

AS IEC 62443.2.1:2024
IEC 62443-2-1:2010



STANDARDS
Australia



Industrial communication networks — Network and system security

**Part 2.1: Establishing an industrial automation and control system
security program**



AS IEC 62443.2.1:2024

This Australian Standard® was prepared by IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 22 April 2024.

This Standard was published on 3 May 2024.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Energy Producers
- Australian Industry Group
- Engineers Australia
- ISACA Sydney
- Institute of Instrumentation, Control and Automation Australia
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR AS IEC 62443.2.1:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76139 625 0

Industrial communication networks — Network and system security

Part 2.1: Establishing an industrial automation and control system security program

First published as AS IEC 62443.2.1:2024.



© IEC Geneva Switzerland 2024 — All rights reserved
© Standards Australia Limited 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of either the IEC or the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth). If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please see the contact details on the back cover or the contact us page of the website for further information.

Preface

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

The objective of this document is to define the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provide guidance on how to develop those elements. This document uses the broad definition and scope of what constitutes an IACS described in SA TS IEC 62443.1.1.

This document is identical with, and has been reproduced from, IEC 62443-2-1:2010, *Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program*.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
FOREWORD	v
INTRODUCTION	vii
0.1 Overview	vii
0.2 A cyber security management system for IACS	vii
0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001	vii
1 Scope	1
2 Normative references	1
3 Terms, definitions, abbreviated terms, acronyms, and conventions	1
3.1 Terms and definitions	1
3.2 Abbreviated terms and acronyms	6
3.3 Conventions	8
4 Elements of a cyber security management system	8
4.1 Overview	8
4.2 Category: Risk analysis	10
4.2.1 Description of category	10
4.2.2 Element: Business rationale	10
4.2.3 Element: Risk identification, classification and assessment	10
4.3 Category: Addressing risk with the CSMS	12
4.3.1 Description of category	12
4.3.2 Element group: Security policy, organization and awareness	12
4.3.3 Element group: Selected security countermeasures	17
4.3.4 Element group: Implementation	23
4.4 Category: Monitoring and improving the CSMS	27
4.4.1 Description of category	27
4.4.2 Element: Conformance	27
4.4.3 Element: Review, improve and maintain the CSMS	28
Annex A (informative) Guidance for developing the elements of a CSMS	30
Annex B (informative) Process to develop a CSMS	134
Annex C (informative) Mapping of requirements to ISO/IEC 27001	143
Bibliography	149

List of Figures

Figure 1 — Graphical view of elements of a cyber security management system	9
Figure 2 — Graphical view of category: Risk analysis	10
Figure 3 — Graphical view of element group: Security policy, organization and awareness	13
Figure 4 — Graphical view of element group: Selected security countermeasures	17
Figure 5 — Graphical view of element group: Implementation	23
Figure 6 — Graphical view of category: Monitoring and improving the CSMS	27
Figure A.1 — Graphical view of elements of a cyber security management system	31
Figure A.2 — Graphical view of category: Risk analysis	32
Figure A.3 — Reported attacks on computer systems through 2004 (source: CERT)	35
Figure A.4 — Sample logical IACS data collection sheet	49
Figure A.5 — Example of a graphically rich logical network diagram	50
Figure A.6 — Graphical view of element group: Security policy, organization, and awareness	58
Figure A.7 — Graphical view of element group: Selected security countermeasures	74
Figure A.8 — Reference architecture alignment with an example segmented architecture	82
Figure A.9 — Reference SCADA architecture alignment with an example segmented architecture	85
Figure A.10 — Access control: Account administration	87
Figure A.11 — Access control: Authentication	91

Figure A.12 — Access control: Authorization	96
Figure A.13 — Graphical view of element group: Implementation	98
Figure A.14 — Security level lifecycle model: Assess phase	102
Figure A.15 — Corporate security zone template architecture	105
Figure A.16 — Security zones for an example IACS	106
Figure A.17 — Security level lifecycle model: Develop and implement phase	109
Figure A.18 — Security level lifecycle model: Maintain phase	113
Figure A.19 — Graphical view of category: Monitoring and improving the CSMS	126
Figure B.1 — Top level activities for establishing a CSMS	134
Figure B.2 — Activities and dependencies for activity: Initiate CSMS program	136
Figure B.3 — Activities and dependencies for activity: High-level risk assessment	137
Figure B.4 — Activities and dependencies for activity: Detailed risk assessment	138
Figure B.5 — Activities and dependencies for activity: Establish security policy, organization and awareness	138
Figure B.6 — Training and assignment of organization responsibilities	140
Figure B.7 — Activities and dependencies for activity: Select and implement countermeasures	141
Figure B.8 — Activities and dependencies for activity: Maintain the CSMS	142

List of Tables

Table 1 — Business rationale: Requirements	10
Table 2 — Risk identification, classification and assessment: Requirements	11
Table 3 — CSMS scope: Requirements	13
Table 4 — Organizing for security: Requirements	14
Table 5 — Staff training and security awareness: Requirements	14
Table 6 — Business continuity plan: Requirements	15
Table 7 — Security policies and procedures: Requirements	16
Table 8 — Personnel security: Requirements	18
Table 9 — Physical and environmental security: Requirements	19
Table 10 — Network segmentation: Requirements	20
Table 11 — Access control – Account administration: Requirements	21
Table 12 — Access control – Authentication: Requirements	22
Table 13 — Access control – Authorization: Requirements	23
Table 14 — Risk management and implementation: Requirements	24
Table 15 — System development and maintenance: Requirements	25
Table 16 — Information and document management: Requirements	26
Table 17 — Incident planning and response: Requirements	27
Table 18 — Conformance: Requirements	28
Table 19 — Review, improve and maintain the CSMS: Requirements	29
Table A.1 — Typical likelihood scale	44
Table A.2 — Typical consequence scale	45
Table A.3 — Typical risk level matrix	45
Table A.4 — Example countermeasures and practices based on IACS risk levels	100
Table A.5 — Example IACS asset table with assessment results	103
Table A.6 — Example IACS asset table with assessment results and risk levels	103
Table A.7 — Target security levels for an example IACS	107
Table C.1 — Mapping of requirements in this standard to ISO/IEC 27001 references	143
Table C.2 — Mapping of ISO/IEC 27001 requirements to this standard	146

FOREWORD

- 1) The International Electrotechnical Commission ([IEC](#)) is a worldwide organization for standardization comprising all national electrotechnical committees ([IEC](#) National Committees). The object of [IEC](#) is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, [IEC](#) publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "[IEC](#) Publication(s)"). Their preparation is entrusted to technical committees; any [IEC](#) National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the [IEC](#) also participate in this preparation. [IEC](#) collaborates closely with the International Organization for Standardization ([ISO](#)) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of [IEC](#) on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested [IEC](#) National Committees.
- 3) [IEC](#) Publications have the form of recommendations for international use and are accepted by [IEC](#) National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of [IEC](#) Publications is accurate, [IEC](#) cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, [IEC](#) National Committees undertake to apply [IEC](#) Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any [IEC](#) Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) [IEC](#) itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to [IEC](#) marks of conformity. [IEC](#) is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to [IEC](#) or its directors, employees, servants or agents including individual experts and members of its technical committees and [IEC](#) National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this [IEC](#) Publication or any other [IEC](#) Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this [IEC](#) Publication may be the subject of patent rights. [IEC](#) shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-2-1 has been prepared by [IEC](#) technical committee 65: Industrial-process measurement, control and automation.

This bilingual version (2012-04) corresponds to the monolingual English version, published in 2010-11.

The text of this standard is based on the following documents:

FDIS	Report on voting
65/457/FDIS	65/461/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

The French version of this standard has not been voted upon.

This publication has been drafted in accordance with the [ISO/IEC](#) Directives, Part 2.

A list of all existing parts of IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the [IEC](#) website. The full list of existing and intended parts can also be found in the [Bibliography](#) of this standard.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the [IEC](#) web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

NOTE The revision of this international standard will be initiated shortly after this standard is published. The next revision will be aligned more closely with ISO/IEC 27001, which addresses many of the same issues but without consideration of the specialized requirements for continuous operation and safety that are common in the industrial automation and control systems environment.

IMPORTANT The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

0.1 Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology ([IT](#)) and business have been concerned with cyber security for many years and have well-established cyber security management systems ([CSMS](#)) in place as defined by the International Organization for Standardization ([ISO](#)) and the International Electrotechnical Commission ([IEC](#)) (see ISO/IEC 17799[23]¹ and ISO/IEC 27001[24]). These management systems provide an organization with a well-established method for protecting its assets from cyber attacks.

Industrial automation and control system ([IACS](#)) organizations have begun using commercial off the shelf ([COTS](#)) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the [IACS](#) equipment. These systems are not usually as robust, in the [IACS](#) environment, as are systems designed specifically as [IACS](#) at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental ([HSE](#)) consequences.

Organizations may try to use the pre-existing [IT](#) and business cyber security solutions to address security for [IACS](#) without understanding the consequences. While many of these solutions can be applied to [IACS](#), they need to be applied in the correct way to eliminate inadvertent consequences.

0.2 A cyber security management system for [IACS](#)

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. This standard addresses the aspects of the elements included in a [CSMS](#) for [IACS](#) and also provides guidance on how to go about developing the [CSMS](#) for [IACS](#).

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cyber security risks with [IACS](#). However, a frequent mistake made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that needs to address the entire set of [IACS](#) as well as the policies, procedures, practices and personnel that surround and utilize those [IACS](#). Implementing such a wide-ranging management system may require a cultural change within the organization.

Addressing cyber security on an organization-wide basis can seem like a daunting task. Unfortunately there is no simple cookbook for security. There is good reason for this. There is not a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is really a balance of risk versus cost. All situations will be different. In some situations the risk may be related to [HSE](#) factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore a cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799[23] and ISO/IEC 27001[24] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to [IACS](#) as well. This standard emphasizes the need for consistency between the practices to manage [IACS](#) cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this standard are encouraged to read ISO/IEC 17799 and ISO/IEC 27001 for additional supporting information. This standard builds on the guidance in these [ISO/IEC](#) standards. It addresses some of the important differences between [IACS](#) and general business/information technology systems. It

1) Numbers in square brackets refer to the [Bibliography](#).

introduces the important concept that cyber security risks with [IACS](#) may have [HSE](#) implications and should be integrated with other existing risk management practices addressing these risks.

Australian Standard®

Industrial communication networks — Network and system security

Part 2.1: Establishing an industrial automation and control system security program

1 Scope

This part of IEC 62443 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 standard uses the broad definition and scope of what constitutes an [IACS](#) described in IEC/TS 62443-1-1.

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 1 Other documents in the IEC 62443 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 author's opinion on how an organization could go about developing the elements and may not work in all situations. The users of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning [CSMS](#) for an organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE 2 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/TS 62443-1-1, ²⁾*Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62443-1-1 and the following apply.

