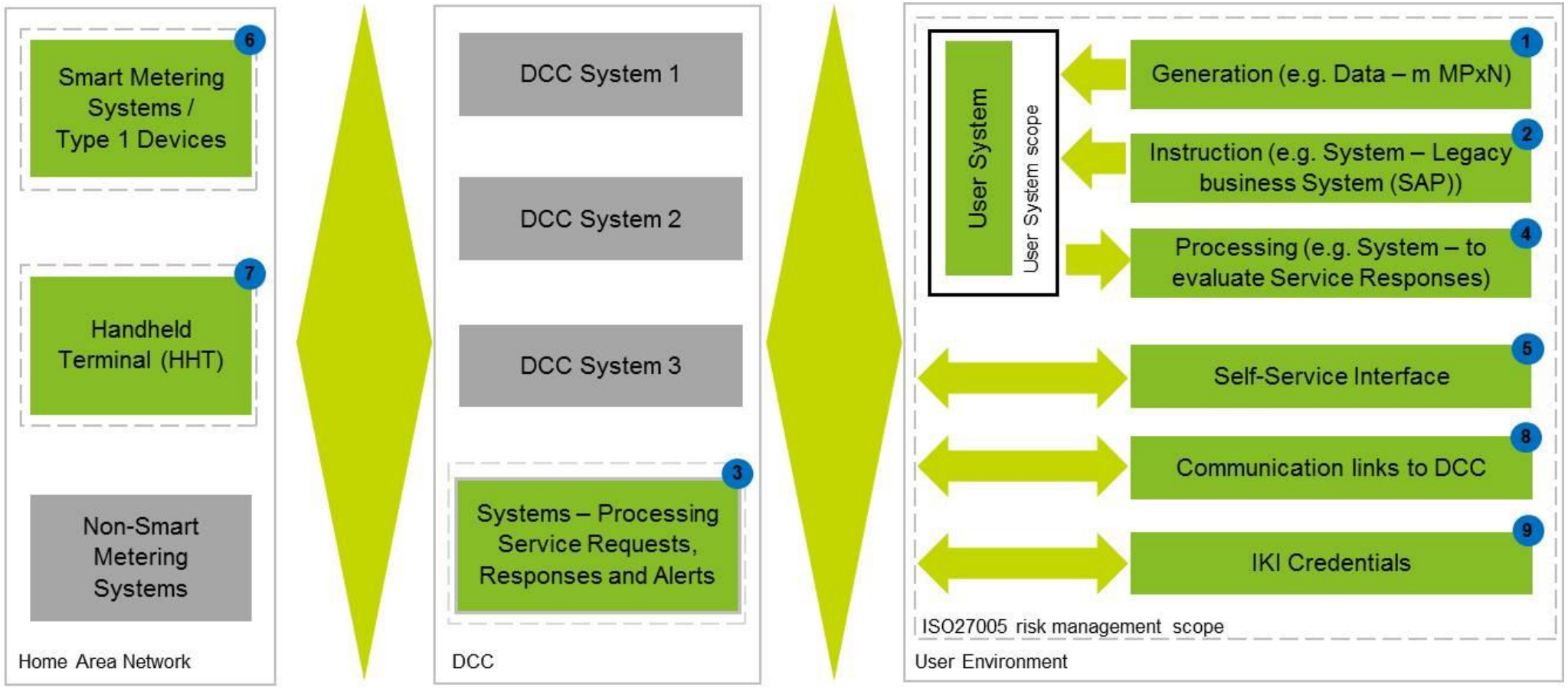
*(d) any Smart Metering Systems for which it is the Responsible Supplier; and*

*(e) any communications links established between any of its Systems and the DCC Total System, and any security functionality used in respect of those communications links or the communications made over them.*

# G5.14: RISK SCOPE

1. *The Data required to generate a Service Request, such as the MPxN contained in an asset inventory, which is fed into the User System.*
2. *The business Systems (e.g. back-office systems) used to instruct the creation of a Service Request, such as a SAP or equivalent system.*
3. *The parts of the DCC Systems used to process a Service Request.*
4. *The business Systems used to process Service Responses or Alerts received from Smart Metering Systems, such as Alert triage and event management Systems.*
5. *Any Data communicated over the Self-Service Interface to the DCC.*
6. *Any Smart Metering Systems for which it is the Responsible Supplier.*
7. *Handheld Terminals (HHTs) that process or store Commands for communications with a Smart Metering System.*
8. *Any communications links established between any of its Systems and the DCC Total System and any security functionality used in respect of those communications links or the communications made over them, including:*
    a) *The connections to DCC SMKI services (Portals and Repository).*
    b) *The transferring of .CSV files containing expected volumes of message types in support of the DCC anomaly detection capability.*
9. *The management of the Infrastructure Key Infrastructure (IKI) credentials stored on e-tokens. The IKI credentials are used to connect to the SMKI Portal for the purposes of submitting CSRs and CRRs.*

# G5.14: RISK SCOPE




Key:

