4.5 ZCR 4: Risk comparison

4.5.1 Overview

Subclause 4.5.2 includes one ZCR to compare initial risk to tolerable risk.

4.5.2 ZCR 4.1: Compare initial risk to tolerable risk

4.5.2.1 Requirement

The initial risk determined in 4.3 shall be compared to the organization's tolerable risk. If the initial risk exceeds the tolerable risk, the organization shall perform a detailed cyber security risk assessment as defined in 4.6.

4.5.2.2 Rationale and supplemental guidance

The purpose of this step is to determine if the initial risk is tolerable or requires further mitigation.

4.6 ZCR 5: Perform a detailed cyber security risk assessment

4.6.1 Overview

This ZCR discusses the detailed risk assessment requirements for an IACS and provides rationale and supplemental guidance on each requirement. The requirements in this ZCR apply to every zone and conduit. If zones or conduits share similar threat(s), consequences and/or similar assets, it is allowable to analyse groups of zones or conduits together if such grouping enables optimized analysis. It is permissible to use existing results if the zone is standardized (for example, replication of multiple instances of a reference design). The flowchart shown in Figure 2 illustrates the cyber security risk assessment workflow.

Any detailed risk assessment methodology (such as, ISO 31000 [14], NIST SP 800-39 [16], and ISO/IEC 27005 [12]) may be followed provided the risk assessment requirements are satisfied by the methodology selected. The initial and detailed risk assessment methodologies should be derived from the same framework, standard or source and have to use a consistent risk ranking scale in order to produce consistent and coherent results.