Cyber Practical Guide

Industrial Control Systems – Cyber Assessment Guide

Date: March, 2016
Version: 3.7
CONTENT

1. AWARENESS OF CYBER THREATS AT ENTERPRISE / ICS-CI OPERATIONS LEVEL .......................8
2. RISK IDENTIFICATION, CLASSIFICATION, AND ASSESSMENT ........................................8
3. RISK ANALYSIS REVIEW – PHYSICAL & CYBER PROTECTION & RESILIENCE PLAN ..........9
4. RISK MANAGEMENT – PHYSICAL & CYBER MEASURES & CONTROLS ................................9
5. SECURITY BY DESIGN: SECURITY REFERENCE ARCHITECTURE ....................................9
6. SECURITY BY DESIGN: ICS SECURITY POLICY & DATA PROTECTION POLICY ............9
7. SECURITY BY DESIGN: CYBER TECHNICAL AGILITY & ADAPTATION ..........................10
8. CONSCIOUSLY SECURE DESIGN OF PRODUCTION FACILITIES & TECHNOLOGY ........10
9. ORGANIZATIONAL & PERSONNEL SECURITY ....................................................................11
10. PHYSICAL AND ENVIRONMENTAL SECURITY .................................................................12
11. INFORMATION AND NETWORK / COMMUNICATION SECURITY .................................12
12. IDENTITY & ACCESS MANAGEMENT ...............................................................................13
13. COMMUNICATIONS, OPERATIONS AND CHANGE MANAGEMENT ...............................14
14. INFORMATION AND DOCUMENT MANAGEMENT ............................................................14
15. SYSTEM DEVELOPMENT AND MAINTENANCE ...............................................................15
16. STAFF TRAINING AND SECURITY AWARENESS .............................................................15
17. COMPLIANCE & PRIVACY ...............................................................................................16
18. INTRUSION DETECTION AND PROTECTION MANAGEMENT .........................................17
19. SECURITY INFORMATION EVENT MANAGEMENT / MONITORING & DATA ANALYTICS ...17
20. INCIDENT PLANNING & RESPONSE ..............................................................................17
21. DISASTER RECOVERY PLANNING (DATA, NETWORKS & SYSTEMS) .........................18
22. BUSINESS CONTINUITY PLAN .......................................................................................18
23. MAINTAINING AND IMPLEMENTING IMPROVEMENTS ................................................19
24. SITUATIONAL AWARENESS ............................................................................................20
OVERVIEW

This guide, ‘Industrial Control Systems – Cyber Assessment Guide’, will help organisations in assessing their current status in Security in Critical Infrastructures. This cyber assessment guide is NOT a Risk Analysis itself, it is a helpful instrument to assess your current security activities, procedures, techniques and controls.

Based on the assessment, improvements in several ICS security areas can be identified. An overall Risk analysis including on site plant visits will identify potential risks that can be assessed and incorporated in the overall Security improvements and implementation plan as part of the cyber governance model.

The purpose of this effort is to provide guidance for industrial control systems sectors in the implementation of appropriate controls. In a broader sense, the guidance provided is aimed at helping sector companies incorporate sound cyber security practices into their overall product stewardship programs.

The accompanied Cyber Governance Model for ICS environments is based on CRC-ICS’s int. best practices in ICS environments and the results of the USA National Institute for Standards and Technology cyber security framework, SCADA reports and the project chartered under the auspices of the USA Critical infrastructure Industry Data Exchange (CIDX). It aligns with the Critical infrastructure Sector Cyber Security Strategy and the Guidance for Addressing Cyber Security in the Chemical Industry.

Information contained in this document is necessary general in nature and is not to be considered a standard or directive that readers are obligated to follow. Instead, readers must independently determine what constitutes appropriate cyber security practice relative to their own needs and circumstances. Readers may need to adopt practices different from those discussed in this document, or employ practices that are not discussed herein, based on their factual situations, the practicality and effectiveness of particular actions and economic and technological feasibility. In making this determination, readers should consider information such as references noted in the document as well as other information that may be relevant. Readers should consult with legal counsel to ascertain their actions comply with relevant NATIONAL and local law.

INTELLECTUAL PROPERTY RIGHTS

This document is the result of intensive research by the Cyber Research Center – Industrial Control Systems (CRC-ICS) and the Institute For Enterprise Architecture Developments combined with international best practices and standards in implementing Cyber Security in Industrial Control Systems / Critical Infrastructures.

