Scottish & Southern Electricity Networks

BN-NET-GOV-501

SHE Transmission

Cyber Security by Design for Project Managers

	Name	Title
Author	Alex Stuart	Digital Programme Lead
Checked by	David Allan	Head of Policy and Standards
Approved by	David McKay	Director of Operations and Asset Management

Contents

1 Introduction

1.1 Cyber Security is the second Principal risk at SSE Group level – "The risk that key infrastructure, networks or core systems are compromised or are otherwise rendered unavailable".

The transition to digitalised networks introduces technology and greater complexity into an area that was previously well understood. From design to implementation and operation there is a requirement to ensure security in projects and programmes have been considered formally by the SSE Security team in artefacts whether they are documents or system configurations.

We need to design security into the network and information systems that support the delivery of essential services and minimise the risk of cyber-attack. This is particularly the case for Operational Technology supporting the SHE Transmission network and the potential consequences were highlighted in the 2015 and 2017 Ukraine electricity blackouts as a result of cyber-attack.

The purpose of this Briefing Note is to highlight the processes to be followed as part of project governance, development, design and execution to ensure that the security of network and information services is not adversely impacted by changes as a result of project execution. Whilst this Briefing Note specifically references the Large Capital Projects Governance Framework Manual these will processes apply to all SHE Transmission projects.

2 References

The documents detailed in Table 2.1 - SSE Documents and Table 2.2 –External Documents below should be used/read in conjunction with this document.

Table 2.1 - SSE Documents

Reference	Title
MA-COR-LCP-001 R 8.0	Large Capital Projects Governance Framework Manual
WI-COR-LCP-001	Business Opportunity Report
WI-ENG-LCP-701	Design Management Plan
WI-PMO-LCP-201	Project Development Plan
FO-COR-IS-102	Supplier Information Security Risk Assessment Form
RS-COR-IS-005	Operational Technology Security and Risk Standard
RS-COR-IS-006	Principles and High-Level Architectures for Operational Technology and Corporate Data Networks Connectivity
RS-COR-IS-007	Operational Technology Security Management Governance Roles and Responsibilities

Table 2.2 –External Documents

Reference	Title
NIST 800-82 R2	Guide to Industrial Control Systems (ICS) Security

3 Process to Assure Cyber Security by Design

3.1 **Gate 0** - Prior to the Opportunity Assessment stage of ANY project (this is Gate 0 for projects governed under the Large Capital Projects Governance Framework Manual) a high-level assessment of cyber security including procured solutions must be made and captured within a Business Opportunity Report (WI-COR-LCP-001) deliverable for assessment at Gate 0. Also, engagement with the Transmission Cyber Risk and Information Security Team (CRIS) is essential for a simplified project triage before progressing beyond Gate 0. **See section 4 below for guidance on this.**

3.2 **Gate 1 -** Prior to the Development stage of ANY project (this is Gate 1 for projects governed under the Large Capital Projects Governance Framework Manual) the Project shall establish communication with Group Security and Cyber Risk and Information Security (CRIS) teams to determine the key aspects of cyber security including procured solutions to inform design. Security requirements shall be documented in the Design Management Plan (WI-ENG-LCP-701) and, as required referenced in the Project Development Plan (WI-PMO-LCP-201).

3.3 **Gate 2** - In consultation with the CRIS team prior to the Refinement stage of ANY project (this is Gate 2 for projects governed under the Large Capital Projects Governance Framework Manual) the key aspects of cyber security shall be developed, agreed and documented in the Design Management Plan (WI-ENG-LCP-701).

3.4 **Gate 3** - In consultation with the CRIS team prior to the Execution stage of ANY project (this is Gate 3 for projects governed under the Large Capital Projects Governance Framework Manual) the key aspects and strategies of cyber security shall be determined and documented in the Design Management Plan (WI-ENG-LCP-701).

