Assurance offers operators an opportunity to assesses the performance and effectiveness of security controls, demonstrating systems are well-protected and consistent with organisational risk posture.​

On reviewing what is available in terms of Assurance Service Providers or Shared Assurance, the type of services offered and how well they address OT systems. It was found that services are heavily focussed on IT and financial assurance (unless bespoke assurance reviews are undertaken by OT cyber specialists).​ There is currently very limited third-party assurance provision that directly addresses OT cyber risks.

How do we ascertain assurance that specifically relates to an OT environment?​ The SOC2 Trusted Services Criteria (TSC) is a mature approach coming from an IT environment. We have explored making this relevant to OT.

SOC2 includes 5 categories covering: Security​, Availability​, Processing integrity​, Confidentiality​, Privacy​. The only criteria that is required to be in a SOC2 examination is the Security criteria, which is also known as the common criteria.​ All other categories are known as ‘Additional Criteria’ and are included as needed based on the scope of review.​ Across the Common Criteria and Additional Criteria, there are 61 principles and 302 Points of Focus.​

**Re-prioritisation of SOC2 Trusted Services Criteria (TSC) for OT**

We have undertaken a review of each of the 302 Points of Focus to understand which are relevant to an OT specific system. We have reprioritised the criteria based on this, for example the Additional Criteria relating to Availability has been prioritised above Privacy.​

**Mapping SOC2 TSC Points of Focus to NCSC Cyber Assessment Framework (CAF)**

To improve alignment to other sector requirements, we have mapped the 302 Points of Focus to the 39 CAF Contributing Outcomes, allowing for organisations that utilise the CAF to easily select the Points of Focus relevant to their OT systems.

**Mapping to IET Code of Practice: Cyber Security and Safety ​**

The IET Code of Practice Annex D – Principles and Indicators of Good Practice - have also been included in the mapping as a value add.​

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2017 Trust Services Criteria (TSC) | | | Criteria | Cyber Assessment Framework (CAF) | | IET Code of Practice Annex D | | |
| TSC  Ref# | Criteria | Points of Focus | Contributing Outcome | Outcome Definition | Principles | The Practice | Indicators of Good Practice |
| The 5 categories of the TSC were reviewed to ascertain inclusion for OT. The order of the TSC are re-prioritised to make Availability a higher priority. | | | The Points of Focus​ are revisited for an OT context as  **Common**(mandatory) or **Additional**. | The 302 Points of Focus are mapped to the 39 CAF Contributing Outcomes,  to enable SOC2 compliance to evidence support for CAF compliance.​ | | The 302 Points of Focus are mapped to the IET Code of Practice Annex D – Principles and Indicators of Good Practice. | | |

Many large organisations have resources to carry out assurance activities or can contract third parties to assist them​. SME organisations may have fewer resources or know-how to engage third parties with their supply chain assurance activities​.

We therefore developed guidance for SMEs on:​

* Understanding why assurance matters and how third-party assurance providers can help them​.
* Advising on steps to select an assurance provider, and outline the importance of understanding the scope, preparations required and outcomes.
* Factors affecting the quality of the assurance engagement​.
* Understanding how to use the TSC to CAF Mapping (e.g., to identify key areas, systems or services for assessment, to define the scope of assurance, or to use as a self-assessment tool for suppliers to complete)​.

|  |
| --- |
| **NCSC ICS Community of Interest Supply Chain Expert Group (SCEG)​**  ​  The SCEG is a volunteer initiative to progress multiple-sector wide approaches to the challenge of overseeing, managing and influencing the cyber security of supply chains to critical infrastructure services.  Co-Led by Paul Dorey (Royal Holloway) and Tania Wallis (University of Glasgow) the group has membership of experienced experts from different sectors and parts of the supply chain.​  **Validating OT security through a trusted third party**  Principal Authors: Lydia Walker & Clare McBrearty  Reviewers:  SCEG Members  **User Feedback is welcomed**  This is a beta release requesting feedback and improvements,  please provide comments to [https://forms.gle/xoJjkJpFKYBaR48YA](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fforms.gle%2FxoJjkJpFKYBaR48YA&data=05%7C01%7CTania.Wallis%40glasgow.ac.uk%7Ca8dc0f0cb3eb48dc028008dbcf3175c8%7C6e725c29763a4f5081f22e254f0133c8%7C1%7C0%7C638331583573131696%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=rbN5PPc9mV%2FLcy2pX9mNhHM9cdlfMCmigpMylZoPSPY%3D&reserved=0) |