CRC-ICS intended not to use any copyrighted material for this publication or, if not possible, to indicate the copyright or source of the respective object. CRC-ICS has thoroughly checked all the references however could not trace out in all situations the original copyright owner; however it is never our intention to infringe anyone’s copyrights. All Trade Marks, Service Marks and registered trademarks / service marks mentioned in this document are the property of their respective organizations. The copyright for any material created by the CRC-ICS is reserved.

CRC-ICS shall retain ownership of all inventions, whether or not patentable, original works of authorship (whether written or visual), developments, improvements or trade secrets developed by or licensed to CRC-ICS or developed by third parties on CRC-ICS’s behalf, either prior to or outside of this IPR statement, including but not limited to methodologies, analysis, frameworks, leading practices, specifications, materials and tools (“CRC-ICS Independent Materials”) and all IPR therein. Organizations may use the CRC-ICS Independent Materials provided to Organizations by CRC-ICS only in furtherance of this IPR statement or with CRC-ICS’s prior written consent. “IPR” means intellectual property rights, including patents, trademarks, design rights, copyrights, database rights, trade secrets and all rights of an equivalent nature anywhere in the world.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us and to return this document by email at info@crc-ics.net

Cyber Research Center – Industrial Control Systems
The Netherlands.
The Industrial Control Systems – Cyber Governance Model / Guide consists of 3 important interrelated domains of actions which together will give your organisation the best position to deal with current and further cyber threats. Be aware that every organisation will be compromised this year and so be prepared to deal with such a situation.

The following is a brief summary of the 24 key elements of the CRC-ICS Assessment and Cyber Governance Model.

**CYBER AWARENESS**

1. Awareness of Cyber Threats at Enterprise & ICS Operations Level: It is important to establish that the company is aware of and that it understands the importance of its operations in relation to information technology (IT) and cyber related technology risks. This extends to production and control systems, value chain operations, joint ventures, third parties, outsourcing partners, as well as Enterprise related IT activities.

2. Risk Identification, Classification and Assessment states that by identifying, prioritizing and analyzing potential (cyber) security threats, vulnerabilities and consequences using accepted methodologies, company efforts can protect the organization and its ability to perform its mission.

3. Risk Analysis, Review – Physical & Cyber Protection & Resilience Plan: Based on the risks identification, classification and assessment a cyber protection / resistance plan as well as a cyber resilience plan need to be developed in line with law and regulations, embraced and supported by top management.

4. Risk Management and Implementation addresses developing and implementing physical & cyber 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.

5. Security by Design: ICS Security Reference Architecture addresses the principles, concepts and structures as reference for a secure ICS environment for sites/plants. The main principle is ‘Defence in Depth’.

6. Security by Design: Industrial Control Systems (ICS) Security Policy addresses senior leadership commitment to continuous improvement through published policies. Providing policies to employees and reviewing them regularly to ensure they remain appropriate is generally beneficial.
7. **Security by Design: Cyber Technical agility & Adoption**, due to continuous changes in technologies as well as the continuous change of cyber threats, organizations must be prepared for that and be technical agile as well be prepared to quickly react and adopt measures and controls to mitigate the risk of new cyber threats. Known vulnerabilities in technology and software must be quickly addressed.

8. **Consciously Secure Design of Production Facilities & Technology.** Creating a risk-conscious and security-aware culture within an organization can provide more protection to an organization’s information infrastructure and associated data assets than any technology- or information-security-related control that currently exists. Adversaries and the threats they pose to information are more advanced and daunting than ever and show no sign of becoming less concerning in the future. To effectively address this issue, information risk management and security functions must create and cultivate cultures within their organizations that embrace information risk management and security as a business benefit rather than another hurdle on the path to success.

---

**CYBER RESISTANCE**

9. **Organizational & Personnel 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 cyber security. Cyber security 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. Production 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 more specific addresses security responsibilities at the recruitment phase, discussing the inclusion of these responsibilities in all contracts and individual monitoring during employment. Recruits can be screened as part of the process, especially for sensitive jobs. Companies may consider having all employees and third party users of information processing facilities sign a confidentiality or nondisclosure agreement.

10. Physical and Environmental Security addresses protecting tangible or physical assets (e.g., locations, buildings, computers, networks, production processes equipment, etc.) from damage, loss, unauthorized access or misuse. Critical information or assets can be better safeguarded by placing them in a secure areas, protected by security perimeter and entry controls (security zones & conduits). These physical security controls work in conjunction with cyber security measures to protect information.