2) This standard is derived from ANSI/ISA 99.02.01:2009 and wholly replaces it for international use. It is intended that the second edition of IEC/TS 62443-1-1 be an International Standard, not a TS, after inclusion of some normative requirements to which conformance is possible.

3.1.1

access account

access control function that allows the user access to a particular set of data or functions for certain equipment

Note 1 to entry: Many times accounts are linked to user identifications (IDs) and passwords. These user IDs and passwords may be linked to an individual or group of individuals such as a control room work team performing the same set of operating tasks.

3.1.2

administrative practices

defined and documented practices/procedures that individuals are personally accountable to follow at all times

Note 1 to entry: These are usually in the conditions of employment for the organization. In the [IACS](#) environment, these often have [HSE](#) implications.

3.1.3

asset

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

[SOURCE: IEC/TS 62443-1-1, 3.2.6]

Note 1 to entry: In this specific case, an asset is any item that should be protected as part of the [CSMS](#).

3.1.4

authentication

security measure designed to establish the validity of a transmission, message or originator or a means of verifying an individual's authorization to receive specific categories of information

[SOURCE: IEC/TS 62443-1-1, 3.2.13]

3.1.5

burner management system

system for the safe start-up, monitoring and shutdown of burner systems associated with boilers, flares, incinerators, gas turbines, thermal oxidizers, and other fired equipment

3.1.6

business continuity plan

document with identified procedures for recovering from a significant disruption and restoring business operations

Note 1 to entry: This umbrella term also refers to other aspects of disaster recovery, such as emergency management, human resources and media or press relations.

Note 2 to entry: A business continuity plan also identifies procedures for sustaining essential business operations while recovering from a significant disruption.

3.1.7

business continuity planning

process to develop a business continuity plan

3.1.8

change management

process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control

3.1.9

compliance

adherence to the requirements in one standard by another

[SOURCE: Adapted from [ISO/IEC 10746-2, 15.1]

Note 1 to entry: This is a relationship between two specifications, A and B, which holds when specification A makes requirements which are all fulfilled by specification B (when B complies with A)

3.1.10

conformance

relationship between an implementation and a standard where any proposition that is true in the standard must be true in its implementation

[SOURCE: Adapted from [ISO/IEC 10746-2, 15.1]

Note 1 to entry: The conformance relationship holds when specific requirements in the specification (the conformance requirements) are met by the implementation. Conformance assessment is the process through which this relation is determined.

3.1.11

consequence

result that occurs from a particular incident

3.1.12

critical

very important device, computer system, process, and the like that, if compromised by an incident, could have high financial, health, safety or environmental ([HSE](#)) impact to an organization

3.1.13

cyber security management system

program designed by an organization to maintain the cyber security of the entire organization's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the [IACS](#) side of the organization

3.1.14

device requirements

countermeasure characteristics necessary for the devices within a zone to achieve the desired target security level

3.1.15

gatekeeper

trusted individual that senior managers consult to prioritize issues they need to address over the remaining issues that others are more suited to address

3.1.16

health, safety and environment

responsibility for protecting the health and safety of workers and the surrounding community and maintaining high environmental stewardship

3.1.17

human-machine interface

aggregate of means by which people (the users) interact with a particular machine, device, computer program or other complex tool (the system)

Note 1 to entry: In many cases, these involve video screens or computer terminals, push buttons, auditory feedback, flashing lights, and the like. The human-machine interface provides means of:

- Input, allowing the users to control the machine;
- Output, allowing the machine to inform the users.

**3.1.18
incident**

event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

**3.1.19
independent audit**

review of an organization (policies, procedures, processes, equipment, personnel, and the like) by an external group not affiliated with the organization

Note 1 to entry: This may be required for public companies.

**3.1.20
information technology**

computer-related assets of an organization that represent nonphysical assets, such as software applications, process programs and personnel files

Note 1 to entry: This use of the term information technology is not abbreviated throughout this document.

Note 2 to entry: Another use of the term information technology ([IT](#)) refers to the company's internal organization (for example, the [IT](#) department) or the items traditionally maintained by this department (that is, the administrative computers, servers and network infrastructure). This use of the term information technology is abbreviated as [IT](#) throughout this standard.

**3.1.21
legacy system**

existing industrial automation and control system in a facility that may not be available as a commercial off the shelf ([COTS](#)) item

Note 1 to entry: A legacy system may have been [COTS](#) at one time, but it may be no longer available and/or supported.

**3.1.22
likelihood**

quantitative estimation that an action, event or incident may occur

**3.1.23
local user**

user who is inside the perimeter of the security zone being addressed

Note 1 to entry: A person in the immediate manufacturing area or control room is an example of a local user.

**3.1.24
manufacturing execution system**

production scheduling and tracking system used to analyze and report resource availability and status, schedule and update orders, collect detailed execution data such as material usage, labor usage, operating parameters, order and equipment status and other critical information

Note 1 to entry: This system accesses bills of material, routing and other data from the base enterprise resource planning system and is typically used for real-time shop floor reporting and monitoring that feeds activity data back to the base system.

Note 2 to entry: Refer to IEC 62264-1 for additional information.

**3.1.25
[MAC](#) address**

hardware address that differentiates one device on a network from another

**3.1.26
operator**

particular type of user that is usually responsible for the correct operation of the equipment under control

3.1.27**patch management**

area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system

Note 1 to entry: Patch management tasks include: maintaining current knowledge of available patches, deciding which patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required remotely across heterogeneous environments according to recognized best practices.

3.1.28**process engineer**

person typically responsible for the technical aspects of the industrial operation and who uses the [IACS](#) and other tools to oversee and manage the industrial automation in the facility

3.1.29**process information management system**

set of systems that provides supporting information to assist with the operation of the facility

3.1.30**programmable logic controller**

programmable microprocessor-based device that is used in industry to control assembly lines and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant

Note 1 to entry: Typically programmed as in [\[14\]](#), a [PLC](#) is designed for real time use in rugged, industrial environments. Connected to sensors and actuators, PLCs are categorized by the number and type of I/O ports they provide and by their I/O scan rate.

3.1.31**process safety management**

regulation intended to prevent a disaster in chemical and biotechnology systems by addressing sound management and engineering design

3.1.32**remote access**

communication with, or use of, assets or systems within a defined perimeter from any location outside that perimeter

3.1.33**remote user**

user who is outside the perimeter of the security zone being addressed

EXAMPLE A person in an office in the same building, a person connecting over the corporate wide area network ([WAN](#)) and a person connecting over public infrastructure networks are all remote users.

3.1.34**risk assessment**

process of identifying and evaluating risks to the organization's operations (including mission, functions, image, or reputation), the organization's assets or individuals by determining the likelihood of occurrence, the resulting impact, and additional countermeasures that would mitigate this impact

Note 1 to entry: Synonymous with risk analysis and incorporates threat and vulnerability analyses.

3.1.35**risk mitigation**

actions to reduce the likelihood and/or severity of an event

3.1.36**risk tolerance**

risk the organization is willing to accept

3.1.37**self-assessment**

review of an organization (that is, policies, procedures, operations, equipment and personnel) by a group inside the organization

Note 1 to entry: This group may be either directly associated with the organization's business process or may be in another part of the organization, but should be intimately familiar with the risks associated with that business process.

3.1.38**Six Sigma®**

process-focused methodology designed to improve business performance through improving specific areas of strategic business processes

3.1.39**social engineering**

practice of obtaining confidential information by manipulation of legitimate users

3.1.40**stakeholder**

individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services

Note 1 to entry: Stakeholders influence programs, products and services. In this particular case, stakeholders are personnel in an organization responsible for promoting and overseeing the cyber security process. These personnel include the manager of the cyber security program as well as the cross-functional team of individuals from all of the departments affected by the cyber security program.

3.1.41**system administrator**

person(s) responsible for managing the security of the computer system

Note 1 to entry: This may include operating system maintenance, network management, account administration and patch management, in accordance with the change management process.

3.1.42**system requirements**

attributes of the desired target security level

3.1.43**ushered access****shadowing**

procedure for monitoring the actions of a remotely connected user

3.1.44**vulnerability assessment**

formal description and evaluation of the vulnerabilities in a system

3.2 Abbreviated terms and acronyms

This subclause defines the abbreviated terms and acronyms used in this document.

ANSI	American National Standards Institute
CFR	U.S. Code of Federal Regulations
ChemITC	Chemical Information Technology Center of the American Chemistry Council
COTS	Commercial off the shelf
CPU	Central processing unit
CSCSP	Chemical Sector Cyber Security Program
CSMS	Cyber security management system
CSVA	Cyber security vulnerability assessment

DCS	Distributed control system
DMZ	Demilitarized zone
DoS,DDoS	Denial of service, Distributed denial of service
FDN	Field device network
FTP	File transfer protocol
HMI	Human machine interface
HSE	Health, safety and environmental
HVAC	Heating, ventilation, and air-conditioning
IACS	Industrial automation and control system(s)
ID	Identification
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
KPI	Key performance indicator(s)
LAN	Local area network
MAC	Media access control
MES	Manufacturing execution system
NERC	North American Electric Reliability Council (applies to U.S. and Canada)
NIST	U.S. National Institute of Standards and Technology
OS	Operating system
PC	Personal computer
PCN	Process control network
PCSRF	NIST Process Control Security Requirements Forum
PIM	Process information management
PIN	Personal identification number
PLC	Programmable logic controller
PSM	Process safety management
RAID	Redundant array of independent disks
RCN	Regulatory control network
SANS	SysAdmin, Audit, Networking, and Security Institute
SCADA	Supervisory control and data acquisition
SI	International System of Units
SIS	Safety instrumented system(s)
SoA	Statement of applicability
SOC	Standard operating condition
SOP	Standard operating procedure
SP	Special Publication (by NIST)
SSL	Secure socket layer
TCP	Transmission control protocol
TR	Technical report
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network

3.3 Conventions

The elements of a [CSMS](#) are the following:

- the objective of the element,
- a basic description of the element,
- a rationale to explain why the element is included and
- the requirements for that element.

A tabular presentation is used to provide a description and requirements for each element. The requirements are numbered similar to subclauses (but are not in themselves subclauses), so that the requirements can be referenced individually and selectively.

4 Elements of a cyber security management system

4.1 Overview

This clause presents the elements that constitute a [CSMS](#) for [IACS](#). These elements represent what shall and should be included in the [CSMS](#) in order to protect [IACS](#) against cyber attacks.

The elements are presented in the following three main categories:

- Risk analysis,
- Addressing risk with the [CSMS](#), and
- Monitoring and improving the [CSMS](#).

Each of these categories is further divided into element groups and/or elements. [Figure 1](#) depicts the relationship between the categories, element groups and elements.



IEC 2312/10

Figure 1 — Graphical view of elements of a cyber security management system

Each element in this clause lists the objective of the element, a basic description of the element, a rationale to explain why the element is included and the requirements for that element.