<Text> – part of the User risk assessment scope

<Text> – not part of the User risk assessment scope

ISO27005 risk management scope

# Agreed Interpretation context

# G5.15: RISK PROCESS

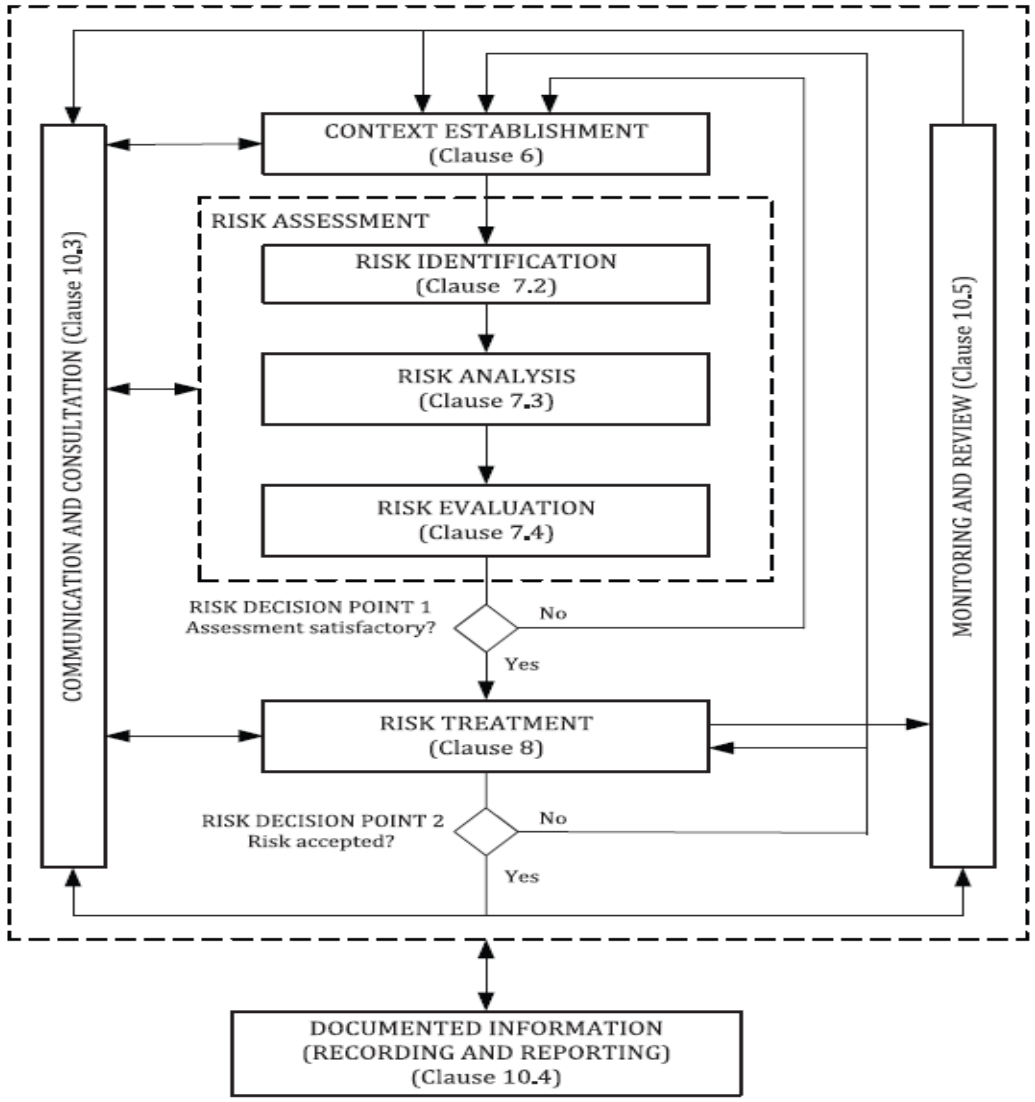
*Each User shall ensure that such processes for the identification and management of risk comply with:*