11. **Information and Network / Communication Security** addresses protecting and securing Information and Network / Communication Security assets / equipment from from damage, loss, unauthorized access or misuse. Critical information or assets can be better safeguarded by placing them in a secure information technology areas, protected by security perimeter and access controls (security zones & conduits).

12. **Identity Access Management** addresses account administration, authorization and authentication. Account administration addresses the creation of 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 are generally 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.

13. Communications, Operations and Change Management addresses processes and procedures being developed and followed to sustain the security of computer systems and information processing facilities. Clearly articulating the operational security aspects can enhance these overall management practices and procedures. The need to address security is very strong in the production and control systems that are
used to operate our facilities because security lapses have the potential to result in safety, health, or environmental issues

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

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

16. Staff Training and Security Awareness states that management commitment is critical to providing a stable computing environment for both information and production and control systems. Effective cyber security 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.

**CYBER RESILIENCE**

17. Compliance addresses scheduling and conducting audits, and compliance with legal, regulatory and security requirements. It describes companies’ periodic assessment of 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 critical infrastructure suppliers, logistics service providers, joint ventures or customers. To help 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 help ensure the security and safe operation of its assets, a validation or audit for compliance to corporate security policies and practices may be necessary.

18. Intrusion Detection & Protection Management: Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. 19. Security Information Event Management / Monitoring & Data Analytics is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.

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

21. Disaster Recovery Planning (DRP) [Data, Networks, Systems & Production Facilities] is the preparation for and recovery from a disaster, whether natural or cyber made. The key role of a DRP is defining how to re-establish operations (data, networks, systems and production) at the location where the organization is usually located.
22. 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 can be developed, implemented and tested to help ensure that business processes can be restored in a timely fashion.

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

24. Situational Awareness: The understanding of the organisation’s own security and cyber strengths, assets and weaknesses; as well as likely adversary tactics, targets and capabilities. In this regard it is important that CISOs ensure that organisations have the capability to continually absorb and assess new information, and refresh this understanding. This is a critical overlap with Cyber resistance and underlines the importance of situational awareness to cyber security as a whole.
1. **AWARENESS OF CYBER THREATS AT ENTERPRISE / ICS-CI OPERATIONS LEVEL**

The following questions are provided to assist with risk identification, classification, and assessment:

A. Is your company aware of the different physical security issues at enterprise and ICS operations level?  
B. Is your company aware of the different cyber threats at enterprise and ICS operations level?  
C. Is your company aware of the different interconnections, including wireless that is present between the enterprise domain and the ICS domain?  
D. Is your company aware of the different cyber threats that potential is entering your organisation from vendors, contractors, etc. that are physical or networked connected to your organisation?  
E. Do you have a cyber threat analysis program in place that will help your organisation in improving their cyber capabilities?

2. **RISK IDENTIFICATION, CLASSIFICATION, AND ASSESSMENT**

The following questions are provided to assist with risk identification, classification, and assessment:

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

The following questions are provided to assist with risk analysis review and to setup a cyber protection & resilience plan:

A. Does your organisation have regular Risk Analysis Reviews related to physical & cyber protection & resilience plans?
B. Does your organisation have regular review of physical and cyber controls, related to cyber threat analysis?
C. Are the cyber protection and resilience plans regular reviewed and tested/exercised?

4. **Risk Management – Physical & Cyber Measures & Controls**

The following questions are provided to assist with risk management and implementation:

A. Does your company have an implemented risk mitigation strategy based upon threats, detected vulnerabilities and consequences?
B. Is a risk mitigation strategy in place to identify and select the required security controls?
C. Are security policies defined and validated?
D. Are procedures developed that provide details like actions to take for preventing, detecting and responding to threats?
E. Have standards and services been developed?
F. Are security tools and products identified?
G. Is the risk tolerance profile understood? Depending on the severity of the impact and consequences, the risk tolerance could be different.
H. Has the cost versus benefits been compared? Select the security controls whose cost is less than the risk it is attempting to reduce.
I. 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.
J. Has a process been established for accepting risk, which includes appropriate management level approval based on scope and documentation?

