CHEMICAL INDUSTRY DATA EXCHANGE

CIDX®

By the Industry....For the Industry

Guidance for Addressing Cybersecurity in the Chemical Sector

Version 2.0

December 2004

Legal and Copyright Notice

Table of Contents

NOTE: Attachment I – Key Element Examples is available to CIDX members only. Information on how to obtain is available via the CIDX web site (www.cidx.org).

1 Executive Summary

This guidance document is designed to educate and inform member companies, customers, and the public about cybersecurity in the chemical sector. It presents a cybersecurity management system (CSMS) that addresses manufacturing and control systems, information technology (IT) systems, and the value chain.

The intended audiences for this guidance are IT security professionals in the chemical or related sectors, manufacturing and control systems engineers, designers, security professionals, chief information officers (CIOs), and company executives responsible for the overall company security and viability.

There are two special features: a collection of self-assessment questions and examples of how chemical companies are implementing cybersecurity practices. The self-assessment questions allow users to evaluate their company's compliance with the cybersecurity guidance provided. The self-assessment questions are located in an appendix. The examples provide practical experience of how companies in the chemical sector are implementing cybersecurity practices. The examples are located at the CIDX website.

Information and guidance is provided to assist any company participating in the chemical sector value chain in implementing a CSMS and controls. The document is meant to stimulate thinking and provide resources that a company can use as it determines its approach to implementing corporate security management practices throughout its information systems and manufacturing and controls systems. The cybersecurity activities should be integrated into a company's security program.

The document structure is consistent for each of the cybersecurity management system elements. For each element, the following sections are provided: introduction, statement of management practice, applicability to the chemical sector, baseline practices, how companies are approaching the topic, a list of examples, and a list of the resources used to support the topic.

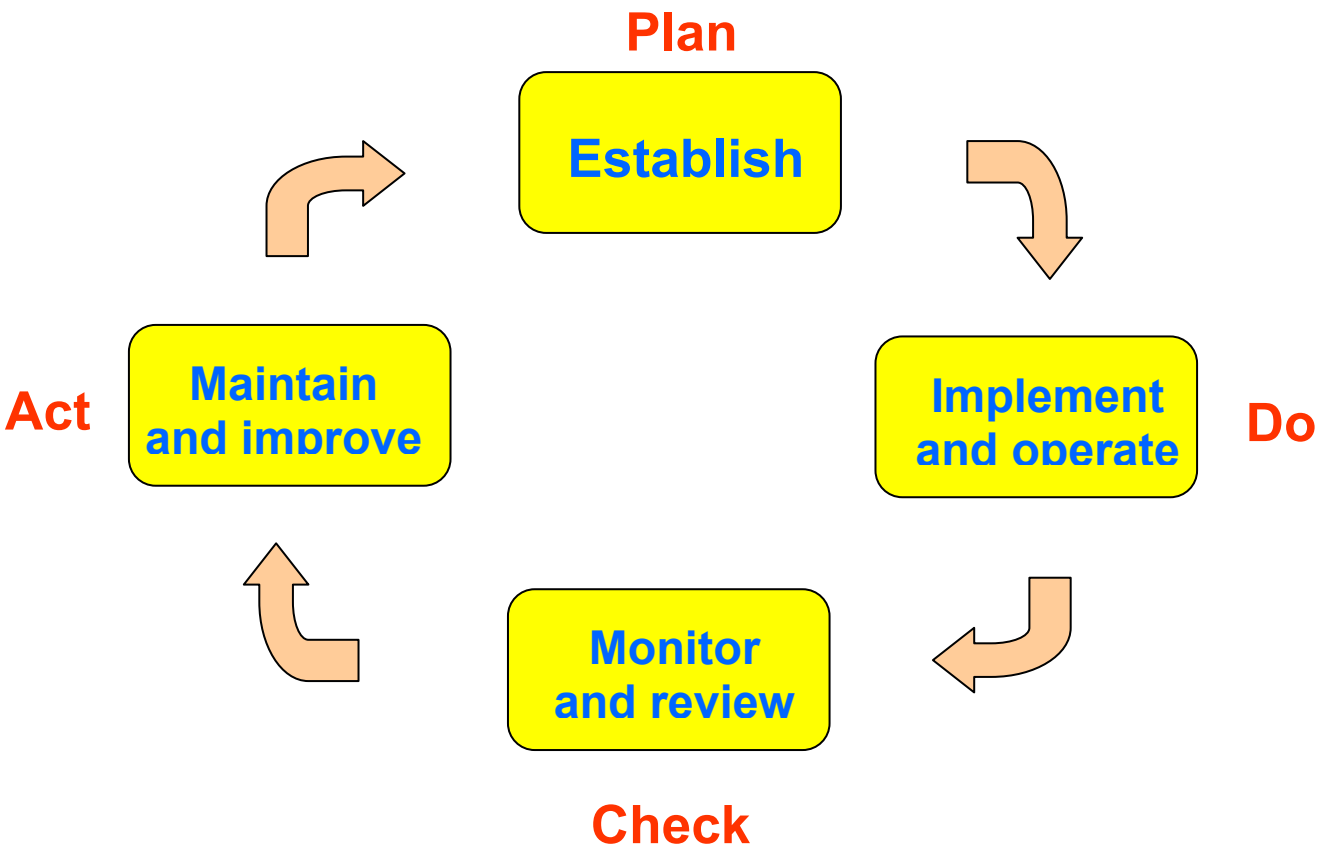
These elements cover the various activities that must be included in order to comprehensively manage cybersecurity. Management systems require that policies, procedures and guidelines be developed, roles and responsibilities assigned, and resources allocated. The heart of a management system is the Plan-Do-Check-Act (PDCA) cycle (see Figure). Its four phases are:

Plan: Establish policy, objectives, targets, requirements, and procedures.

Do: Implement and operate the management system and its processes.

Check: Monitor, assess and measure performance and report results to management for review.

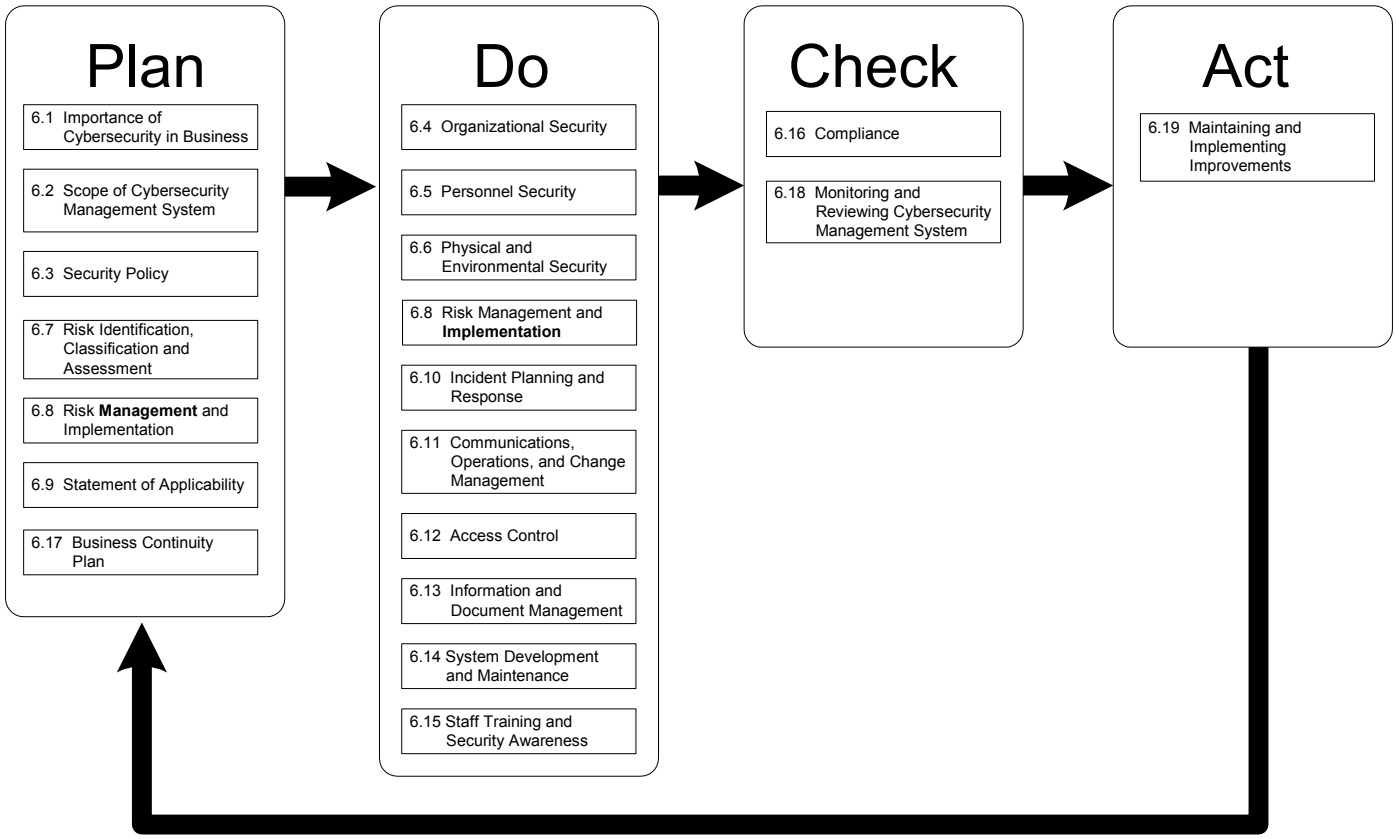
Act: Take corrective and preventive actions and continually improve performance.



They are conducted as a continuous cycle because its purpose is to ensure that best practices of the organization are documented, reinforced and improved over time. The key feature of the PDCA cycle is that it provides feedback on performance so that corrective actions can be taken.

Management systems can be applied to any organization regardless of its type, size, or business. The level of detail, extent of documentation, and resources required depend on the size of the organization and the nature of its activities. Management systems do not specify performance levels. Their intention is to provide a framework for an overall, strategic approach to an organization's policy, plans, and actions for performance.

The cybersecurity management system presented here uses elements of the BS 7799-2:2002, *Information security management systems – Specification with guidance for use*, which is a management system for information security. It also incorporates elements of ISO/IEC 17799, *Information Technology – Code of Practice for information security management*. The CSMS provides for comprehensive management of cybersecurity. It is an overall management system framework that allows organizations adopting the CSMS to tailor it to their own specific needs.



There are 19 elements in the CSMS. The following is a brief summary of the 19 key elements of the management system:

Importance of Cybersecurity in Business states that it is important to establish that the company is aware of and that it understands the importance of its business(es) in relation to information technology (IT) and IT risks. This extends to manufacturing and control systems, value chain operations, joint ventures, third parties, outsourcing partners, as well as business related IT activities.

Scope of Cybersecurity Management System (CSMS) addresses that management consciously determine the scope of their CSMS. The scope can include all aspects of their business information systems, manufacturing and control systems, integration points with business partners, customers, and suppliers. A management framework (i.e., organization) can be established to initiate and control the implementation and ongoing operations of cybersecurity within the company.

Security Policy addresses senior leadership commitment to continuous improvement through published policies. The policies should be provided to employees and reviewed regularly to ensure it remains appropriate.

Organizational Security addresses establishing an organization, structure, or network with responsibility for overall security recognizing there are physical as well as cyber components to be addressed. Organizational security requires that accountability be established to provide direction and oversight to a company's cybersecurity. Cybersecurity in the broadest sense covers not only data but also systems (hardware and software) that generate or store this information and includes elements of physical security as well. Manufacturing and control systems specialists, value chain partners, third party contractors, joint venture partners, outsourcing partners, and physical security specialists can be considered by the organization as part of the overall security structure, and hence included in the scope of responsibility.

Personnel Security addresses security responsibilities at the recruitment phase, include these responsibilities in all contracts, and monitor during an individual's employment. Recruits should be screened especially for sensitive jobs. Companies may consider having all employees and third party users of information processing facilities sign a confidentiality or nondisclosure agreement.

Physical and Environmental Security addresses protecting tangible or physical assets (e.g., computers, networks, manufacturing processes equipment, etc.) from damage, loss, unauthorized access or misuse. Critical information or assets should be placed in a secure area, protected by security perimeter and entry controls. These physical security controls work in conjunction with cybersecurity measures to protect information.

Risk Identification, Classification, and Assessment states that by identifying, prioritizing, and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies companies protect the organization and its ability to perform their mission.

Risk Management and Implementation addresses developing and implementing security measures that are commensurate with risks. The security measures may take into account inherently safer approaches to process design, engineering and administrative, manual and procedural, controls, and prevention and mitigation measures. The importance of the risk mitigation is to convert all the risk management plans into actions and have a program plan in place to monitor effectiveness.

Statement of Applicability (SOA) addresses documenting the results for each of the security controls as well as elements of the security controls. Documented results aid in the decision making process, facilitate the communication of the decisions, provide a basis for training and education, responses to incidents and threats, and provide a basis for subsequent self-assessment or auditing of the compliance with these security controls.

Incident Planning and Response addresses the need to be vigilant in efforts to deter and detect any cybersecurity incident. If an incident occurs, the company needs to promptly respond and involve government agencies as appropriate. After investigating the incident, the company may consider incorporating key learnings and, if appropriate, share those learnings and with others in the industry and government agencies and implement corrective actions.

Communications, Operations, and Change Management addresses processes and procedures being developed and followed to sustain the security of computer systems and information processing facilities. These overall management practices/procedures should clearly articulate all the operational security aspects. The need to address security is very strong in the manufacturing and control systems that are used to operate our facilities because security lapses have the potential to result in safety, health, or environmental issues.

Access Control addresses account administration, authorization, and authentication. Account administration should establish rules to ensure that users' access to systems and data is controlled. There are rules that are enforced administratively and those that are enforced automatically through the use of technology. Both kinds of rules need to be addressed as part of the overall access control strategy. Authorization addresses the need for businesses to establish and employ a set of authentication practices commensurate with the risk of granting unauthorized users, hosts, applications, services, and resources access to critical system resources. Authentication describes the process of positively identifying network users, hosts, applications, services, and resources for some sort of computerized transaction using a combination of identification factors or credentials. Authentication is the prerequisite to allowing access to resources in a system.

Information and Document Management addresses processes associated with the classification of all data and the safeguarding of information and document management associated with a cybersecurity management system. Document management is generally a part of the company records retention and document management system.

System Development and Maintenance addresses security being built into the information system and sustained through normal maintenance tasks.

Staff Training and Security Awareness states that management commitment is critical to providing a stable computing environment for both information and manufacturing and control systems. Effective cybersecurity training and security awareness programs provide each employee with the information necessary to identify, review and remediate control exposures, and helps ensure their own work practices are utilizing effective controls.

Compliance addresses scheduling and conducting audits, and compliance with legal, regulatory, and security requirements. It states that companies should periodically assess their security programs and processes to affirm those programs and processes are in place and working and corrective actions are taken as appropriate. In appropriate circumstances, assessments also apply to the programs and processes of other companies with whom the company conducts business such as chemical suppliers, logistics service providers, joint ventures, or customers. To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and security requirements, a validation or audit for compliance may be necessary. To ensure the security and safe operation of its assets, a validation or audit for compliance to corporate security policies and practices may be necessary.

Business Continuity Plan addresses providing a course of action to respond to the consequences of disasters, security failures, and loss of service to a business. Contingency plans need to be developed, implemented, and tested to ensure that business processes can be restored in a timely fashion.

Monitoring and Reviewing CSMS addresses continuous monitoring and reviewing the management system. Monitoring and reviewing performance of a company's management system provides the checks and balances the company has in place to monitor and evaluate its performance. Internal checking methods such as auditing of the management system; compliance audits; and incident investigations allow the company to determine the effectiveness of the management system and whether it is operating according to expectations. Finally, through a management review process, the company's senior leaders review information on the management system, developed through the measurement and corrective action process, and any deviations from the goals, targets, and objectives set in the planning process. If there are deviations or nonconformance, a revisit of the original assumptions and appropriate corrective actions may be necessary.

Maintaining and Implementing Improvements states that it is important to maintain and implement improvements of the CSMS. Since practices for addressing security are evolving, it is anticipated that company security programs and measures will evolve, reflecting new knowledge and technology. Companies should continually be tracking, measuring, and improving security efforts to keep people, property, products, processes, information, and information systems more secure.

2 Background

This project was chartered in late 2003 under the auspices of the Chemical Industry Data Exchange (CIDX). It aligns with the *U.S. Chemicals Sector Cyber-Security Strategy*. The purpose of this effort is to provide guidance to the chemical sector in the implementation of appropriate controls. In a broader sense, the guidance provided is aimed at helping sector companies incorporate sound cybersecurity practices into their overall product stewardship program. This document supersedes the previous version: *Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0*. Version 2.0 is written for the chemical sector and to be accepted globally. The framework is structured around industry standards.

3 Introduction

The chemical sector provides the essentials of modern life. Because the sector touches so many aspects of how we live our lives and how business is conducted throughout the world, communications technology, connectivity, and information exchange are essential aspects of all company operations and processes in the sector. However, the same technologies that make business operations and manufacturing processes more efficient can introduce new vulnerabilities. As the world faces increased threats, the chemical sector needs to increase its capability to manage exposure to cybersecurity risk and protect against the threat of unauthorized access to information being used to facilitate or cause a physical attack or disruption in the supply chain.

Cybersecurity is an integral part of overall chemical sector security, and the industry is addressing the risk as a sector-wide initiative, to minimize the potential impact to both public safety and the economy.

Reducing current and future cybersecurity risks requires a combination of leading edge technology, accepted sector practices, and timely information sharing throughout the sector. This type of sector-wide cooperation to address cybersecurity issues has many precedents in the chemical sector.

Established, proven programs are in place to help the sector confront the current threat. One example is an emergency communications network to global industry associations. Another example is the existence of standards bodies that provide groundwork for improving current security processes and establishing better cybersecurity practices for the future. The sector's culture of safety gives the industry an added advantage – from its longstanding voluntary initiatives to its adherence to governmental standards, support for research and effective partnerships with local, state, and federal government agencies.

CIDX is the standards body engaged to develop cybersecurity chemical sector guidance and practices, and encourage acceleration of improved security technology and solutions development. CIDX recognizes that *ISO/IEC International Standard 17799*, *British Standard 7799: 2 2002*, ISA-*TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems*, and *ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment* are frameworks important to the chemical sector. They have been used as reference material in the development of this guidance document as the first voluntary guidance for companies in the industry to follow in devising risk-based cybersecurity plans for their organizations. The *ISO/IEC International Standard 17799, Information Technology – Code of Practice for Information Security Management*, provides a comprehensive set of controls comprising the best practices in information security. The *British Standard 7799: 2 2002* is also used as a road map for structuring this document. Elements of the *ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems* were used for security controls, and elements of *ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment* were used for the management system content of this document.