*(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.*

# G5.15 - ISO/IEC 27005

# G5.15 - ISO/IEC 27005




**ISO/IEC 27005: 2022 Section 5.1 - Figure 1 – Information security risk management process**

# G5.15 - ISO/IEC 27005 – SECTION 6

Organisation risk context, requirements and application

6.1-6.3

6.4

Establish Criteria

- Risk Appetite
- Risk Acceptance

6.4.2

6.4.3

Risk Criteria

- Consequence
- Likelihood
- Overall Risk

# G5.15 - ISO/IEC 27005 – SECTION 7.2

Risk Identification

7.2

7.2.1

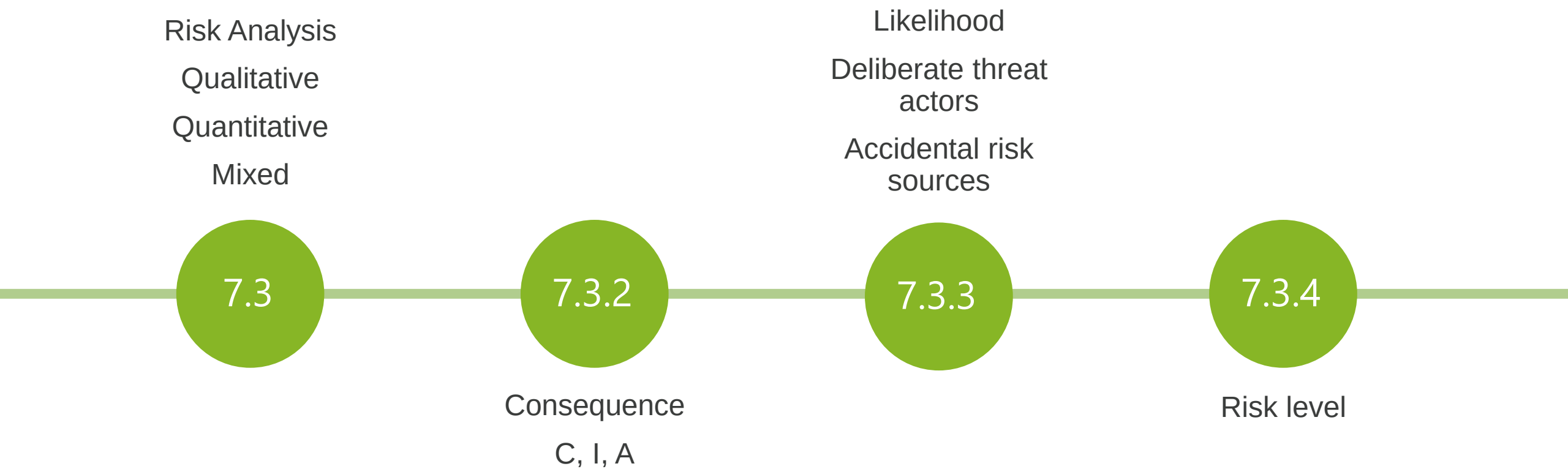
Identify risks

Asset vs event

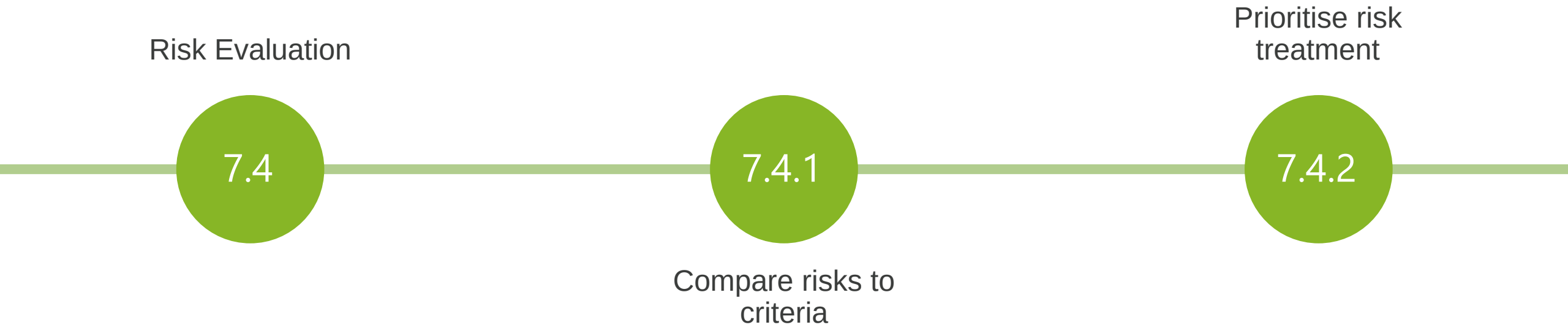
Risk owners

7.2.2

# G5.15 - ISO/IEC 27005 – SECTION 7.3



# G5.15 - ISO/IEC 27005 – SECTION 7.4



# G5.15 - ISO/IEC 27005 – SECTION 8

Treatment Options

- Avoidance
- Modification
- Retention
- Sharing

8.2

8.3

Determine Controls

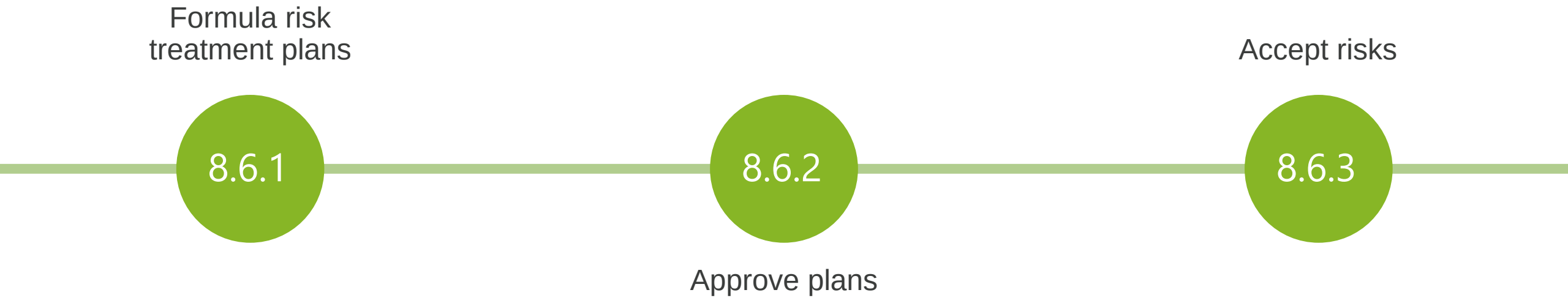
Compare to ISO27001 Annex A

8.4

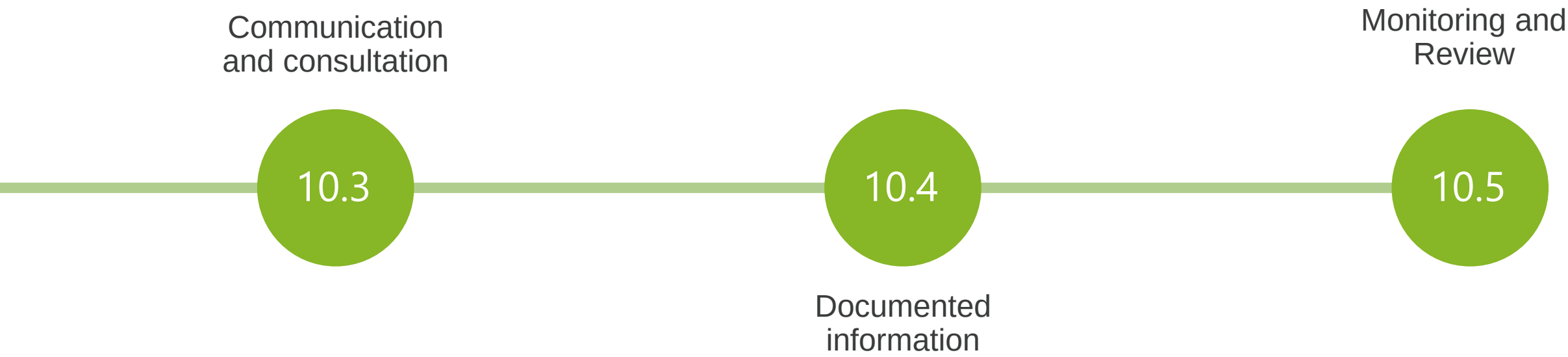
8.5

Produce a Statement of Applicability

# G5.15 - ISO/IEC 27005 – SECTION 8.6



# G5.15 - ISO/IEC 27005 – SECTION 10



# G5.16 – RISK ASSESSMENT TRIGGERS

*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 User Systems*
- *(ii) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;*
- *(iii) any other Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface; or any Smart Metering Systems for which it is the Responsible Supplier; and*

*(c) on the occurrence of any Major Security Incident in relation to its User Systems.*

# G5.16

Annual – A full risk assessment must be performed every 12 calendar months

Material change – A risk assessment must be performed **prior** to the change taking effect

Major Security Incident – A risk assessment must be performed on the **occurrence** of the incident