5. **Security by Design: Security Reference Architecture**

The following questions are provided to assist with defining the Cyber Security Reference Architecture:

A. Is there management commitment, involvement and support in the creation and enforcement of the Cyber Security Reference Architecture?
B. Is a Cyber Security Reference Architecture review performed by all affected business units and departments, including critical infrastructure / plant management?
C. Is the Cyber Security Reference Architecture formal validated by security experts and management?
D. Is the Cyber Security Reference Architecture mandatory for all critical infrastructures / plants?
E. Is the Cyber Security Reference Architecture distributed to all critical infrastructure / plant managers and operators?
F. Is there documentation or a procedure to describe how updates to the Cyber Security Reference Architecture are handled?
G. How are exceptions to the Cyber Security Reference Architecture approved and documented?
H. Is compliance verified of the Cyber Security Reference Architecture with international standards and best practices?


The following questions are provided to assist with defining security policy:
A. Is there management commitment, involvement and support in the creation and enforcement of policies?
B. Is there a formal security policy for Computing Infrastructure Control Networks?
C. Is there a formal Data Protection Policy?
D. Is a review performed by all affected business units and departments, including site management?
E. Are policy owners identified?
F. Is the official policy statement distributed to employees?
G. Is there documentation or a procedure to describe how updates to policy are handled?
H. How are exceptions to the policy approved and documented?
I. Is compliance verified?

7. Security by Design: Cyber Technical Agility & Adaptation

The following questions are provided to assist with defining cyber technical agility & adaptation:

A. Is your organisation aware of the need for cyber technical agility and adaption?
B. Is your organisation aware of the continuous changes in technologies as well the continuous change of cyber threats?
C. Is your organisation aware that the organisations must be prepared for that and be technical agile as well be prepared to quickly react and adopt measures and controls to mitigate the risk of new cyber threats?
D. Is your organisation aware that it must be prepared to quickly address Known vulnerabilities in technology and software?
E. Is your organisation aware that (cyber) security is today the most important quality of services in designs and implementations?

8. Consciously Secure Design of Production Facilities & Technology

The following questions are provided to assist with defining consciously secure design of production facilities and technology:

A. Does your organisation have a risk-conscious and security-aware culture within your organization?
B. Is your organisation aware that a risk-conscious and security-aware culture within your organization can provide more protection to an organization’s information infrastructure / production facilities and associated data assets than any technology- or information-security-related control that currently exists?
C. Is your organisation aware that production facility security layout and design is an important component of a business’s overall operations, both in terms of maximizing the effectiveness and security of the production process and meeting the needs of employees?
D. Is your organisation aware that the key to good secure facility layout and design is the integration of the needs of the organisation (safety and security), people (personnel and customers), materials (raw, finishes, and in process), and machinery in such a way that they create a safe and secure well-functioning system and facility.
E. Is your organisation aware that the basic components of the physical security measures to address an explosive threat considers the establishment of a protected perimeter, the prevention of progressive collapse, the design of a debris mitigating façade, the isolation of internal explosive threats that may evade detection through the screening stations or may enter the public spaces prior to screening and the protection of the emergency evacuation, rescue and recovery systems?
F. Is your organisation aware that one of the most serious threats may come from persons who have authorized access to a facility. These may include disgruntled employees or persons who have gained access through normal means (e.g., contractors, support personnel, etc)?
G. Does your organisation understand and has identified the information and production assets you are trying to protect?
H. Is your organisation providing software and hardware devices to detect, monitor, and prevent unauthorized access to or the destruction of sensitive information?

9. ORGANIZATIONAL & PERSONNEL SECURITY

The following questions are provided to assist with the guidance for organizational security:

A. Does your company vest the responsibility for cyber security to an individual or individuals?
B. Is there a cross functional team or group of individuals representing the various departments and business units designated with oversight for cyber security?
C. Is physical security represented?
D. 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?
E. Are risk assessments completed prior to engaging third party contractors or outsourcers?
F. 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?
G. Are there processes to remove 3rd party access in a timely manner at the conclusion/termination of the contract?
H. Are personnel assigned responsibility for cyber security, and an appropriate level of funding to implement?
I. Is there commitment from executive management?
J. Is there a company-wide security team (or organization) that provides clear direction, commitment, and oversight?
K. Do contracts exist that address cyber security for business partners, third party contractors, and outsourcing partners, etc.?
L. Are there metrics for organizational success?
M. 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?