This guidance document has been prepared for companies to use as a resource to address cybersecurity-related issues as they work to develop and implement corporate security practices. It also provides guidance on the implementation of security measures to company manufacturing and control systems and information technology systems. The *ISO/IEC International Standard 17799, Information Technology – Code of Practice for Information Security Management*, and the *BS 7799-2:2002* describes a possible framework for creating a cybersecurity program that forms the basis of guidance provided. The guidance provided herein does not attempt to provide an all-inclusive list of cybersecurity considerations, but does provide a framework that could be used when implementing a cybersecurity program. For purchasing information, see the web site addresses provided: ISO/IEC 17799 and BS 7799-2:2002 (www.bsi-global.com/index.xalter), ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems (www.isa.org), and ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment (www.isa.org). A discount is available for CIDX members to purchase the ISA technical reports via the web site (www.cidx.org).

For ease of integration of cybersecurity considerations with overall security activities, this guidance document is aligned with the chemical sector product stewardship programs such as American Chemistry Council's Responsible Care® Security Code of Management Practices (www.americanchemistry.com).

4 Purpose and Scope of this Document

The purpose of this document is to provide information and guidance to assist any company participating in the chemical sector value chain in implementing cybersecurity management system and controls. It is suggested that cybersecurity activities be integrated into a company's security program. Therefore, this document describes activities relating to cybersecurity only, with the expectation that these activities can be integrated into a company's entire security program. This document provides guidance on how to implement the practices and controls in a manner that addresses both information systems and manufacturing and control systems within companies. The document does not describe a one size fits all approach. The document is meant to stimulate thinking and provide resources that a company can use as it determines its approach to implementing corporate security management practices throughout its information systems and manufacturing and controls systems. Companies should look holistically at their security programs to ensure that cybersecurity activities are included.

The scope of this document covers traditional IT assets as well as manufacturing and control systems and is applicable to the chemical sector value chain components. For additional information concerning value chain components, refer to www.cidx.org/CyberSecurity/publications/default.asp. A CIDX team comprising members with diverse backgrounds was formed to address this issue.

The intended audiences for this guidance are IT security professionals in the chemical or related sectors, manufacturing and control systems engineers, designers, security professionals, CIOs, and company executives responsible for the overall company security and viability.

5 Anticipated Benefits

The mission of the Chemicals Sector Cybersecurity Program is cybersecurity risk management and reduction to provide open, secure information systems and manufacturing and control systems that help protect employees and communities, and enable collaborative business operations. This section describes potential benefits of implementation of the guidance provided in this document.

Companies receive the greatest amount of benefit when a holistic, management system approach is implemented. This Guidance does not necessitate new stand-alone programs, but rather, suggests reliance upon and adaptation to other management systems. The fundamental objective is to use familiar management systems to enhance cybersecurity. Through an integrated approach, indirect benefits can be anticipated. The chemical sector contains unique characteristics of manufacturing and control systems and information systems. Those two characteristics combined with the value chain create a potential physical security impact.

For specific examples of the benefits of cybersecurity, see the business cases for cybersecurity: A Case for Taking Action on Cybersecurity and Addressing Cybersecurity in Process Control.

6 The Key Elements

Each section consistently follows this structure for the cybersecurity key elements:

- ***Introduction***- describes the topic along with citing the appropriate reference documents.
- ***Statement of Management Practice*** identifies the scope and objectives of the key elements.

- ***Applicability to Cybersecurity in the Chemical Sector*** describes the objective in relevant terms for the chemical sector focusing on applicability to traditional IT assets, manufacturing and control systems and chemical sector value chain components.
- ***Baseline Practices*** are used to outline recommendations for chemical sector companies to achieve a baseline level of cybersecurity. Here the authors seek to identify the building blocks of the key elements.
- ***How Chemical Companies Are Approaching [the topic]*** builds upon the baseline practices and describes some of the innovative approaches chemical sector companies are using to further enhance cybersecurity.
- ***Examples*** includes a list of "sanitized" policies, procedures, and case studies for CIDX members only. A link is provided on the CIDX web site to the actual examples attachment. The goal, although not achieved in each section was to provide a range of examples that are representative of the diversity of the chemical sector in terms of size, region and level of complexity of operation. The list of examples reflects what was available at the time of publication. Additional examples may be subsequently added in the attachment document.
- ***Resources Used*** lists sources for additional information as well as documents referenced are included.

6.1 Importance of Cybersecurity in Business

This section describes practical guidance on how to establish the importance of cybersecurity in business as covered in BS 7799-2:2002. Sections 0.2 and 4.2.

6.1.1 Statement of Management Practice

Establish that the company is aware of and understands the importance of their business(es) in relation to information technology (IT) and IT risks. This extends to manufacturing and control systems, value chain operations, joint ventures, third parties, outsourcing partners, as well as business related IT activities.

6.1.2 Applicability to Cybersecurity in the Chemical Sector

There are risks associated with traditional information, IT assets, manufacturing and control systems, business partners, joint ventures, outsourcing partners. Risks are also associated with a host of other business arrangements that are increasingly prevalent in the chemical sector. Risks for traditional IT assets focus on the confidentiality, integrity, and availability of information. Risks in manufacturing and control systems are different as the drivers focus more on safety and operational reliability in addition to the traditional protection of information confidentiality, integrity, and availability. Risks using outsourcing, third party contractors, or other partners in the chemical sector value chain include sensitive information transmitted, stored, or processed. The integration of these business partners into a company's operations potentially permits unintentional access into the company's systems.

It is critical to establish and understand the value proposition related to the company IT resources and investment. Establishing a cybersecurity management system (CSMS) requires an understanding of the roles that IT plays in the business of a company. Key in the CSMS is the need to define the company's risk tolerance and the benefits of a CSMS that identifies potential cybersecurity risks, consequences and controls and establishes a process to implement, operate, monitor, review, maintain and improve cybersecurity.

6.1.3 Baseline Practices

Example baseline practices that chemical companies use to establish the importance of information security in business include:

- Identifying and documenting the business objectives, critical business processes and critical IT processes. Include manufacturing and control systems and interfaces with value chain partners where sensitive information is transferred, stored or processed.
- Identifying dependence of the business on IT systems. Categorize the business dependence low, medium, high, or an alternate ranking system.

- Identifying various damage scenarios by the loss of confidentiality, integrity or availability of information. Include the manipulation of manufacturing and control systems and the consequences of such actions for those businesses, which use these systems. Include safety and operational integrity and reliability for drivers of manufacturing and control systems. 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 chemical shipments, including types of chemicals, quantities, shipping routes, mode of transportation, etc.
- Developing business impact analyses for information system security
- Developing business impact analyses for manufacturing and control system security
- Developing business impact analyses for value chain or other third party business partner
- Establishing a risk tolerance profile for the organization defined in terms of:
  - Safety of personnel (serious injury or fatality)
  - Financial loss or impact including provisions in Sarbanes Oxley
  - Environmental/regulatory consequence
  - Damage to company image
  - Impact to investment community
  - Loss of customer base or confidence
  - Impact on infrastructure

Note the risk tolerance varies depending on the business. Simply put the company's risk tolerance is its threshold of pain. The 'risk tolerance' may be very low (e.g., 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 (e.g., in terms of production loss) if the company has multiple production sites of a commodity chemical. The financial impact for one business may not be appropriate for other businesses. However, while there may be differences, a consolidated standard (even if it is a range) is the recommended approach. Companies with multiple businesses look at the interdependencies of business upon another when determining risk tolerance.

6.1.4 How Chemical Companies Are Approaching the Importance of Cybersecurity in Business

Examples of how chemical companies are establishing the importance of cybersecurity in business include:

- Identifying and documenting the business objectives, critical business processes, and critical IT processes. This is best done with a cross section of the organization representing the functional areas as well as the business units of the company. This group is chaired by a senior executive responsible for the IT organization and includes other senior executives from throughout the organization.
- Identifying dependence of business on IT systems. Categorize the business dependence low, medium and high or alternate ranking system. The ad hoc group described above would be responsible for these tasks.

- Identifying various damage scenarios by the loss of confidentiality, integrity, availability of information, operational reliability, or safety. This could be based on experience, published cases/incidents for your industry. Categorize from low, medium, and high. Higher risk requires more protection. Bringing in a security expert adds significantly to this step and providing a third party (and perhaps more objective) perspective of the scenarios and consequences.
- Analyzing the data and determining what are acceptable risks and the appropriate time period for action. This forms the basis of a risk tolerance profile. As risk assessments are completed, the risk tolerance profile helps determine which risks are addressed and the relative priority for addressing them.
- Developing a business impact analyses that describes the issues and consequences of inaction and benefits of action. If at all possible these actions are quantified in terms of dollars, lost sales, system or plant downtime, environmental, operational reliability and safety (in the case of manufacturing and control systems). Note that the impact on the collective company (e.g., unintended consequences of poorly managed devices, safety issues of one site and the public image impact on the company as a whole) are considered.
- Documenting and approving (by the appropriate level of management) the remaining risks that cannot be remedied.
- Defining the business impact that helps to validate where and how companies spend their money.

6.1.5 Examples

There are currently no examples available for this publication.

6.1.6 Resources

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Sections 0.2 and 4.2
- *U.S. Chemicals Sector Cyber-Security Strategy*, June 2002
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6
- CIDX Cybersecurity Guidance for Risk Assessment Version 2.0
- Sarbanes – Oxley website at www.sarbanes-oxley.com

6.2 Scope of Cybersecurity Management System

This section describes practical guidance for defining the scope for a cybersecurity management system (CSMS) as covered in BS 7799-2:2002, Section 4, annex B. The CSMS defines the security policy, objectives, targets, processes, and procedures relevant to managing risk and improving cybersecurity so that information technologies deliver results in accordance with the organization's overall policies and objectives.

6.2.1 Statement of Management Practice

Management should consciously determine the scope of their CSMS. The scope should include all aspects of their business information systems, manufacturing and control systems, integration points with business partners, customers, and suppliers. A management framework (i.e., organization) should be established to initiate and control the implementation of cybersecurity within the company.

6.2.2 Applicability to Cybersecurity in the Chemical Sector

An organization responsible for determining and communicating corporate policies as they relate to cybersecurity is key to protect corporate assets from a cybersecurity perspective. Companies need to recognize that in today's Internet-driven business world, electronic information connectivity is an integral part of doing business, and thus cybersecurity is essential. Business transactions are not contained within the company's information technology (IT) firewall, but are extended to customers, vendors, third-party contractors, and outsourcing partners.

6.2.3 Baseline Practices

Example baseline practices that chemical companies use to define CSMS scope include:

- Describing the organization responsible for the establishment, communication, and monitoring of cybersecurity within the company.
- Stating the scope of the CSMS can include the following:
  - Information systems - including all operating systems, data bases, applications of the company, including joint ventures, and other third party business activities.
  - Manufacturing and control systems - - including all process control systems, Supervisory Control And Data Acquisition (SCADA), Programmable Logic Controller (PLC), Distributed Control System (DCS), configuration workstations and plant or lab information systems for both real-time and historical data.
  - Networks, local area networks (LANs), wide area networks (WANs) - including hardware, applications, firewalls, intrusion detection systems
  - Integration points with value chain partners
  - User responsibilities - including policies to address authentication and auditability
  - Information protection - including access requirements and individual accountability
  - Risk management - including processes to identify and mitigate risks, and document residual risk
  - Disaster recovery - including identification of critical software/services
  - Training requirements
  - Compliance and audit

  - Asset identification
- Characteristics associated with the organization responsible for CSMS, include:
  - Organization structure
  - Location
  - Budget
  - Roles and responsibilities associated with the CSMS processes.

6.2.4 How Chemical Companies Are Approaching the Scope of Cybersecurity Management System

Examples of how chemical companies are defining CSMS scope include:

- Having management endorse the scope and responsibilities of the CSMS.
- Having a clear understanding of the roles and responsibilities associated with the organization responsible for the CSMS, and well as the rest of the company.
- Documenting the scope of the CSMS with separate sections addressing specific components (see 6.2.3 Baseline Practices)
- Addressing business, legal (e.g., Data Privacy), or regulatory requirements and responsibilities.
- Having a list of criteria against which risk is evaluated along with the structure of the risk assessment. (See section 6.1 Importance of Cybersecurity in Business – Baseline Practices for list, and see Examples.)
- Identifying and documenting the dependency of process safety on cybersecurity and physical security practices and procedures including a framework for organizational interaction.

6.2.5 Examples

There are currently no examples available for this publication.

6.2.6 Resources Used

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 4, annex B
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6
- Section 6.1 Importance of Information Security in this document
- Section 6.4 Organizational Security in this document

6.3 Security Policy

This section describes practical guidance of a comprehensive cybersecurity policy as covered in ISO Security Policy, section 3.

6.3.1 Statement of Management Practice

Senior leadership should have commitment to continuous improvement through published policies that are provided to employees, contractors, and third-parties. The policies should be reviewed regularly to ensure they remain appropriate.

6.3.2 Applicability to Cybersecurity in the Chemical Sector

Leadership commitment relating to security policy activities involves company leadership recognizing security policy as a business responsibility shared by all members of the management team and as a policy that includes physical and cyber components. Companies develop their overall policies and activities including security policy issues. These activities include information systems and manufacturing and control systems, as well as connectivity with business partners, customers, suppliers and other third party entities. Development and implementation of security policies and activities involve senior leadership commitment from all areas of the company with responsibility for these types of systems, and include joint venture operations and outsourcing. Security policy needs to be incorporated into the overall business policies and strategies and have visible, top-level support.

6.3.3 Baseline Practices

Example baseline practices that chemical companies use to "define security policy" include:

- Management commitment, involvement, and support in the creation and enforcement of policies.
- Review by all affected business units and departments, including manufacturing management.
- A published document that describes the values and policy of the company.
- Regular validation and confirmation that policies are up to date and being followed.
- Communication and dissemination of information to employees.

6.3.4 How Chemical Companies Are Approaching Security Policy

Examples of how chemical companies are defining their security policy include:

- Creating consistent policies with a 3-5 year lifecycle. The policies are neither changed constantly nor are they changed in reaction to "hot topics."
- Creating security policies to address a number of security concerns, to mitigate risks, or change human behavior.
- Aligning the security policy with the corporate American Chemistry Council's Responsible Care® program or overall corporate policies and strategies.

- Integrating the cybersecurity policy with or a part of an overall security policy that addresses physical elements too.
- Identifying how the policy is enforced, and by whom.
- Identifying how users need to comply with the provisions of the policy.
- Providing a consistent policy management framework.
- Knowing what policy applies to users or user groups.
- Identifying how to measure policy compliance requirements.

During the creation of a policy for cybersecurity, the enforcement must be defined (e.g., Intranet publishing, additional user training and education, and user sign off for understanding). Once the enforcement is defined, there needs to be compliance. Automation is the preferred approach. For example, automation can be used to avoid the need for users to encrypt messages before they are sent via the Internet.

Integration of a consistent policy management framework is essential. The policy management framework consists of people, roles, processes for identification, development and review, and communication and enforcement mechanisms. For example, key roles like sponsor, owner, custodian, subject matter expert, and stakeholder are created. Also, a template with help functions on how a policy statement must be structured with definitions on content and details is created. Not all policies or statements are applicable to all users. Dividing users into groups or roles improves the direct alignment between policy and user. Possible roles or groups for cybersecurity identified are general user, operations, system managers, and executives.

A yearly survey or a questionnaire on knowledge and user compliance on policy statements is one example of how to measure policy compliance. Additional ways to measure policy compliance requirements include identifying any classes of systems or users where special requirements may apply, and explaining how these are addressed by the security policy. Physical access control or password restrictions may not be feasible or practical (from a safety or operations point of view) for some process control systems. Exceptional procedural safeguards may be required to compensate.

6.3.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Internet Access Policy
- E-mail
- Virus protection
- Data classification
- Physical Access Control Administrative Policy
- Physical Security IT Policy

6.3.6 Resources Used

The following are resources used in the creation of this section:

- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 3
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6 and Annex A
- SANS web site (www.sans.org) for Cybersecurity policy primer and samples
- *U.S. Chemicals Sector Cyber-Security Strategy*, June 2002
- Guidance for Cybersecurity Vulnerability Assessment Methodology Process Version 1.0, available from CIDX at www.cidx.org

6.4 Organizational Security

Organizational security includes both cyber and physical aspects. Companies should establish an organization, structure, or network with responsibility for overall security recognizing there are physical as well as cyber components that should be addressed. This section describes practical guidance of the ISO/IEC 17799, Section 4 and includes appropriate input from ISA-TR99.00.02-2004 to address both traditional information technology (IT) and manufacturing control systems.

Organizational security requires that accountability be established to provide direction and oversight to a company's cybersecurity. Cybersecurity in the broadest sense covers not only data but systems (hardware and software) that generate or store this information and includes elements of physical security as well. Manufacturing and control systems, value chain partners, third party contractors, joint venture partners, outsourcing partners, and physical security specialists should be considered by the organization as part of the overall security structure, and hence included in the scope of responsibility.

6.4.1 Statement of Management Practice

A management framework should be established to initiate and control the implementation of an overall security program. The scope and responsibilities on cybersecurity for organizations should include physical security and information security for information systems, manufacturing and control systems, third party contractors, outsourcing partners, and the value chain components of the organization. An overall security program should be extended to include joint venture operations.

6.4.2 Applicability to Cybersecurity in the Chemical Sector

Companies establish a framework with management leadership to approve cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity across the organization. This is not limited to traditional IT systems, but rather extends to manufacturing and control systems and the company's value chain as well. A holistic approach is employed that seeks out and uses security specialists from outside the company, in conjunction with company resources, to collaborate on cybersecurity. The chemical sector has increasing electronic interdependence among trading partners, joint venture operations, distribution and production systems, transportation, third party contractors, and outsourcing partners.

6.4.3 Baseline Practices

Example baseline practices that chemical companies use for organizational security include:

- Personnel are assigned responsibility for information and systems security, and an appropriate level of funding to implement.
- Executive management has commitment.
- A company-wide security team (or organization) provides clear direction, commitment, and oversight. The team can be an informal network, organizational, or hierarchical structure. This team assigns responsibilities and confirms that processes are in place to protect company assets and information.

- Contracts exist that address information and system security for business partners, third party contractors, and outsourcing partners, etc.
- Metrics for organizational success are established.
- Coordination with or integration with the physical security organization exists that addresses security recognizing the overlap and synergy between physical and information systems security risks.