3.5 **Gate 4** - In consultation with the CRIS team prior to the Commissioning stage of ANY project (this is Gate 4 for projects governed under the Large Capital Projects Governance Framework Manual) the key aspects and strategies of cyber security shall have been delivered and documented in the Design Management Plan (WI-ENG-LCP-701).

3.6 **Gate 5** - The cyber security requirements of any project shall be met and form part of the deliverables for the Handover to Operations stage for ANY project. (this is Gate 5 for projects governed under the Large Capital Projects Governance Framework Manual)

4 Engagement With the CRIS Team

4.1 The project team shall engage with the CRIS team as outlined within Section 3.

4.2 The CRIS team can provide advice and guidance from the start of any project. Support can include production of a Security Plan including a cyber risk assessment and recommended

actions which can be incorporated into project deliverables, security support for project tenders and supplier selection and security input to project deliverables.

4.3 The CRIS Team should be engaged via Cyber Secure Project Assurance area within the IT Service Catalogue (ITSC). Inside the ITSC Portal simply search in the white search box for "Cyber Secure Project Assurance" and choose the very first option. The PT or LT number can be used in lieu of the IR number.

4.4 When annotating details about the project in ITSC identify whether it is 'Transmission Triage' or 'Transmission Security Assurance' being requested which will enable Transmission dedicated security assurance officers to be identified by the CRIS team.

4.5 The project triage is completed very quickly by the CRIS team and this assesses whether further CRIS engagement is required. The flow chart for this is shown below:

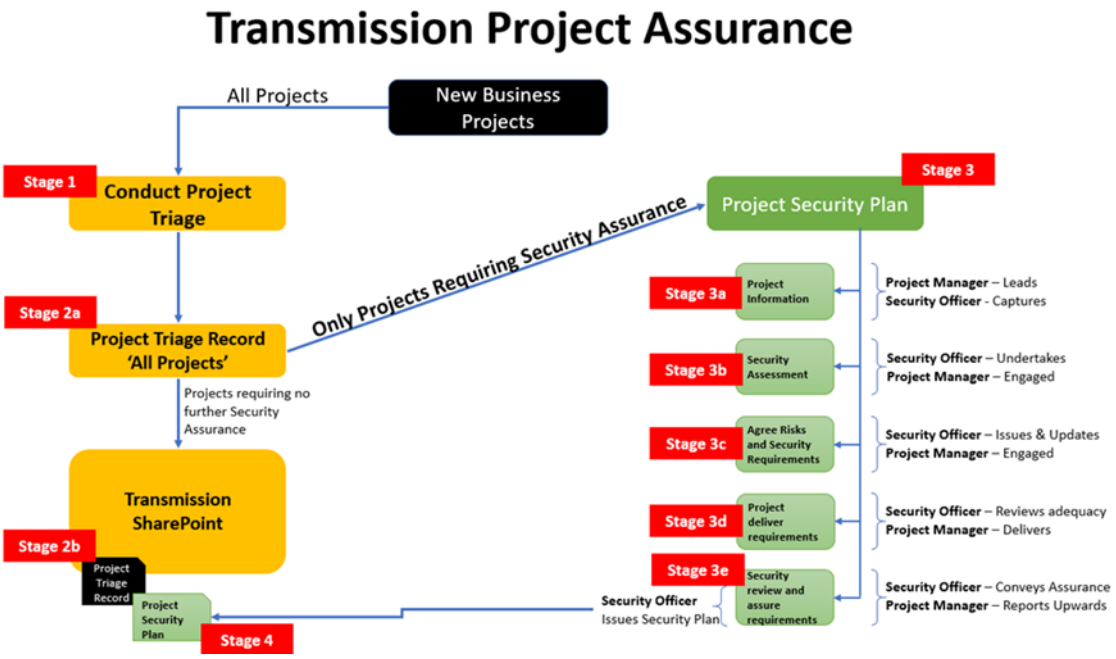


Figure 4.1 - Transmission Project Assurance Flow Chart

See **Appendix A** for more details on the CRIS Triage process

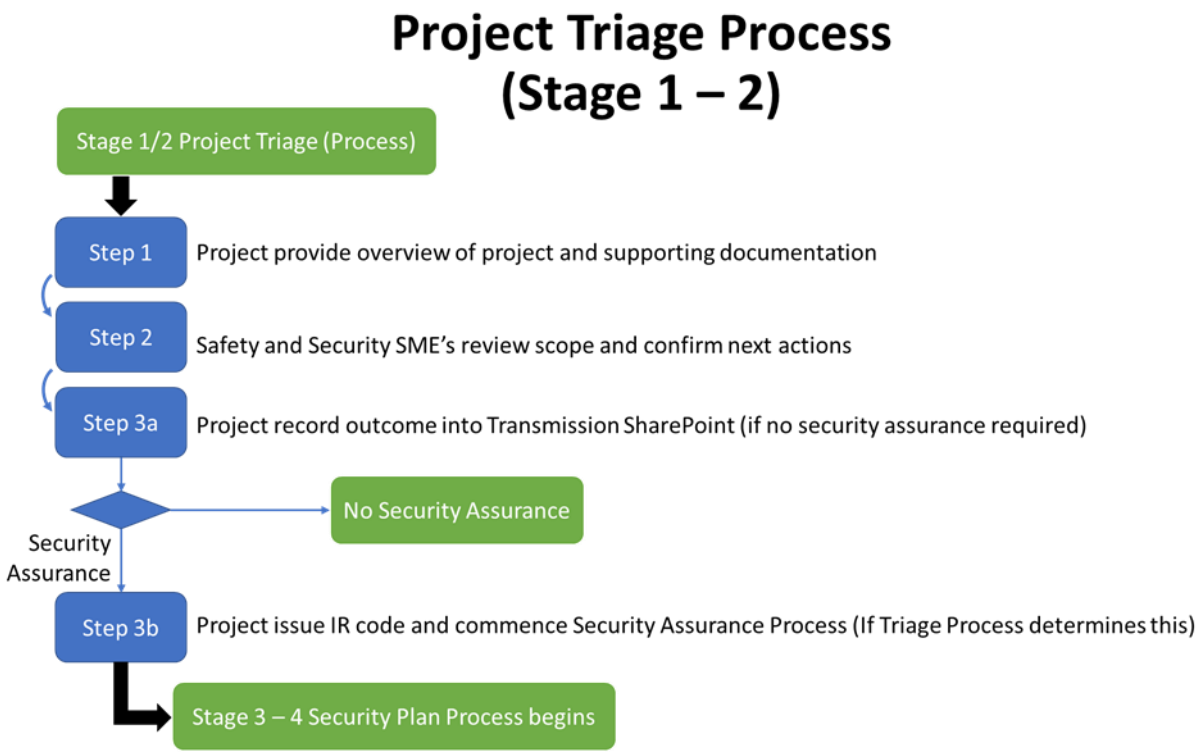
4.6 In the case of procurement assurance, the CRIS Team request a completed Supplier Information Security Risk Assessment Form (FO-COR-IS-102). At early project assessment or development stages the supplier may not yet be selected and therefore it has been agreed with the CRIS Team that Supplier Information Security Risk Assessment Form is not mandated when engaging at these project stages.