# RISK MANAGEMENT

## What the User CIO needs to understand:

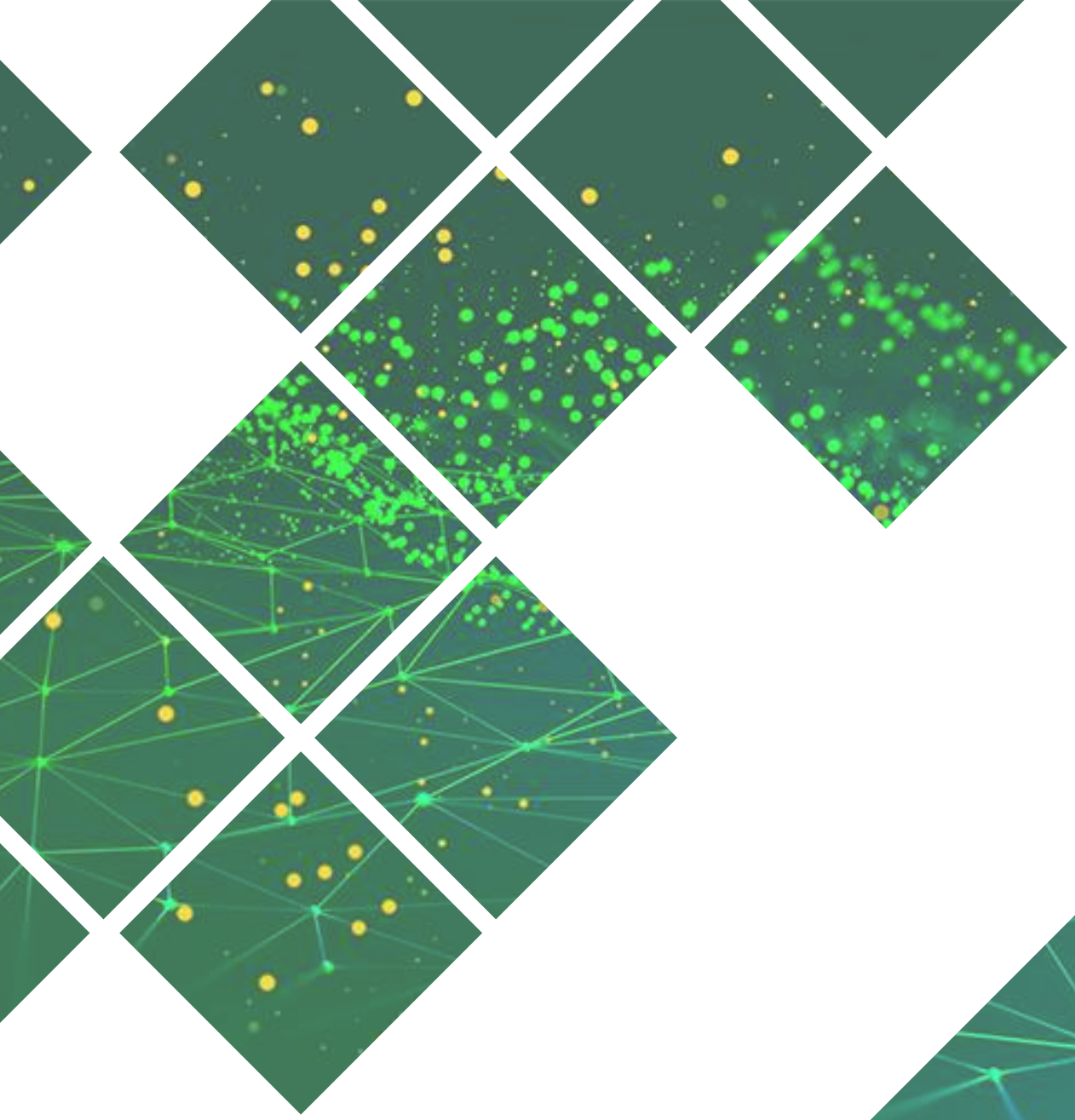
- ✓ What is in scope for your risk assessment?
- ✓ What is your risk methodology?
- ✓ What does your risk assessment look like?
- ✓ What feeds into risk calculation? (i.e. threat intel)
- ✓ When will you review your risk assessment?

## What the User CIO may expect to see:

- ✓ A scope statement or diagram for the risk assessment.
- ✓ Evidence of risk management artefacts, e.g. risk treatment.
- ✓ Evidence of inherent and residual risk analysis.
- ✓ Evidence of changes to the User System and Major Security Incidents triggering a risk assessment.

# MDR ROLE

- If you are a new User who doesn't currently have a DCC User role, you will need to undertake role or initial Full User Security Assessment, aligned to any new Party wishing to become a New User;
- If you have an existing DCC User role, you will need to raise a Material Change to the SSC highlighting that you wish to add this as a User role.
- Depending on your existing DCC User role security posture, you will either need to undertake a top-up Security Assessment for the new risk areas associated with the MDR role or follow the normal Material Change process with sign off at SSC.
- A further discussion of the process is included within the SCF Part 1 within Appendix A - FAQs, and the full list of applicable SEC obligations for an MDR is included within the SCF Part 1 Appendix B.
- Please find the Material Change Notification on the website here.
- Please find more information on going live with a new DCC User role in the Security Controls Framework Part 1 here (page 30).



# THANK YOU FOR LISTENING

## ANY QUESTIONS?

SEC
Smart Energy Code

# SECAS VALIDATION PROCESS

29 November 2024

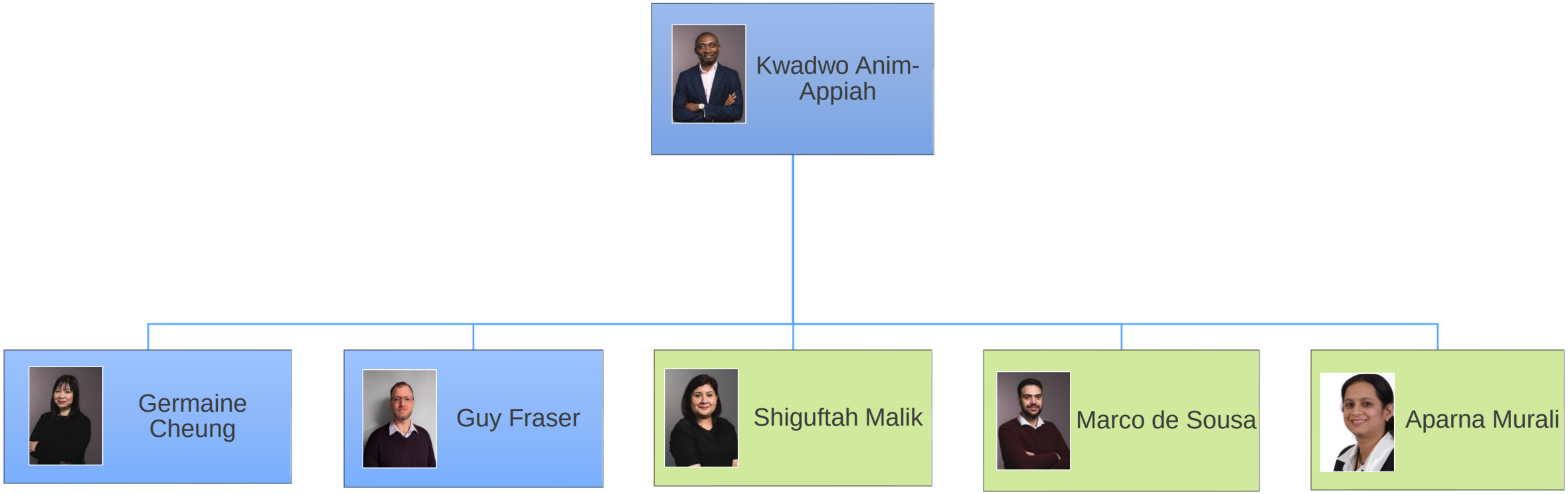
Germaine Cheung
Senior Information Security Consultant

