# Appendix F: User Security Self-Assessment Return

## Introduction

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

The SSC has approved a User Security Self-Assessment Return that will enable the User to provide the relevant information for the User CIO to determine compliance with the SEC security obligations.

## Questions

All the following questions should be completed in relation to the changes which have been made since the date on which the previous User Security Assessment report was released, up to the date at which this Self-Assessment Return is completed.

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| **Reference** | **Question** | | **User Response** |
| 1. **Introductory Information**   *Please answer in relation to changes which have taken place since your last User Security Assessment* | | | |
| **A.1** | [Energy Suppliers and Network Operators only]How has the number of SMETS 2 Smart Metering Systems enrolled with the DCC which you are responsible for changed? | |  |
|  | *E.g. The number of meters we are responsible for has increased from <insert number> to <insert number>.* | |
| **A.2** | Have there been any changes to your contractual or operational arrangements with any Shared Resources upon which you are reliant for all or part of your User System? | |  |
|  | *E.g. The previous arrangement with Shared Resource A was terminated and replaced with a new arrangement with Shared Resource B, effective from DD/MM/YYYY.* | |
| **A.3** | Aside from Shared Resources, 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 User System (whether these are suppliers of hardware, software and/or resources)? | |  |
|  | *E.g. The new arrangement with XYZ Vendor for the provision of Hardware Security Modules within our User System replaced the previous arrangement with ABC Vendor for provision of XXX services effective from DD/MM/YYYY.*  *E.g. The former arrangement with XYZ Vendor for our network monitoring was terminated on DD/MM/YYYY and this service is now delivered in-house.* | |
| **A.4** | 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 new CRM system was implemented on DD/MM/YYYY. The new contract is in place with XYZ CRM Vendor. It replaced previous arrangement with ABC CRM Vendor for provision of CRM system support services.* | |  |
| 1. **B. How has the scope or method of operation of your User System 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* | | | |
| **B.1** | Have there been any changes to the functionality that you offer to customers with regards to your Smart Metering solution and/or the Service Request Variants you communicate to DCC? If so, please explain the impact of these changes. | |  |
|  | *E.g. During the last User Security Assessment we had not yet introduced pre-payment services for our customers. The new pre-payment service was introduced to customers on DD/MM/YYYY.*  *E.g. During the last User Security Assessment we did not make use of the ‘Remote Disconnect’ Service Request Variant and had set our Anomaly Detection Threshold to ‘zero’ to reflect this. We began to make use of this Service Request Variant on DD/MM/YYYY and are now sending an average of x per month.* | |
| **B.2** | Have there been any material changes to your User System technical design? | |  |
|  | *E.g. The User System was updated to a new version on DD/MM/YYYY to support the ‘pre-payment’ functionality.* | |
| **B.3** | Have there been any changes to the in-scope ‘backend systems’, as defined within SEC G5.14 part (c)? | |  |
|  | *E.g. New XYZ CRM system was implemented on DD/MM/YYYY which replaced ABC CRM system.* | |
| **B.4** | 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 User System and in-scope ‘backend systems’)? | |  |
|  | *E.g. Updated the network design and there are new communication links in place between our backend systems and our Shared Resource. Previously we used XYZ method, but we have replaced this with ABC method.* | |
| 1. **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? | |  |
|  | *E.g. We have increased the potential impact of compromise to our User System 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 Smart Metering Information Exchange (SMIE).* | |
| **C.5** | Do you consider the threat landscape has changed, and if so, how are the changes reflected in your risk assessment?  at all? | |  |
|  | *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.*  *With recent rise of the hacktivist groups who are specifically targeting Energy Companies to disrupt services to demand lower energy bills and better quotas, we reassessed and increased the Capability and Motivation rating for this threat actor.* | |  |
|  | Have there been any changes to your contractual or operational arrangements with third party suppliers that provide Risk Management consultation services? | |  |
|  |  | |
|  |  | |  |
|  |  | |
| **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. Definition of Material Change has been updated to include material changes to backend CRM system. Financial and reputational damage has now been added to the definition of a Major Security Incident and has been aligned with the Shared Resource.* | |
| 1. **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 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 CRM system and communication links, the respective controls of XXX and YYY were phased out.* | |

Completed by:

| Name | Job Title | Date |
| --- | --- | --- |
|  |  |  |

The User is required to supply associated evidence, in line with that specified by the SCF for SEC obligation G5.14, to support the responses to the above questions.