4.7.9.2   Rationale and supplemental guidance

It is important that stakeholders are aware of the organization's established tolerable risk level in order to ensure that the SUC risk level is in alignment.

4.7.10   ZCR 6.9: Regulatory requirements

4.7.10.1   Requirement

Any relevant cyber security regulatory requirements that apply to the SUC shall be included in the CRS.

4.7.10.2   Rationale and supplemental guidance

This is important to ensure regulatory compliance.

4.8   ZCR 7: Asset owner approval

4.8.1   Overview

Subclause 4.8.2 includes one ZCR to attain asset owner approval.

4.8.2   ZCR 7.1: Attain asset owner approval

4.8.2.1   Requirement

Asset owner management who are accountable for the safety, integrity and reliability of the process controlled by the SUC shall review and approve the results of the risk assessment.

4.8.2.2   Rationale and supplemental guidance

Risk assessments are often facilitated by third-parties with participation by various subject matter experts who have intimate knowledge of the operation of the industrial process and the functionality of the IACS and related IT systems. While these personnel have the knowledge and skills to perform the risk assessment, they typically do not have the authority to make decisions to accept risk. Therefore, the results of the assessment have to be presented to the appropriate management with the authority to make such decisions.