Licensed copy: National Library of Scotland , National Library of Scotland, Version correct as of 16/11/2020

4.6.14 ZCR 5.13: Document and communicate results

4.6.14.1 Requirement

The results of the detailed cyber risk assessment shall be documented, reported and made available to the appropriate stakeholders in the organization. Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation shall include the date each session was conducted as well as the names and titles of the participants. Documentation that was instrumental in performing the cyber risk assessment (such as, system architecture diagrams, PHAs, vulnerability assessments, gap assessments and sources of threat information) shall be recorded and archived along with the cyber risk assessment.

4.6.14.2 Rationale and supplemental guidance

Cyber security risk assessments should be documented and made available to the appropriate personnel in the organization. Cyber security risk assessments are living documents that may be used for multiple purposes including testing, auditing and future risk assessments. However, it is also important to properly protect this information as it often contains sensitive details about the systems, known vulnerabilities and existing safeguards.

4.7 ZCR 6: Document cyber security requirements, assumptions and constraints

4.7.1 Overview

Subclauses 4.7.2 through 4.7.10 describe the requirements for documenting cyber security requirements, assumptions and constraints within the SUC as needed to achieve the SL-T and provides rationale and supplemental guidance for each requirement.

4.7.2 ZCR 6.1: Cyber security requirements specification

4.7.2.1 Requirement

A cyber security requirements specification (CRS) shall be created to document mandatory security countermeasures of the SUC based on the outcome of the detailed risk assessment as well as general security requirements based upon company or site-specific policies, standards and relevant regulations.

At a minimum, the CRS shall include the following:

- ZCR 6.2: SUC description (see 4.7.3);
- ZCR 6.3: Zone and conduit drawings (see 4.7.4);
- ZCR 6.4: Zone and conduit characteristics (see 4.7.5);
- ZCR 6.5: Operating environment assumptions (see 4.7.6);
- ZCR 6.6: Threat environment(see 4.7.7);
- ZCR 6.7: Organizational security policies (see 4.7.8);
- ZCR 6.8: Tolerable risk (see 4.7.9);
- ZCR 6.9: Regulatory requirements (see 4.7.10).

4.7.2.2 Rationale and supplemental guidance

Cyber security requirements should be documented in order to ensure the requirements are clearly communicated to all stakeholders and are properly implemented. The CRS does not need to be a single document. Many organizations create a cyber security requirements section in other IACS documents.

NOTE ISA-TR84.00.09 provides additional guidance on the recommended elements in a CRS.