

SEC USER SECURITY ASSESSMENTS - SUSTAINING THE INITIATIVE

YEAR 2 USER SECURITY ASSESSMENTS AND BEYOND

As you are aware, under the SEC, you will be subject to annual ongoing User Security Assessments and it is important that the initiative gained at your first User Security Assessment is sustained and the hard work that has gone in to your initial Full User Security Assessment (FUSA) does not go to waste.

The Year 2 User Security Assessment will move away from emphasis on the design phase of your solution to live implementation. In this phase, you are live and there are real SMETS2 meters on the wall. The User CIO appointed to conduct the User Security Assessments will now be looking for demonstrable evidence to support the commitments set out in your security policies and ensure business processes are being followed.

Preparing for the year one initial FUSA may have felt like hard work, but it is fair to say that the hard work begins now as you prepare for your next User Security Assessment.

After the initial FUSA, you may feel that nothing much remains to be achieved. In reality, you should be looking at the initial FUSA as a milestone and not a destination. It is important to avoid the degeneration of the initiative from the first year, which could lead to a less-than-successful year two User Security Assessment.

WHAT NEEDS TO BE DONE?

Year two User Security Assessment success can only be achieved through continued buy-in from your management and staff, together with effective internal adherence and management reviews to ensure everyone is consistently and habitually adhering to the policies and procedures.

Oftentimes, when an organisation returns to normality, they lose momentum as the organisation starts striking a balance between business operations, fire-fighting and security. Sustaining the initiative greatly depends on the organisation's capability to retain the buy-in of its stakeholders and to implement and adhere to its policies and procedures. Doing so makes for a smoother and more seamless year two User Security Assessment.

YEAR 2 USER SECURITY ASSESSMENT APPROACH

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

The User CIO will be looking to assess you against all applicable SEC Sections G3-G6 obligations, looking for the DCC User to clearly evidence and demonstrate the following:

- 3rd Party relationships have been assured;
- Where using a Shared Resource Provider, all joint activities have been conducted;
- G3-G6 obligations have been implemented and are being followed;
- New risks have been captured and existing risks have been reviewed;
- Regular security governance meetings have been held;
- Assessment of the initial controls has been conducted to see whether they are effective and amended if not;
- On-going Anomaly Detection Threshold management
- On-going Supply Sensitive Check management;
- Whether any security incidents been captured and if so, how were they dealt with;
- Documentation of any material changes;
- Whether there have been any Material Changes; and
- Whether all SSC reporting obligations have been fulfilled.

WHO ARE ADEPTICA?

Adeptica are very well placed to help your organisation through its year 2 User Security Assessment successfully.

Adeptica have, so far, successfully helped over 50 organisations through their initial Full User Security Assessments and their year 2 User Security Assessments.

Adeptica are the trusted 'go-to' company for all cyber security matters related to the Smart Energy Code and the wider energy sector.

Adeptica work very closely with the leading Shared Resource Providers and have intimate knowledge of their systems, SEC security document set and their business processes, significantly aiding the User Security Assessment process for you.

Adeptica were heavily involved in shaping the SEC G3-G6 security requirements and defining the security standards for GB Smart Metering, bringing a wealth of knowledge and experience to the client.

HOW CAN ADEPTICA HELP?

Adeptica can help you through your User Security Assessments and sustain the initiative by providing a tailored bespoke service to your organisation aimed specifically at ensuring you have all in place to successfully pass your User Security Assessments.

Alternatively, Adeptica can provide a SEC Managed Cyber Security Service, acting as your in-house security 'experts' for all matters related to SEC G3-G6 and ensuring your on-going commitments are met in order to best prepare you for your next User Security Assessment.

For further details of Adeptica's SEC Managed Cyber Security Service and other bespoke services please contact us on:

Email: client.services@adeptica.co.uk

Web: <https://adeptica.co.uk>

**Note: SMETS1 security obligations
come into force soon!**