THE YEAR 2 USER CIO SECURITY ASSESSMENTS

BUILDING ON SOLID FOUNDATIONS

Preparing for the initial assessments required as part of the Smart Energy Code (SEC) was a significant undertaking for many organisations. With the next stage in the process looming, it is important to ensure the focus is maintained.

BACKGROUND

Assessments are a key part of the process under the SEC to enable businesses to connect to smart metering systems as Users of services provided by the Data Communications Company (DCC).

The initial Full User Security Assessment (FUSA) carried out in the first year was aimed at ensuring organisations met the system, organisational and information security obligations set out under the Security Controls Framework.

The next 'Year 2' stage will see Verification User Security Assessments (VUSAs) carried out by the User Competent Independent Organisation (CIO) to review evidence and validate this based on the network architecture designs provided to the auditor in Year 1. It is also an opportunity to understand any material increase in security risk since the FUSA in addition to demonstrating a risk assessment and mitigating controls for SMETS 1 meters as part of enrollment and adoption.

Gemserv

WHAT IS REQUIRED?

Organisations should view the initial Year 1 assessment as just one of the milestones on the journey of being involved in the Smart Metering Programme within the UK and to build on the foundations it established.

They now need to be able to demonstrate that they are continuing the good practices implemented ahead of that initial assessment and to show they are successfully moving from the design phase of the solution to live business processes where compliance can be clearly evidenced through policies and procedures.

Management teams have an important role to play in continuing to support and embed best practices and ensure staff are engaged in adhering to policies and procedures. That will also help ensure organisations have a well-presented suite of documents in place which would make a good impression to auditors of an organisation's approach to the process.

SPECIFIC VUSA USER CIO TASKS

The User CIO for the Year 2 audit will expect to see compliance against SEC sections G3-G6 which address implementation compared with the design phase which was the focus for the Year 1 audits.

The VUSA audits will primarily focus on seeing evidence of operational controls which will require DCC Users to detail:

- 'Material' changes to network architecture (and if so changes to initial Risk Management - ISO27005)
- Any incidents arising and how they were managed
- Role alignment to ensure accountability of tasks
- HR screening for employees where applicable in Smart Metering roles
- Proof of contracts with 3rd parties if new agreements established since initial audit
- Evidence of regular security meetings to ensure continual review management
- Evidence that ISMS document suite has been maintained, version controlled and approved through change management channels
- Evidence of setting of anomaly detection with user system provider
- Evidence of SMETS 1 risk assessment and controls are in place

It is important to note ISMS maintenance is the sole responsibility of the DCC User. However, some documents may require input and ownership from Shared Resource Providers or other 3rd party solution providers.

In such cases, the expectation is that 3rd party providers are to maintain documents on behalf of the DCC User. Ultimately, the DCC User needs to be assured that the 3rd party documentation meets SEC obligations and that this is accepted by the DCC User for the life-cycle of the 3rd party relationship.

HOW GEMSERV CAN HELP

Gemserv has a dedicated expert team that has successfully supported over 30 energy suppliers in becoming DCC Users. Preparing for CIO audits and the experience gained means we are well-placed to help you ensure you are fully prepared as quickly and cost-effectively as possible.

We have extensive experience of the SEC requirements including the Security Controls and Privacy Controls Framework that are crucial to the success of the programme.

To help you achieve the next milestone in the Year 2 VUSA, Gemserv offers a bespoke package to ensure you are aligned to SEC obligations and meet the criteria set out for the security standards. We can also assist in helping organisations with their preparations for their Year 3 self-assessments.

CONTACT US

To understand more about how Gemserv can help you, please contact one of our team on:

E: bd@gemserv.com
T: +44 (0)20 7090 1091
W: www.gemserv.com
@gemservinfosec

London Office

8 Fenchurch Place
London
EC3M 4AJ

Company Reg. No: 4419878