# AGENDA

- Security Expert Team
- Security Expert Roles
- FUSA/VUSA Validation Process
- Setting the Assurance Status
- Material Change Notification
- Incident and Vulnerabilities Management
- Key Obligations - Common Issues
- Validation Top Tips
- Guidance Links

# SECURITY EXPERTS TEAM

SEC
Smart Energy Code



# SECURITY EXPERT ROLES

SEC
Smart Energy Code

- Validation of response from SEC Parties
- Validation of Remediation Plans
- Conduct additional Evidence Reviews
- Analyse and review vulnerability and incident reports
- Produce and present papers for SSC review when needed
- Standards and Best Practices review for SSC and SMKI
- Manage User queries
- Review subsequent User System requirements
- Review material change and provide recommendations
- Review the SSC risk register & RA iteration
- DCC CIO Assurance Validation
- Triage Assurance Validation

# WHY THE VALIDATION PROCESS?

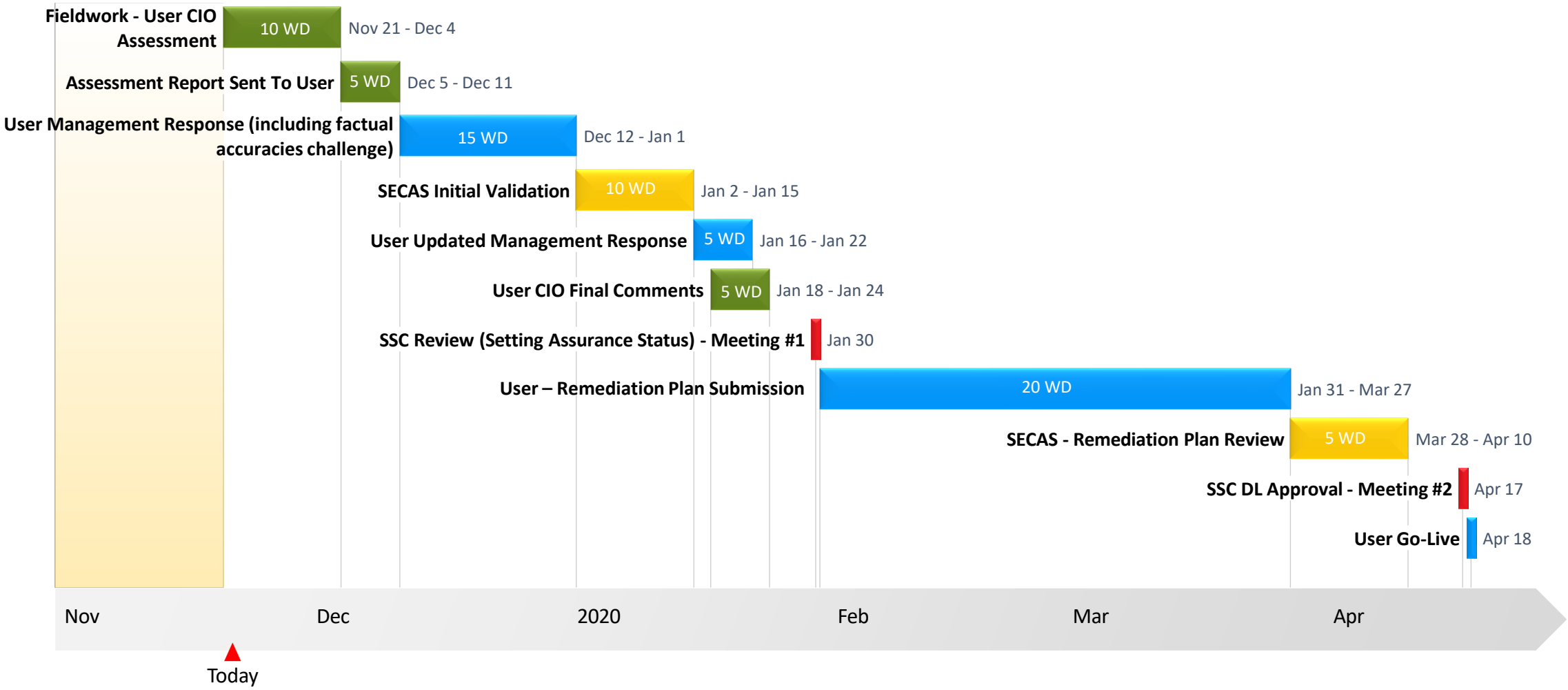
- The validation process is mandated by the SSC
- It allows the SSC to manage high volumes of work effectively while balancing other priorities beyond assurance
- The process helps identify issues early, enabling the Users to resolve them efficiently
- Save time for both the Users and the SSC
- The SECAS validation process is designed to mitigate any potential impacts that Smart Metering could have on Critical National Infrastructure (CNI) and the broader energy system

# FUSA & VUSA VALIDATION PROCESS

- SECAS will review the User Management Response (MR) to ensure that it:
  - Addresses the observations in the User CIO report
  - Is comprehensive and appropriate in relation to the materiality of the observations
  - Aligns with the mandatory SEC requirements

- Timeline:
  - The User must provide an updated Management Response within 5 WDs (if required)
  - The User CIO will have 5 WDs to add final comments – FUSA
  - SECAS will have 5 WDs to add final comments - VUSA

