NIST Cybersecurity Framework Core:
Informative Reference Standards

ISA 62443-2-1:2009

4/1/14

ANSI/ISA–62443-2-1 (99.02.01)–2009

(formerly designated as ANSI/ISA-99.02.01-2009)

Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program

Approved 13 January 2009

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, Annex 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. 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 in this category:

- Business rationale
- 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, health, safety, environmental, and other potential consequences should IACS cyber incidents occur.

Rationale:

Establishing a business rationale is essential for an organization to maintain management buy-in to an appropriate level of investment for the IACS cyber security program.

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 abilities to perform their missions by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. The first set of requirements presents the actions an organization takes to carry out both a high level and a 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. The last few requirements (4.2.3.10 to 4.2.3.14) are general requirements that apply to the overall risk assessment process. Section 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:

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 its 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 industrial automation and control systems**	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.

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 abilities to perform their missions by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. The first set of requirements presents the actions an organization takes to carry out both a high level and a 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. The last few requirements (4.2.3.10 to 4.2.3.14) are general requirements that apply to the overall risk assessment process. Section 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:

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 its 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 industrial automation and control systems**	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.
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 three element groups:

- Security policy, organization and awareness
- Selected security countermeasures
- 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 entities responsible for cyber security, and the awareness within the organization of cyber security issues. Figure 3 depicts the five elements in the element group:

- CSMS scope
- Organizing for security
- Staff training and security awareness
- Business continuity plan
- Security policies and procedures

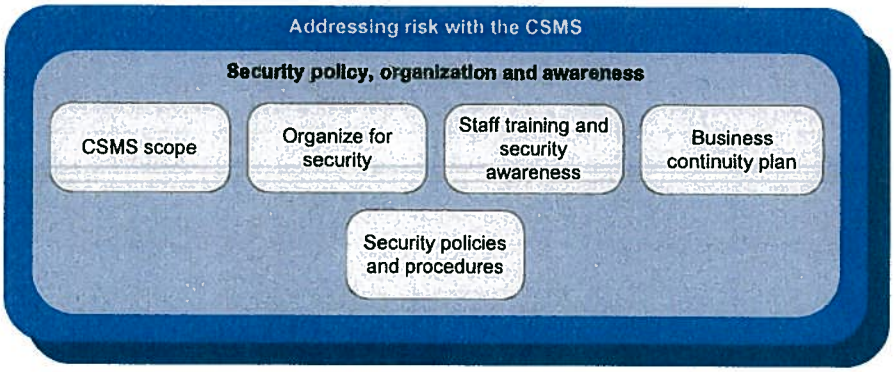

Figure 3 – Graphical view of element group: Security policy, organization, and awareness

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, including 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:

	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 skill sets 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 people 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:

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 industrial automation and control systems, 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:

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

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.
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 others to clearly understand a company's perspective of cyber security and their roles and responsibilities in securing the company's assets.

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.
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
- Access control: Authorization

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.
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
- Access control: Authorization

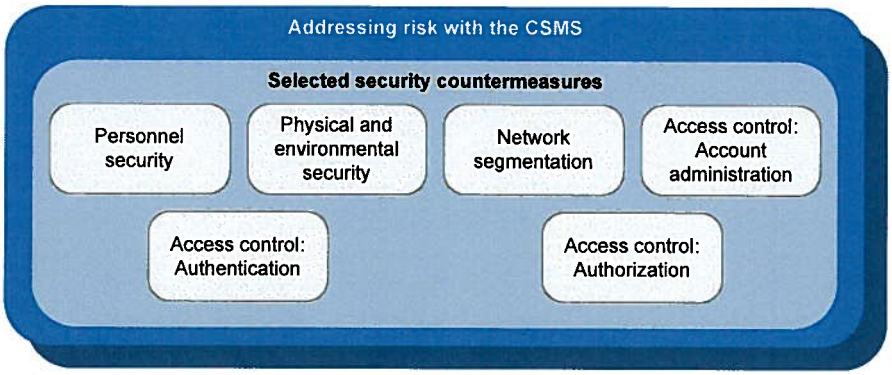

Figure 4 – Graphical view of element group: Selected security countermeasures

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:

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 an employee'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 among 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 ANSI/ISA–99.01.01–2007). 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 an end in themselves. In modern control systems the physical assets provide the means by which the cyber system operates. Therefore, the assets have value in themselves, but also as integral parts of the control system. Since both the assets and the control system require each other, both must 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:

Description		Requirement
4.3.3.3.1	**Establish complementary physical and cyber security policies**	Security policies and procedures shall be established that address both physical and cyber security in the protection of assets.
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, or 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 a network barrier device. IACS should be designed in a manner that filters/removes nonessential communication packets from reaching the IACS devices.

