1 Scope

This standard defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This document uses the broad definition and scope of what constitutes an IACS described in ANSI/ISA–99.01.01–2007. [1]

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

NOTE   Other documents in the ISA-99 series and in the Bibliography discuss specific technologies and/or solutions for cyber security in more detail.

The guidance provided on how to develop a CSMS is an example. It represents the authors' opinion on how an organization could go about developing the elements and may not work in all situations. The user of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning CSMS for their organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE   There may be cases where a pre-existing CSMS is in place and the IACS portion is being added or there may be some organizations that have never formally created a CSMS at all. The authors of this standard cannot anticipate all cases where an organization will be establishing a CSMS for the IACS environment, so this standard does not attempt to create a solution for all cases.