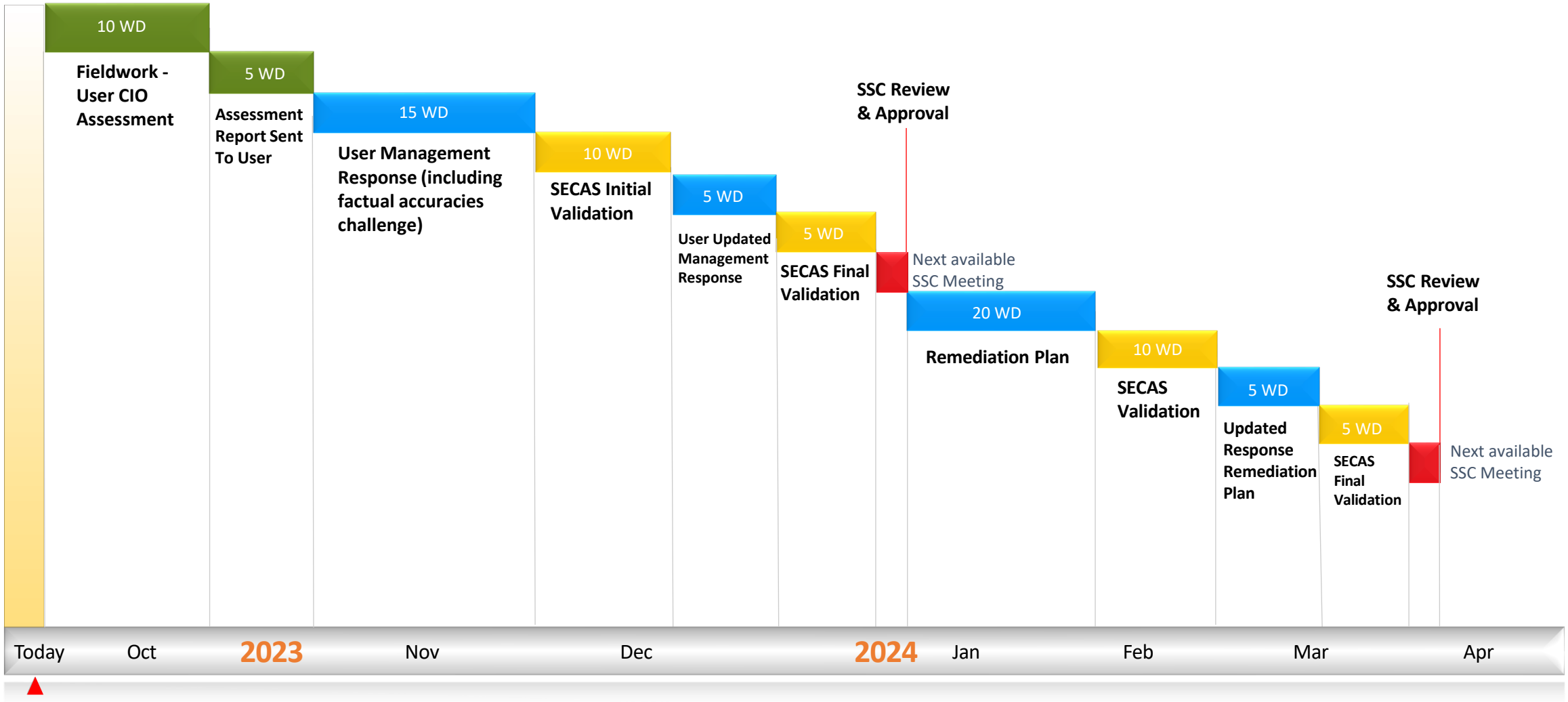
# FULL USER SECURITY ASSESSMENT - FUSA





49

# VERIFICATION USER SECURITY ASSESSMENT - VUSA



# SSC REVIEW – SETTING THE ASSURANCE STATUS

**Refer to G8.36**

SSC Review

- **Approved**
- **Approved, subject to the Party:**
  - ➢ Taking such steps as proposed in accordance with G8.26(b) or
  - ➢ both taking such steps and being subject to a Follow-up Security Assessment by such date as the Panel (SSC) may specify,
  - ➢ Taking such steps as proposed in accordance with G8.26(b)
  - ➢ Submitting a Director's Letter with detailed action plan showing that all actions were complete
- **Deferred**
  - ➢ Taking such steps as proposed in accordance with G8.26(b) and being subject to a follow-up assessment
  - ➢ Panel (SSC) determining satisfaction on evidence of a Follow-up Assessment
- **Rejected**
  - ➢ Having a second FUSA to address any issues not adequately addressed in that response as submitted to the SSC; and
  - ➢ Upon completion of second FUSA reconsider assurance status in accordance with G8.35

# MATERIAL CHANGE NOTIFICATION

- The SEC sections G3.9 (b) requires that after

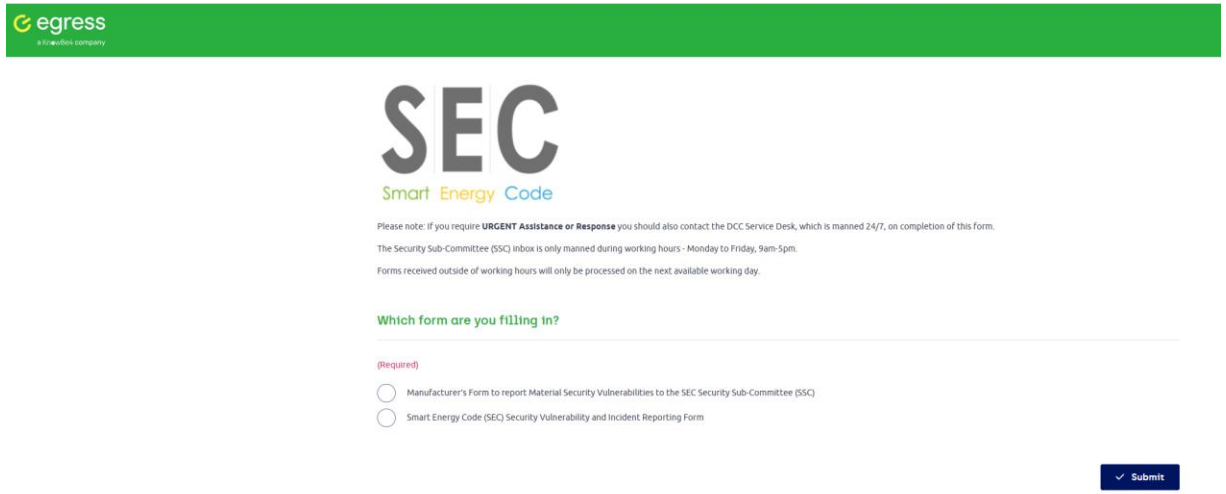
*"…any material vulnerability has been detected, a User shall ensure that it: promptly notifies the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed."*

The SSC will require the following to consider risks associated with the end-to-end smart metering system.

- A fully completed Material Change Notification Form
- Risk Assessment
- Detailed Roadmap
- Architecture diagram

# INCIDENT AND VULNERABILITIES MANAGEMENT

- The SEC places obligations on the DCC and DCC Users to notify the Security Sub-Committee (SSC) of any vulnerability or incident that occurs in, or causes a material adverse effect on, the security of hardware, software, firmware, or a Device. These obligations are set out in SEC Sections G2.11, G2.15, G2.30, G3.5, G3.9(a) and G3.18.
- Please submit the Security Vulnerability and Incident Reporting Form https://gemserv.egressforms.com/. The information you provide will be made available to the SSC and/or SMKI PMA via SECAS. We use Egress secure web forms for these notifications to ensure confidentiality.