[Annex A](#) follows the same basic structure of this clause with categories, element groups and elements. However, the annex provides guidance on how to develop the elements of the CSMS. The reader should read [Annex A](#) in order to understand the special needs and issues involved with developing a CSMS for IACS. The guidance discussed in [Annex A](#) should be tailored to the special requirements of each organization.

This standard specifies the elements required for a CSMS. It is not the intent of the standard to specify a particular sequential process for identifying and addressing risk that incorporates these elements. Thus an organization will create such a process in accordance with its culture, organization and the current status of its cyber security activities. To assist organizations with this aspect of applying the standard, [A.3.4.2](#) provides an example of a process for identifying and addressing risk. In addition, [Annex B](#) offers insights on effective ordering for activities related to all of the elements discussed in this standard.

While a [CSMS](#) is an excellent tool for managing risk within a large company it is equally applicable to small companies as well. The [CSMS](#) may be more formalized in a large company so it can be used in many different situations and geographies. In a small company, similar [CSMS](#) activities need to be conducted, but they may not be as formal. [Clause 4](#) and [Annex A](#) provide guidance to help the user better understand the elements and activities of a [CSMS](#).

4.2 Category: Risk analysis

4.2.1 Description of category

The first main category of the [CSMS](#) is Risk analysis. This category discusses much of the background information that feeds into many of the other elements in the [CSMS](#). [Figure 2](#) shows the two elements that are part of the category:

- Business rationale and
- Risk identification, classification and assessment.

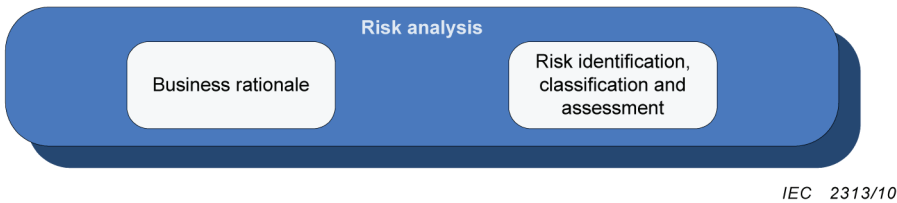


Figure 2 — Graphical view of category: Risk analysis

4.2.2 Element: Business rationale

Objective:

Identify and document the unique needs of an organization to address cyber risk for [IACS](#).

Description:

A business rationale is based on the nature and magnitude of financial, [HSE](#), and other potential consequences should [IACS](#) cyber incidents occur.

Rationale:

Establishing a business rationale is essential in order for an organization to maintain management buy in to an appropriate level of investment for the [IACS](#) cyber security program.

Requirements:

Table 1 — Business rationale: Requirements

Description	Requirement
4.2.2.1 Develop a business rationale	The organization should develop a high-level business rationale, as a basis for its effort to manage IACS cyber security, which addresses the unique dependence of the organization on IACS.

4.2.3 Element: Risk identification, classification and assessment

Objective:

Identify the set of [IACS](#) cyber risks that an organization faces and assess the likelihood and severity of these risks.

Description:

Organizations protect their ability to perform their mission by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. The first set of requirements present the actions an organization takes to carry out both a high-level and detailed risk assessment that incorporates vulnerability assessment, in a typical chronological order. Among these requirements, those related to preparing for high-level and detailed risk assessments are [4.2.3.1](#), [4.2.3.2](#) and [4.2.3.8](#) below. The last few requirements ([4.2.3.10](#) to [4.2.3.14](#)) are general requirements that apply to the overall risk assessment process. Subclause [4.3.4.2](#) covers the process of taking action based upon this assessment.

Rationale:

Since the purpose of investing in cyber security is to lower risk, it is driven by an understanding of level of risk and potential mitigations.

Requirements:

Table 2 — Risk identification, classification and assessment: Requirements

Description	Requirement
4.2.3.1 Select a risk assessment methodology	The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets.
4.2.3.2 Provide risk assessment background information	The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks.
4.2.3.3 Conduct a high-level risk assessment	A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised.
4.2.3.4 Identify the IACS	The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk and group the devices into logical systems.
4.2.3.5 Develop simple network diagrams	The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types and general locations of the equipment.
4.2.3.6 Prioritize systems	The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system.
4.2.3.7 Perform a detailed vulnerability assessment	The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks.
4.2.3.8 Identify a detailed risk assessment methodology	The organization's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment.
4.2.3.9 Conduct a detailed risk assessment	The organization shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment.
4.2.3.10 Identify the reassessment frequency and triggering criteria	The organization shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, organization, or industrial operation changes.

Table 2 (continued)

Description	Requirement
4.2.3.11 Integrate physical, HSE and cyber security risk assessment results	The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk.
4.2.3.12 Conduct risk assessments throughout the lifecycle of the IACS	Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement.
4.2.3.13 Document the risk assessment	The risk assessment methodology and the results of the risk assessment shall be documented.
4.2.3.14 Maintain vulnerability assessment records	Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS.

4.3 Category: Addressing risk with the [CSMS](#)

4.3.1 Description of category

The second main category of the [CSMS](#) is Addressing risk with the [CSMS](#). This category contains the bulk of the requirements and information contained in the [CSMS](#). It is divided into the following three element groups:

- Security policy, organization and awareness,
- Selected security countermeasures, and
- Implementation.

4.3.2 Element group: Security policy, organization and awareness

4.3.2.1 Description of element group

The first element group in this category discusses the development of the basic cyber security policies, the organizations responsible for cyber security and the awareness within the organization of cyber security issues. [Figure 3](#) shows a graphical representation of the five elements contained in this element group:

- [CSMS](#) scope,
- Organizing for security,
- Staff training and security awareness,
- Business continuity plan and
- Security policies and procedures.



Figure 3 — Graphical view of element group: Security policy, organization and awareness

4.3.2.2 Element: [CSMS](#) scope

Objective:

Identify, assess and document the systems, processes and organizations to which the [CSMS](#) applies.

Description:

The scope includes all aspects of the [IACS](#), integration points with business partners, customers and suppliers.

Rationale:

Management should understand the boundaries where the [CSMS](#) applies to the organization as well as establish a direction and focus for the [CSMS](#). By developing a clearly defined scope, it is easier for management to convey its goals and purpose for the [CSMS](#).

Requirements:

Table 3 — [CSMS](#) scope: Requirements

Description	Requirement
4.3.2.2.1 Define the scope of the CSMS	The organization shall develop a formal written scope for the cyber security program.
4.3.2.2.2 Define the scope content	The scope should explain the strategic goals, process, and timing for the CSMS.

4.3.2.3 Element: Organizing for security

Objective:

Establish the entities responsible for managing, conducting and assessing the overall cyber security of the organization's [IACS](#) assets.

Description:

Senior leadership establishes an organization, structure or network of people to provide oversight and direction for managing cyber security risks associated with [IACS](#). They also provide the personnel necessary to conduct and assess the cyber security programs throughout the organization over the life of the [CSMS](#). An organization at any level may implement this standard, including a company or other overall enterprise, division, plant or subset of a plant.

Rationale:

Commitment to a security program begins at the top of the organization. Because cyber security of [IACS](#) involves several different sets of skills not often found in any one particular section or department of an organization, it is imperative that senior leadership formulate an approach to managing security with clear identification of accountability and responsibility that makes good use of skills and labor resources. This may take several different forms from a single organization to a network of people working together to address different security aspects. The particular approach is highly dependent upon an organization's operational culture.

Requirements:**Table 4 — Organizing for security: Requirements**

Description	Requirement
4.3.2.3.1 Obtain senior management support	The organization shall obtain senior management support for a cyber security program.
4.3.2.3.2 Establish the security organization(s)	There shall be an organization, structure or network of stakeholders established (or chosen) under management leadership, with the responsibility to provide clear direction and oversight for the cyber aspects of the IACS.
4.3.2.3.3 Define the organizational responsibilities	Organizational responsibilities shall be clearly defined for cyber security and related physical security activities.
4.3.2.3.4 Define the stakeholder team makeup	The core team of stakeholders should be cross-functional in nature to bring together the skills necessary to address security in all parts of the IACS.

4.3.2.4 Element: Staff training and security awareness**Objective:**

Provide all personnel (including employees, contract employees and third-party contractors) with the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to [IACS](#) and to help ensure their own work practices are using effective countermeasures.

Description:

All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering.

Rationale:

In the area of [IACS](#), the same emphasis should be placed on cyber security as on safety and operational integrity, because the consequences can be just as severe. Security awareness for all personnel is an essential tool for reducing cyber security risks. Knowledgeable and vigilant staff are one of the most important lines of defense in securing a system. It is therefore important for all personnel to understand the importance of security in maintaining the safe operation of the system.

Requirements:**Table 5 — Staff training and security awareness: Requirements**

Description	Requirement
4.3.2.4.1 Develop a training program	The organization shall design and implement a cyber security training program.

Table 5 (continued)

Description	Requirement
4.3.2.4.2 Provide procedure and facility training	All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities.
4.3.2.4.3 Provide training for support personnel	All personnel that perform risk management, IACS engineering, system administration/maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks.
4.3.2.4.4 Validate the training program	The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training.
4.3.2.4.5 Revise the training program over time	The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities.
4.3.2.4.6 Maintain employee training records	Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis.

4.3.2.5 Element: Business continuity plan

Objective:

Identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

Description:

A business continuity plan should address the recovery objectives for the various systems and subsystems involved based on typical business needs, a list of potential interruptions and the recovery procedures for each, as well as a schedule to test part or all of the recovery procedures. One of the primary recovery objectives should be to maintain maximum availability of the control system.

Rationale:

No set of defenses can prevent all disruptions due to cyber security incidents. A detailed Business Continuity Plan ensures that [IACS](#) information can be restored and utilized as soon as possible after the occurrence of a significant disruption.

Requirements:

Table 6 — Business continuity plan: Requirements

Description	Requirement
4.3.2.5.1 Specify recovery objectives	Prior to creating a business continuity plan, the organization shall specify recovery objectives for the systems involved based on business needs.
4.3.2.5.2 Determine the impact and consequences to each system	The organization should determine the impact to each system due to a significant disruption and the consequences associated with loss of one or more of the systems.
4.3.2.5.3 Develop and implement business continuity plans	Continuity plans shall be developed and implemented to ensure that business processes can be restored in accordance with recovery objectives.
4.3.2.5.4 Form a business continuity team	A business continuity team should be formed including IACS and other process owners. In the event of a significant disruption, this team should determine the priority of critical business and IACS systems to re-establish operations.

Table 6 (continued)

Description	Requirement
4.3.2.5.5 Define and communicate specific roles and responsibilities	The business continuity plan shall define and communicate the specific roles and responsibilities for each part of the plan.
4.3.2.5.6 Create backup procedures that support business continuity plan	The organization shall create backup and restore procedures (see 4.3.4.3.9) that support the business continuity plan.
4.3.2.5.7 Test and update the business continuity plan	The business continuity plan shall be tested on a regular basis and updated as necessary.