6.4.4 How Chemical Companies Are Approaching Organizational Security

Some examples of how chemical companies are approaching organizational security are:

- A single individual is responsible. This individual chairs a cross-functional team representing the various business units and functional departments of the organization that includes legal and process safety, human resources, internal audit and physical security. The team demonstrates commitment to cybersecurity and sets clear direction for the organization. This includes asset and process ownership as well as providing the appropriate resources for addressing security issues.
- An independent review (e.g., other organization or third party) is conducted to confirm the charter and actions of this team reflect the intent of the overall security policy.
- An overall security team is responsible for both information and physical assets. In this hierarchical structure, security is under a single organization with separate teams responsible for physical and information systems. This approach is useful in smaller organizations where resources may be limited.
- A separate team responsible for the security of manufacturing and control systems under either a manufacturing or engineering organization. While this approach has the advantage of having leadership knowledgeable of the risks associated with manufacturing control systems, the benefits of such an approach can be lost if this team does not coordinate closely with those responsible for traditional IT assets and physical security.
- Companies coordinate efforts with law enforcement agencies, regulators and Internet service providers along with other relevant organizations, as it relates to terrorist or other external threats. Companies that have established relationships with local emergency response personnel expand these relationships to include information sharing as well as response on cybersecurity incidents.
- Third party contractor access is subject to a risk assessment to determine security implications. Appropriate controls are established. Contracts with third party contractors govern physical as well as logical (e.g., information systems, databases) access. Confidentiality or nondisclosure agreements are a necessity. All individuals working at a site or remotely are covered by nondisclosure agreements. These agreements are reviewed thoroughly with each person by their employer or by the host company.
- Controls specified in third party contracts include incorporation of the general security policy, destruction of information or assets, restrictions on copying, and responsibilities with respect to legal matters taking into account different national legal systems. Intellectual property rights, access methods, change management procedures, training, notification, and reporting requirements are included as well.

- Outsourcing contracts include the same elements as those for third party contractors. There may be an additional level of detail to be addressed in the contract to address the availability and integrity of data. It is important to note that the use of outsourcing may introduce additional risks that need to be considered and actively managed as part of the security system. Companies consider the increased security risk associated with outsourcing as part of the decision making process to determine what to outsource, and outsourcing partner selection.
- Procedures are set up to remove third party access at the conclusion/termination of the contract. The timeliness of this is critical and is clearly detailed in the contract.

6.4.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Information Services Security

6.4.6 Resources Used

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 4
- SANS web site (www.sans.org) for cybersecurity policy primer and samples
- US Chemical Sector Cyber-Security Strategy
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6.6

6.5 Personnel Security

This section describes practical guidance of the ISO/IEC 17799 objective and includes appropriate input from ISA-TR99.00.01-2004 to address both traditional information technology (IT) and manufacturing and control systems.

6.5.1 Statement of Management Practice

Companies should address security responsibilities at the recruitment phase, include these responsibilities in all contracts, and monitor during an individual's employment. Recruits should be screened especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality or nondisclosure agreement.

6.5.2 Applicability to Cybersecurity in the Chemical Sector

Companies store and process vast amounts of sensitive data. Some examples include financial data, pricing, customer information, as well as the critical process data used to operate manufacturing facilities. Employees, contractors, or temporary personnel that have access to this information or the networks, hardware, and software create a potential exposure if sensitive information is revealed, modified, or if unauthorized access to IT systems (including manufacturing systems) is granted. Companies engage in practices that inform, train, and create trustworthy employees, third party contractors, and temporary employees in sensitive positions. Companies practice segregation of duties so that only authorized updates to sensitive information occur. Auditing of practices and maintaining appropriate checks and balances are important.

6.5.3 Baseline Practices

Example baseline practices that chemical companies use for personnel security include:

- Screening of personnel during the recruitment phase. Activities such as background checks prior to hiring or movement to sensitive jobs.
- Security responsibilities are clearly documented and regularly communicated to employees and third party contractors.
- Duties are segregated amongst employees to maintain appropriate checks and balances (so that no single individual has total control over sensitive transactions).
- Employees, third party contractors (individually or through the third party company), and temporary employees sign a confidentiality or nondisclosure agreement.

6.5.4 How Chemical Companies Are Approaching Personnel Security

Some examples of how chemical companies are approaching personnel security are:

- Security responsibilities are documented and included in job descriptions, contracts, or other third party agreements. This applies to all employees and contractors job descriptions, not just those involved in security functions. Where possible the responsibilities are specific and measurable. Security roles and responsibilities for a given job are periodically reviewed and revised to meet the changing needs of the company.
- Security roles and responsibilities are divided amongst personnel to maintain an appropriate level of checks and balances. For example, a single individual is not responsible for establishing (creating) vendor records and writing (processing) checks.
- Employees, including internal transfers to sensitive positions (privileged access) are screened during the job application process and include personal and employment references and verification of academic credentials and identity. Background screenings to include credit history and criminal activity are also useful in determining the applicants' suitability (subject to local Data Privacy Laws).
- Third parties, contractors, etc. are subject to background screening at least as rigorous as employees in comparable positions.
- Companies train managers to observe employee behavior that may lead to theft, fraud, error, or other security implications. Awareness of cybersecurity threats and traditional threats are important for managers.
- Confidentiality agreements are reviewed with and signed by employees as part of the initial employment process. Third party contractors, casual staff, or temporary employees not covered by a formal nondisclosure agreement also sign a confidentiality agreement prior to beginning work. Employees, contract employees, and temporary employees review the agreements on an annual basis and validate understanding.
- Terms and conditions of employment clearly state the employees' responsibility for cybersecurity. These responsibilities extend for a reasonable period of time after employment ceases. In most cases, one year is a sufficient period.
- Employees, contract employees, and temporary employees are trained initially and periodically thereafter (usually annually). Users are trained in the correct security procedures and the correct use of information processing facilities to minimize possible risks. This extends to individuals responsible for operating and maintaining manufacturing and control systems. Training should also include legal responsibilities, business controls, and individual security responsibilities.
- Companies develop and test procedures so that security incidents are discovered, reported in a timely manner, and used to continuously improve performance. The procedure or policy clearly states responsibilities for reporting security breaches; software, hardware, or system malfunctions, and identifying the appropriate notification process. If the process is different for off-hour operations, it is clearly noted. Testing is done on an annual basis.
- An incident process is in place to address issues that are discovered and ensure they are corrected. This information should be reviewed periodically and used to update security policies and procedures. The responsibility of this process should be clearly articulated to personnel.
- A disciplinary process is in place for employees, contract employees and temporary employees who have violated the security policies and procedures.

6.5.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Employment screening and personnel policies

6.5.6 Resources Used

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 6
- SANS web site (www.sans.org) for cybersecurity policy primer and samples
- US Chemical Sector Cyber-Security Strategy
- ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 10.2

6.6 Physical and Environmental Security

This section describes practical guidance of physical and environmental security as covered in ISO/IEC 17799 objective and includes appropriate input from ISA-TR99.00.01-2004 to address both traditional information technology and manufacturing and control systems.

6.6.1 Statement of Management Practice

Physical and environmental security should protect tangible or physical assets (e.g., computers, networks, manufacturing processes equipment, etc.) from damage, loss, unauthorized access or misuse and complement cybersecurity measures taken to protect information. Critical information or assets should be placed in a secure area, protected by security perimeter and entry controls.

6.6.2 Applicability to Cybersecurity in the Chemical Sector

Cybersecurity policies and practices are important for the proper protection of information and control systems. However, in order to have truly effective protection, they should be complemented by the appropriate level of physical security. For example, maintaining tight controls such as authentication and access control does little to protect system integrity if it is possible to enter a facility and physically remove electronic media.

In the chemical sector, the environmental and physical perimeter security is mainly dictated by the nature of the business, and is not expected to fulfill the cybersecurity requirements as well. Because of the sometimes integrated infrastructures and organizations, like joint ventures, contractors at the plants, and even at a specific site differences in plant criticalities, additional physical security protection for information technology assets is required.

In manufacturing facilities, physical security is focused more at protecting manufacturing assets than it is to the manufacturing information itself. The concern is not so much the actual theft or corruption of the computing and control devices, but rather the impact this would have on the ability to sustain production in a safe manner. This difference in focus is reflected in *How Chemical Companies Are Approaching Physical and Environmental Security.*

6.6.3 Baseline Practices

Examples of baseline practices that chemical companies use for physical and environmental security include:

- One or more physical security perimeters are established to provide barriers to unauthorized access to facilities. Multiple perimeters may be “nested” to provide successively tighter controls.
- At each barrier or boundary, appropriate entry controls are provided.
- Physical assets (equipment) are protected against environmental damage from threats such as fire, water, smoke, dust, radiation, impact, etc.
- System availability requirements (depending on the nature of the application and the information) may require the use of redundant sources of power. Avoid single points of failure where possible.

- All external connections (power, communications, etc.) are adequately protected from tampering or damage.
- All equipment including auxiliary environmental equipment is properly maintained to assure proper operation.
- Proper procedures are established and audited with respect to the addition, removal, and disposal of all equipment. Proper asset tracking is a good practice. Baseline practices would include workstation disposal, format, clean drive, etc.
- All information that is expressed in a physical form (e.g., written or printed documents, magnetic storage media, card-access readers, etc.) are also be adequately protected against physical threats.

6.6.4 How Chemical Companies Are Approaching Physical and Environmental Security

Physical and environmental security of information systems is a well-established discipline that draws knowledge and experience from other areas of physical or facilities security. In many chemical companies, this area has been thoroughly addressed for corporate or centralized information or communications facilities, but perhaps not as consistently applied in areas such as manufacturing and control systems. Also, the increased use of smaller and less expensive information systems in an office environment can lead to an increased potential for loss, since these systems may not be subject to strict physical control.

Some examples of how chemical companies are approaching physical and environmental security are:

- Using security cables, locked cabinets, protected entrance of home office, keeping equipment out of sight, labeling and tagging assets, and making user accountable for loss for off-site locations, like home office for sales people.
- Using password settings on boot and login commands, encrypted file system, store minimum amount of data on the laptop by using client-server synchronization techniques, etc.
- Protecting computer equipment not in control rooms such as routers or firewall in a locked environment.
- Having clean and locked desks, offices, or computer room areas to reduce unauthorized access, damage, and removal of sensitive information.
- Having control rooms staffed 7 X 24 can often be the first line of defense in physical protection. Use control rooms to house information and technology assets.
- Having personnel who are leaving the company return the equipment.

When developing a program for physical security of information assets (including information systems and manufacturing and control systems), it is important to include all systems in scope, and not just limit the effort to traditional “computer room” facilities.

Computers in manufacturing operations are tools used to operate the facility safely. They are a means to the end rather than the asset that must be protected. In some cases, safety is threatened by locking equipment behind doors because the response time to access the equipment may be increased.

Although it is common practice to locate routers and other network equipment in locked environments, few overall security or safe operation improvements are achieved by following this practice. Valve actuators and motor starters out in the open are an easier point of direct attack than the network or control devices. Practical engineering judgment based on risk will determine the physical security practices for the assets to be protected. Cost and benefit will be considered.

A physical security vulnerability analysis of risk is used to determine the appropriate physical security practices to be implemented.

6.6.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Cyber Risk Ranking Methodology
- Physical security standards for data centers or manufacturing sites (possibly based on tiers)

6.6.6 Resources Used

The following are resources used in the creation of this section:

- Guidance for Cybersecurity Vulnerability Assessment Methodology Process Version 1.0, available from CIDX at www.cidx.org
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 7
- ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 10
- Carlson, Tom, *Information Security Management: Understanding ISO 17799*, 2001, www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf

6.7 Risk Identification, Classification, and Assessment

This section describes the identification, classification, and assessment of cybersecurity risks as covered in BS 7799-2:2002, Sections 3.7 and 3.8.

6.7.1 Statement of Management Practice

Organizations should protect their ability to perform their mission by identifying, prioritizing, and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies.

6.7.2 Applicability to Cybersecurity in the Chemical Sector

Risk assessment addresses the analysis of threats, vulnerabilities and consequences. Section 4.5.3 of the "*U.S Chemicals Sector Cyber-Security Strategy* (June 2002)" explicitly recommends risk assessment as a component of a corporate cybersecurity program. There are various methodologies available to use for risk assessment.

Risk assessment and analysis identifies how to further enhance security of product sales, distribution and cybersecurity. A value chain risk management (e.g., application service provider (ASP) or distribution functionality, like transmitting shipping instructions) analysis may require involvement of the appropriate people in the organization. The importance of confidentiality, integrity, and availability depends on the specific business or functional requirements. In manufacturing, the highest priority is typically safety. Regardless of which methodology is selected, the assessment should be coordinated with physical security, wherever possible.

The significance of the risk assessment is that there may be weaknesses in a company's manufacturing control systems or information systems that could allow inappropriate access to systems and data.

6.7.3 Baseline Practices

Example baseline practices that chemical companies use to identify, classify, and assess risk include:

- Establishing criteria for identifying critical business and manufacturing and control systems.
- Identifying critical business and manufacturing and control systems processes and the IT systems that support these processes. See section 6.1 Importance of Cybersecurity in Businesses.
- Prioritizing risk assessment activities based on criticality.
- Scoping boundaries of the system to be assessed, identifying all information assets and critical components.
- Maintaining an up-to-date record to know what to protect.
- Positioning a change management system to identify reassessment criteria based on technology, organization or process changes.
- Classifying the information assets and components based on confidentiality, integrity, availability, safety, or environmental impact.

- Conducting a risk assessment by analyzing threats, vulnerabilities, likelihood and consequences including the potential costs associated with each.
- Conducting risk assessment through all stages of the technology lifecycle like development, implementation, updates, and retirement.
- Understanding that risk tolerance and acceptability of countermeasures may vary.

6.7.4 How Chemical Companies Are Approaching Risk Identification, Classification, and Assessment

Examples of how chemical companies are identifying, classifying, and assessing risk include:

- Identification and classification of assets is an important step in the definition of the companies' risk. Important focus areas should be people involved and technologies used. The creation on a checklist helps group the assets into categories. For an example checklist, see Attachment I.
- A good starting point is to develop a diagram of an application portfolio, a computer system, or a network. A diagram is a graphical representation of the applications or devices identified in the information systems or manufacturing and process control environments.
- Individual information assets should be classified on the confidentiality, integrity and availability or safety. An application, system, or network could have different levels of classification. The following is an example of application "X:"
  - Confidentiality: very high, the business critical data should be maintained at the highest confidential level.
  - Integrity: medium, the data is verified at various stages and changes to it would be detected.
  - Availability: low, the system is not required 7 X 24 on line. A delay of up to one or two days would be acceptable.

  The next example is a step approach to identify risks:

  - From the previous steps is a comprehensive list of all the critical assets whose failure could impact the business. Additionally, there are the confidentiality, integrity, availability, and safety rating for each of the assets, which helps identify suitable protection measures. Every asset is exposed to numerous threats.
  - Use the risk tolerance profile established for the organization to assign a risk level to each asset in scope. See section 6.1 - Importance of Cybersecurity in Business.
  - Vulnerability is a flaw or weakness in the design of a system, which could be exploited by a threat. Discovering such vulnerabilities is the objective of the analysis.
  - Using a comprehensive list of threats, risk tolerance, and vulnerabilities evaluate the likelihood that businesses or manufacturing is exposed to each.
- Probability or estimated frequency establishes a confidence level that a threat will be successful, in view of the current level of controls. Estimated frequency is directly related to the overall vulnerability and threats and could be expressed in percentage or "high-medium-low."
- Consequences or impact of a successful threat attempt are based on the business or manufacturing risk evaluation.

6.7.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Example checklist on groupings for identifying and classifying the assets

6.7.6 Resources Used

The following are resources used in the creation of this section:

- NIST special publication 800-30, Section 3.
- Responsible Care Security Code of Management Practice, Section 4.2
- *U.S. Chemicals Sector Cyber-Security Strategy*, June 2002. Section 4.5.3
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Sections 3.7 and 3.8
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6.4.1
- CIDX reference model
- CIDX - CSVA version 2
- CIDX – Self-Assessment

6.8 Risk Management and Implementation

This section describes practical guidance of BS 7799-2:2002, sections 3.9, 3.10, 3.11, and the identification of the security controls. The reference used to guide the risk management documents on security controls are the ISO 17799 domain controls.

6.8.1 Statement of Management Practice

Security measures should be developed and implemented commensurate with risks and take into account inherently safer approaches to process design, engineering and administrative, manual and procedural, controls, and prevention and mitigation measures. The importance of risk mitigation is to convert the risk management plans into actions and see that a program plan is in place to monitor effectiveness.

6.8.2 Applicability to Cybersecurity in the Chemical Sector

Companies take action after they identify and assess potential security risks. Actions can include putting additional or different security measures into place to provide greater protections for manufacturing and control systems, and information systems.

The information gathered during the cybersecurity risk assessment as described in the previous section (Risk Identification, Classification and Assessment) identifies the required cybersecurity controls to mitigate unacceptable cybersecurity risks. The importance of a risk assessment is to identify the weaknesses for your critical systems, the related cybersecurity risks, and the mitigation approach to reduce these risks.

For general information technology systems, the ISO/IEC 17799 process includes this as part of step #6 of a 10-step process.

In the case of manufacturing and control systems, ISA-TR99.00.02-2004 provides detailed guidance on the design of a risk mitigation strategy (Section 10), but gives less detail on the actual implementation (Section 11). This shortcoming is expected to be addressed in a future edition of this document.

6.8.3 Baseline Practices

Example baseline practices that chemical companies use for risk management and implementation include:

- Defining and validating security policies. Detailed security policy statements define the operational level commitment to mitigate each of the security risks during the risk assessment.
- Developing procedures. These provide details like actions to take for preventing, detecting and responding to threats.
- Developing standards and services. Organizations may decide to adopt some international standards in the area of cybersecurity (e.g., S/MIME for secure e-mail).
- Identifying security tools and products. It may be necessary to select products to implement clauses of security policy, like firewalls.

- Understanding risk tolerance profile. Depending on the severity of the impact and consequences, the risk tolerance could be different.
- Identifying the controls required to mitigate each risk. Take the detailed risk assessment, identify the cost of mitigation, compare with the cost of a risk occurrence, and select the preferred security controls.
- Comparing cost versus benefits. Select the security controls of which cost is less than the risk it is attempting to reduce. Accept the risks of which consequences are less costly than the cost of implementing the controls required to mitigate them.
- Achieving risk management by mitigation, acceptance of risk, avoiding, or transferring.
- Establishing a process for accepting risk, which includes appropriate management level approval based on scope and documentation.

The specific controls to be implemented have been identified and documented as part of the risk mitigation strategy. Selection of controls, method used and degree of implementation are based on an analysis of the level of risk assumed. In general, the lower the level of acceptable risk, the higher the level of controls applied.

Controls are implemented in a manner that minimizes administrative overhead and burden on the end user without compromising effectiveness. Well-designed controls often leave behind their own audit trail that can be used for verification later.

6.8.4 How Chemical Companies Are Approaching Risk Management and Implementation

Risk mitigation involves prioritization, evaluation and implementation of the appropriate cybersecurity controls to reduce the risk to an acceptable level as been recommended by the risk assessment process.