The following questions are provided to assist with personnel security:
A. Does your company include security requirements in job descriptions?
B. Are duties segregated for checks and balances?
C. 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.)?
D. Are confidentiality or nondisclosure agreements reviewed, signed, and maintained for: employees, third party contractors, and temporary employees?
E. Are security responsibilities clearly stated in the terms and conditions of employment for employees, third party contractors, and temporary employees?
F. Is there a security training program relevant to the particular job function (initial plus periodic)?
G. Does your company have a disciplinary process for security policy or procedure violations?

10. PHYSICAL AND ENVIRONMENTAL SECURITY
The following questions are provided to assist with the guidance for physical and environmental security:
A. Does a general description of the building access exist?
B. Does a description of physical access controls for computer rooms and control rooms exist?
C. Are secure areas restricted by additional controls?
D. Is equipment that is used off-site protected to the same degree afforded to on-site?
E. Are password-protected screen savers used?
F. Are removable media devices secured or disabled?
G. Are one or more physical security perimeters established to provide barriers to unauthorized access to facilities?
H. Are appropriate entry controls provided at each barrier or boundary?
I. Are physical assets (equipment) protected against environmental damage from threats such as fire, water, smoke, dust, radiation, impact, etc.?
J. Are single points of failure avoided where possible?
K. Are all external connections (power, communications, etc.) adequately protected from tampering or damage?
L. Is all equipment including auxiliary environmental equipment properly maintained to ensure proper operation?
M. Are proper procedures established and audited with respect to the addition, removal, and disposal of all equipment?
N. 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?

11. INFORMATION AND NETWORK / COMMUNICATION SECURITY
The following questions are provided to assist with information and network / communication security:
A. Does a general description and visualisation of the information and network / communication access possibilities (network architecture) exist?
B. Does a description of information and network / communication access paths to control systems and devices exist?
C. Are information and network / communication secure zones restricted by additional technology controls?
D. Is information and network / communication equipment that is used off-site protected to the same degree afforded to on-site?
E. Is information and network / communication equipment access pass-word or token protected?
F. Are removable media devices in the information and network / communication zones secured or disabled?
G. Are one or more technology security perimeters established to provide barriers to unauthorized access to information and network / communication assets?
H. Are appropriate conduits implemented at each security level?
I. Are information and network / communication assets (equipment) protected against environmental damage from threats such as fire, water, smoke, dust, radiation, impact, etc.?
J. Are single points of failure in the information and network / communication avoided where possible?
K. Are image backups created for each time that a change in software or hardware is implemented in the information and network / communication equipment’s / devices?
L. Are all external connections (information and network / communication, etc.) adequately protected from tampering or damage?
M. Is all the information and network / communication equipment properly maintained to ensure proper operation?
N. Are proper procedures established and audited with respect to the addition, removal, and disposal of all information and network / communication equipment?
O. Is all information that is expressed in an electronic format (e.g., electronic storage devices, mobile devices, computer equipment, etc.) adequately protected against information and network / communication threats?

12. **IDENTITY & ACCESS MANAGEMENT**

**Account Administration**
The following questions are provided to assist with the guidance for account administration:

A. Is there a formalized process for adding and approving new users on industry and control systems that includes standard principles around the separation of responsibilities? If so, does it have an audit trail of all changes?
B. Is there an established cycle to review user accounts to make sure they are correct and still needed?
C. Are users assigned the minimum privileges and authorizations necessary to perform their tasks?
D. Is every user individually identifiable and each access controlled by an appropriate method of authentication (e.g., user ID and password)?
E. Is an alternative identification for forgotten password?
F. Is access granted, changed, or terminated on the authority of an appropriate manager?
G. Is a record maintained of all access accounts, including details of the individual, their permissions, and the authorizing manager?
H. Are access accounts suspended or removed and access permissions revoked as soon as they are no longer needed (e.g., job change)?
I. Is the need for access to critical systems explicitly reconfirmed on a regular basis?
J. Are default passwords changed immediately?

**Authentication**
The following questions are provided to assist with the guidance for authentication:

A. 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?
B. Do the authentication practices address the differing vulnerabilities associated with locations of varying physical security levels?
C. Are there processes in place to communicate and remind users of administrative procedures employed for authentication and their personal responsibility to adhere to them?
D. Are all application users authenticated via the application to use the application? Note: This requirement may be waived when there are compensating physical controls.
E. Is the minimum level of authentication a user-id & password?
F. Are authenticators and credentials protected while in storage and during transmission?
G. Are users trained to keep passwords confidential?