4.3.2.6 Element: Security policies and procedures

Objective:

Address how an organization defines security, operates its security program, defines and addresses its tolerance for risk and reviews its program to make further improvements.

Description:

Cyber security policies for the [IACS](#) environment should be developed based on existing high-level policies, characterized risks and the risk tolerance levels identified by management. Cyber security procedures are developed from the cyber security policies and identify how the policies are to be implemented.

Rationale:

These written policies and procedures allow employees, contractors, third parties, and the like to clearly understand the company perspective of cyber security and their roles and responsibilities in securing the company's assets.

Requirements:

Table 7 — Security policies and procedures: Requirements

Description	Requirement
4.3.2.6.1 Develop security policies	The organization shall develop high-level cyber security policies for the IACS environment which are approved by management.
4.3.2.6.2 Develop security procedures	The organization shall develop and approve cyber security procedures, based on the cyber security policies and provide guidance in how to meet the policies.
4.3.2.6.3 Maintain consistency between risk management systems	Cyber security policies and procedures that deal with IACS risks should be consistent with or extensions of policies created by other risk management systems.
4.3.2.6.4 Define cyber security policy and procedure compliance requirements	Cyber security policies and procedures, for the IACS environment, shall include compliance requirements.
4.3.2.6.5 Determine the organization's tolerance for risk	The organization shall determine and document its risk tolerance as a basis for creation of policy and risk management activities.
4.3.2.6.6 Communicate the policies and procedures to the organization	Cyber security policies and procedures, for the IACS environment, shall be communicated to all appropriate personnel.
4.3.2.6.7 Review and update the cyber security policies and procedures	The cyber security policies and procedures shall be reviewed regularly, validated to confirm that they are up-to-date and being followed and updated as required to ensure that they remain appropriate.

Table 7 (continued)

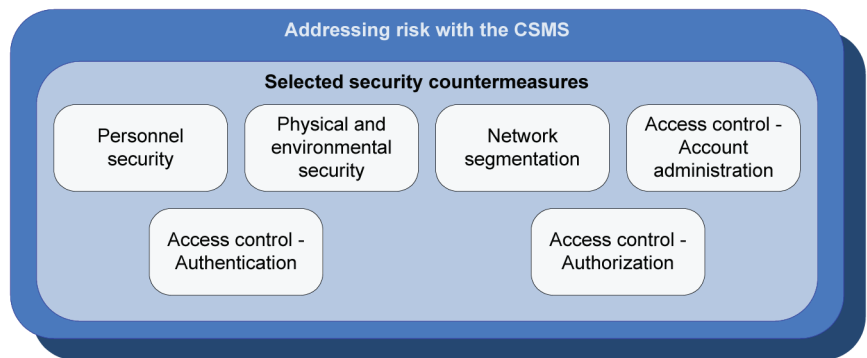
Description	Requirement
4.3.2.6.8 Demonstrate senior leadership support for cyber security	Senior leadership shall demonstrate commitment to cyber security by endorsing the cyber security policies.

4.3.3 Element group: Selected security countermeasures

4.3.3.1 Description of element group

The second element group within this category is Selected security countermeasures. The elements within this group discuss some of the main types of security controls that are part of a well designed [CSMS](#). This document does not attempt to describe the full implementation of any of these selected security countermeasures. It discusses many of the policy, procedure and practice issues related to these particular security countermeasures. [Figure 4](#) shows a graphical representation of the six elements in the element group:

- Personnel security,
- Physical and environmental security,
- Network segmentation,
- Access control – Account administration,
- Access control – Authentication and
- Access control – Authorization.



IEC 2315/10

Figure 4 — Graphical view of element group: Selected security countermeasures

These particular countermeasures were selected for inclusion because their broad impact on policy and architecture makes it essential to consider them up front when constructing any [CSMS](#). It is not the intent of this standard to specify a complete and sufficient list of countermeasures, since completeness is determined through the process of risk assessment and management described in the standard.

4.3.3.2 Element: Personnel security

Objective:

Establish the policies and procedures to determine whether personnel will maintain the [IACS](#) security of the organization throughout the lifecycle of their employment.

Description:

Personnel security involves looking at new and current personnel to determine if they will maintain the [IACS](#) security for the organization. For new personnel, it evaluates them prior to their entry into the organization making sure they demonstrate behaviors consistent with their future security responsibility. For current personnel, it establishes that they continue to demonstrate behavior consistent with their current security responsibilities.

Rationale:

In many organizations, personnel security requirements are driven by concerns about insider threats and the possibility of accidents caused by inattention to detail or by personnel unfit for a job due to lack of proper background or the use of substances that might cloud judgment. By implementing personnel security policies it may be possible to reduce these types of problems.

Requirements:

Table 8 — Personnel security: Requirements

Description	Requirement
4.3.3.2.1 Establish a personnel security policy	There shall be a personnel security policy established, clearly stating the organization's commitment to security and the security responsibilities of personnel. (Personnel include employees, prospective employees, contract employees, and third-party contractors.)
4.3.3.2.2 Screen personnel initially	Unless government regulation prohibits it, all personnel with access to the IACS (both physical and cyber), including new hires and internal transfers to sensitive positions shall be screened, including validation of their identity and background checks, during the job application process.
4.3.3.2.3 Screen personnel on an ongoing basis	Personnel should also be subject to ongoing scrutiny for changes that might indicate a conflict of interest or concern for performing the job in an appropriate manner.
4.3.3.2.4 Address security responsibilities	The personnel security policy should address security responsibilities from recruitment through the end of employment, especially for sensitive positions.
4.3.3.2.5 Document and communicate security expectations and responsibilities	Security expectations and responsibilities shall be clearly documented and regularly communicated to personnel.
4.3.3.2.6 State cyber security terms and conditions of employment clearly	Terms and conditions of employment shall clearly state the personnel's responsibility for cyber security. These responsibilities shall extend for a reasonable period of time after employment ceases.
4.3.3.2.7 Segregate duties to maintain appropriate checks and balances	Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the IACS.

4.3.3.3 Element: Physical and environmental security

Objective:

Create a secure environment for the protection of [IACS](#) assets. An asset is any physical or logical object owned by, or under the custodial duties of, an organization, having either a perceived or actual value to the organization (see IEC/TS 62443-1-1). [IACS](#) assets are those assets that are a part of the [IACS](#), either physical or cyber or that can affect the operation of the [IACS](#). Physical security measures ensure that all assets, specifically those related to the [IACS](#) of an organization, are protected physically from unauthorized access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organization are protected against environmental conditions that would make them unusable or damage the information they contain.

Description:

Physical and environmental security measures should be designed to complement the cyber security measures taken to protect assets that are part of the [IACS](#) and coordinated with the physical security of the remainder of the plant. When developing a program for physical security of assets, it is important to include all systems in the scope and not just limit the effort to traditional computer room facilities. Practical engineering judgment should be used to balance the risks when determining physical security procedures. Physical segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level.

Rationale:

Physical assets are a means to an end as well as the end itself. In modern control systems the physical assets provide the means by which the cyber system operates. Therefore, the asset has value in itself but also has value as an integral part of the control system. Since both the asset and the control system require each other, both shall be protected in order for the system to be secure. The overriding security premise is that the use of security countermeasures should be commensurate with the level of risk. While physical segmentation is an important security countermeasure employed in conjunction with other layers of defense to reduce the risk that may be associated with [IACS](#), it may not be necessary if the security risks are within accepted limits.

Requirements:**Table 9 — Physical and environmental security: Requirements**

Description	Requirement
4.3.3.3.1 Establish complementary physical and cyber security policies	Security policies and procedures that address both physical and cyber security in the protection of assets shall be established.
4.3.3.3.2 Establish physical security perimeter(s)	One or more physical security perimeters shall be established to provide barriers to unauthorized access to protected assets.
4.3.3.3.3 Provide entry controls	Appropriate entry controls shall be provided at each barrier or boundary.
4.3.3.3.4 Protect assets against environmental damage	Assets shall be protected against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion and impact.
4.3.3.3.5 Require employees to follow security procedures	Employees shall be required to follow and enforce the physical security procedures that have been established.
4.3.3.3.6 Protect connections	All connections under the control of the organization shall be adequately protected from tampering or damage.
4.3.3.3.7 Maintain equipment assets	All equipment assets, including auxiliary environmental equipment, shall be properly maintained to ensure proper operation.
4.3.3.3.8 Establish procedures for monitoring and alarming	Procedures shall be established for monitoring and alarming when physical or environmental security is compromised.
4.3.3.3.9 Establish procedures for the addition, removal, and disposal of assets	Procedures should be established and audited with respect to the addition, removal and disposal of all assets.
4.3.3.3.10 Establish procedures for the interim protection of critical assets	Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster.

4.3.3.4 Element: Network segmentation**Objective:**

Group and separate key [IACS](#) devices into zones with common security levels in order to manage security risks and to achieve a desired target security level for each zone.

Description:

Network segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level. The zone may be an isolated standalone network segment or a network segment separated from the organization’s network by some sort of network barrier device. [IACS](#) should be designed in a manner that filters/prevents nonessential communication packets from reaching the [IACS](#) devices.

For Transmission Control Protocol / Internet Protocol ([TCP/IP](#)) based networks, the most common barrier devices in use are firewalls, routers and layer 3 switches. For non-[TCP/IP](#) type networks, the barrier devices may be standalone gateways or integrated into the network interface module of an [IACS](#) device.

Rationale:

The overriding security premise is that the use of security countermeasures should be commensurate with the level of risk. While network segmentation is an important security countermeasure employed in conjunction with other layers of defense to reduce the risk that may be associated with [IACS](#), it may not be necessary if the security risks are low.

Requirements:

Table 10 — Network segmentation: Requirements

Description	Requirement
4.3.3.4.1 Develop the network segmentation architecture	A network segmentation countermeasure strategy employing security zones shall be developed for IACS devices based upon the risk level of the IACS.
4.3.3.4.2 Employ isolation or segmentation on high-risk IACS	High-risk IACS shall be isolated from or employ a barrier device to separate it from other zones with different security levels or risks.
4.3.3.4.3 Block non-essential communications with barrier devices	Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment.

4.3.3.5 Element: Access control – Account administration

Objective:

Ensure, on an ongoing basis, that only appropriate entities have accounts that allow access and that these accounts provide appropriate access privileges.

Description:

Access control is the method of controlling who or what entities can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

Rationale:

The misuse of data and systems may have serious consequences, including harm to human life, environmental damage, financial loss and damaged corporate reputation. These risks are increased when employees, contractors or temporary personnel have unnecessary access to data and systems.