Because the elimination of all risk is usually impractical or impossible, focus is on the most critical applications and infrastructures to decrease risk to an acceptable level. An early detection of the risk creates additional risk mitigation opportunities with a minimum impact on cost.

Risk mitigation is a systematic methodology to reduce risk and can be achieved using many of the following options:

- Mitigating the risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls. The implemented security controls and countermeasures need to lower the risk to an acceptable level and minimize the adverse impact of a threat's exploiting a vulnerability (e.g., use of supporting, preventive, and detective controls)
- Avoiding the risk by eliminating the root cause and/or consequence (e.g., give up certain functions of the system or shut down the system when risks are identified)
- Transferring the risk by using other options to compensate for the loss, such as purchasing insurance.
- Residual risk remains when security controls lower the risk but not eliminate the risk. Select alternatives like administrative and physical controls to reduce likelihood or impact. An example is workstations stored in a locked room or cabinet.

In some cases the risk is known, but the solution to avoid the risk is for example too costly. The decision could be to live with the risk and accept the consequences.

- Accepting the potential risk and continue operating the manufacturing and process systems or information systems environment as defined.
- Some risks are not acceptable like major safety or environmental impacts, because the cost of accepting these risks is essentially open-ended and therefore to high to bear.

Depending of the technology lifecycle, the selection of options and controls may vary.

Differences in manufacturing, process control, and information systems occur due to the nature of impact and consequences.

There are several sources of information with regard to established practices for implementation, including case studies from similar industries or companies, research reports, security texts, etc.

The following overview lists several subject areas to address:

- Managerial controls, such as span of control, separation of duties, background checks, and personnel awareness, training, and education;
- Identification and authentication controls to establish accountability and to prevent unauthorized persons from gaining access to the systems;
- Logical access controls to establish who or what has access to a specific type of information resources and the type of access permitted;
- Accountability controls through management audit trails that maintain a record of all user and system activity;
- Controls over information transmitted and stored to ensure confidentiality, authenticity, integrity, and non-repudiation;
- Systems development life cycle process controls to ensure that security is considered as an integral part of the process and explicitly examined during each phase of the process;
- Physical and environmental controls to ensure that adequate measures are taken against threats emanating from the physical environment;
- Computer support and operations controls to ensure that these routine but critical activities enhance the overall level of security; and
- Business continuity planning controls to ensure that an organization can prevent interruptions, and recover and resume processing in the event of a partial or total interruption to information systems availability.

The ISO 17799 provides 10 control domains, which can be deployed to reduce the risk. However, these controls are general in nature. Selection of specific controls should be based on threat, risk tolerance, and risk assessment performed.

- Develop a risk mitigation strategy by referencing the ISO 17799 – 10 control domains and selecting the appropriate controls until risk is reduced to an acceptable level.

- Perform cost benefit analysis to allocate and implement cost effective controls, after identifying all possible controls and evaluating their feasibility and effectiveness, determine which controls are required and appropriate for usage.
- Document selected controls and justification for not implementing recommended controls (residual risk may be acceptable and depends on the company risk tolerance).
- Identify responsible party for implementing the security controls.

6.8.5 Examples

There are currently no examples available for this publication.

6.8.6 Resources Used

The following are resources used in the creation of this section:

- NIST special publication 800-30, section 4.
- Responsible Care Security Code of Management Practice, section 4.2
- *U.S. Chemicals Sector Cyber-Security Strategy*, June 2002. Section 4.5.3
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Sections 3.9 and 3.10
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Sections 9 and 10
- Carlson, Tom, *Information Security Management: Understanding ISO 17799*, 2001, www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000
- CIDX reference model
- CIDX - CSVA version 2
- CIDX – Self-Assessment

6.9 Statement of Applicability (SoA)

This statement of applicability section describes the relevant controls selected as covered in BS 7799-2:2002, Section 3.12. It is an evolving practice and it may not be widely in place.

6.9.1 Statement of Management Practice

As each of the security controls is addressed, the result should be documented, including elements of the security controls. Documenting results aid in the decision making process, facilitate the communication of the decisions and provide a basis for training and education, and responses to incidents and threats, as well as providing a basis for subsequent self-assessment or auditing of the compliance with these security controls.

6.9.2 Applicability to Cybersecurity in the Chemical Sector

The statement of applicability is a working document and is updated during the lifecycle changes of applications and infrastructure components. These lifecycle changes include creation, implementation, update, and retirement phases. It describes how an organization has interpreted and applied ISO/IEC 17799, ISA-TR99.00.01-2004, and references supporting evidence.

6.9.3 Baseline Practices

This section identifies the control objectives and the security controls that are relevant and applicable based on the results and conclusions of the risk assessment and risk management processes. It also provides the reasons for their selection or rejection. Control objectives and controls are taken from ISO/IEC 17799, and ISA-TR99.00.01-2004. The selection of controls can also be related back to policy statements. Security controls are practices, procedures, or mechanisms that reduce security risk.

The SoA records the decision whether to implement each control fully, partially or not at all. For fully and partially implemented controls, it describes the method employed. It also provides justifications for partial or non-implementation in quantitative terms.

This section is the key deliverable of the control selection process. The SoA is input to the security implementation project that begins on the completion of the risk assessment. It is a vital component of the cybersecurity management system (CSMS) and is a key document in the audit process. The SoA is also used as a base document in the next round of risk assessment.

6.9.4 How Chemical Companies Are Approaching Statement of Applicability

Larger companies may benefit more from the SoA due to the number of audits and audit responses. These benefits include efficiency from the use of a standard template, productivity improvements, reusability, etc. Smaller companies may adapt this approach using a simple template or apply the strategy to only critical applications. It is an evolving practice for information security and manufacturing and control systems.

Examples of how chemical companies are approaching the statement of applicability include:

- Having a template and process in place and being used for preparing a SoA.
- Justifying quantitatively the decision taken for or against control objectives and controls.
- Recording the inclusion or exclusion of any control objectives and controls listed in ISO/IEC 17799 and ISA-TR99.00.01-2004.

6.9.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Example Statement of Applicability

6.9.6 Resources Used

The following are resources used in the creation of this section:

- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 4.2.1.
- Common Criteria (ISO/IEC 15408)

6.10 Incident Planning and Response

This section addresses incident planning for and response to cybersecurity attacks on facilities.

6.10.1 Statement of Management Practice

Companies should be vigilant in efforts to deter and detect any cybersecurity incident. If an incident should occur, the company should respond promptly and involve government agencies as appropriate. After investigating the incident, the company should incorporate key learnings and, if appropriate, share those learnings and with others in the industry and government agencies and implement corrective actions.

6.10.2 Applicability to Cybersecurity in the Chemical Sector

Incident planning and response has become an important program of information technology (IT). Technology vulnerabilities continue to exist and external threats are increasing in number and sophistication, therefore requiring a robust strategy on determination of the appropriate planning and response.

Incident planning and response should be distinguished from business continuity. The former addresses short-term actions to be taken as a cyber attack is being mounted and in the immediate aftermath. The latter addresses longer term strategies for keeping an organization operating following an attack. Responding to emergencies, ensuring personnel safety, and getting systems back on line are part of incident response. Ensuring the stability of critical business functions and reducing the overall impact of an attack on the organization are part of business continuity.

Incident planning and response is a key element of the management system for any type of risk to an organization, including cybersecurity risks. Sound information management practices recognize the need to have a formal incident planning and response system in place. For example ISO 17799 section 6.3 “Responding to security incidents and malfunctions” and 6.3.1 “Reporting security incidents” illustrate that incident planning and response is recognized in the cybersecurity realm.

6.10.3 Baseline Practices

Example baseline practices that chemical companies use for incident planning and response include:

- Establishing incident planning and response procedures such as:
  - Naming the responsible person for executing the plan when the need arises.
  - Structuring an incident response team, including additional personnel, which can be called in.
  - Establishing responsibility for coordinating defense and response to an incident.
- Handling incident from initiation through final review.
- Creating procedures for different types of incidents like denial of access, system attacks, malicious code, unauthorized access and inappropriate usage.
- Identifying proactive measurements to identify attacks during early stage.
- Doing base planning on threat scenarios identified from vulnerability analysis and risk assessment.

- Developing written response procedures.
- Communicating manufacturing and process control system incidents to the IT organization as well as the process safety organization.
- Communicating IT incidents to the manufacturing and process control organization for awareness building.
- Communicating metrics and incidents to executive management.
- Documenting the details of the incident, the lessons learned, and the course of action to prevent from occurring again.
- Conducting drills to test the plan.

6.10.4 How Chemical Companies Are Approaching Incident Planning & Response

Some examples of how chemical companies are approaching incident planning and response are to:

- Develop a process for immediate reporting of cybersecurity incidents. Ensure this process has links to the company's crisis management team. Educate employees with examples of reportable incidents so they can better comply with reporting requirements.
- Understand fully any potential links between IT, safety, and manufacturing and process control systems and incorporate this understanding into security incident response procedures.
- Develop, test, deploy, and fully document an incident investigation process.
- Specify roles and responsibilities with respect to Federal Agencies, local law enforcement, and/or other critical stakeholders in an internal and shared incident investigation program. Consider classifying incidents based on the potential outcome rather than the actual outcome. The level of incident investigation may need to be upgraded depending on the potential seriousness of the incident.
- Develop a mechanism to ensure that corrective actions identified as the result of a cybersecurity incident are fully implemented.
- Provide security incident response training to company cross-functional training teams.
- Implement processes and mechanisms to evaluate security incidents with regard to the appropriate response.
- Review final incident investigation results with all personnel whose job tasks are relevant to the findings. Review the incident in light of trends, and record it so it can be used for subsequent trend analyses.
- Expand relationships with local authorities to include security agencies.
- Promote peer to peer and cross industry mutual assistance activities in order to learn from others' experiences regarding security incident evaluation, response, investigation, communication, and corrective.

- Identify previously unforeseen consequences, especially those that may affect future application of the plan. Incidents may include risk events, near misses, and malfunctions. Also included are any observed or suspected weaknesses in the system or risks that may not have been previously recognized.
- Plan to detect, report, document, and investigate incidents, weaknesses, and unrecognized risks. Establish an incident reporting and investigation program that addresses:
  - Recording the incident planning
  - Being alert to incidents experienced by other organizations and learn from them. This element provides input to the element "Managing preventive and corrective actions."
  - Responding successfully, managing, and recovering from incidents.
  - Recording response planning.
- Incorporating emergency response and planning into incident response and planning.

6.10.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Examples of what an incident reporting and investigation program might address.

6.10.6 Resources Used

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- NIST Special Publication 800-61

6.11 Communications, Operations, and Change Management

This section describes practical guidance of the ISO17799 Communications and Operations Management security objective.

Processes and procedures should be formalized and followed for this aspect of ongoing support of computer applications and systems. Historically these processes were established to preserve the functional operation of the system. Now the same diligence should be applied to verify that change or the lack of change does not compromise security of the systems.

The need to address security is very strong in the manufacturing and control systems that are used to operate our facilities because security lapses have the potential to result in safety, health, or environmental issues. This section recommends integrating the change management processes of the manufacturing and control systems with the change management practices associated with site Process Safety Management (PSM) procedures.

6.11.1 Statement of Management Practice

Processes and procedures should be developed and followed to sustain the security of computer systems and information processing facilities. These overall management practices/procedures should clearly articulate all the operational security and safety aspects.

6.11.2 Applicability to Cybersecurity in the Chemical Sector

The organization's security policy is reduced to a clear statement of procedure, planning activities, and good practices for operation of computer and network systems that ensure the availability, confidentiality, and integrity of systems and data.

6.11.3 Baseline Practices

Example baseline practices that chemical companies use for communications, operations, and change management include:

- A process for change management is be documented and followed.
- A process for incident management is be documented and followed.
- A process for patch management (identifying and fixing vulnerabilities) is documented and followed. The process defines how the organization monitors information sources for announcement of new vulnerabilities and patches, evaluates the relevance of those patches, and implements patches required to reduce risk to an acceptable level.
- A process and practice for antivirus management is documented and followed. The practice defines the types of computer systems that require antivirus software, defines which antivirus products are used in each case, and how these antivirus products are deployed.
- Procedures and practices for backup and restore of computer systems are defined, used, and verified by appropriate testing.

- A system of controls over information exchanged with between organizations (i.e., between your company and other companies) is documented and followed.

6.11.4 How the Chemical Companies Are Approaching Communications, Operations, and Change Management

Some examples of how chemical companies are approaching communications, operations, and change management are to:

- Purchase or internally develop a formal change management system, document how it is used, and require that all changes to infrastructure and applications use it. Appoint staff to run weekly change management meetings. Develop a process for emergency changes but require a higher level of management approval for these than normally processed changes.
- Purchase or internally develop a formal incident management system, document how it is used, and require that all incidents and responses be logged in that system. Appoint staff to own all incident management activities.
- Evaluate new security patches to reduce malware attacks. Appoint staff to evaluate and test patches. Prioritize patches and establish a schedule when patches of each priority are applied. Isolate systems that cannot be patched to this schedule (e.g., control systems) from the business systems.
- Enforce the updating of antivirus signatures automatically by a central policy system. Antivirus is too critical to be left to chance. The same system can also be used to monitor and measure compliance with policy, even for computers it does not control. Isolate systems that cannot be monitored by this software (e.g., control systems) from the rest of the network connecting the devices updated by the central policy system.
- Test restores on a regular basis. Nearly everyone backs up servers, but far fewer verify that files and systems can be restored.
- Use appropriate access control methods for all systems that connect your network to other networks, or for systems that support exchange of information between your company and external organizations. (See Section 6.12 Access Control of this document for guidance).
- Establish a disaster recovery site somewhere outside normal business facilities. A disaster (e.g., fire, flood, tornado, terrorism) that disables your facility does not impact the recovery site. Business owners identify the maximum time their systems may be unavailable before computer operations transfers that application to the disaster recovery site.

Historically the IT organization and the manufacturing organizations operated in two mutually exclusive areas and the expertise of each group was not understood or appreciated by each organization. The culture and motivating values of each organization were very different. Today's open IT technologies are used extensively in the manufacturing and control systems, and networks that operate the facilities. Additional knowledge is needed to safely employ these technologies. There are three options for dealing with this:

- Train the manufacturing and process control personnel to understand the technology and cybersecurity issues.

- Train the IT personnel to understand the manufacturing practices/technologies and the PSM process and methodology.
- Develop the practices to join the skill sets of the two organizations to collaboratively deal with cybersecurity in manufacturing.

There is no right or wrong approach. All three approaches may be appropriate for differing operations within the same company. This is especially true when operating in multiple regions around the world. It requires management support at the top of the company to bring about the right actions and change in culture.

The IT organization is most likely to be the first to learn of new cybersecurity vulnerabilities. A process needs to be formalized that establishes a clear path of communication of this vulnerability to the organization/group that is accountable for secure and safe operation of the manufacturing facilities. The impact to process safety and continuity of production is assessed and acted upon commensurate with the risk.

6.11.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Business Computer System Examples
- Manufacturing and Control System Examples

6.11.6 Resources Used

The following are resources used in the creation of this section:

- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 8.
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6.8.

6.12 Access Control

This section provides practical guidance with respect to access control as described in ISO 17799 Section 9. Access control is the process of controlling who or what resources can access premises and systems and the type of access permitted.

There is a real time aspect to access control and an off-line aspect. The off-line activity is the first step in the process and includes defining the user privileges and resource needs for the user. These are based upon the role of the user and the job to be performed. The off-line process includes an approval step by a responsible party before the user account is configured to provide the proper access.

The real time aspects of access control are the sequential steps of authentication and authorization. These take place at the time of the user request to access information. Authentication is generally the prerequisite to authorization. Because the tasks are tightly linked, yet are often implemented using totally different hardware devices and software applications, they are addressed in separate sections below.

Access control section consists of the following topics:

6.12.1 Statement of Management Practice – General Access Control

Rules should be established to confirm that users' access to systems and data is controlled. The rules generally should be applied to roles or groups of users. They should have access to systems and data that are required to meet defined business requirements. They should not have access if there is no defined business purpose for it.

There are rules that are enforced administratively and those that are enforced automatically through the use of technology. Both kinds of rules need to be addressed as part of the overall access control strategy. An example of an administrative rule that a company might have is "separation of an employee or contractor initiates the removal of their accounts." A possible example of technology enforced rule is "users connecting to the corporate network over the Internet must run a virtual private network (VPN) session in order to connect."

In addition to rules, there are both physical security practices and cybersecurity practices that work together to establish the overall security framework for the system. Physical security practices include such measures as locked rooms where user interface equipment is located. This section does not attempt to provide guidance on physical security practices. However, it is important to understand the complimentary nature of physical and cybersecurity and employ both security components appropriately to establish the overall level of security for the system.

6.12.2 Applicability to Cybersecurity in the Chemical Sector

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.

Authentication in the manufacturing and control system operating arena has several challenges not typically found in normal business IT situations. Current authentication technologies have several limitations that are not well suited for this work environment and could actually result in increased safety risks at the expense of decreased cybersecurity risks. The *How Chemical Companies Are Approaching Authentication* subsection offers guidance for this subject area.

As discussed in the *Authentication* subsection, the work team approach to control room operation may require a different set of practices for authorization. See *How Chemical Companies Are Approaching Authorization* subsection for additional details.

6.12.3 Introduction – Account Administration

The account administration subject addresses the administrative process associated with initially setting up permission and privileges to access specific resources on the network or computer system. Privileges often include access to file directories, hours of access, amount of allocated storage space, etc. Several steps are involved that include identification of the resources needed to perform that person's job function, independent approval by a trusted person, and setup/configuration of the computer account that automatically assigns the resources when requested.

6.12.3.1 Statement of Management Practice – Account Administration

A standard administrative process shall be followed for the creation of all user accounts. The accounts should be role based and grant the user only those privileges and access to resources that are needed to perform the particular job function. The account administration process includes principles of separation of duties with separate approvers and implementers of account configuration.

The management process shall include periodic reviews of user accounts to make sure the roles, access needs, or users are still correct, and to remove inactive and unneeded accounts.

6.12.3.2 Account Administration Baseline Practices

Example baseline practices that chemical companies use for account administration include:

- Users are assigned the minimum privileges and authorizations necessary to perform their tasks. Access should be granted on the basis of the need to support a particular job function.
- Every user is individually identifiable and each access is controlled by an appropriate method of authentication (e.g., user ID and password). These personal credentials (e.g., passwords, and personal identification numbers, tokens, etc.) are not shared except in certain special situations. One special case is in a manufacturing control room where the operators function as a single work team. (Additional discussion is provided on this subject in the Authentication section.)
- A process exists for alternative identification in the event of a forgotten password.