For transmission control protocol / internet protocol (TCP/IP) based networks, the most common barrier devices currently 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:

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 which 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 must 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 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:

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 which resources can access premises and systems and which type of access is permitted. There are three key aspects associated with access control: account administration, authentication, and authorization. All three aspects must 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 those of other users; and remote users are typically not subject to complementary physical access controls. Automatic account lockout 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 typically is great emphasis on combining physical authentication measures with electronic authentication practices.

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 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 he or she 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 his or her 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 which resources can access premises and systems and which type of access is permitted. There are three key aspects associated with access control: account administration, authentication, and authorization. All three aspects must 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 jobs due to lack of authorization. Authorization to perform specific job functions is provided by the application. Safety implications must be considered when developing the authorization strategy.

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 depicts the four elements in the element group:

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

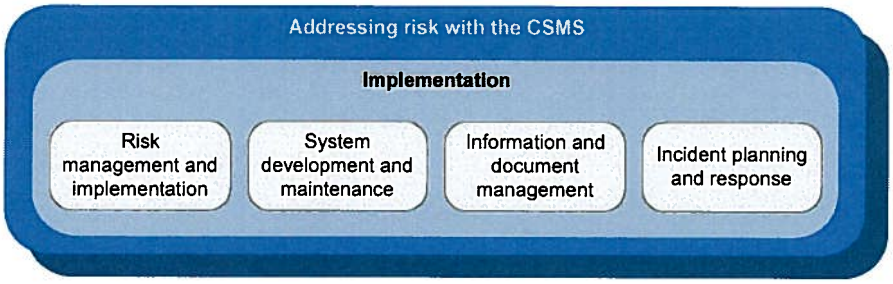

Figure 5 – Graphical view of element group: Implementation

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 use of products with strong inherent security capabilities, manual and procedural security controls, and technology-based controls to prevent or reduce security incidents.

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 depicts the four elements in the element group:

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

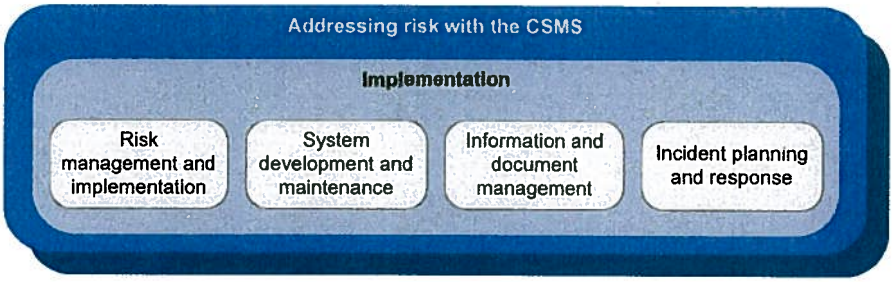

Figure 5 – Graphical view of element group: Implementation

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 use of products with strong inherent security capabilities, manual and procedural security controls, and technology-based controls to prevent or reduce security incidents.

Rationale:

For the results from the risk identification classification and assessment element of this standard to be useful, they must be effectively turned into concrete actions under the risk management and implementation element. Although never totally eliminated, risk can be managed in a manner that balances the cost of risk avoidance to the potential cost of the incident.

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 and 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 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:

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 the 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:

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, or 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 consequences of 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 classifications, 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 per the established company practice. 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:

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 monitoring and improving the CSMS. It involves both ensuring that the CSMS is being used, and reviewing the CSMS itself for effectiveness. Figure 6 depicts a graphical representation of the two elements in the category:

- Conformance
- 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:

Regardless of the quality of a CSMS, if it is not used it does not add any value to the organization and does not help reduce risk.

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 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 must 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:

	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.

4.4.2.5	**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 must 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:

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.