Authorization
The following questions are provided to assist with the guidance for authorization:
A. Does our company include security requirements in job descriptions?
B. 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.)?
C. Are confidentiality or nondisclosure agreements reviewed, signed, and maintained for employees, third party contractors and temporary employees?
D. Are security responsibilities clearly stated in the terms and conditions of employment for employees, third party contractors, and temporary employees?
E. Is there a training program (initial plus periodic)?
F. Does a disciplinary process exist for security policy or procedure violations?
G. 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?
H. Is some form of access control present for all systems and data?
I. 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?
J. Is all access to critical computer systems, successful or failure, logged by the system to be reviewed?

Industrial and Control Systems Authorization
The following questions are provided to assist with the guidance for industry and control systems’ authorization practices:
A. 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?
B. Are user accounts setup with non-expiring passwords?
C. Have user account privileges been defined with geographical location in mind for the user?

13. COMMUNICATIONS, OPERATIONS AND CHANGE MANAGEMENT
The following questions are provided to assist with the guidance for communications, operations, and change management:
A. Is a change management process documented and followed?
B. Is an incident management process documented and followed?
C. Is a process for antivirus management documented and followed?
D. Does a process to track status on deployment and use of antivirus software exist?
E. Does a process to identify new cyber security vulnerabilities and address the safety implications created by the new vulnerabilities exist?
F. Is a patch management process that incorporates risks and consequences into the development of the implementation plan documented?
G. Are procedures and practices for backup and restore of computer systems defined, used, and verified by appropriate testing?
H. Is a system of controls over information exchanged with between organizations (i.e., between your company and other companies) documented and followed?

14. INFORMATION AND DOCUMENT MANAGEMENT
The following questions are provided to assist with information and document management:
A. Is a data classification system in place that accounts for varying levels of need, priority, sensitivity, and criticality of information?
B. Are policies and procedures documented detailing the record retention of information?
C. Are policies and procedures documented detailing the destruction and disposal of written records, equipment, and other media?
D. Are guidelines documented explaining when information and documents should be retained/destroyed?
E. Are roles and responsibilities associated with information and document management documented?
F. Does a process exist to review policy compliance (e.g., audit)?
G. Are processes developed and employed to prevent data corruption around backup processes and logging?
H. 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?
I. 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?
J. Does appropriate information requiring special control or handling get dated and reviewed?

15. SYSTEM DEVELOPMENT AND MAINTENANCE
The following questions are provided to assist with the guidance for system development and maintenance:
A. Does the software design review assess the cyber security functions and features needed for the risk level of the application?
B. Before deploying the application in the field, was a cyber security assessment conducted to verify that the system did not introduce unacceptable safety or security risks?
C. 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?
D. Is a process/checklist documented that identifies the need to assess security functions and risks during maintenance activities?
E. Is a policy covering the types of risks that are managed with cyber security controls established?
F. Is a process for patching operating systems and applications documented and followed?
G. Does the process:
   o Define how the organization monitors information sources for announcement of new vulnerabilities and patches?
   o Evaluate the relevance of those patches, and
   o Implement patches required to reduce risk to an acceptable level?
H. Has outsourced software development staff signed a confidentiality agreement?

16. STAFF TRAINING AND SECURITY AWARENESS
The following questions are provided to assist with staff training and security awareness:
A. Does each employee have a documented training plan that is updated annually and does it include activities associated with broadening cyber security knowledge?
B. Does senior management support cyber security training?
C. Is there a documented security awareness communication program with timing and communication content identified?
D. Are new employees aware of the corporate security policies?
E. Does the awareness program accurately reinforce corporate policies associated with cyber security
F. 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?
G. Are subject matter experts for each course who can provide additional information and consulting identified, documented, and communicated?
H. For requirements identified in the curriculum, are there courses or on the job related training to address these requirements for each role?
I. Are periodic reviews and validation of training curriculum and associated training conducted to ensure effectiveness?

J. Is there a document process to ensure that up-to-date information is available regarding recently identified control exposures?

17. **COMPLIANCE & PRIVACY**

**Compliance with Legal, Regulatory, and Security Requirements**
This section provides assessment questions to assist with legal, regulatory, and security requirements:

A. Has our company identified applicable and changing legislation (e.g., encryption, data privacy, etc.)?

B. 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?

C. Do we have records retention and disposal procedures?

D. Are our company assets protected from inappropriate use?

E. Do we have appropriate procedures around the collection and chain of evidence to support action against a person or organization?