- Access is granted, changed, or terminated on the authority of an appropriate manager (from your company or a partner organization). A record is maintained of all access accounts, including details of the individual, their permissions, and the authorizing manager.
- Access accounts are suspended or removed and access permissions are revoked as soon as they are no longer needed (e.g., job change).
- The need for access to critical systems is explicitly reconfirmed on a regular basis. All established accounts are reviewed regularly to ensure they are authorized and still in use.
- If an access account remains unused for an extended period, the need for it is explicitly reconfirmed.
- Default passwords are changed immediately.

6.12.3.3 How Chemical Companies Are Approaching Account Administration

Some examples of how chemical companies are approaching account administration are:

- Tools (e.g., provisioning, and identity management) are used to manage the process of account creation, suspension, and deletion. A provisioning system also manages the approval workflow by which the business owner approves access, including logging. It may also automate the process of account creation/suspension on the target systems.
- The Account Administration process is linked to the HR process so that employee changes trigger reviews and updates to user accounts.
- The application information owner or delegate has defined and documented the application roles/user privileges (i.e., job functions mapped to application roles, access entitlements for each role).
- Special consideration is given for users with privileged access (e.g., more frequent reviews, background checks, see also Personnel Security).
- Assigning one user identification per person to minimize the confusion of managing and updating accounts across multiple platforms.

6.12.3.4 Unique Aspects of Account Administration for Manufacturing and Control Systems

Manufacturing and control systems and business systems may have different sets of people providing administrative control of the account creation and maintenance process. Similarly the approvers of user accounts for operating functions may be a different set of people than are approving users for the business systems. Approvals are made by supervision familiar with the manufacturing and operating tasks.

In addition to the task of creating users and assigning users to roles at the operating system level, many manufacturing applications require additional role assignments. System administrators are skilled and trusted to perform these account administrative functions on live process control applications. The change management process for making these account changes clearly identifies any timing constraints that must be followed due to the safety risks during certain sequences of the control operation. These changes are treated with equal importance as other software and equipment changes. The standard process safety management practices are followed along with standard approval and documentation steps.

All user accounts are reviewed on an established frequency to ensure that the account is still needed and that the role has not changed for the user. Documentation is retained for all administrative actions.

6.12.3.5 Examples

The following lists an example that is available as an attachment to CIDX members only:

- Access Control

Note: No example is provided for manufacturing and control systems.

6.12.3.6 Resources Used

ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 5 Authentication and Authorization Technologies

6.12.4 Introduction - Authentication

Authentication describes the process of positively identifying network users, hosts, applications, services, and resources for some sort of computerized transaction using a combination of identification factors or credentials. Authentication is the prerequisite to allowing access to resources in a system.

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.

6.12.4.1 Baseline Practices - Authentication

Companies have an authentication strategy or approach that defines the method of authentication to be used. The method may vary depending on the risks, the criticality of the business process, and the sensitivity of the data.

The authentication strategy may be different for users connecting from different geographical locations (including non-company facilities) or to devices with special security requirements. This takes into account the physical security characteristics that interact with the cybersecurity characteristics to establish the overall security level for the user.

Example baseline practices that chemical companies use for authentication include:

- All users are authenticated via the application to use the requested application. This requirement may be waived when there are compensating physical controls.
- The minimum level of authentication uses a userid & password. User authentication is not based on software/files on the client machine alone.
- Authenticators and credentials are protected while in storage and during transmission.
- Users are trained to keep passwords confidential.

6.12.4.2 How Chemical Companies Are Approaching Authentication

Some examples of how chemical companies are approaching authentication are:

- Password quality and aging are enforced.
- Stronger forms of authentication (e.g., token, smart card, soft certificate) are used for more critical tasks (e.g., authorizing payments, and system administrator).
- Stronger forms of authentication (e.g., token, smart card, soft certificate) are used for, single sign on concept, wireless connectivity, and remote access (e.g., virtual private network (VPN), dial-up, and terminal server).
- After five failed login attempts, the system disables the user's account for 30 minutes. This helps deter brute force hacks.
- After 15 minutes of inactivity, the user is required to authenticate again.

6.12.4.3 Unique Aspects of Authentication for Manufacturing and Control Systems

The physical location of the user may have a significant impact on the risk level of the access. For example, the user connecting to a system from inside a building that employs a guard and badge-in system to enter the building is less of a risk than a user connecting from some other region in the world. The authentication strategy addresses the combined physical and cybersecurity controls to be used to control overall risk. The strategy clearly defines the authentication requirements for special situations.

6.12.5 Authentication for Local Users

It is very important that only trained and designated resources take actions on manufacturing control human machine interfaces (HMI) stations such as operator control stations. Many chemical manufacturing operations control their processes from control rooms staffed by several operators. These operators often function as a team and perform actions on multiple HMI stations as part of their normal job function. Common user accounts shared by all operators are frequently employed. Current authentication technologies have several limitations that are not well suited for this work environment and could actually result in increased safety risks at the expense of decreased cybersecurity risks. Until these limitations are removed and cost effective, robust, "strong authentication" schemes are available on the HMI stations, the recommended practice is to use physical controls to ensure that only designated individuals are performing actions on control HMI stations. Access to control rooms is managed by appropriate combinations of entrance control technologies and administrative authentication practices. Consideration of the safety implications are considered when developing the access control practices.

Entrance controls include but are not limited to:

- Manual locks (e.g., key and combination)
- Automated locks (e.g., badge and card readers)

Administrative authentication controls include:

- Control rooms staffed 24 X 7 X 52
- Individual accountability by control room personnel to keep access limited to designated personnel.
- Individual accountability by control room personnel to make sure that only trained and designated personnel perform actions on operator control stations.

Normal "good username and password authentication practices" may be inappropriate if they introduce the potential to delay an operator's ability to locally make quick corrective action to the process from the HMI control station. Some examples of common IT practices that **may not be applicable** in a manufacturing and control systems environment:

- Individual usernames and passwords for each operator for work-team environments
- Login operation that requires access to non-local domain controllers and active directory servers for user account authentication
- User account lockout after some number of failed login attempts
- Robust long passwords that contain a mix of alpha, numeric, and special characters
- Required password change after a specified number of days

A common security practice for most desktop work stations is to employ a screen saver with password protection to provide added security for the unoccupied work station. This is not necessarily a good practice for manufacturing and control systems. Many manufacturing HMI stations are designed to "report by exception." The operator may not need to take any action on the operator station until an alert occurs. Screen savers have the potential to interfere with the operator by blocking the view to the process and delaying response to an emergency situation.

The system administrator is a special local user. This person does not typically need quick access to perform system level tasks on the computers. It is more important that untrained users be prevented from performing system level functions than it is to provide quick access. Good username and password practices are used on all system administrator and process control system manager accounts. Default passwords are changed promptly after initial installation of the application.

On highly critical systems, it is a good practice to perform all system manager functions or configuration functions locally at the device to reduce the potential for a network interruption causing a problem with the control of the process. The system manager coordinates all changes with the operator for the area so that production is not impacted during a configuration change.

6.12.6 Authentication for Remote Users

In the discussion that follows, the term remote user is anyone who is not physically present in the immediate manufacturing area or control room. The person in an office in the same building or the person connecting over the corporate wide area network (WAN) are both remote users as is the person connecting over public infrastructure networks.

Physical and administrative controls that rely on visual authentication do not work for remote interactive users. However, there are numerous technology based authentication schemes that can be used. It is important to employ an authentication scheme with an appropriate level of "strength" to positively identify the remote interactive user. Processes with low potential to create a SHE (safety, health, or environmental) incident or have low financial impact are protected using "weak" authentication methods such as simple username and password. However, processes where there is a large financial or SHE stake are protected using "strong authentication" technologies. In either case the need to securely authenticate the user takes precedence over any need to quickly respond to the process condition.

Examples of "weak" authentication include:

- Modems directly connected to the process control devices or network that employ simple username and password authentication.
- Connections to process control devices or network from the corporate local area network (LAN) or WAN that employ simple username and password authentication.
- Windows' username and password authentication at the application level on the process control device.

Examples of "strong" authentication include:

- Physical token authentication that employs both a physical device that must be in the possession of the remote user and knowledge of a personal identification number (PIN).
- Smartcard authentication
- Biometric authentication
- Location based authentication

ISA-TR99.00.01-2004 provides a good explanation of these technologies, their strengths, and weaknesses.

The discussion above focused on interactive users. It is just as important to employ appropriate authentication schemes for task-to-task communication between application servers. The communications interface employs methods to verify that the requesting device is indeed the correct device to perform the task. Critical interfaces check the Internet protocol (IP) address, check multi-port adaptor card (MAC) address, use a secret code, or use an encryption key to verify that the request is coming from the expected device. Interfaces with low risk use less secure methods for authentication. An example of non-secure communications would be anonymous file transfer protocol (FTP).

6.12.6.1 Authentication Examples

The following lists examples that are available as an attachment to CIDX members only:

Manufacturing and Control Systems Examples:

- Case 1 – High volume textile fiber spinning process
- Case 2 – Commodity low dollar product, chemical process has a potential for toxic fume release
- Case 3 – Palletizing and shrink wrapper control system

6.12.6.2 Resources Used

The following are resources used in the creation of this section:

- *ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems*, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 5 Authentication and Authorization Technologies
- ISO 17799:2000. Section 7 Physical and Environmental Security
- ISO 17799:2000. Section 9 Access Control

6.12.7 Introduction - Authorization

This section 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 (e.g., employees, applications, services, devices, and business partners) have access to required information assets.

Authorization is the automated process performed by the computer system to issue access privileges to resources upon successful authentication of the user and assignment of an account. The privileges granted are determined by the account configuration setup during the *Account Administration* step in the process.

Information assets cover a lot of territory. Information that is sensitive to disclosure needs to be properly protected both to maintain competitive advantage and to protect employee privacy. Examples of information assets include:

- Research information
- Technical information and "know-how" on processes and systems
- Earnings reports, sales forecasts, business strategies
- Information on investments, proposed mergers and divestitures
- Customer information
- Shipment information
- Sensitive employee data, such as salaries and performance reviews
- Real time process control parameters and information

6.12.7.1 Statement of Management Practice – Authorization

The business shall establish and employ a set of authentication practices commensurate with the risk of granting unauthorized users, hosts, applications, services, and resources access to critical system resources.

6.12.7.2 Baseline Practices – Authorization

Example baseline practices that chemical companies use for authorization include:

- The security policy that defines the access control rules and procedures is clearly documented and communicated to employees, joint ventures, third party contractors, and temporary employees.
- Some form of access control is present for all systems and data. The permission to access this may 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.
- Employees, joint ventures, third party contractors (individually or through the third party company), and temporary employees agree in writing to conform to security policy, including access control policies.
- All access to critical computer systems, success or failure, is logged by the system to be reviewed.

6.12.7.3 How Chemical Companies Are Approaching Authorization

Some examples of how chemical companies are approaching authorization are:

- Network connections between your company and other organizations are protected with a professionally managed firewall.
- An authenticating proxy server is used for all outbound access to the Internet.
- Native Address Translation (NAT) is used to mask your internal IP addressing
- The internal Domain Name Service (DNS) is not exposed outside the organization.
- Two-factor authentication is required for modem access (e.g. dial back, token, etc.).
- Ushered (or shadowing, which is the procedure for monitoring a remotely connected users) access is used when high risk tasks are performed (e.g. safety consequences or critical business systems).
- Information of high sensitivity and business criticality is segregated from other internal information.
- Stronger authentication – more than a simple user ID and password – is used for remote access to the network, especially from the Internet. Tokens, smart cards, soft certificates, and other techniques are appropriate.
- All communications of private information over the Internet are encrypted with Secure Socket Layer (SSL) or (if non-web) with encryption of equivalent or better strength.
- An access control device is used to separate the business systems network from the manufacturing and control systems network.

6.12.7.4 Unique Aspect of Authorization for Manufacturing and Control Systems

Some standard authorization practices employed in the general IT workspace may be inappropriate for manufacturing and control systems. For safety reasons, operators may have user accounts with passwords set not to expire. Similarly, individual role based user accounts may be inappropriate for control room work team environments.

6.12.8 Authorization for Local Users:

Many chemical manufacturing operations control their processes from control rooms staffed by several operators. These operators often function as a team and perform actions on multiple HMI stations as part of their normal job function. Authorization to perform specific job functions is provided by the application. The local user is granted access to certain nodes or operational displays based upon a job role based user account. The actual log-on username and password are common for the job role. This work team approach to control room operation may conflict with standard IT authorization policy and practice.

Safety implications are considered when developing the authorization strategy. For high vulnerability processes, privileges are set at the local process control device level and do not require access to devices at the LAN or WAN level. This supports the basic control principle of "minimizing the potential points of failure."

Operator and user accounts are configured to grant the minimum privileges required for the job role. Training is employed to establish common levels of skills for job roles. Customizing individual user accounts to match skill levels of personnel is avoided. All users in the same job function utilize the same role based user account.

6.12.9 Authorization for Remote Users

In the discussion that follows, the term remote user is anyone who is not physically present in the immediate manufacturing area or control room. The person in an office in the same building or the person connecting over the corporate WAN are both remote users as is the person connecting over public infrastructure networks.

User accounts are role based rather than user based. For example, the user does not utilize an account with system manager level privileges to perform a control room operator task. This practice is clearly defined in administrative procedures.

Role based user accounts take into account geographic location. A person may utilize one user account when working on-site and a different one when dialing in from home to assist local personnel. This practice is clearly defined in administrative procedures. Compliance to administrative procedures is based on individual accountability.

The authorization process discussed thus far basically places the authorization function at the end-node device and application level. In critical control environments, an additional destination authorization strategy is employed at a barrier device (firewall or router) for the process control network. Once a user is authenticated at the barrier device, role based destination access rights are assigned to the user so that the user can only attempt to connect to pre-assigned devices on the process control network. The end-node logon establishes the users final privileges for performing the function on the device. Facilities with high vulnerabilities take advantage of this additional level of destination authorization.

6.12.9.1 Authorization Examples

The following lists examples that are available as an attachment to CIDX members only:

Manufacturing Control System Examples:

- Case 1 – High volume textile fiber spinning process
- Case 2 – Commodity low dollar product, chemical process has a potential for toxic fume release
- Case 3 – Palletizing and shrink wrapper control system
- Case 4 – Controlling the action of connecting a laptop to the manufacturing and control system network

6.12.9.2 Resources Used

- Guidance for Cybersecurity Vulnerability Assessment Methodology Process Version 1.0, available from CIDX at www.cidx.org
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 9 Access Control.
- SANS web site (www.sans.org) for cybersecurity policy primer and samples
- US Chemical Sector Cybersecurity Strategy
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society.
- *ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems*, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 5 Authentication and Authorization Technologies."

6.13 Information and Document Management

This section provides practical guidance as described in both the BS 7799-2:2002, Section 4.3 of processes associated with the classification of all data and the safeguarding of information and document management associated with an information security management system (ISMS) and ISO/IEC 17799, Section 5.2. Document management is generally a part of the company records retention and document management system.

6.13.1 Applicability to Cybersecurity in the Chemical Sector

Companies use both comprehensive information and document management policy for their CSMS. Information associated with the development and execution of a CSMS is important, sensitive, and should be managed. Risk analyses, business impact studies, risk tolerance profiles, etc. contain sensitive company information and need to be protected. Security controls, philosophy, and implementation strategies are other examples. Additionally business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

6.13.2 Baseline Practices

Example baseline practices that chemical companies use for information and document management include:

- Classifying all information to indicate the need, priority, and level of protection required commensurate with its sensitivity and criticality.
- Assigning information classifications (e.g., restricted, classified, general, etc.) different levels of access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.
- Reviewing information that requires special control or handling on a periodic basis to validate special handling is still required.
- Developing and including policies and procedures detailing the record retention of company information.
- Developing and including policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall records retention policy. This also includes the method of disposal, disk erasing, or destruction.
- Assigning roles and responsibilities associated with the information and document management policies and procedures.
- Having a process that includes a compliance mechanism (e.g., audit) that may be internal or external.
- Developing and employing processes to prevent data corruption around backup processes and logging.

- Taking special care to confirm that the security, availability, and usability of control system configuration, which includes the logic used in developing the configuration or programming for the life of the manufacturing and control system.

6.13.3 How Chemical Companies Are Approaching Information and Document Management

Examples of how chemical companies are approaching information and document management include:

- Classifying information according to sensitivity and criticality. They employ a simple classification scheme of public, company use, restricted, and confidential. Special consideration should be given for data protected by data privacy regulations. Company workforce or subsets are assigned access to these document classifications according to their need (related to their job description). Other schemes use additional classification levels.
- Considering information that would be declassified due to passage of time or change of events.
- Developing documented procedures that detail the types of information and documents covered, and for each classification along with the corresponding retention and destruction schedule.
- Developing and employing documented procedures that explain the recommended technique to destroy and dispose of information and documents no longer needed.
- Employing the appropriate measures to ensure extended retention period information can be accessed.
- Having an annual date when clean-up of information is performed by the workforce in accordance with data retention policy.
- Developing and employing documented procedures that explain the process of decommissioning and disposing of the asset, especially where resource recovery is possible. Verification of decommissioning effectiveness is part of the procedure.
- Performing periodic reviews of compliance to the information and document management policy.
- Performing legal reviews of the retention policies to ensure compliance with any laws or regulations.

6.13.4 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Cybersecurity Information Classification

6.13.5 Resources Used

- The following are resources used in the creation of this section:
- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 4.3

- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 5.2
- See ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment for the discussion on "Conduct Risk Assessment and Gap Analysis."
- See ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems for the discussion on Personal Security Controls.

6.14 System Development and Maintenance

This section describes practical guidance for the security aspects of system design, development, and maintenance as specified in ISO 17799, section 10. The principles and guidance apply across the breadth of computer systems and applications.

Manufacturing and control systems are not particularly unique in the need for good cybersecurity development and maintenance practices. The only difference being that the systems integrate with the physical manufacturing process and are an integral part of safe operation of a facility. As such the system design, development, and maintenance practices dovetail with process safety reviews to ensure safe operation of the facility.

6.14.1 Statement of Management Practice

The overall objective of this section is to provide guidance that security is built into the information system and sustained through normal maintenance tasks. Just as one would clearly define and test the functional operation of the information system, the security functions should be defined, implemented, and tested.

6.14.2 Applicability to Cybersecurity in the Chemical Sector

Security is most effective when it is initially designed into the system and sustained throughout the life of the system as part of the maintenance process. “Bolt-on” equipment and applications added to reduce certain vulnerabilities have a definite place in reducing cybersecurity risks, but the better approach is to address it right up front as part of the design of the system.

6.14.3 Baseline Practices

Each of the component devices comprising the computer system has certain security functions that work with the security functions of the other devices to provide a level of security for the overall integrated system. The security functions/capabilities of each component are defined up front, developed, and tested collectively so that the entire system meets the desired security level. Certification of security functional compliance at the component level does not ensure that the overall integrated system is secure.