Requirements:

Table 11 — Access control – Account administration: Requirements

Description	Requirement
4.3.3.5.1 Access accounts implement authorization security policy	Access privileges implemented for access accounts shall be established in accordance with the organization's authorization security policy (see 4.3.3.7.1).
4.3.3.5.2 Identify individuals	As for all cyber security controls, the choice of access accounts for individuals versus access accounts for a crew shall be determined by considering threats, risks and vulnerabilities. In this case, considerations include HSE risks of individual controls, mitigation using complementary physical security controls, requirement for accountability and administrative/operational need.
4.3.3.5.3 Authorize account access	Access shall be granted, changed, or terminated on the authority of an appropriate manager.
4.3.3.5.4 Record access accounts	A record shall be maintained of all access accounts, including details of the individual(s) and devices authorized to use the account, their permissions and the authorizing manager.
4.3.3.5.5 Suspend or remove unneeded accounts	Access accounts shall be suspended or removed as soon as they are no longer needed (for example, job change).
4.3.3.5.6 Review account permissions	All established access accounts shall be reviewed regularly to ensure that the individual(s) and devices have only the minimum required permissions.
4.3.3.5.7 Change default passwords	Default passwords for access accounts shall be changed before the IACS is put into service.
4.3.3.5.8 Audit account administration	Periodic reviews of compliance to the account administration policy should be performed.

4.3.3.6 Element: Access control – Authentication

Objective:

Positively identify network users, hosts, applications, services and resources for computerized transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

Description:

Access control is the method of controlling who or what resources can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

There are several types of authentication strategies and each has varying degrees of strength. Strong authentication methods are ones that are quite accurate in positively identifying the user. Weak authentication methods are ones that can be easily defeated to provide unwanted access to information. Physical location of the user may have a significant impact on the risk of accessing the [IACS](#).

Rationale:

Authentication requirements are more stringent for administration/configuration users and remote users, than for other users. This is because administration/configuration users have broader privileges and their actions have potentially more impact than other users; and remote users are typically not

subject to complementary physical access controls. Automatic account logout due to failed logins or periods of inactivity increases authentication strength, but is considered carefully in the [IACS](#) environment, since failure to authenticate a valid user could have [HSE](#) implications if the user is not able to perform tasks in a critical situation. In the [IACS](#) environment, there is a great emphasis on combining physical authentication measures with electronic authentication practices.

Requirements:

Table 12 — Access control – Authentication: Requirements

Description	Requirement
4.3.3.6.1 Develop an authentication strategy	Companies shall have an authentication strategy or approach that defines the method(s) of authentication to be used.
4.3.3.6.2 Authenticate all users before system use	All users shall be authenticated before using the requested application, unless there are compensating combinations of entrance control technologies and administrative practices.
4.3.3.6.3 Require strong authentication methods for system administration and application configuration	Strong authentication practices (such as requiring strong passwords) shall be used on all system administrator access accounts and application configuration access accounts.
4.3.3.6.4 Log and review all access attempts to critical systems	Log files should record all access attempts to critical systems and should be reviewed for successful and failed access attempts.
4.3.3.6.5 Authenticate all remote users at the appropriate level	The organization shall employ an authentication scheme with an appropriate level of strength to positively identify a remote interactive user.
4.3.3.6.6 Develop a policy for remote login and connections	The organization shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity.
4.3.3.6.7 Disable access account after failed remote login attempts	After some number of failed login attempts by a remote user, the system should disable the access account for a certain amount of time.
4.3.3.6.8 Require re-authentication after remote system inactivity	After a defined period of inactivity, a remote user should be required to re-authenticate before the remote user can re-access the system.
4.3.3.6.9 Employ authentication for task-to-task communication	Systems should employ appropriate authentication schemes for task-to-task communication between applications and devices.

4.3.3.7 Element: Access control – Authorization

Objective:

Grant access privileges to resources upon successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

Description:

Access control is the method of controlling who or what resources can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

Authorization explores the controls aimed at protecting information and assets from deliberate and inadvertent destruction, change or disclosure. It focuses specifically on measures designed to ensure that the authenticated agents have access to required information assets. As with authentication, authorization is dependent upon the location of the user.

Rationale:

It is important in the [IACS](#) environment to make sure that the right people have access to the correct information and systems and are not prevented from doing their job due to lack of authorization. Authorization to perform specific job functions is provided by the application. There is a need to consider safety implications when developing the authorization strategy.

Requirements:

Table 13 — Access control – Authorization: Requirements

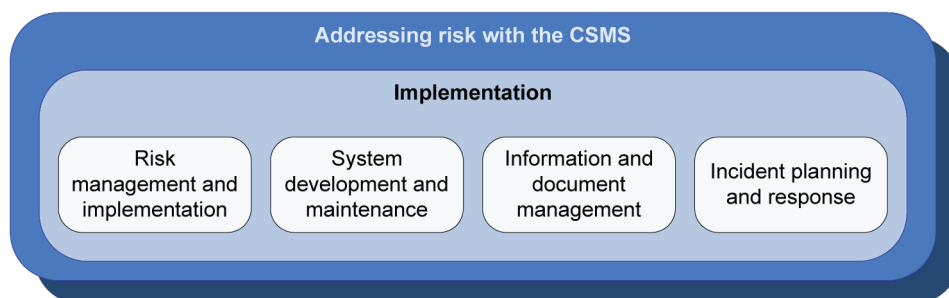
Description	Requirement
4.3.3.7.1 Define an authorization security policy	Rules that define the privileges authorized under access accounts for personnel in various job roles shall be defined in an authorization security policy that is clearly documented and applied to all personnel upon authentication.
4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices	The permission to access IACS devices shall be logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras, and other controls that restrict access to an active computer console), or both.
4.3.3.7.3 Control access to information or systems via role-based access accounts	Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications shall be considered when defining roles.
4.3.3.7.4 Employ multiple authorization methods for critical IACS	In critical control environments, multiple authorization methods should be employed to limit access to the IACS.

4.3.4 Element group: Implementation

4.3.4.1 Description of element group

The third element group in this category is Implementation. This element within this group discusses issues related to implementing the [CSMS](#). [Figure 5](#) shows a graphical representation of the four elements in the element group:

- Risk management and implementation,
- System development and maintenance,
- Information and document management and
- Incident planning and response.



IEC 2316/10

Figure 5 — Graphical view of element group: Implementation

4.3.4.2 Element: Risk management and implementation

Objective:

Reduce risk to and maintain risk at an acceptable level in the [IACS](#) based upon the organization's tolerance for risk.

Description:

Risk management and implementation addresses the selection, development and implementation of countermeasures that are commensurate with risks. The countermeasures may take into account the use of products with strong inherent security capabilities, manual and procedural security controls and technology based controls to prevent or reduce security incidents.

Rationale:

The risk management and implementation element is used to turn the results from the risk identification classification and assessment element of this standard into effective and concrete actions. Although it can never be eliminated totally, risk can be managed in a manner that balances the cost of risk avoidance against the potential cost of the incident.

Requirements:

Table 14 — Risk management and implementation: Requirements

Description	Requirement
4.3.4.2.1 Manage IACS risk on an ongoing basis	The organization shall adopt a risk management framework that includes selection and implementation of IACS devices and countermeasures to manage risk to an acceptable level over the life of the facility.
4.3.4.2.2 Employ a common set of countermeasures	A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organization wherever a specific risk is identified.

4.3.4.3 Element: System development and maintenance

Objective:

Ensure that the organization's desired risk tolerance level is maintained as its [IACS](#) assets evolve through the maintenance of existing systems as well as development and procurement of new systems.

Description:

This element addresses designing cyber security into systems from the earliest development stages. It also involves the maintenance of those cyber security policies and procedures as the system changes throughout its lifecycle.

Rationale:

Organizations have found that maintenance of the [CSMS](#) is more challenging than establishing it. For this reason, procedures that proactively address cyber security as part of the natural evolution of the [IACS](#) systems are critical.

Requirements:

Table 15 — System development and maintenance: Requirements

Description	Requirement
4.3.4.3.1 Define and test security functions and capabilities	The security functions and capabilities of each new component of the IACS shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile.
4.3.4.3.2 Develop and implement a change management system	A change management system for the IACS environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest.
4.3.4.3.3 Assess all the risks of changing the IACS	Using clearly defined criteria, proposed changes to IACS shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals technically knowledgeable about the industrial operation and the IACS system.
4.3.4.3.4 Require security policies for system development or maintenance changes	The security requirements of a new system being installed in the IACS environment in an existing zone shall meet the security policies and procedures required for that zone/environment. Similarly, maintenance upgrades or changes shall meet the security requirements for the zone.
4.3.4.3.5 Integrate cyber security and process safety management (PSM) change management procedures	Cyber security change management procedures should be integrated with existing PSM procedures.
4.3.4.3.6 Review and maintain policies and procedures	The operations and change management policies and procedures shall be reviewed and kept current to ensure that security changes do not increase risks to safety or business continuity.
4.3.4.3.7 Establish and document a patch management procedure	A procedure for patch management shall be established, documented, and followed.
4.3.4.3.8 Establish and document antivirus/malware management procedure	A procedure for antivirus/malware management shall be established, documented, and followed.
4.3.4.3.9 Establish backup and restoration procedure	A procedure for backing up and restoring computer systems and protecting backup copies shall be established, used, and verified by appropriate testing.

4.3.4.4 Element: Information and document management

Objective:

Classify, manage, safeguard and present the information associated with the [IACS](#) and [CSMS](#) at the appropriate time to authorized personnel.

Description:

Organizations should employ comprehensive information and document management policies for information assets within the scope of their [IACS](#) and [CSMS](#). Care should be given to protect this information and verify that the appropriate versions are retained. Information classification systems that allow information assets to receive the appropriate level of protection are the key to meeting this objective.

Rationale:

Much of the information about the [IACS](#) may be stored electronically or in hardcopy outside the [IACS](#) and is not protected by [IACS](#) authorization controls. Unauthorized access and use of this information is a threat to [IACS](#) security. This information needs to be appropriately controlled and managed.

Requirements:

Table 16 — Information and document management: Requirements

Description	Requirement
4.3.4.4.1 Develop lifecycle management processes for IACS information	A lifecycle document management process shall be developed and maintained for IACS information.
4.3.4.4.2 Define information classification levels	Information classification levels (for example, company confidential, restricted and public) shall be defined for access and control, including sharing, copying, transmitting, and distributing appropriate for the level of protection required.
4.3.4.4.3 Classify all CSMS information assets	All logical assets within the scope of the CSMS (that is, control system design information, vulnerability assessments, network diagrams and industrial operations programs) shall be classified to indicate the protection required commensurate with the consequence of its unauthorized disclosure or modification.
4.3.4.4.4 Ensure appropriate records control	Policies and procedures should be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.
4.3.4.4.5 Ensure long-term records retrieval	Appropriate measures should be employed to ensure long-term records can be retrieved (that is, converting the data to a newer format or retaining older equipment that can read the data).
4.3.4.4.6 Maintain information classifications	Information that requires special control or handling should be reviewed on a periodic basis to validate that special handling is still required.
4.3.4.4.7 Audit the information and document management process	Periodic reviews of compliance to the information and document management policy should be performed.