F. Do we conduct regular checks against compliance against cyber security polices and implementation standards?

**Scheduling and Conducting Audits**
This section provides assessment questions to assist with scheduling and conducting audits:

A. Has the organization established a program and procedure for a CSMF audit?

B. Are the program and procedures designed to 1) determine conformance to the CSMF and 2) determine conformance any standards being used?

C. Are audit reports communicated to top management?

D. Are areas of non-conformance audited more frequently?
E. Does the audit program require competency of the auditors?

18. INTRUSION DETECTION AND PROTECTION MANAGEMENT

The following questions are provided to assist with intrusion detection and protection management:

A. Does your organisation have Network monitoring, which monitors network traffic for particular network segments or devices and analyses the network and application protocol activity to identify suspicious activity?

B. Does your organisation have Wireless monitoring, which monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves at enterprise and production level?

C. Does your organisation have Network Behaviour Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems)?

D. Does your organisation have Host-Based monitoring, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity?

E. Does your organisation have Wireless Intrusion Prevention systems that monitors the wireless radio frequencies for suspicious activities and can shut down wireless network components in the case of that?

19. SECURITY INFORMATION EVENT MANAGEMENT / MONITORING & DATA ANALYTICS

The following questions are provided to assist with Security Information Event Management / Monitoring and Data Analytics:

A. Are adequate solutions implemented to monitor the status of systems, networks and devices to detect security incidents?

B. Are technologies implemented and monitored on a 24x7 base like Security Information Event Monitoring; Anti-Virus & Malware detection; Intrusion Detection Systems; Intrusion Protection Systems; Data Loss Prevention systems?

C. Is real-time log monitoring implemented to facilitate Data Analytics to do Initial Diagnostics and Incident Isolation; Incident Correlation; Problem Correction and Predictive Analytics?

D. Are the risks of Advanced Persistent Threats recognized and are measures and controls implemented to detect APT’s?

E. Are Security Systems and Security Software maintained on a regular base and are Updates and DAT definitions tested?

F. Are corrective IDS/IPS and Firewall Rules applied on a daily / hourly base?

G. Are Computing Equipment and Endpoint Devices facilitated by a remote administration and antivirus updates provided on a daily base?

H. Are HIPS alerts tuned and whitelists configured on a daily base?

I. Are procedures in place to escalate incidents to next tier level?

J. Are procedures in place to close Incidents?

K. Is coordination established with end users and system administrators?

L. Is coordination established with tier levels?

M. Is work with Third-Party Vendors regulated in processes and procedures?

20. INCIDENT PLANNING & RESPONSE

The following questions are provided to assist with the guidance for incident planning and response:

A. Are there written incident planning and response plans?

B. Has the incident response plan been tested?
C. Does the plan address worst-case and most credible scenarios?
D. Who has the overall responsibility for coordinating and executing the plan?
E. Are incident planning and response procedures established?
F. Is a person responsible for executing the plan when the need arises named?
G. Is an incident response team structured, including additional personnel, who can be called in?
H. Has responsibility for coordinating defence and response to an incident been established?
I. Can an incident from initiation through final review be handled?
J. Have procedures for different types of incidents like denial of access, system attacks, malicious code, unauthorized access, and inappropriate usage been created?
K. Have proactive measurements to identify attacks during early stage been identified?
L. Has base planning on threat scenarios from vulnerability analysis and risk assessment been completed?
M. Have written response procedures been developed?
N. Have industry and process control systems incidents been communicated to the IT organization as well as the process safety organization?
O. Have IT incidents been communicated to the plant / site and process control organization for awareness building?
P. Have the details of the incident, the learning’s, and the course of action to prevent from occurring again been documented?
Q. Have drills been conducted to test the plan?

21. DISASTER RECOVERY PLANNING (DATA, NETWORKS & SYSTEMS)
The following questions are provided related to the status of Disaster Recovery Planning (DRP) for data, networks, systems and operations / production facilities.
   A. Do you understand the need for contingency planning (CP) for your organization?
   B. Do you know the major components of contingency planning for your organization?
   C. Do you have in place a simple set of contingency plans, using business impact analysis?
   D. Are you prepared to execute and test the contingency plans for your organization, BU’s or production facilities?
   E. Do you understand the unified contingency plan approach for your organization?
   F. To ensure continuity across all of the CP/DRP processes during the planning process, does the contingency planners of your organization have identified the following items?:
      ☑ Identification of the mission- or business-critical functions.
      ☑ Identification of the mission- or business-critical data.
      ☑ Identification of the mission- or business-critical systems and networks.
      ☑ Identification of the mission- or business-critical operations or production facilities.
      ☑ Identification of the resources that support these critical functions, data, systems and networks as well as operations or production facilities .
      ☑ Anticipation on potential contingencies or disasters.
      ☑ Selecting contingency planning strategies.
      ☑ Implementing selected strategy.
      ☑ Tested and revised contingency plans.