Security is an evergreen process. Changing threats and vulnerabilities of the system are examined on a periodic basis. Each system has its own security lifecycle with a review step that audits the effectiveness of the implemented security counter-measure controls versus the current threat risks. Risk tolerance dictates when new system security controls or compensating controls are necessary for safe and reliable operation.

Example baseline practices that chemical companies use for system development and maintenance include:

- Establishing a policy covering the types of risks that are managed with cybersecurity controls.
- Documenting and following a process for patching operating systems and applications. The process:

  - Defines how the organization monitors information sources for announcement of new vulnerabilities and patches
  - Evaluates the relevance of those patches
  - Implements patches required to reduce risk to an acceptable level
- Having outsourced software development staff sign a confidentiality agreement.

Test environments for IT systems are used wherever possible to evaluate and test program changes prior to implementing in the production environment. Due to cost, system stability, and difficulty simulating a test environment for manufacturing and control systems, changes are typically made during manufacturing shutdowns.

6.14.4 How Chemical Companies Are Approaching System Development and Maintenance

6.14.4.1 Business IT System Design and Maintenance

Some examples of how chemical companies are approaching system development and maintenance are:

- Involving the computer security organization at the beginning of all computer projects.
- Selecting and employing cryptographic products supporting encryption, digital signatures, and key management commensurate with risk.
- Using change management for application changes as well as infrastructure changes.

6.14.4.2 Unique Aspects of System Design and Maintenance for Manufacturing and Control Systems

The development and maintenance activities of manufacturing and control systems are not unique. Many of the same processes can be followed. The minor differences come from the level of safety risk that may be associated with the manufacturing and control system. These systems have a much longer operational life expectancy than many information systems. This presents several challenges as technology advances and vulnerabilities change over time. A system is likely to be comprised of components from several generations of technology and components from multiple vendors. This represents a significant challenge to ensure that risks are held to an acceptable level and that security does not erode over time.

Some examples of how chemical companies are approaching system development and maintenance are:

- The security requirements are specified as part of the front-end design activity and are tested as part of the site acceptance test of the system. The system security requirements undergo a process safety review as part of the overall operational process hazards review conducted on the design for the facility.
- Security requirements are considered and assessed during all maintenance activities on the system. This includes system and component configuration changes, operating system level revision changes/patches, application revision changes, and general enhancements.

- For high risk environments it is recommended that security assessments and reviews are conducted as part of the periodic Process Safety Management (PSM) process. Just as a site would test safety interlocks on a fixed schedule or as part of a standard restart of a line taken down for maintenance, the security functions of the manufacturing and control system are verified based upon the degree of risk of a security failure. Reassessment and testing are documented and recorded. A qualification process is employed to verify that people who make configuration changes to the control system have the appropriate training and experience. Individuals have to be re-qualified on a regular (e.g., annual) basis.

The NIST Process Control Security Requirements Forum (PCSRF) has developed an Industrial Control System Protection Profile (ICSPP) using the Common Criteria for describing the security requirements of information systems and their components. The methodology is quite rigorous and provides a framework for certification testing to demonstrate compliance to specification. The Common Criteria can be used to define the security requirements of off the shelf devices as well as custom systems. The ICSPP can be used to define the security capabilities needed in a manufacturing or control system.

6.14.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- IT System Examples
- Manufacturing and Control System Examples

6.14.6 Resources Used

The following are resources used in the creation of this section:

- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 10 Systems Development and Maintenance.
- ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, ISA—The Instrumentation, Systems and Automation Society. Section 6.9
- NIST PCSRF ICS-SPP (National Institute of Standards Process Control Security Requirements Forum Industrial Control System Protection Profile issued

6.15 Staff Training and Security Awareness

This section describes a practical guidance example of training employees, staff and other stakeholders and creating cybersecurity awareness as covered in both BS 7799-2:2002, Section 5 and ISO/IEC 17799, Section 6. Cybersecurity training and security awareness programs are most effective if they are tailored to the audience, consistent with company policy, and communicated regularly.

6.15.1 Statement of Management Practice

Management's commitment to training and ensuring adequate cybersecurity awareness is critical to providing a stable computing environment for both information and manufacturing and control systems. Effective cybersecurity training and security awareness programs should provide each employee with the information necessary to identify, review and remediate control exposures, and help ensure their own work practices are using effective controls.

6.15.2 Applicability to Cybersecurity in the Chemical Sector

Security awareness for all employees/contractors/et al. is an essential tool in improving compliance with corporate processes associated with cybersecurity, and reduces exposures and incidents. In the area of manufacturing and control systems, the same emphasis must be placed on cybersecurity control training as safety and operational integrity, since the consequences can be as severe. Technical resources should receive adequate technical training associated with known exposures of hardware, software, and social engineering, which help provide a strong defense against cyber attacks. Other companies in the value chain that handle products/raw material, and/or access systems must be considered and included in the company's security awareness training.

6.15.3 Baseline Practices

Example baseline practices that chemical companies use to train and create awareness include:

- Having senior level management support for cybersecurity training and awareness programs
- Addressing the various roles associated with maintaining a secure systems environment within the cybersecurity training curriculums.
- Having courses or having formal on the job related training to address requirements for each role.
- Validating user understanding via course evaluation.
- Having subject matter experts for each course who can provide additional information and consulting.
- Reviewing and validating the training curriculum periodically and evaluating its effectiveness.
- Communicating key messages to employees/contractors/etc. in a timely fashion via a security awareness communication program.
- Confirming the awareness program accurately reinforces corporate policies associated with cybersecurity.

- Establishing a process that provides up to date information for recently identified technical risks or control exposures.

6.15.4 How Chemical Companies Are Approaching Staff Training and Security Awareness

Examples of how chemical companies are training staff and creating security awareness include:

Senior level management supports the cybersecurity training and awareness programs and it is evident from the assignment of resources, funds, and participation.

- Training curriculums have a progression of material that is tailored for a given role in the organization. These roles can include, but are not limited to:
  - management
  - technical support staff
  - application support staff
  - manufacturing and control systems staff
  - end users (including home users)
  - new employees
  - cybersecurity professionals
  - third parties with access to company systems (value chain, service providers, vendors, onsite, offsite)
- Training curriculums address areas associated with cybersecurity such as:
  - physical security
  - risk management
  - corporate security and Internet policy
  - network exposures, including patch management and wireless networks
  - software exposures, including patch management (application and operating system)
  - disaster recovery
  - information protection/data privacy/encryption
  - access controls including authentication (i.e., password requirements, remote access)
  - Internet usage exposures
  - virus scan and update process
  - incident identification and reporting
- Cybersecurity training is a component of the company's overall training organization. The cybersecurity training staff has defined responsibilities and is also accountable to the cybersecurity management system (CSMS) team.
- Records of employee competencies are maintained and are reviewed against skill requirements for their position (subject to applicable Data Privacy Laws).
- Cybersecurity training is included in the standard employee processes that address basic employee work requirements.
- Companies leverage training provided software/hardware vendors. Typically the training provides an in-depth discussion of tools and associated exposures. Also, subscription to a security alert service ensures up-to-date knowledge of recently identified control exposure.

- Companies leverage training provided by established organizations that specialize in the field of cybersecurity. These include MIS Training Institute (www.misti.com), SANS Institute (www.sans.org), and NIST (www.nist.gov), etc.
- The security awareness communication program is a documented process that establishes the timing, frequency, and content of periodic communications to enhance the organizations' understanding of cybersecurity controls.
- The security awareness communication program includes an overview for new employees, contractors, and other third parties to ensure they are aware of the security practices on their first day. Many organizations have developed a web-based training program to provide this overview.
- The training and the security awareness program is reviewed annually for effectiveness, applicability, content, and consistency with tools currently used and corporate practices.

6.15.5 Examples

There are currently no examples available for this publication.

6.15.6 Resources Used

The following are resources used in the creation of this section:

- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 5
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000. Section 6
- SANS Training and Your Career Roadmap - www.sans.org/conference/trainingroadmap.php
- MIS Training Institute (www.misti.com)
- NIST (US National Institute of Standards and Technology) (www.nist.gov)
- See ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment for the discussion on "Developing a Secure Program."
- See ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems for the discussion on "Physical and Security Controls."

6.16 Compliance

This section provides practical guidance with respect to compliance as described in ISO/IEC 17799, Section 12.2. It also provides guidance on the BS 7799-2:2002, Section 6.4: Scheduling & Conducting an Audit of an information security management system (ISMS).

The purpose of this section is to provide specific guidance on carrying out these activities. Note that a cybersecurity audit may be performed as part of a broader audit program. Also included are audit procedures examples relating to cybersecurity.

The Compliance section consists of the following topics:

- 6.16.3 Compliance with Legal, Regulatory, and Security Requirements
- 6.16.4 Scheduling and Conducting Audits

6.16.1 Statement of Management Practice – General Compliance

Companies should periodically assess their security programs and processes to affirm those programs and processes are in place and working, and take corrective action as appropriate. In appropriate circumstances, assessments also apply to the programs and processes of other companies with whom the company conducts business such as chemical suppliers, logistics service providers, joint ventures, or customers. To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and security requirements, management should validate or audit for compliance. For security and safe operation of its assets, management should validate or audit for compliance to corporate security policies and practices.

6.16.2 Applicability to Cybersecurity in the Chemical Sector

The cybersecurity focal point would normally be responsible for ensuring that the organization has put suitable processes in place to undertake cybersecurity audits and also to monitor the level of compliance with cybersecurity policies, guidelines and procedures. Management should validate or audit for compliance to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations as it relates to cybersecurity. This is a broad-ranging task and needs to be properly structured to ensure that all key aspects of the cybersecurity process are effectively monitored.

An effective compliance program checks that a company's management practices are being implemented and adhered to. Either informal or formal audits of the information security and process control security processes, procedures, policies, and documentation are a good way to:

- Determine if there are any major components of the cybersecurity process that have been overlooked.
- Provide assurance on the appropriateness of the control environment and compliance with the overall cybersecurity objectives.
- Detect if parameters, patch levels, maintenance releases, etc. have introduced security exposures.
- Establish the appropriate control measures and verify that they are working as intended, consistently, and continuously.

- Verify compliance with any criminal and civil law or statutory, regulatory, and contractual cybersecurity obligations and requirements.
- Confirm that over a specified regular audit period (which should last no more than a year) that all aspects of the CSMS are functioning as intended. A sufficient number of audits should be planned so that the audit task is spread uniformly over the chosen period. Management should ensure periodic audits are conducted at least annually. Management should ensure that there is evidence that confirms that:
- Verify that the cybersecurity policy is still an accurate reflection of the business requirements.
- Verify that documented procedures are being followed (i.e., within the scope of the CSMS), and are meeting their desired objectives.
- Validate that technical controls (e.g., firewalls, access controls, etc.) are in place and are working as intended.
- Assess that residual risks are correct and that they are still acceptable to the management of the organization.
- Validate that agreed actions from previous audits and reviews have been implemented.

6.16.3 Introduction – Compliance with Legal, Regulatory, and Security Requirements

This section describes practical guidance of compliance. This subject is fairly broad and includes several topics that are all related and intertwined. This section addresses:

- Verifying compliance with legal, regulatory, and other external requirements (e.g., ACC Responsible Care Security Code)
- Verifying compliance to corporate security policies and practices
- Verifying compliance with the cybersecurity management system (CSMS) practices
- Making improvements in response to audits for compliance in these areas

6.16.3.1 Baseline Practices – Compliance with Legal, Regulatory, and Security Requirements

Legal, regulatory, and external compliance considerations:

- Identify applicable and changing legislation (e.g., encryption, data privacy, etc.)
- Establish policies and procedures to comply with legal restrictions on the use of materials in respect to intellectual property rights and the use of proprietary information
- Develop and manage record retention procedures and processes
- Apply controls to protect personal information in accordance with relevant legislation.
- Establish procedures to protect company assets against inappropriate use
- Establish appropriate procedures around collection and chain of evidence to support action against a person or organization.

System compliance with cybersecurity policies and practices based on the use, type, or version of the system:

- Verify compliance with cybersecurity policy and practices
- Have a process in place to assess and update policies and practices to match changing vulnerabilities an threats
- Have a process in place to conduct regular checks against compliance with cybersecurity implementation standards

Consider the results of the audits to be treated as inputs to continuously improve the processes for each subject area. Assess the CSMS for improvement opportunities.

6.16.3.2 How Chemical Companies Are Approaching Compliance with Legal, Regulatory, and Security Requirements

Corporate policies identify the objectives to be achieved, rather than how it is achieved. Audits in the manufacturing space measure compliance to security and safety objectives rather than company wide information technology (IT) standards. Audits must take into account the manufacturing architecture and any mitigating security controls (physical, cybersecurity, and EH&S controls) implemented to achieve the corporate objectives. Practices must be commensurate with the risk level.

Policies have compliance guidelines that help describe what steps can be taken to be compliant.

A public policy focal point is identified who monitors new legislation and regulatory requirements related to cybersecurity.

The CSMS establishes the working relationships between the IT and manufacturing and process control organizations. Cooperation between these organizations is imperative for a successful CSMS. The review of the CSMS examines the effectiveness of these different organizations to work together toward improved cybersecurity.

6.16.3.3 Examples – Compliance with Legal, Regulatory, and Security Requirements

The following lists examples that are available as an attachment to CIDX members only:

- Cyber Assessment and Audit Plan

6.16.3.4 Resources Used

COBIT provides controls that address operational and compliance objectives.

6.16.4 Introduction – Scheduling and Conducting Audits

This section describes a practical guidance on scheduling and conducting audits.

6.16.4.1 Statement of Management Practice – Scheduling and Conducting Audits

The organization shall periodically evaluate its compliance with relevant health, safety, security and environmental legislation and regulations. The organization shall periodically evaluate the effectiveness of its management system to determine whether or not it has been properly implemented and maintained. Information on the results of the evaluations shall be provided to management.

Management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements.

6.16.4.2 Baseline Practices – Scheduling and Conducting Audits

There are many practices companies may undertake that relate to audits for cybersecurity activities. A company may choose to implement, or appropriately modify, a combination of several of the below listed practices, commensurate with risk, and dependent upon its culture, existing systems, and size or complexity of its manufacturing control systems.

- Develop an audit program and related procedures that define an audit plan of the CSMS. In addition the program defines the frequency of the audit process.
- The audit procedures specify the methodology of the audit process, including the auditors qualifications and competency for auditing the specific systems that are in scope. The methodology should include a process for making risk-based audit decisions.
- Segregation of duties confirms independence (unbiased auditors); the auditor should not be the administrator of the system being audited.
- Interview a combination of the following individuals as appropriate to gain an understanding of the cybersecurity risks and mitigation measures taken: chief executive officer; chief operations officer; chief financial officer; chief information officer; IT planning committee members; IT steering committee members; IT security managers; IT senior managers; senior business managers, including those responsible for process control systems; environment, health & safety (EH&S) managers; manufacturing and engineering executives.
- Based on the results of the interviews and risk assessment, the audit plan could include both general control reviews (e.g., system development and maintenance process, change management process) and specific system audits (e.g., SAP, manufacturing and control systems) in areas of high and medium risks. The scope of the audit requirements should be consistent with the scope of the other management practices. In essence, an audit confirms compliance with the other management practices. All applications and systems should be included in the inventory of "auditable" entities. Applications and systems to be audited could be selected from the inventory based on the results of a risk assessment.
- Submit the audit reports to top management. It is critical that an audit report that includes nonconformance be promptly forwarded to the senior accountable person in management.
- Audit reports provide recommendations directed at correcting any reported nonconformance that was discovered in the audit process.
- Include a right to audit clause in the contract with external partners,
- Audit suppliers and service providers on cybersecurity criteria prior to forming cyber-related business relationships (e.g., e-business, application service providers)

- Address any items of concern identified from the audit in corrective action plans. Have a process in place to take corrective actions.

6.16.4.3 How Chemical Companies Are Approaching Scheduling and Conducting Audits

The people who perform the self-assessment for compliance and implementation of improvements to the CSMS should be interviewed during an audit.

Audit Types:

- Independent audits: publicly held companies have both internal and external auditors that execute this task. Internal auditors typical maintain management independence by reporting to an audit committee. The external auditors are hired by the Controllers on behalf of the Audit Committee.
- Security health checks/compliance reviews: Some organizations have individuals focused on information security and execute audit-like tasks to validate compliance.
- Self-assessments: in some organizations the system administrators and data owners conduct self-assessments to validate compliance.

Audit Frequency:

- The generally accepted practice for independent internal audits is to have components of the management system throughout the year based on some rotation where all components are addressed over a period of time. Typically, critical systems are audited every three to five years.
- Self-assessments should be conducted every twelve to eighteen months, with some companies conducting at the midpoint of the audit cycle.
- During the implementation phase of a management system a more frequent audit of the management system might be appropriate.
- Any part of the management system that has been previously determined to be in nonconformance should be audited with an increased frequency.

The methodology of the audit process includes two distinct steps:

- Determine whether the management system conforms to the requirements of particular standard being followed (e.g., IS 14001, ACC RCSMS, BS 7799:2)
- Check that the system has been managed as described in the cybersecurity policy statement, the cybersecurity objectives and targets, and the related work descriptions and procedures.

6.16.4.4 Unique Aspects of Scheduling and Conducting Audits for Manufacturing and Control Systems:

Compliance audits can be very challenging to conduct and tracked metrics may be misleading. Differences include:

- Compliance metrics for manufacturing and control systems are handled separately from metrics tracked for desktop and business systems. The right situation from a safety and reliability perspective may not be to install the latest patch(es) or release.

- Patching and upgrades are examined on a system-by-system basis. Vendor certification of the compatibility of a patch is obtained before installing the patch or upgrade in a running manufacturing environment.
- The potential environmental, safety, and health implications of all software changes, including security patches and software upgrades, are assessed as part of standard site EH&S processes prior to making any changes.

Automated Compliance Scanning Tool:

- As a general practice, automated scanning tools to audit for installed software patches and revision levels are avoided on manufacturing and control devices. Certain older installed devices do not have sophisticated error handing routines and scans can overload the device and effectively create a denial of service interruption. This could have serious consequences depending upon the function of the device. Damage to equipment, loss of production, or a safety incident could occur.
- Extra care is taken to ensure that a manufacturing or control system is not accidentally included in the network range configured in an automated scanning tool. An accidental scan or an intentional scan can have the same adverse consequence.

6.16.4.5 Examples – Scheduling and Conducting Audits

There are currently no examples available for his publication.