4.3.4.5 Element: Incident planning and response

Objective:

Predefine how the organization will detect and react to cyber security incidents.

Description:

When developing a program for incident planning and response, it is important to include all systems in scope and not just limit the effort to traditional computer room facilities. Part of the incident response plan should include procedures for how the organization will respond to incidents, including notification and documentation methods, investigations, recoveries and subsequent follow-up practices.

Rationale:

Identifying an incident early and responding appropriately can limit the consequences of the event. Incident planning and response provides the organization the opportunity to plan for security incidents and then to respond according to the established company practices. No matter how much care is taken in protecting a system, it is always possible that unwanted intrusions might compromise the system. Technology vulnerabilities continue to exist and external threats are increasing in number and sophistication, therefore requiring a robust strategy for determining the appropriate planning and response. Insight gained from actual incidents is captured because it is critical for evaluating and improving the [CSMS](#).

Requirements:

Table 17 — Incident planning and response: Requirements

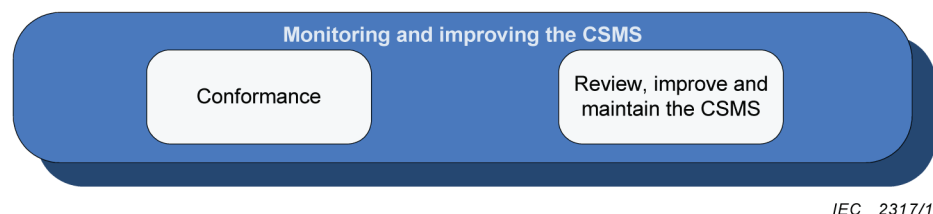
Description	Requirement
4.3.4.5.1 Implement an incident response plan	The organization shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals.
4.3.4.5.2 Communicate the incident response plan	The incident response plan shall be communicated to all appropriate organizations.
4.3.4.5.3 Establish a reporting procedure for unusual activities and events	The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents.
4.3.4.5.4 Educate employees on reporting cyber security incidents	Employees should be educated on their responsibility to report cyber security incidents and the methods of reporting these incidents.
4.3.4.5.5 Report cyber security incidents in a timely manner	The organization should report cyber security incidents in a timely manner.
4.3.4.5.6 Identify and respond to incidents	If an incident is identified, the organization shall promptly respond in accordance with the established procedures.
4.3.4.5.7 Identify failed and successful cyber security breaches	The organization should have procedures in place to identify failed and successful cyber security breaches.
4.3.4.5.8 Document the details of incidents	The details of an identified incident shall be documented to record the incident, the response, the lessons learned, and any actions taken to modify the CSMS in light of this incident.
4.3.4.5.9 Communicate the incident details	The documented details of an incident shall be communicated to all appropriate organizations (that is, management, IT, process safety, automation and control engineering security and manufacturing) in a timely manner.
4.3.4.5.10 Address and correct issues discovered	The organization shall have a business methodology in place to address issues discovered and ensure they are corrected.
4.3.4.5.11 Conduct drills	Drills should be conducted to test the incident response program on a routine basis.

4.4 Category: Monitoring and improving the [CSMS](#)

4.4.1 Description of category

The third main category of the [CSMS](#) is titled Monitoring and Improving the [CSMS](#). It involves both ensuring that the [CSMS](#) is being used and also reviewing the [CSMS](#) itself for effectiveness. [Figure 6](#) shows a graphical representation of the two elements in the category:

- Conformance and
- Review, improve and maintain the [CSMS](#).

**Figure 6 — Graphical view of category: Monitoring and improving the [CSMS](#)**

4.4.2 Element: Conformance

Objective:

Ensure that the [CSMS](#) developed for an organization is followed.

Description:

Conformance with a [CSMS](#) means the organization is adhering to its stated policies, executing the procedures at the correct time and producing the appropriate reports to allow for future review.

Rationale:

Irrespective of the quality of a [CSMS](#), if it is not used, then it does not add any value to the organization and does not help reduce risk.

Requirements:

Table 18 — Conformance: Requirements

Description	Requirement
4.4.2.1 Specify the methodology of the audit process	The audit program shall specify the methodology of the audit process.
4.4.2.2 Conduct periodic IACS audits	Validate that the IACS conforms to the CSMS. The CSMS shall include periodic audits of the IACS, to validate that the security policies and procedures are performing as intended and meet the security objectives for the zone.
4.4.2.3 Establish conformance metrics	The organization should define performance indicators and success criteria, which are used to monitor conformance to the CSMS. The results from each periodic audit should be expressed in the form of performance against these metrics to display security performance and security trends.
4.4.2.4 Establish a document audit trail	A list of documents and reports required to establish an audit trail shall be developed.
4.4.2.5 Define punitive measures for non-conformance	The organization shall state what non-conformance with the CSMS means, and any related punitive measures shall also be defined.
4.4.2.6 Ensure auditors' competence	The required competency for auditing the specific systems that are in scope should be specified. The level of independence required should be determined as part of the governance.

4.4.3 Element: Review, improve and maintain the [CSMS](#)

Objective:

Ensure that the [CSMS](#) continues to meet its goals over time.

Description:

Reviewing, improving and maintaining the [CSMS](#) establishes a continuing oversight of the [CSMS](#) to check that it functions effectively and to manage required changes to the [CSMS](#) over time.

Rationale:

Review and monitoring are required for the [CSMS](#) to remain effective, since the [CSMS](#) shall respond to changes in internal and external threats, vulnerabilities and consequences, as well as changes in risk tolerance, legal requirements and evolving technical and non-technical approaches to risk mitigation.

Requirements:

Table 19 — Review, improve and maintain the **CSMS**: Requirements

Description	Requirement
4.4.3.1 Assign an organization to manage and implement changes to the CSMS	An organization shall be assigned to manage and coordinate the refinement and implementation of the CSMS changes and use a defined method in making and implementing changes.
4.4.3.2 Evaluate the CSMS periodically	The managing organization shall periodically evaluate the overall CSMS to ensure the security objectives are being met.
4.4.3.3 Establish triggers to evaluate CSMS	The organization should establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS and perhaps a change. These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk and major changes to the IACS. The thresholds should be based on the organization's risk tolerance.
4.4.3.4 Identify and implement corrective and preventive actions	The organization shall identify and implement appropriate corrective and preventive actions that modify the CSMS to meet security objectives.
4.4.3.5 Review risk tolerance	A review of the organization's tolerance for risk should be initiated when there are major changes to the organization, technology, business objectives, internal business and external events including identified threats and changes in social climate.
4.4.3.6 Monitor and evaluate industry CSMS strategies	Management system owners should monitor the industry for CSMS best practices for risk assessment and risk mitigation and evaluate their applicability.
4.4.3.7 Monitor and evaluate applicable legislation relevant to cyber security	The organization shall identify applicable and changing legislation relevant to cyber security.
4.4.3.8 Request and report employee feedback on security suggestions	Employee feedback on security suggestions should be actively sought and reported back to senior management as appropriate on performance shortcomings and opportunities.

Annex A (informative)

Guidance for developing the elements of a [CSMS](#)

A.1 Overview

This annex provides informative guidance to the reader on how to develop a [CSMS](#) that meets the requirements specified in [Clause 4](#). The guidance presented here provides an overall management system framework that allows organizations adopting the [CSMS](#) to tailor it to their own specific needs. It should be thought of as a starting point or baseline for a [CSMS](#). Not all guidance may be applicable and depending on the application, the organization may require more security than what is presented. It is also not meant to be a step-by-step process, as was previously stated in [4.1](#).

This annex is organized with the same categories, element groups, and elements as those listed in [Clause 4](#) (see [Figure A.1](#)). Each element in this annex uses the following organization:

- Description of element – a basic description of the topic;
- Element-specific information – one or more subclauses providing detailed guidance regarding this element. Their structure and content is element-specific;
- Supporting practices:
 - Baseline practices – recommendations for organizations to achieve a baseline level of cyber security. These practices become the building blocks of the requirements for each element.
 - Additional practices – innovative security practices used by some organizations to further enhance cyber security;
- Resources used – sources for additional information as well as documents referenced (in addition to the current document).



Figure A.1 — Graphical view of elements of a cyber security management system

A.2 Category: Risk analysis

A.2.1 Description of category

The first main category of the [CSMS](#) is risk analysis. This category discusses much of the background information that feeds into many of the other elements in the [CSMS](#). [Figure A.2](#) shows the two elements that are part of the category:

- Business rationale and
- Risk identification, classification and assessment.

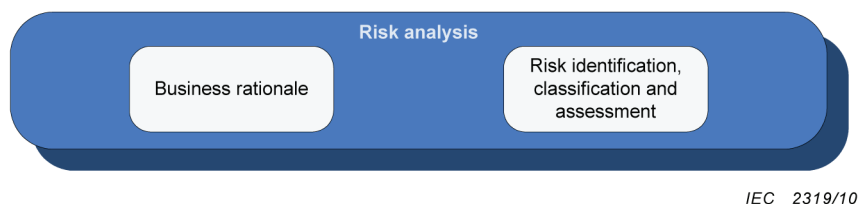


Figure A.2 — Graphical view of category: Risk analysis

A.2.2 Element: Business rationale

A.2.2.1 Description of element

This element establishes that the organization is aware of and understands the importance of cyber security for information technology as used in [IACS](#). This understanding is based upon an understanding of the roles that information technology plays in the mission of the organization, associated risks to this mission and the cost and other business impacts of mitigating this risk.

A.2.2.2 Cyber security risk, business rationale and business case

The first step to implementing a cyber security program for [IACS](#) is to develop a compelling business rationale for the unique needs of the organization to address cyber risk. An organization may derive the rationale for its [IACSCSMS](#) and related individual projects from existing policies related to safety, general risk management or compliance with regulatory requirements. Other organizations may require that the business rationale take the form of a formal or informal business case for cyber security management activities in order to establish that the cost of mitigating cyber risk is justified by its financial benefit. A business rationale or business case for taking the first steps to build a [CSMS](#) will depend upon an assessment of risk, generally at a high level. Once risk is acknowledged, an organization is ready to take appropriate steps to mitigate it. An effort to perform more systematic and detailed risk assessment (as described later in this standard) and individual decisions about countermeasures, may themselves require a business rationale, possibly in the form of a business case.

A business rationale captures the business concerns of senior management while being founded in the experience of those already dealing with many of the same risks. This subclause deals with the key components of the resulting business rationale and key resources to help identify those components. A business rationale may have as its scope the justification of a high-level or detailed risk assessment, other specific aspects of a full [CSMS](#) as described herein, or implementation of a single countermeasure.

Experience has shown that embarking on a cyber security program without an agreed business rationale often results in eventual loss of program resources in favor of other business requirements. Typically these other business requirements have a more direct business benefit and easily understood rationale.