# REMEDIATION PLAN AND DIRECTOR'S LETTER

- A Remediation Plan will be required for a User that has not fully addressed all observations raised by the User CIO
- During the Remediation Plan validation, the Security Expert will ensure that mitigating actions described in the previous validation stages have been implemented as described, with the supporting evidence
- Ensure adherence to commitments made to the SSC during the FUSA/VUSA stage without deviation
- The Remediation Plan workbook should provide a detailed explanation of the action taken, steps completed and any updated documentary evidence
- Review the FUSA - SSC outcome before completing the SECAS validation workbook
- The Director's Letter should confirm that all steps outlined in the User management response have been completed and signed off

# KEY OBLIGATIONS - COMMON ISSUES

# G3.9 REMEDIATION OF VULNERABILITIES

- Conducted all required vulnerability assessment.
- Ensure severity ratings (High, Medium, Low) are aligned with CVSS scoring levels as defined in the policy and remediated within the specified timeframe.
- Categorise vulnerabilities based on their materiality and align them with the categorisation framework of your CHECK/CREST tester (G3.7).
- Implement effective processes to mitigate the impact of vulnerability that cannot be rectified.
- Develop a comprehensive remediation plan and validate the effectiveness of controls.

# G4.2/G4.3 SECURITY SCREENING OF INDIVIDUALS

- Revocation of system access for individuals without security clearance
- BS7858:2019 compliance including Global Watchlist checks and provide screening training for personnel involved in conducting the screening process. Update relevant policies accordingly.
- Verify that third party screening provider perform assurance checks in accordance with the BS7858:2019 standard
- Provide documented evidence of compliance with BS7858:2019 requirements
- Establish contract with third parties to ensure alignment with the User's security requirements

# G5.15 INFORMATION SECURITY RISK MANAGEMENT

- Assess all risks related to the User's smart metering system and address User CIO observations with evidence
- Select appropriate risk treatment options and define necessary controls with justifications
- Obtain risk owners’ approval of the treatment plan and track risks with regular reviews
- Include security clauses and audit rights in third-party contracts, and document risk tolerance levels
- Train employees on risk assessment and establish governance mechanisms to validate risk management
- Ensure consistent and comparable results from repeated risk assessments.

# G6.3/G6.4/G6.10 - ANOMALY DETECTION THRESHOLDS

- Maintain a documented process for notifying the DCC of Anomaly Detection Thresholds including roles and responsibilities.
- Provide evidence of any necessary ADT adjustments, especially when forecasted values significantly decrease.
- Show any deviations between Security Sub-Committee advice and the implemented ADTs.
- Maintain a comprehensive list of commands and their corresponding ATDs, ensuring these are set at an appropriate level to minimize the risk of compromise.
- Provide evidence that ATDs reviews have been conducted in accordance with the established due process and been adjusted with justifications and approvals.
- Provide evidence confirming that the DCC has been notified of updated ADTs after modification.
- Provide evidence to demonstrate that the User Shared Resource Provider followed TADP steps in response to an ADT breach.

# VALIDATION TOP TIPS

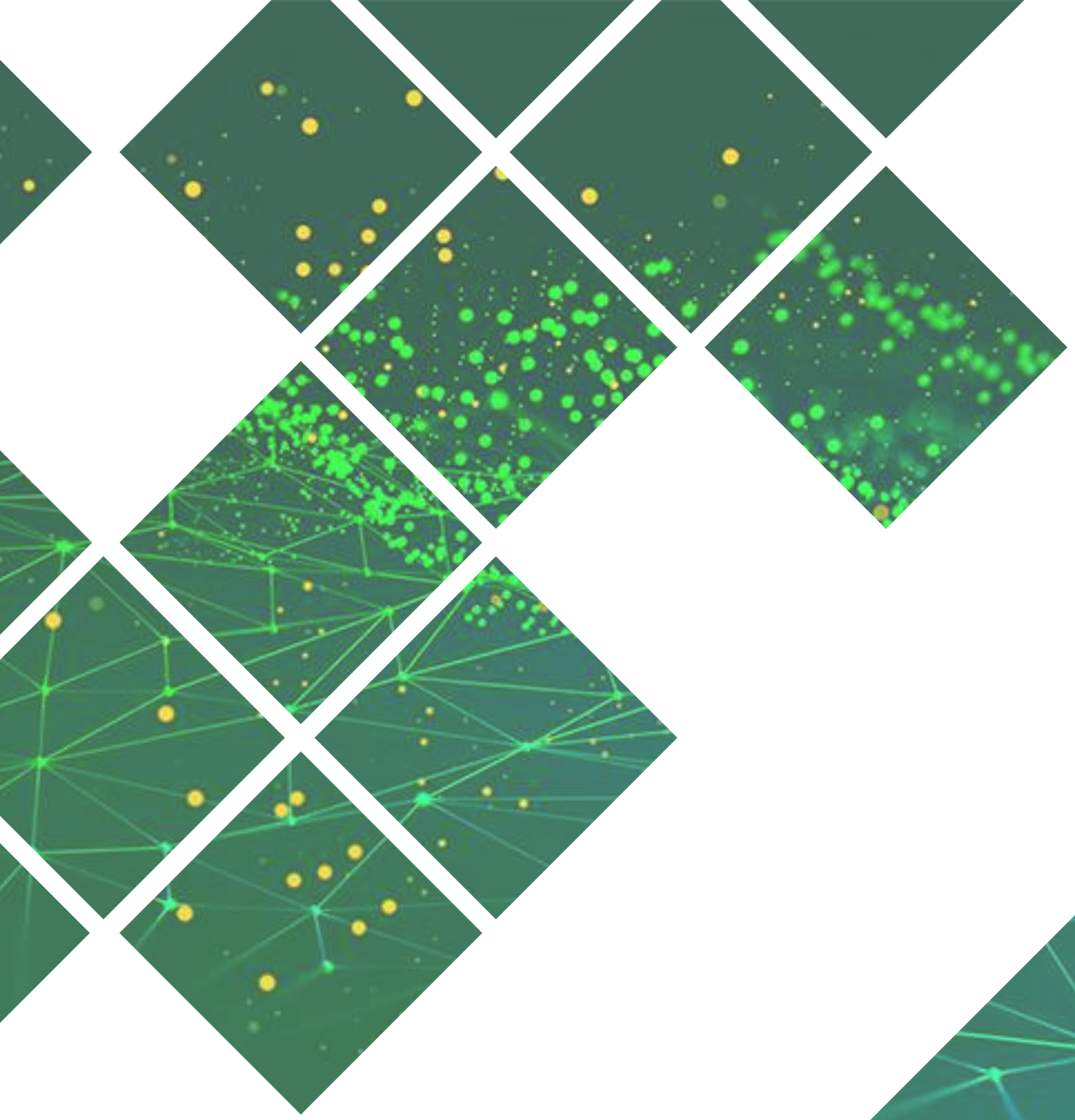
- Responsibility for compliance rests with the User, and this must be clearly demonstrated in the management response
- Don’t assume the SECAS Security Experts are aware of evidence and discussions between the User and the User CIO, ensure all relevant information is explicitly shared
- Avoid editing the SECAS comments within Egress
- The User’s Management Response should be comprehensive and detailed, addressing all aspects of the User CIO’s observations.
- Ensure that all required fields in the Validation workbook are completed
- Adhere to submission timelines to avoid unnecessary delays
- For obligations that are not fully understood, contact SECAS for guidance. If necessary, SECAS can facilitate a call with the User CIO to provide further clarification