6.16.4.6 Resources Used

- Information Systems Technology Audit Programs: The following collection of audit programs was contributed by auditors from around the world. (Note: some programs may require a contribution of an audit program). Refer to www.auditnet.org/asapind.htm
- Control objectives for information and related technology (COBIT) can be used as an industry standard supplement. Refer to www.isaca.org
- *ISO/IEC 17799, Information Technology – Code of Practice for information security management*, First Edition, 2000. Section 12.2: Review of security policy and technical compliance and 12.3: System audit considerations could be used as a guideline for developing the audit program.
- *BS 7799-2:2002, Information Security Management. Specification with Guidance for Use*, September 2002. It could be used as a guideline for developing the audit program. BS7799-2:2002 standard can be purchased via www.bspsl.com/secure/17799/cvm.cfm (Note: It is less expensive when you purchase ISO/IEC 17799:2000 (Part 1) and BS7799-2:2002 (Part 2) together as a kit).
- The eScan Security Assessment can help determine how well your company's information technology systems are protected against failure or intrusion. The tool contains a series of questions and provides recommendations in the following areas: computer virus protection; file permissions; computer system physical environment; back-up policies and procedures; potential computer system mechanical failures; IT contingency planning; information technology and security policies; international eCommerce concerns; Internet and eCommerce; operating systems, and security concerns. www.escan.nist.gov/sat/index.nist

6.17 Business Continuity Plan

This section provides practical guidance as described in ISO/IEC 17799*,* Section 11. It discusses appropriate business continuity and disaster recovery planning. This section provides guidance on this subject, including the creation and verification of a formal plan, and planning for recovery from specified events (e.g., disasters).

6.17.1 Statement of Management Practice

The purpose of the business continuity plan is to provide a course of action to respond to the consequences of disasters, security failures and loss of service to a business. Contingency plans should be developed and implemented to ensure that business processes can be restored in a timely fashion. Business continuity plans "include controls to identify and reduce risks, limit the consequences of damaging incidents and ensure the timely resumption of essential operations."[1]Disaster recovery is a plan to restore computing services in the event of a disaster.

6.17.2 Applicability to Cybersecurity in the Chemical Sector

While the primary focus of a cybersecurity management system is to prevent or avoid the occurrence of a security event, plans are needed in the event one occurs. An effective cybersecurity management system includes a detailed plan to ensure that regular business information, and manufacturing and control systems can be restored and utilized as soon as possible after the occurrence of a significant security event. This plan includes anticipation of and adequate preparation for various types of "disasters," including the definition of a recovery team and specification of what is required to establish backup operations. Inherent in the planning process is determination of the impact of business information, and manufacturing and control systems on each business and the determination of consequences associated with loss of one or more of the systems. (See section *6.1 Importance of Cybersecurity in Business*.)

6.17.3 Baseline Practices

A business continuity plan builds on the analysis and preparation that has been done in other parts of the cybersecurity program. For example, the risk analysis contributes specific actions to be taken in a disaster situation. It also highlights external dependencies.

Business continuity planning is divided into two sections: plan development and plan content and execution.

Example baseline practices that chemical companies use in "business continuity plans" for each of the sections are below:

[1] Extracted from ISO/IEC 17799:2000(E).

Plan development:

- The business owners, IT personnel, and manufacturing and control personnel form a business continuity team.
- This team determines the priority of critical business and manufacturing and control systems based on the nature of the system and the time required for restoration. This is based on the company risk tolerance. (See section 6.1 Importance of Cybersecurity in Business.)
- The team determines the amount of time/resources required for system restoration, location of back up files, hardware, frequency of backup, need for hot spares, etc. to ensure critical systems can be restored in the event of a disaster situation.
- The team considers the possible impact on third parties such as joint ventures and value chain.
- The team determines the need for additional business insurance.
- The team needs to determine the appropriateness of the type and manner of disaster recovery backup. Options include:
  - Hot site – location where infrastructure and applications are readily available
  - Cold site – empty location where the company can bring in infrastructure and applications, when needed

Plan content and execution

- Define and communicate the specific roles and responsibilities for each part of the plan. Some companies divide the team into sub teams reporting to an executive committee. Sub teams can include damage assessment, restoration and recovery, communications (internal and external), emergency response, etc.
- Assign the responsibility for initiating the business continuity/disaster recovery plan, and clearly define the circumstances under which to activate the plan.
- Detail the communications to the team members along with contingencies for loss of email, phone disruption, etc.
- Define the frequency and method to test and validate the continuity. Use these results to improve and update the plan for increased effectiveness.
- Detail the risks associated with operating under the continuity plan and how are they going to be addressed and/or mitigated.
- Describe the process for resuming normal operations.
- Detail in the plan under what circumstances to take specific emergency measures. The choice of measures varies according to the specific scenario.
- Define the type, number, and identity of the resources needed and their assignments.
- Identify data that requires special handling and protection, as well as the information that is critical to continued operation.
- Detail interim procedures to continue business operations.

- Identify backup systems and applications software, along with appropriate instructions for making the systems operational, store in a safe location, and inspect regularly.
- Locate back-up equipment such as computers, communications, and supporting equipment for the team (in the event of damaged equipment) in a safe area and inspect regularly.
- Identify miscellaneous supplies for normal operation and personnel responsible for acquiring them.
- Identify alternate facilities for contingent business operations. Arrangements for the use of these facilities may include licensing of required software or other applicable/required licenses or permits.
- Consider the consequences of an IT or manufacturing and control systems disaster having physical impact to production facilities:
  - Alternate sources of raw materials for production may be required if the event interrupts the normal supply.
  - Finished products to be produced under the backup plan are identified. A reduced product slate may be appropriate during business continuity plan operation.

6.17.4 How Chemical Companies Are Approaching Business Continuity Plan

The following are examples of how chemical companies are approaching business continuity:

- Prioritize business systems (IT systems) and manufacturing control systems by criticality to the business or operation based on company risk tolerance.
- Locate in different geographic areas critical systems backups with system copies (hot spares). If this is not feasible, store backup data and equipment (cold spares) at least ten miles from the primary system.
- Test and update business continuity plans annually.
- Tie business continuity plans to a management of change system that ensures a plan update in the event of significant changes in system or business criticality.
- Test communications plans annually and assign responsibility to keep call lists up to date.
- Keep written copies of the plan at home by each of the team resources.
- Detail and test the adequacy of the procedures for bringing up spares/backups using resources that are not responsible for the primary system.
- Identify data that requires special handling and protection, as well as the information that is critical to continued operation.
- Detail interim procedures to continue business operations. These can include manual collection of data to be entered into the system, recovery or reconstruction of lost data, procedures for taking sales orders, tracking shipments, etc.
- Identify backup locations for critical operations and arrange for use along with the necessary equipment and tools required for operation. Inspect these sites along with off site storage sites annually.
- Have procedures in place to purchase additional hardware, software, and supplies if needed.
- Establish service level agreements with providers of your disaster recovery service in advance.

- Provide critical contact information to the core team (in form of card carried by each team member).

In the case of manufacturing and control systems, such plans are typically developed as part of the overall disaster plan for the facility and are the responsibility of operations. If these operations plans do not include adequate provision for the electronic control systems, this could represent a significant gap. It is important that the continuity plan balance the replacement times for manufacturing and control systems with the replacement times for the process equipment being controlled. In some cases, process equipment may have long lead times for repair/replacement that greatly exceed the replacement time of the control systems.

6.17.5 Examples

The following lists examples that are available as an attachment to CIDX members only:

- Disaster Recovery & Business Continuity Plan

6.17.6 Resources Used

The following are resources used in the creation of this section:

- ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004, the Instrumentation, Systems and Automation Society
- ISO/IEC 17799, Information Technology – Code of Practice for information security management, First Edition, 2000
- Corporate Governance Task Force “Information Security Governance- A call to action” www.cyberpartnership.org/InfoSecGov4_04.pdf
- ANSI Standard www.webstore.ansi.org/ansidocstore

6.18 Monitoring and Reviewing CSMS

This section describes practical guidance of BS 7799-2:2002, Section 4.2.3, Monitor and Review Cybersecurity Management System (CSMS).

6.18.1 Statement of Management Practice

Management should continuously monitor and review their management system. Monitoring and reviewing performance of a company's management system provides the checks and balances the company has in place to monitor and evaluate its performance. Internal checking methods such as auditing of the management system; compliance audits; and incident investigations allow the company to determine the effectiveness of the management system and whether it is operating according to expectations. Finally, through a management review process, the company's senior leaders review information on the management system, developed through the measurement and corrective action process, and any deviations from the goals, targets and objectives set in the planning process. If there are deviations or nonconformance, company leaders revisit the original assumptions and take appropriate corrective actions.

6.18.2 Applicability to Cybersecurity in the Chemical Sector

Companies should include a process for monitoring and reviewing the performance of their CSMS. Monitoring detects cybersecurity incidents, including failed and successful cybersecurity breaches in the company's environment. This enables management to determine whether the cybersecurity activities delegated to people or implemented by information technology are performing as expected. Regular review of the CSMS should also be done to validate the effectiveness of it in meeting cybersecurity policy and objectives taking into account results of cybersecurity audits, incidents, suggestions, and feedback from key stakeholders.

6.18.3 Baseline Practices

Example baseline practices that chemical companies use to monitor and review CSMS include:

- Procedures are in place to identify failed and successful cybersecurity breaches.
- Actions to take to resolve a breach of cybersecurity are defined in light of the business priorities.
- Processes are employed to collect metrics (e.g., audits, incidents) that help verify that the cybersecurity activities (manual or automated) are performing as expected.
- A process is employed to trigger a review of the level of residual risk and acceptable risk taking when there are changes to the organization, technology, business objectives, processes and external events including identified threats and changes in social climate.
- Operational data is analyzed, recorded, and reported to assess the effectiveness or performance of the CSMS.

6.18.4 How Chemical Companies Are Approaching Monitoring and Reviewing CSMS

Examples of how chemical companies are approach the monitoring and reviewing of their CSMS include:

- Implementing and testing an incident response process on a routine basis. The process includes a mechanism so that corrective actions identified as the result of a cybersecurity incident are fully implemented. The process facilitates understanding any interdependencies between IT (business and manufacturing and control systems), process safety, and physical security incident processes to ensure all implications of incident(s) are explored. The incident response process has links to the company's crisis management team.
- Employing processes for timely reporting of cybersecurity incidents.
- Educating employees on their responsibility to report cybersecurity incidents. Examples of reportable incidents are provided so employees can better comply with reporting requirements.
- Reviewing the results of audits, self-assessments, cybersecurity incident reports, and feedback provided by key stakeholders regularly to understand the effectiveness of the CSMS.
- The cybersecurity metrics program is in place built upon the seven key steps listed below:

  1. Define the metrics program goal(s) and objectives;
  2. Decide what metrics to generate;
  - Provide a retrospective view of security preparedness by tracking the number and severity of past security incidents, including patterned small events.
  - Proactively assess and potential security vulnerabilities (e.g., % of security audits fixed by agreed date).
  - Track implementation and usage of security and preventative measures (e.g., % of value chain partners in compliance with security standards)
  3. Develop strategies for generating the metrics;
  4. Establish benchmarks and targets;
  5. Determine how the metrics will be reported and to whom;
  6. Create an action plan and act on it; and
  7. Establish a formal program review/refinement cycle.
- The incident response processes includes the manufacturing and control systems.

6.18.5 Examples

There are currently no examples available for this publication.

6.18.6 Resources Used

The following are resources used in the creation of this section:

- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 4.2.3

- NIST (the US National Institute of Standards and Technology) has a Security Metrics Guide for Information Technology Systems.
  Refer to www.csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

6.19 Maintaining and Implementing Improvements

This section describes practical guidance of the BS 7799-2:2002, Section 7.0, maintain and implement improvements for a cybersecurity management system (CSMS).

6.19.1 Statement of Management Practice

Since practices for addressing security are evolving, it is anticipated that company security programs and measures will evolve, reflecting new knowledge and technology. Companies should continually be tracking, measuring, and improving security efforts to keep people, property, products, processes, information, information systems, and manufacturing and control systems more secure.

The organization should seek to continually improve the effectiveness of the CSMS using the policy, objectives, monitoring of progress and performance, analysis of trends and development and implementation of corrective actions.

6.19.2 Applicability to Cybersecurity in the Chemical Sector

The overall objective is to ensure the CSMS remains effective by ensuring there are regular reviews of the results and improvements made where needed. This should include a description of procedures for the management and operation of the controls in the CSMS and processes for ongoing review of risks and their treatment in the light of changing technology, threats, or functions.

Continual attention to security provides an indicator to company employees that cybersecurity is a core company value. Additionally, by integrating changes continually, there is less of a need for significant amounts of time to be spent updating a company's entire cybersecurity program periodically. Companies should strive to improve, not only in absolute terms, but also relative to continually escalating threats

6.19.3 Baseline Practices

Example baseline practices that chemical companies use to maintain and implement improvements to a CSMS include:

- Improving the effectiveness of the CSMS using the cybersecurity policy and objectives, results of self-assessments reviews and independent audits, corrective and preventative actions, and management reviews.
- Measuring and reviewing the performance of the CSMS in meeting cybersecurity policy and objectives.
- Conducting reviews of the performance results to determine:
  - If the current state of cybersecurity is satisfactory, then attention is given to evaluating changes in technology and business requirements and the identification of new threats and vulnerabilities to anticipate future changes to the CSMS to ensure its continued effectiveness in the future.
  - If the current state is unsatisfactory, then ineffective CSMS processes and procedures or non-conformities are further investigated to identify root cause and areas where there are systemic problems. Actions are identified not only to resolve the issue but also to minimize and prevent reoccurrences.

- Involving the focal points in the organizations for information security and manufacturing and control systems in the reviews.
- Identifying appropriate corrective and preventative actions to further improve the performance process.
- Prioritizing improvements in the CSMS and put plans in place to implement them (e.g., budgets, project planning etc.).
- Implementing all changes using the management of change processes within the organization.
- Communicating action plans and areas of improvement to key stakeholders.
- Identifying areas where improvement is needed using trend analysis as a tool.

6.19.4 How Chemical Companies Are Approaching Maintaining and Implementing Improvements

Companies undertake many different strategies to drive continuous improvement in cybersecurity activities. The strategies are commensurate with risk and dependent upon corporate culture, existing systems, and size or complexity of digital systems. Some potential strategies are listed below:

- Processes are in place to continue to evaluate new strategies or technologies that may improve current cybersecurity activities. The evaluations and processes are commensurate with risk.
- Benchmarking activities are conducted both within and outside of the industry. External validation can be used to help validate improvements.
- Employee feedback on security suggestions is actively sought and is reported back to senior management as appropriate on performance shortcomings and opportunities.
- Employees are encouraged to help visitors and contractors comply with cybersecurity requirements.
- Performance is evaluated through key performance indicators such as threat or incident trends within the group to ensure that CSMS strengths are commensurate with cybersecurity objectives.
- Target completion dates are assigned to improvement activities along with appropriate follow-up processes.
- Improvement approaches are adjusted depending on the degree of standardization and centralization.
- Standard corporate business methodologies such as Six Sigma (a process-focused methodology designed to improve business performance through improving specific areas of strategic business processes) are used for measuring, analyzing, improving and sustaining cybersecurity improvements.
- Security trained process engineers conduct operational security reviews on the manufacturing and control systems. In addition, security issues are frequently reviewed at a broader level by a governance body.

6.19.5 Examples

There are currently no examples available for this publication.

6.19.6 Resources Used

The following are resources used in the creation of this section:

- The IDEAL[SM1] model is an organizational improvement model that serves as a roadmap for initiating, planning, and implementing improvement actions. IDEAL model is named for the five phases it describes: initiating, diagnosing, establishing, acting, and learning. : www.sei.cmu.edu/ideal/ideal.html
- Chemical Industry Data Exchange Guidance for Addressing Cybersecurity in the Chemical Sector Version 1.0, available from CIDX at www.cidx.org
- BS 7799-2:2002, Information Security Management. Specification with Guidance for Use, September 2002. Section 7.0

7 Project Team Acknowledgement

The table below is an alphabetical list of those people who participated in or contributed to the "Guidance Document" and the development or review of this report.

The goal was to assemble a team with diverse backgrounds and varying skill sets. This included individuals from CIDX member companies as well as service providers. Those with a broad background in IT security, engineering, manufacturing and control systems, audit, and risk management were sought. The effort to obtain team members did not intentionally exclude anyone.

Name	**Company**	**Location**	**Background**
Barbara Ayers	ExxonMobil	Houston, TX, USA	IT Security
Paul Baybutt	Primatech	Columbus, OH, USA	Risk Management, Manufacturing & Control Systems
Eric Cosman	DOW Chemical	Midland, MI, USA	Manufacturing & Control Systems
Tom Good	DuPont Chemical	Wilmington, DE, USA	Manufacturing & Control Systems
Theresa Grant	DOW Chemical	Midland, MI, USA	IT Security
John Lellis	Aspentech	Houston, TX, USA	Manufacturing & Control Systems
Blair Moore	CIDX	Dallas, TX, USA	Risk Management
Steve Sarnecki	OSIsoft	Baltimore, MD, USA	Manufacturing & Control Systems
Ron Sielinski	Microsoft	Redmond, WA, USA	Manufacturing & Control Systems
Ton Van Kerkhoven*	DOW Chemical	Terneuzen, Netherlands	IT Security
Mark Winzenburg	British Petroleum	Naperville, IL, USA	IT Security

*Team leader

8 Road Map of CIDX Cybersecurity Management Program

A thorough evaluation of the various sections of the ISO, ISA, and Responsible Care documents revealed similarities in topics addressed. Here the team worked to consolidate topics that overlapped and added topics not addressed by the publications. In the end, the team combined several control domains, reorganized sub sections of control domains into a more logical grouping and added a new section on information and document management. Below are the organizational changes:

- ISO control domain “Security Policy” was combined with the BS control domain “Define Security Policy”
- BS control domain “Establish the Security Organizational Structure” was combined with the ISO control domain “Organizational Security”
- BS control domains “Prepare and Implement risk mitigation strategy” and “Implement Identified Controls” were combined with “Risk Management and Implementation”
- BS control domain “Schedule and conduct audits” was combined with the ISO control domain “Compliance”
- The information classification section of ISO “Asset Classification” and Control” and BS information classification part in control domain “Identify, Classify and Assess the Risk” were combined into “Information and Documentation Management”
- For clarity, ISO control domain “Access Control” was divided into three sections: authorization, authentication, and administration.
- A section in the BS control domain was added to address “Information and Document Management”

Appendix I – CIDX Key Element Self-assessment Questions

This section provides self-assessment questions to validate if your company is in compliance with the guidance for each of the following:

6.1 Importance of Cybersecurity in Business

The following questions are provided to validate company compliance with establishing the importance of cybersecurity in business:

- Does your company identify and document the business objectives, critical business processes and critical IT processes?
- Does your company identify dependence of business on IT systems?
- Has your company identified various damage scenarios by the loss of confidentiality, integrity, availability of information, operational reliability and/or safety?
- Have business impact analyses for IS, manufacturing and control systems and business ventures (value chain partners, third parties, outsourcing partners, etc.) been developed?
- Is there an established risk tolerance profile for your company?