A.2.2.3 Key components of business rationale

There are four key components of a business rationale: prioritized business consequences, prioritized threats, estimated annual business impact and cost of countermeasures.

a) Prioritized business consequences

The list of potential business consequences needs to be distilled to the particular business consequences that senior management will find the most compelling. For instance, a food and beverage company that handles no toxic or flammable materials and typically processes its product at relatively low temperatures and pressures might not be concerned about equipment damage or environmental impact but might be more concerned about loss of production availability and degradation of product quality. The insight here is based on histories of past incidents as well as knowledge of how [IACS](#) are actually used in the business and the potential

business impact that unauthorized technical changes could cause. Regulatory compliance might also be a concern.

b) Prioritized threats

The list of potential threats needs to be refined, if possible, to those threats that are deemed credible. For instance, a food and beverage company might not find terrorism a credible threat but might be more concerned with viruses and worms and disgruntled employees. The insight here is primarily based on histories of past incidents.

c) Estimated annual business impact

The highest priority items shown in the list of prioritized business consequences should be scrutinized to obtain an estimate of the annual business impact preferably, but not necessarily, in financial terms. For the food and beverage company example, it may have experienced a virus incident within its internal network that the information security organization estimated as resulting in a specific financial cost. Because the internal network and the controls network are interconnected, it is conceivable that a virus originating from the controls network could cause the same amount of business impact. The insight here is primarily based on histories of past incidents. Regulatory compliance may entail specific financial or business penalties for non-compliance.

d) Cost

The estimated cost of the human effort and technical countermeasures that this business rationale intends to justify.

NOTE A business impact estimate in financial terms and cost estimates for countermeasures are required to create a business case, but a successful business rationale may not always include this information.

There are a number of resources for information to help form this business rationale: external resources in trade organizations and internal resources in related risk management programs or engineering and operations.

External resources in trade organizations often provide useful tips about factors that most strongly influenced their management to support their efforts and what resources within their organizations proved most helpful. For different industries, these factors may be different but there may be similarities in the roles that other risk management specialists can play.

Internal resources associated with related risk management efforts (that is, information security, [HSE](#) risk, physical security, and business continuity) can provide tremendous assistance based on their experience with related incidents in the organization. This information is helpful from the standpoint of prioritizing threats and estimating business impact. These resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might prove the most appropriate or receptive to serving as a champion.

Internal resources associated with control systems engineering and operations can provide insight into the details of how control systems are actually used within the organization. How are networks typically segregated? How are high-risk combustion systems or safety instrumented systems ([SIS](#)) typically designed? What security countermeasures are already commonly used? Keeping in mind the organization's history with mergers and acquisitions, it is also important to understand how representative any particular site might be of the entire business unit, region or overall organization.

Remember that in the early stages of the industrial operation, the primary focus will be on identifying one or two high-priority issues that justify continued effort. As the [IACS](#) cyber security program develops further, other items may appear on the list and priorities may shift, as the organization applies a more rigorous risk analysis methodology. However, these changes should not detract from the result of this original effort to justify initiating the program.

A.2.2.4 Content suggestions for IACS business rationale

Within each organization, the journey to develop an effective cyber security program for IACS starts with individuals who recognize the risks the organization is taking and begin to articulate these risks internally, not just in technical terms, but in business terms that resonate with upper management. A business rationale is not a detailed risk assessment; it is rather a high-level description of risks sufficient to justify the next planned steps in building a CSMS. It may be as brief or detailed as required to support the decision processes in the particular organization.

The negative business consequences of cyber attacks against IACS can include the following:

- reduction or loss of production at one site or multiple sites simultaneously;
- injury or death of employees;
- injury or death of persons in the community;
- damage to equipment;
- environmental damage;
- violation of regulatory requirements;
- product contamination;
- criminal or civil legal liabilities;
- loss of proprietary or confidential information;
- loss of brand image or customer confidence;
- economic loss.

In prioritizing the risk of these consequences occurring, it is also important to consider the potential source or threat that initiates a cyber attack and the likelihood that such an event would occur. Cyber threats could arise from sources inside or outside an organization; threats could be the result of either intentional or unintentional actions; and threats could either be directed at a specific target or undirected. Cyber security incidents can result from many different types of threat agents such as the following:

- Thrill-seeking, hobbyist, or alienated individuals who gain a sense of power, control, self-importance and pleasure through successful penetration of computer systems either via undirected attacks (viruses and worms) or directed attacks (hacking) to steal or destroy information or disrupt an organization's activities.
- Disgruntled employees or contractors who damage systems or steal information for revenge or profit.
- Well-intentioned employees who inadvertently make changes to the wrong controller or operating equipment.
- Employees who break quality, safety or security policies or procedures to meet other urgent needs (for example, production goals).
- Terrorists typically motivated by political beliefs for which cyber attacks offer the potential for low-cost, low-risk, but high-gain attacks especially when linked with coordinated physical attacks.
- Professional thieves (including organized crime) who steal information for sale.
- Adversary nations or groups who use the Internet as a military weapon for cyber warfare to disrupt the command, control and communication capabilities of a foe.

Documented cases provide insight into how and how often one of these threat agents succeeds in inflicting negative business consequences. The rapid adoption of new network technologies has led to the development of new tools to enable cyber attacks. With the lack of a recognized publicly accessible incident reporting system, it will be extremely difficult in the near future to determine a quantitative likelihood of any specific type of event occurring. Likelihood will need to be evaluated qualitatively based on an organization's own internal incident history and on the few cases that have been publicly documented. Several examples of these cases are:

EXAMPLE 1 In January, 2003, the SQL Slammer Worm rapidly spread from one computer to another across the Internet and within private networks. It penetrated a computer network at Ohio's Davis-Besse nuclear power plant and disabled a monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. It occurred due to an unprotected interconnection between plant and corporate networks. The SQL Slammer Worm downed one utility's critical [SCADA](#) network after moving from a corporate network to the control center local area network ([LAN](#)). Another utility lost its Frame Relay Network used for communications and some petrochemical plants lost human-machine interfaces (HMIs) and data historians. A 911 call center was taken offline, airline flights were delayed and canceled and bank ATMs were disabled.

EXAMPLE 2 Over several months in 2001, a series of cyber attacks were conducted on a computerized waste water treatment system by a disgruntled contractor in Queensland, Australia. One of these attacks caused the diversion of millions of gallons of raw sewage into a local river and park. There were 46 intrusions before the perpetrator was arrested.

EXAMPLE 3 In September, 2001, a teenager allegedly hacked into a computer server at the Port of Houston to target a female chat room user following an argument. It was claimed that the teenager intended to take the woman's computer offline by bombarding it with a huge amount of useless data and he needed to use a number of other servers to be able to do so. The attack bombarded scheduling computer systems at the world's eighth largest port with thousands of electronic messages. The port's web service, which contained crucial data for shipping pilots, mooring companies and support firms responsible for helping ships navigate in and out of the harbor, was left inaccessible.

The CERT organization has been monitoring and tracking the number of attacks occurring on Internet-connected systems since 1988. None of the reported incidents were for control systems. As of 2004, they have stopped tracking the number of attacks, because the prevalence of automated attack tools has led to attacks becoming so commonplace that the number of incidents reported provides little information with regard to assessing the scope and impact of attacks. A graph of their incident data is shown in [Figure A.3](#) to demonstrate the dramatic increase that has occurred over the last 15 years.

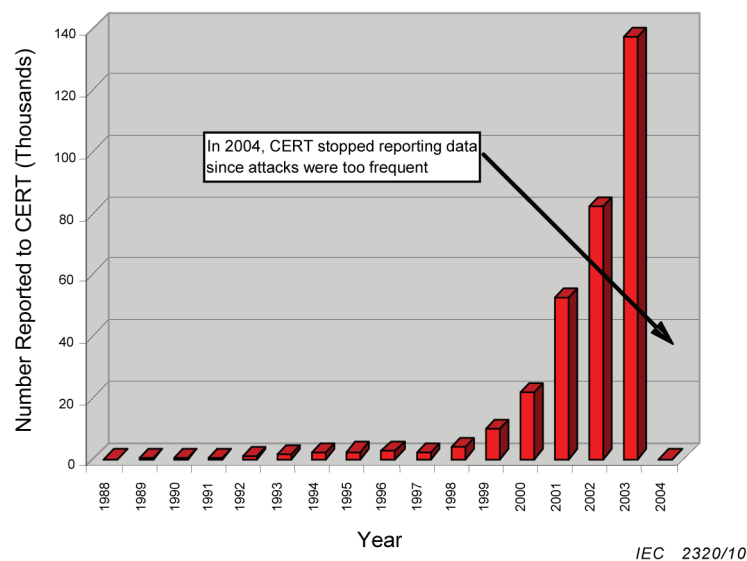


Figure A.3 — Reported attacks on computer systems through 2004 (source: CERT)

A.2.2.5 Supporting practices

A.2.2.5.1 Baseline practices

The following six actions are baseline practices:

- a) Identifying and documenting the business objectives, critical business processes and critical information technology processes. Include [IACS](#) and interfaces with value chain partners where sensitive information is transferred, stored, or processed.
- b) Identifying the dependence of the business on information technology systems. Categorize the business dependence low, medium, high, or an alternate ranking system.
- c) Identifying various damage scenarios by the loss of confidentiality, integrity or availability of information. Include the manipulation of [IACS](#) and the consequences of such actions for those businesses, which use these systems. Include [HSE](#) and operational integrity and reliability for drivers of [IACS](#). Capture risks associated with value chain and other third-party business partners. These risks often include the loss or alteration of sensitive information. An example is the interception of information associated with manufacturing products shipments, including types of materials, quantities, shipping routes, mode of transportation, and the like.
- d) Developing business impact analyses for [IACS](#) security.
- e) Developing business impact analyses for value chain or other third-party business partner.
- f) Determining the organization's risk tolerance profile defined in terms of:
 - 1) Safety of personnel (serious injury or fatality);
 - 2) Financial loss or impact including regulatory penalties;
 - 3) Environmental/regulatory consequence;
 - 4) Damage to company image;
 - 5) Impact to investment community;
 - 6) Loss of customer base or confidence;
 - 7) Impact on infrastructure.

NOTE Risk tolerance varies depending on the business. Simply put, the organization's risk tolerance is its threshold of pain. The risk tolerance may be very low (for example, a single serious injury may not be acceptable and must be addressed immediately) when it comes to safety in plant manufacturing or may be very high (for example, in terms of production loss) if the organization has multiple production sites of a commodity product. The financial impact for one business may not be appropriate for other businesses. Organizations with multiple businesses should look at the interdependencies of one business upon another when determining risk tolerance.

[IT](#) security managers typically will be familiar with the organization's risk tolerance profile for some, but not all of these consequences. Other managers who are responsible for managing the risks associated with [HSE](#) consequences will be familiar with the organization's risk tolerance profile in these areas. The overall risk tolerance profile needs to be determined by integrating information from these sources as well as those from the [IACS](#) environment.