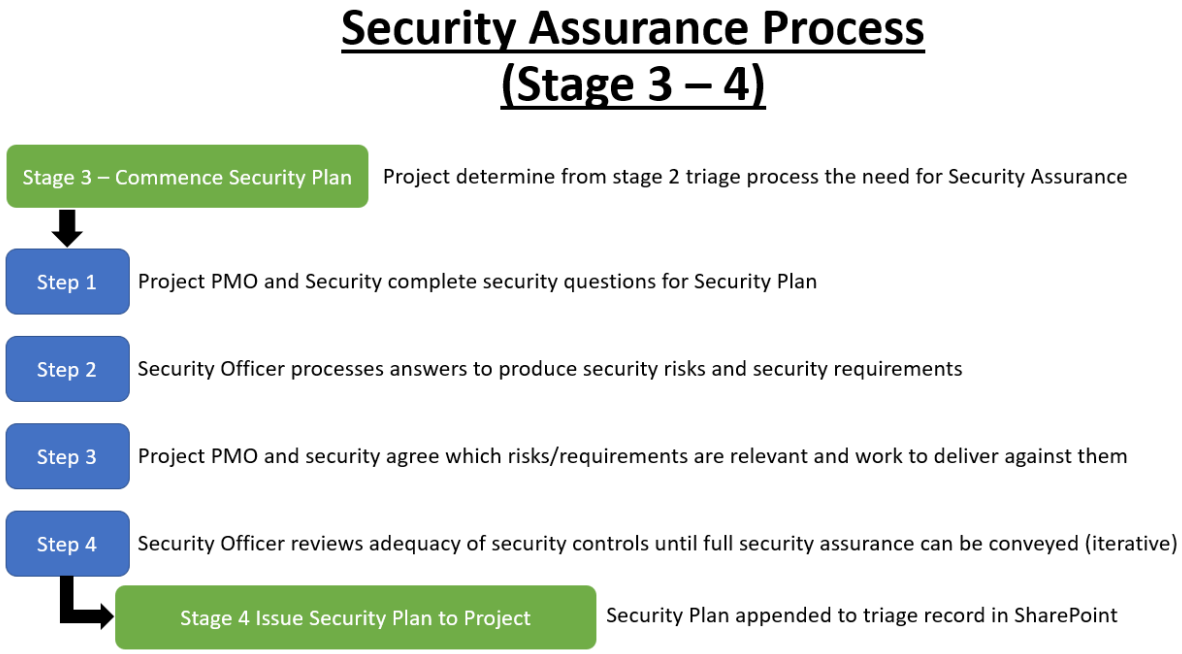
4.7 Further support on Cyber Security for Operational Technology is available from the Networks Operational Technology team and the SHE Transmission Digital and Technical Services teams.

5 Revision History

No	Overview of Amendments	Previous Document	Revision	Authorisation
01	New document created	n/a	1.00	David McKay
02				

Appendix A CRIS Triage Process





Appendix B Example Response Form from CRIS Triage Process

This is an example of the response that CRIS would give from the initial triage. It shows a clear action and the expected number of days that this process will take.

Project Scope *'Project Name' + Harmony Code*

Logical *– Network connectivity onward to supplier cloud service. Supplier cloud security management, data handling, etc...*

Physical *– A perimeter camera is being installed at the substation sending pictures back to off-site supplier security systems hosted in the cloud.*

Cyber Summary (Logical/Physical)

Function	Is Function Implemented	CRIS Security Decision
Identify	Yes	Small CRIS Security Plan
Protect	Yes	Medium CRIS Security Plan
Detect	Yes	Small CRIS Security Plan
Respond	Yes	Small CRIS Security Plan
Recover	Yes	Small CRIS Security Plan
Aggregate Decision		CRIS Security Plan and Resource

Summary statement:

Sensitive pictures potentially being transferred over unprotected lines which could be captured by an attacker. Suppliers cloud security to be reviewed. Possible GDPR issues if cameras film public activity.

Operational Safety Summary

The purpose of the camera is related to the secure and safe status of the sub-station which may require the Process Hazard Assessment to be updated and any new data collected included in a Data Privacy Screening assessment to confirm if a Data Protection Impact Assessment were required to be completed.

Project Summary Actions

Project Decision Reference*: 124/NET/2020*

Cyber Decision*:* CRIS Security Plan and Resource

Operational Safety Decision*: Review PHA and draft a DPS.*

Next Actions*: Engage CRIS Security Assurance Officer and submit a request on ITSC for a resource, requesting up to medium level of support, between 5 and 7 days.*