6.2 Scope of Cybersecurity Management System

The following questions are provided to validate company compliance with defining the CSMS scope:

- Is there an organization responsible for the establishment, communication, and monitoring of cybersecurity within the company and has senior management agreed to the scope and structure of the CSMS?
- Is the scope of the CSMS clearly documented to include:
  Information systems
  Manufacturing and control systems
  Networks, LANs, WANs and include integration points with value chain partners
  User responsibilities
  Information protection
  Risk management
  Disaster recovery (training requirements, compliance and audit, and asset identification)
- Are all employees aware of the CSMS, and can refer to the appropriate sections?
- Are those with “key” roles in the system aware of their responsibilities?
- Has an adequate budget been established for the CSMS?

6.3 Security Policy

The following questions are provided to validate company compliance with defining security policy:

- Is there management commitment, involvement, and support in the creation and enforcement of policies?
- Is there a formal security policy?
- Is a review performed by all affected business units and departments, including manufacturing management?
- Are policy owners identified?
- Is the official policy statement distributed to employees?
- Is there documentation or a procedure to describe how updates to policy are handled?
- How are exceptions to the policy approved and documented?
- Is compliance verified?

6.4 Organizational Security

The following questions are provided to validate company compliance with the guidance for organizational security:

- Does our company vest the responsibility for cybersecurity to an individual or individuals?
- Is there a cross functional team or group of individuals representing the various departments and business units designated with oversight for cybersecurity?
- Is physical security represented?
- Do third party or outsourcing contracts include provisions for destruction of information or assets, restrictions on copying and responsibilities with respect to legal matters taking into account different national legal systems, intellectual property rights, access methods, change management procedures, training, and notification and reporting requirements?
- Are risk assessments completed prior to engaging third party contractors or outsourcers?
- Does our company have established relationships with law enforcement, regulators and Internet service providers for the purpose of information sharing around security incidents or preventive measures?
- Are there processes to remove 3rd party access in a timely manner at the conclusion/termination of the contract?
- Are personnel assigned responsibility for cybersecurity, and an appropriate level of funding to implement?
- Is there commitment from executive management?
- Is there a company-wide security team (or organization) that provides clear direction, commitment, and oversight?
- Do contracts exist that address cybersecurity for business partners, third party contractors, and outsourcing partners, etc.?
- Are there metrics for organizational success?
- Is there coordination with or integration with the physical security organization that addresses security recognizing the overlap and synergy between physical and information systems security risks?

6.5 Personnel Security

The following questions are provided to validate company compliance with personnel security:

- Does our company include security requirements in job descriptions?
- Are duties segregated for checks and balances?
- Is there a formal screening procedure in place for new hires? Does the procedure look at movement into sensitive jobs (i.e., promotions, transfers, etc.)?
- Are confidentiality or nondisclosure agreements reviewed, signed, and maintained for: employees, third party contractors, and temporary employees?
- Are security responsibilities clearly stated in the terms and conditions of employment for employees, third party contractors, and temporary employees?
- Is there a security training program relevant to the particular job function (initial plus periodic)?
- Does our company have a disciplinary process for security policy or procedure violations?

6.6 Physical and Environmental Security

The following questions are provided to validate company compliance with the guidance for physical and environmental security:

- Does a general description of the building access exist?
- Does a description of physical access controls for computer rooms and control rooms exist?
- Are secure areas restricted by additional controls?
- Is equipment that is used off-site protected to the same degree afforded to on-site?
- Are password-protected screen savers used?
- Are removable media devices secured or disabled?
- Are one or more physical security perimeters established to provide barriers to unauthorized access to facilities?
- Are appropriate entry controls provided at each barrier or boundary?
- Are physical assets (equipment) protected against environmental damage from threats such as fire, water, smoke, dust, radiation, impact, etc.?
- Are single points of failure avoided where possible?
- Are all external connections (power, communications, etc.) adequately protected from tampering or damage?
- Is all equipment including auxiliary environmental equipment properly maintained to ensure proper operation?
- Are proper procedures established and audited with respect to the addition, removal, and disposal of all equipment?
- Is all information that is expressed in a physical form (e.g., written or printed documents, magnetic storage media, card-access readers, etc.) adequately protected against physical threats?

6.7 Risk Identification, Classification, and Assessment

The following questions are provided to validate company compliance with risk identification, classification, and assessment:

- Does your company maintain an up-to-date record to know what to protect?
- Do you classify the information assets and components based on confidentiality, integrity, availability, safety, and environmental?
- Is there a risk assessment process developed that conducts a risk assessment by analyzing threats, vulnerabilities, costs and consequences?
- Is criteria established for identifying critical business and manufacturing and control systems processes and the IT systems, which support these processes?
- Are the risk assessment activities prioritized based on criticality?
- Are all information assets and critical components identified and boundaries of the system scoped?
- Is the change management system positioned to identify reassessment criteria based on technology, organization or process changes?
- Is risk assessment conducted through all stages of the technology lifecycle like development, implementation, updates, and retirement?

6.8 Risk Management and Implementation

The following questions are provided to validate company compliance with risk management and implementation:

- Does your company have an implemented risk mitigation strategy based upon threats, detected vulnerabilities and consequences?
- Is a risk mitigation strategy in place to identify and select the required security controls?
- Are security policies defined and validated?
- Are procedures developed that provide details like actions to take for preventing, detecting and responding to threats?
- Have standards and services been developed?
- Are security tools and products identified?
- Is the risk tolerance profile understood? Depending on the severity of the impact and consequences, the risk tolerance could be different.
- Has the cost versus benefits been compared? Select the security controls whose cost is less than the risk it is attempting to reduce.
- Have the controls required to mitigate each risk been identified? Take the detailed risk assessment, identify the cost of mitigation, compare with the cost of a risk occurrence, and select the preferred security controls.

- Has a process been established for accepting risk, which includes appropriate management level approval based on scope and documentation?

6.9 Statement of Applicability

The following questions are provided to validate company compliance with statement of applicability:

- Is there a written SoA?
- Does the SoA document control objectives and controls to accomplish them?
- Are the controls selected based on risk assessment?
- Are reasons provided for the selection or exclusion of controls?
- Is the SoA a controlled document?

6.10 Incident Planning and Response

The following questions are provided to validate company compliance with the guidance for incident planning and response:

- Are there written incident planning and response plan?
- Has the incident response plan been tested?
- Does the plan address worst-case and most credible scenarios?
- Who has the overall responsibility for coordinating and executing the plan?
- Are incident planning and response procedures established?
- Is a person responsible for executing the plan when the need arises named?
- Is an incident response team structured, including additional personnel, who can be called-in.
- Has responsibility for coordinating defense and response to an incident been established?
- Can an incident from initiation through final review be handled?
- Have procedures for different types of incidents like denial of access, system attacks, malicious code, unauthorized access, and inappropriate usage been created?
- Have pro-active measurements to identify attacks during early stage been identified?
- Has base planning on threat scenarios from vulnerability analysis and risk assessment been completed?
- Have written response procedures been developed?
- Have manufacturing and process control systems incidents been communicated to the IT organization as well as the process safety organization?
- Have IT incidents been communicated to the manufacturing and process control organization for awareness building?

- Have the details of the incident, the learning's, and the course of action to prevent from occurring again been documented?
- Have drills been conducted to test the plan?

6.11 Communications, Operations, and Change Management

The following questions are provided to validate company compliance with the guidance for communications, operations, and change management:

- Is a change management process documented and followed?
- Is an incident management process documented and followed?
- Is a process for antivirus management documented and followed?
- Does a process to track status on deployment and use of antivirus software exist?
- Does a process to identify new cybersecurity vulnerabilities and address the safety implications created by the new vulnerabilities exist?
- Is a patch management process that incorporates risks and consequences into the development of the implementation plan documented?
- Are procedures and practices for backup and restore of computer systems defined, used, and verified by appropriate testing?
- Is a system of controls over information exchanged with between organizations (i.e., between your company and other companies) documented and followed?

6.12 Access Control

Account Administration

The following questions are provided to validate company compliance with the guidance for account administration:

- Is there a formalized process for adding and approving new users on manufacturing and control systems that includes standard principles around the separation of responsibilities? If so, does it have an audit trail of all changes?
- Is there an established cycle to review user accounts to make sure they are correct and still needed?
- Are users assigned the minimum privileges and authorizations necessary to perform their tasks?
- Is every user individually identifiable and each access controlled by an appropriate method of authentication (e.g., user ID and password)?
- Is an alternative identification for forgotten password?
- Is access granted, changed, or terminated on the authority of an appropriate manager?
- Is a record maintained of all access accounts, including details of the individual, their permissions, and the authorizing manager?

- Are access accounts suspended or removed and access permissions revoked as soon as they are no longer needed (e.g., job change)?
- Is the need for access to critical systems explicitly reconfirmed on a regular basis?
- Are default passwords changed immediately?

Authentication

The following questions are provided to validate company compliance with the guidance for authentication:

- Have a set of authentication practices been developed and implemented that are commensurate with the risk consequence of unauthorized access to the specific control systems?
- Do the authentication practices address the differing vulnerabilities associated with locations of varying physical security levels?
- Are there processes in place to communicate and remind users of administrative procedures employed for authentication and their personal responsibility to adhere to them?
- Are all application users authenticated via the application to use the application? Note: This requirement may be waived when there are compensating physical controls.
- Is the minimum level of authentication a userid & password?
- Are authenticators and credentials protected while in storage and during transmission?
- Are users trained to keep passwords confidential?

Authorization

The following questions are provided to validate company compliance with the guidance for authorization:

- Does our company include security requirements in job descriptions?
- Is there a formal screening procedure in place for new hires? Does the procedure look at movement into sensitive jobs (i.e., promotions, transfers, etc.)?
- Are confidentiality or nondisclosure agreements reviewed, signed, and maintained for employees, third party contractors and temporary employees?
- Are security responsibilities clearly stated in the terms and conditions of employment for employees, third party contractors, and temporary employees?
- Is there a training program (initial plus periodic)?
- Does a disciplinary process exist for security policy or procedure violations?
- Is the security policy that defines the access control rules and procedures clearly documented and communicated to employees, joint ventures, third party contractors, and temporary employees?
- Is some form of access control present for all systems and data?

- Do employees, joint ventures, third party contractors (individually or through the third party company), and temporary employees agree in writing to conform to security policy, including access control policies?
- Is all access to critical computer systems, successful or failure, logged by the system to be reviewed?

Manufacturing and Control Systems Authorization

The following questions are provided to validate company compliance with the guidance for manufacturing and control systems' authorization practices:

- Have a set of authorization practices been developed and implemented that are commensurate with the risk consequence of their action for the specific control systems?
- Are user accounts setup with non-expiring passwords?
- Have user account privileges been defined with geographical location in mind for the user?

6.13 Information and Document Management

The following questions are provided to validate company compliance with information and document management:

- Is a data classification system in place that accounts for varying levels of need, priority, sensitivity, and criticality of information?
- Are policies and procedures documented detailing the record retention of information?
- Are policies and procedures documented detailing the destruction and disposal of written records, equipment, and other media?
- Are guidelines documented explaining when information and documents should be retained/destroyed?
- Are roles and responsibilities associated with information and document management documented?
- Does a process exist to review policy compliance (e.g., audit)?
- Are processes developed and employed to prevent data corruption around backup processes and logging?
- Is special care taken to ensure the security, availability, and usability of controls system configuration including the logic used in developing the configuration or programming?
- Are information classifications (e.g., restricted, classified, general etc.) assigned a different level of access and control to include copying, transmittal, and distribution appropriate for the level of protection required?
- Does appropriate information requiring special control or handling get dated and reviewed?

6.14 System Development and Maintenance

The following questions are provided to validate company compliance with the guidance for system development and maintenance:

- Does the software design review assess the cybersecurity functions and features needed for the risk level of the application?
- Before deploying the application in the field, was a cybersecurity assessment conducted to verify that the system did not introduce unacceptable safety or security risks?
- During system commissioning and testing, is there a process to verify the security features function as designed and that they meet the needs of the process?
- Is a process/checklist documented that identifies the need to assess security functions and risks during maintenance activities?
- Is a policy covering the types of risks that are managed with cybersecurity controls established?
- Is a process for patching operating systems and applications documented and followed?
- Does the process:
  - define how the organization monitors information sources for announcement of new vulnerabilities and patches,
  - evaluate the relevance of those patches, and
  - implement patches required to reduce risk to an acceptable level?
- Has outsourced software development staff signed a confidentiality agreement?

6.15 Staff Training and Security Awareness

The following questions are provided to validate company compliance with staff training and security awareness:

- Does each employee have a documented training plan that is updated annually and does it include activities associated with broadening cybersecurity knowledge?
- Does senior management support cybersecurity training?
- Is there a documented security awareness communication program with timing and communication content identified?
- Are new employees aware of the corporate security policies?
- Does the awareness program accurately reinforce corporate policies associated with cybersecurity
- Do documented training curriculums exist, and are they specific to the individual roles associated with maintaining a secure systems environment at both the plant and corporate level?
- Are subject matter experts for each course who can provide additional information and consulting identified, documented, and communicated?
- For requirements identified in the curriculum, are there courses or on the job related training to address these requirements for each role?
- Are periodic reviews and validation of training curriculum and associated training conducted to ensure effectiveness?
- Is there a document process to ensure that up-to-date information is available regarding recently identified control exposures?

6.16 Compliance

Compliance with Legal, Regulatory, and Security Requirements

This section provides self-assessment questions to validate if your company is in compliance with legal, regulatory, and security requirements:

- Has our company identified applicable and changing legislation (e.g., encryption, data privacy, etc.)
- Does our program have procedures to ensure compliance with legal restrictions on the use of materials in respect to intellectual property rights and the use of proprietary information?
- Do we have records retention and disposal procedures?
- Are our company assets protected from inappropriate use?
- Do we have appropriate procedures around the collection and chain of evidence to support action against a person or organization?
- Do we conduct regular checks against compliance against cybersecurity polices and implementation standards?

Scheduling and Conducting Audits

This section provides self-assessment questions to validate if your company is in compliance with scheduling and conducting audits:

- Has the organization established a program and procedure for a CSMS audit?
- Are the program and procedures designed to 1) determine conformance to the CSMS and 2) determine conformance any standards being used?
- Are audit reports communicated to top management?
- Are areas of nonconformance audited more frequently?
- Does the audit program require competency of the auditors?

6.17 Business Continuity Plan

Full verification of business continuity plans is typically only possible by exercising the plan as part of a drill or "dry run." The simpler drills are conducted as paper exercises, but in the case of large, complex systems where the stakes are high, it is important to conduct as realistic of a test as possible.

The following questions are provided to validate company compliance with business continuity plan:

- Does the company have a business continuity planning team consisting of business, IT, and manufacturing and control systems personnel?
- Are critical business, other IT, and manufacturing and control systems identified, prioritized and consequences of failure detailed?
- Have responsibilities for the aspects of the business continuity planned been assigned?
- Are adequate resources available?

- Have alternatives such as business insurance been investigated and reviewed?
- Does the business continuity plan contain the following:
  - Communications (internal and external)
  - The circumstances under which the plan is to be activated
  - The specific emergency measures to be taken, and under what circumstances
  - The type and number of resources needed and their assignments
  - Data that requires special handling and protection, as well as the information critical to continued operation
  - Interim procedures to continue business operations
  - Storage locations and inspection frequency for backup systems and applications software along with appropriate instructions for making the systems operational
  - Storage locations and inspection frequency for back up equipment such as computers, communications and supporting equipment for the team (in the event equipment is damaged)
  - Identification and responsibility for obtaining miscellaneous supplies for normal operation
  - Locations and arrangements for alternate facilities for contingent business operations
  - Alternate sources of raw materials for production
  - Finished products to be produced under the backup plan
  - The frequency and method to test and validate the plan
  - The risks associated with operating under the continuity plan and how are they going to be addressed
  - The process for resuming normal operations
  - A backup configuration licensed for operation by the appropriate authorities in advance

6.18 Monitoring and Reviewing CSMS

The following questions are provided to validate company compliance with monitoring and reviewing CSMS:

- Are cybersecurity incidents reported through appropriate channels as quickly as possible?
- Are observed or suspected cybersecurity related weaknesses or threats noted and/or reported?
- Are incidents monitored and quantified by type, volume, and cost?
- Are violations of organizational policies and procedures by system users dealt with through a formal disciplinary process?
- Are procedures developed to identify failed and successful cybersecurity breaches?
- Are the actions determined to resolve a breach of cybersecurity in light of the business priorities?

- Have metrics been developed and monitored (e.g., audits, incidents) to help determine that the cybersecurity activities (manual or automated) are performing as expected?
- Has a process been developed to trigger a review of the level of residual risk and acceptable risk taking when there are changes to the organization, technology, business objectives, processes and external events including identified threats and changes in social climate?
- Are all performances that could have a significant impact on the effectiveness or performance of the CSMS analyzed, recorded, and reported?

6.19 Maintaining and Implementing Improvements

The following questions are provided to validate company compliance with maintaining and implementing improvements:

- Do processes for evaluating new strategies or technologies that may improve current cybersecurity activities exist? If so, do they take into account your company's risk profile?
- Is benchmarking used either within or outside of the industry as a means to validate improvements?
- Does a method for obtaining employee feedback on security suggestions exist? If so, is reported to senior management?
- Is cybersecurity performance through key performance indicators such as threat or incident trends evaluated?
- Are completion dates to improvement actions/tasks assigned?
- Does a follow-up process for monitoring completion of improvements that have been committed to exist?
- Is the effectiveness of the CSMS through the use of the cybersecurity policy and objectives, results of self-assessments reviews and independent audits, corrective and preventative actions and management reviews improving?
- Is performance of the CSMS in meeting cybersecurity policy and objective measured?
- Are reviews of the performance results conducted to determine:
  - The current state of cybersecurity is satisfactory, in which case attention should be given to evaluating changes in technology and business requirements and the identification of new threats and vulnerabilities to anticipate future changes to the CSMS to ensure its continued effectiveness in the future?
  - The ineffective CSMS processes and procedures or non-conformities that have been collected during the check phase – monitor & review, schedule and conduct audits. Where these areas exist further investigations should be conducted to identify root cause and areas where there are systemic problems of the event and actions identified not only to resolve the issue but also to minimize and prevent reoccurrences.
- Are appropriate corrective and preventative actions to further improve the performance process identified?
- Are improvements in the CSMS and put plans in place to implement them (e.g., budgets, project planning etc.) prioritized?

- Are planned changes using the management of change processes within the organization implemented?
- Are areas of improvement and action plans to key stakeholders communicated?
- Are areas identified where improvement is needed using trend analysis as a tool?