A.2.2.5.2 Additional practices

The following three actions are additional practices:

- a) Identifying and documenting the business objectives, critical business processes, and critical [IT](#) processes. This process is best performed with a cross-section of the organization representing the functional areas, as well as the business units of the company. This group typically is chartered either by a senior executive who is responsible for the [IT](#) organization, or

by a leadership team that includes other senior executives from throughout the organization. This charter specifically includes the risk associated with [IACS](#).

- b) Developing a business impact analysis that describes the issues and consequences of inaction and benefits of action. Where practical, these actions are quantified in terms of financial impacts (that is, lost sales or fines), market impacts (that is, loss of confidence or public image), as well as [HSE](#) impacts (that is, environmental release, equipment damage and loss of life). Especially when considering consequences like public image, it is important to understand that an incident due to one particular business unit can affect the organization as a whole.
- c) Documenting and approving (by the appropriate level of management) the risks outside the scope of the [CSMS](#).

A.2.2.6 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [\[24\]](#), [\[26\]](#), [\[27\]](#), [\[30\]](#), [\[42\]](#).

A.2.3 Element: Risk identification, classification and assessment

A.2.3.1 Description of element

Organizations protect their ability to perform their mission by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. Risk is formally defined as an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence (see IEC/TS 62443-1-1). As described under the related element Risk Management and Implementation (see [A.3.4.2](#)), an organization defines its risk tolerance in terms of the characteristics of threats, vulnerabilities and potential consequences it identifies. The organization then implements this risk tolerance decision by taking action where indicated to reduce the likelihood of a security threat occurring by mitigating vulnerabilities and/or reducing the consequences in case the security threat is realized.

A.2.3.2 Cyber risk for [IACS](#)

The risk management approach outlined in [A.2.2](#) applies in general for all types of cyber risks as well as other types of risks. This discussion is about the unique aspects of the analysis of cyber risk for [IACS](#).

Although various industries may find certain types of business impact of more concern and may feel that certain types of threats are more likely, all industries that use [IACS](#) should be concerned that they are entering a new risk environment. At the same time that [IACS](#) have adopted commercial [IT](#) operating systems and network technologies and users have interconnected their private networks with their [IACS](#) networks, the number of threats has also increased greatly. There are risks associated with traditional information (electronic or paper), classical [IT](#) systems and applications, [IACS](#), business partners, joint ventures, outsourcing partners, and the like.

Risks for traditional [IT](#) assets focus on the confidentiality, integrity, and availability of information. Risks in [IACS](#) are different as the drivers focus more on [HSE](#) factors and operational reliability in addition to the traditional protection of information confidentiality, integrity and availability. In [IACS](#) the priorities are generally reversed with focus on availability, integrity and confidentiality in that order. This means that cyber risk assessment for [IACS](#) should be coordinated with physical security and [HSE](#), wherever practical. Some organizations fully integrate risk assessment efforts related to all of these areas. Risks using outsourcing, third-party contractors or other partners in the manufacturing value chain include sensitive information transmitted, stored or processed. The integration of these business partners into an organization's operations potentially permits unintentional access into the company's systems.

In virtually all of these cases, the security-related industrial operations and technologies developed for classical [IT](#) applications have not been deployed for [IACS](#) partly due to ignorance, but partly due to risk

constraints that do not exist in classical [IT](#) applications. The objective of this standard is to address both issues.

A.2.3.3 Risk assessment process

A.2.3.3.1 General

An overview of risks is required to establish the business rationale for a [CSMS](#). The more detailed priorities addressed by this system are determined based upon a methodology that systematically considers risk at a greater level of granularity than typically assessed to establish an initial business rationale.

A.2.3.3.2 Risk assessment and vulnerability assessment

In the general literature, the terms vulnerability assessment and risk assessment are sometimes used interchangeably. These two kinds of analyses can be distinguished in accordance with the definitions of vulnerability and risk in this standard. Recall that a vulnerability is defined as a flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's integrity or security policy (see IEC/TS 62443-1-1). As an example, the observation that passwords in a control center are seldom changed is an example of a vulnerability that would be identified in a vulnerability assessment. There may be several risks associated with this vulnerability, for example:

- A low likelihood that the password becomes well known in the plant over time and that a legitimate employee not trained for control system operations uses the password while pitching in to solve a problem and causes a loss of production for several hours due to input errors.
- A low likelihood that a disgruntled former employee successfully breaks through corporate firewall defences to access the control system network remotely, logs in to an [HMI](#) and deliberately takes actions that can cause a loss of production for several days.

Thus as these terms are used in this standard, risk assessment has as its output a set of risks and a vulnerability assessment has as its output a set of vulnerabilities, which have not yet been analyzed in terms of the risks they create. In this way, a vulnerability assessment is an input to a risk assessment. Note that some existing methodologies titled vulnerability assessment methods include risk concepts and others do not.

Returning to the above example of the control room password, it is clear that there are also risks involved in changing the control system password periodically, for example, a low likelihood that an operator may not remember a new password in an emergency situation and will be unable to login to resolve the situation, resulting in serious collateral environmental damage. The tradeoff between the risk addressed by a countermeasure and the risk introduced by a countermeasure such as in this case, is discussed under the Risk Management and Implementation element of this standard (see [A.3.4.2](#)).

A.2.3.3.3 High-level and detailed risk assessment

Risk assessment can be carried out at several levels. This standard requires risk assessment at two levels of detail, called high-level risk assessment and detailed risk assessment.

High-level risk assessment examines what might be the impact of general types of cyber security vulnerabilities and the likelihood that a threat might exercise these vulnerabilities, but does not consider particular instances of these vulnerabilities or related countermeasures already in place. Thus examples of risks identified in a high-level risk assessment might be:

- A medium likelihood that a malware infestation occurs and causes control network congestion and thus a lack of visibility to the status of the industrial process in the control room, resulting in potential emergency shutdown and resulting costs.

- A low likelihood that a contractor with criminal connections and with physical access to the control system network media taps this media and successfully modifies control commands in a way that causes damage to the facility.

High-level assessment is required because experience has shown that if organizations start out by looking at detailed vulnerabilities, they miss the big picture of cyber risk and find it difficult to determine where to focus their cyber security efforts. Examination of risks at a high level can help to focus effort in detailed vulnerability assessments. The high-level assessment can typically cover all control networks owned by an organization, possibly by dividing them into groups that share common characteristics. Resources may not be available to cover all [IACS](#) at the detailed level.

A detailed risk assessment, as defined for this standard, is supported by a detailed vulnerability assessment that includes examining details such as existing technical countermeasures, adherence to account management procedures, patch and open port status by individual host on a specific control system network and network connectivity characteristics such as firewall separation and configuration. Thus an example output from a detailed risk assessment might be:

- Direct connection of process engineering workstations to both the corporate network and the control system network in the South facility, bypassing the control network internal firewall, contribute to risk of malware infection on the control network. In combination with lack of antivirus protection on 50 % of the hosts on the South facility control network, this results in a medium likelihood of a virus-triggered network congestion incident causing a lack of visibility to the status of the industrial operation in the control room and resulting in potential emergency shutdown and resulting costs.
- All control system network media (for example, addresses 192.168.3.x) and connections to other networks are either physically protected by walls, ceilings or floors, or in locked rooms accessible to three authorized control system network administrators. Therefore the risk of a successful attempt at tapping this media is low.

These detailed risk assessment results support related results from a high-level assessment according to the related examples above. However, the detailed risk assessment may in many cases determine that risks are lower or higher than suspected in the high-level assessment. The detailed risk assessment may also uncover risks not considered in the high-level assessment. Finally, since the detailed assessment identifies specific vulnerabilities, it provides direction for how an organization might address risks deemed unacceptable.

A.2.3.3.4 Types of risk assessment methodologies

A.2.3.3.4.1 General

There are a variety of risk assessment methods that have been developed and marketed by different organizations. In general, these can be classified according to two factors: how they characterize the individual risks (qualitatively versus quantitatively) and how they structure the risk identification exercise (scenario-based versus asset-based).

A.2.3.3.4.2 Qualitative versus quantitative

Qualitative risk assessment typically relies on the input of experienced employees and/or experts to provide information regarding likelihood and severity of specific threats impacting specific assets. In addition, different levels of likelihood and severity are identified by general classes such as high, medium and low rather than specific probabilities or economic impacts. Qualitative risk assessment is preferred when there is a lack of reliable information regarding the likelihood of specific threats affecting specific assets or estimating the overall impact of damage to specific assets.

Quantitative risk assessment typically relies on extensive data sets that document the rate at which damage occurs to assets based on exposure to defined combinations of threats and vulnerabilities. If this information is available, it can provide more precise risk estimates than qualitative risk assessment methods. Due to the recent exposure of [IACS](#) to cyber security threats, the relative infrequency at which

incidents occur and the rapidly evolving nature of the threats, extensive data sets do not yet exist to aid in the assessment of cyber security threats to [IACS](#). At this stage, qualitative risk assessment is the preferred method for evaluating these risks.

A.2.3.3.4.3 Scenario-based versus asset-based

In conducting a risk assessment, it is usually helpful to focus the participant's thoughts along one of two lines: the scenarios by which threats take advantage of vulnerabilities to impact assets or the assets themselves. The scenario-based approach tends to take advantage of experience with actual incidents or near-incidents. However, the approach may not penetrate to discover threats or vulnerabilities to sensitive assets that have not been previously threatened. The asset-based approach tends to take advantage of knowledge of an organization's systems and work methods and particular assets whose compromise would lead to high economic impact. However, this approach may not penetrate to discover types of threats or vulnerabilities that would place these assets in jeopardy or scenarios that involve more than one asset. Whichever general approach is used, it is recommended that some aspect of the other approach be included to provide a more thorough risk assessment.

EXAMPLE An organization that has identified assets as devices, applications and data is considered as an example that integrates scenario and asset-based methods. In the next step, the organization lists possible scenarios related to these assets and determines consequences as follows. Application scenarios are very similar to the device scenarios shown.

a) Device scenarios

- 1) Scenario: Unauthorized user locally accessing an [IACS](#) device
What is the consequence of someone walking up to the device and performing the tasks allowed at this device?
- 2) Scenario: Remote access of an [IACS](#) device by an unauthorized user
What is the consequence of an unauthorized user gaining remote access to this device and performing any of the tasks allowed by this device?
- 3) Scenario: [IACS](#) device disabled or destroyed
What is the consequence of a cyber incident that blocks the device from performing all or a subset of its normal functions?

b) Data scenarios

- 1) Scenario: [IACS](#) data theft
What is the consequence of someone stealing this data set?
 - Does the data set have high intellectual property value?
 - Is the data set of business value to a competitor?
 - If publicly released, would the data set be an embarrassment to the organization?
 - Is the data set required for regulatory compliance?
 - Is the data set under a litigation hold order?
- 2) Scenario: [IACS](#) data corruption
What is the potential consequence if:
 - The data set was intercepted and changed between the source and destination?