# OTHER TIPS

- Provide detailed Management Responses and relevant evidence to address observations and SECAS' comments
- A well-maintained ISMS is essential for managing Section G obligations effectively
- Ensure proper document management and maintain high quality control throughout the process
- Actively challenge any factual inaccuracies during the first management response stage
- Strictly adhere to the required timelines for the submission of Management Responses
- 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

# GUIDANCE

- User Guidance - Threshold Anomaly Detection Procedure – DCC
- Security Controls Framework (SCF) Parts 1 & 2
- Agreed Interpretation (AI)
- Standards and Best Practice Review Document



# THANK YOU FOR LISTENING

## ANY QUESTIONS?

SEC
Smart Energy Code

# CONTACT DETAILS AND USEFUL LINKS

- Security Assessment Process
- Security Obligations
- Security Controls Framework
- AMS Booking System (Security)
- Email - SSC@gemserv.com

slido

Please download and install the Slido app on all computers you use

# Did you achieve your goals for this session?

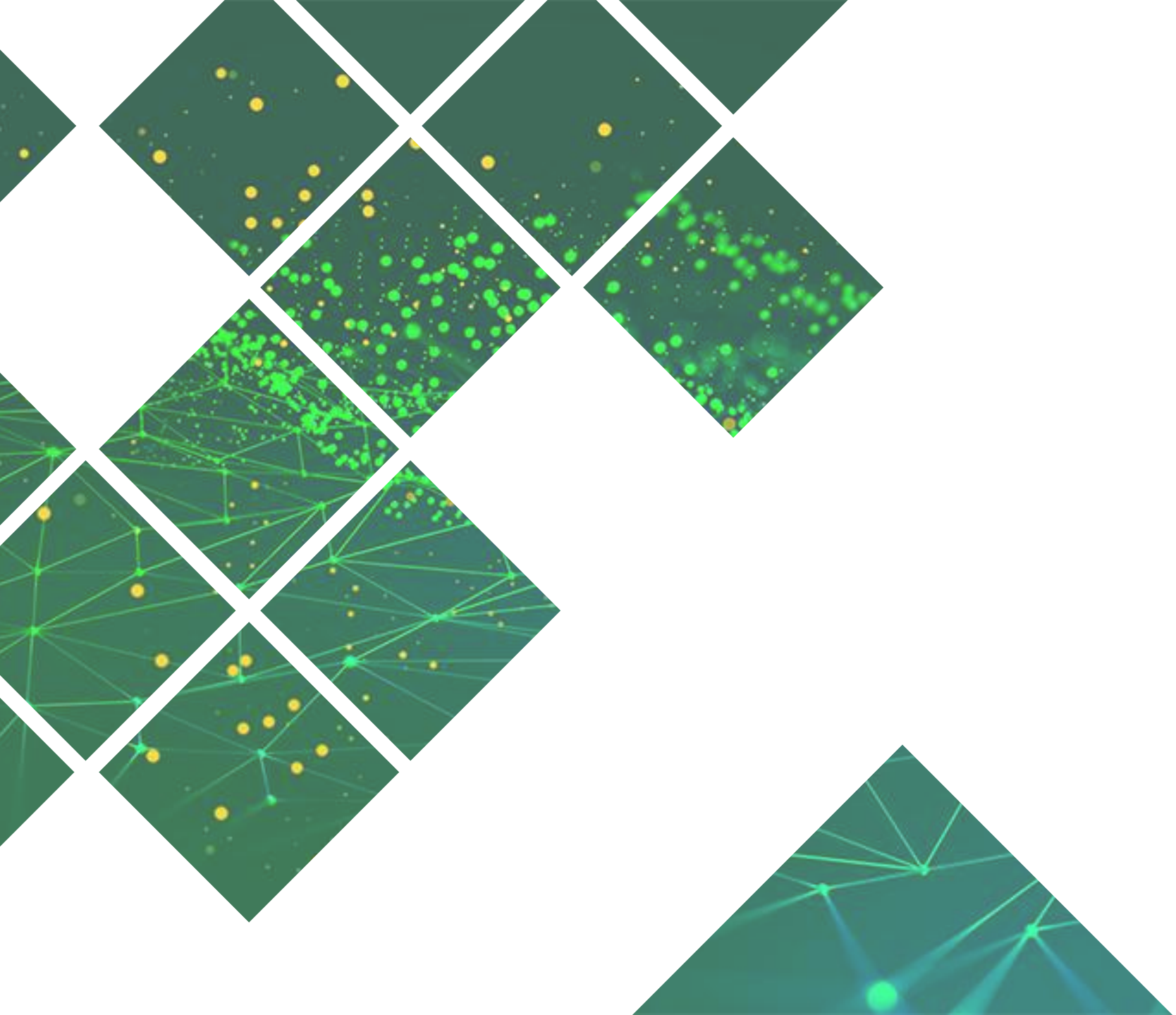
ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

# What topics would you like to see in future SECAS-led Webinars?

ⓘ Start presenting to display the poll results on this slide.



# THANK YOU

SEC
Smart Energy Code