

# Interview Protocol/Guide

## 1 PRE-SCREEN

The following question set and associated notes are to be applied during the pre-screening phase.

- Do you work for an ICS operator?  
*Probe: What is your role title?*
- Do you work for a Cyber Security consultancy?  
*Probe: What is your role title?*
- Do you conduct Cyber-Security risk assessments?  
*Definition: The assessment of a threat, exploiting a vulnerability, and thereby causing harm to an asset, where there includes a component of computational resource.*

## 2 PREFACE

The following question set and associated notes are to be applied during the preface phase.

- Reiterate the purpose of the interviews based on the interview guide, and the expected timescale.
- Confirm the participant knows the full interview will be recorded, and that they will be told when the recording is due to begin, and when it is due to end.
- Turn ON the recording now.
- What do you understand the term ICS to include?  
*Definition: Any Operational Technology (OT) systems residing across the organisation (Manufacturing, DMZ, and Enterprise). We exclude Enterprise systems that do not interact with OT systems/data (e.g. an accountants workstation).*

## 3 RISK ASSESSMENT QUESTIONS

The following question set and associated notes are to be applied during the risk assessment questions phase.

- At a high level, what are the core steps you go through when conducting an assessment?  
*Probe: If steps seem to be missing, read back the steps to clarify this is all the interviewee does.*  
*Note: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment (ISO 31010).*  
*Note: Prepare for Assessment, Identify Threat Sources and Events, Identify Vulnerabilities and Predisposing Conditions, Determine Likelihood of Occurrence, Determine Magnitude of Impact, Determine Risk, Communicate Results, Maintain Assessment. (NIST 800-30).*  
*Note: Holistic Steps, Sub-Steps, Tools/Techniques Categories,*

*Individual Tools/Techniques, External Resources (Summarised Process).*

- What are your design/implementation influences in the described steps?  
*Probe: If some/all steps are bespoke - Please could you explain the justification for creating a bespoke methodology?*  
*Probe: If a step is missed, read back the steps to clarify all are covered.*  
*Note: Do not suggestion any standards and guidelines to avoid leading.*
- Which of the defined steps is the most important, and which proves the most challenging to accomplish and why?  
*Probe: Read back the individual steps to refresh the interviewees memory.*
- Please can you summarise the process you go through for (Read Back Step 1, then Step 2, etc.)?  
*Probe: If the response is not clear, ask for clarification.*  
*Probe: Enquire as to the use of any accompanying tools.*  
*Probe: If this step has been based on an external resource - How closely does this follow resource X?*  
*Note: Do not suggestion how you might do this, only ask for clarification or an example if unclear.*

## 4 CONCLUDE

The following question set and associated notes are to be applied during the interviews conclusion.

- What do you think of currently available standards and guidelines?  
*Probe: Why effective/not effective?*
- Confirm that the interview questions have been completed, and ask the interviewee if they would like to add anything in addition which may be relevant.
- If supporting documentation has been described and offered throughout the process, politely remind the interviewee to forward it on via E-Mail.
- Turn OFF the recording now.
- Thank the interviewee for their time and input into the project.
- Inform the interviewee that if at any time they think of any points deemed relevant to the discussed topic area, that I would greatly appreciate them being sent via E-Mail.
- Reiterate the options for withdrawal as described in the participant information sheet.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

Conference'17, July 2017, Washington, DC, USA

© 2017 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnnn.nnnnnnn>