22. 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 assist with business continuity planning:
   A. Does the company have a business continuity planning team consisting of business, IT, and industry and control systems personnel?
B. Are critical business, other IT, and industry and control systems identified, prioritized and consequences of failure detailed?
C. Have responsibilities for the aspects of the business continuity planned been assigned?
D. Are adequate resources available?
E. Have alternatives such as business insurance been investigated and reviewed?
F. 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

23. MAINTAINING AND IMPLEMENTING IMPROVEMENTS
The following questions are provided to assist with maintaining and implementing improvements:

A. Do processes for evaluating new strategies or technologies that may improve current cyber security activities exist? If so, do they take into account your company’s risk profile?
B. Is benchmarking used either within or outside of the industry as a means to validate improvements?
C. Does a method for obtaining employee feedback on security suggestions exist? If so, is reported to senior management?
D. Is cyber security performance through key performance indicators such as threat or incident trends evaluated?
E. Are completion dates to improvement actions/tasks assigned?
F. Does a follow-up process for monitoring completion of improvements that have been committed to exist?
G. Is the effectiveness of the CSMF through the use of the cyber security policy and objectives, results of self-assessments reviews and independent audits, corrective and preventative actions and management reviews improving?
H. Is performance of the CSMF in meeting cyber security policy and objective measured?
I. Are reviews of the performance results conducted to determine:
   - The current state of cyber security 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 CSMF to ensure its continued effectiveness in the future?
   - The ineffective CSMF 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.

J. Are appropriate corrective and preventative actions to further improve the performance process identified?

K. Are improvements in the CSMF, and plans put in place to implement them (e.g., budgets, project planning etc.), prioritized?

L. Are planned changes using the management of change processes within the organization implemented?

M. Are areas of improvement and action plans to key stakeholders communicated?

N. Are areas identified where improvements is needed using trend analysis as a tool?

24. SITUATIONAL AWARENESS

The following questions are provided to assist with situational awareness:

A. Does your organisation understand the organisation’s own security and cyber strengths, assets and weaknesses; as well as likely adversary tactics, targets and capabilities?

B. Does your organisation have the capability to continually absorb and assess new threat information, and refresh this understanding?

C. Is your organisation aware about the importance of situational awareness to cyber security as a whole?

D. Is your organisation capable and trained to accurately predict and respond to potential problems that might occur?

E. Is your organisation aware that can be / will be faced with the total capabilities of nation-state attackers or state-sponsored cybercriminals?

F. Is your organisation able to deploy effective controls quickly enough or spend enough money to completely mitigate the totality of the threats you are facing?
ABOUT THE CYBER RESEARCH CENTER – INDUSTRIAL CONTROL SYSTEMS

The Cyber Research Center - Industrial Control Systems / Critical Infrastructures is a cyber knowledge platform and expert center focusing on the latest research and developments in protecting, detecting and making industrial control systems / critical infrastructures more resilient against current and future cyber threats that organisations are facing. The ultimate goal is to help critical infrastructures / industries to incorporate cyber protection and resilience in their current and future industrial designs / architectures and procedures as part of their day to day or future operations. To achieve that goal critical infrastructures / industries must be aware about the fast changing cyber threats and understand how critical infrastructures / industries can better protect themselves and become more resilient.

Security and Cyber Security is a constant challenge facing many aspects of our society including production environments and critical infrastructures. Even in the face of significant threats, society seemingly has insatiable thirst for greater cyber capabilities, and that thirst is accelerating at an increasingly rapid pace. We eagerly adopt new cyber capabilities in the name of efficiency, convenience, entertainment, and even safety; but often, we do so without considering the potentially significant risk. Recent changes in the way we use computers have not only affected where and how computers are used but also the way networks are architected and interconnected: today’s network boundaries constantly morph. We are rapidly moving toward a paradigm in which embedded systems will be highly interconnected and pervasive in nearly every aspect of our lives.

The Cyber Research Center - Industrial Control Systems / Critical Infrastructures is a not for profit research & information sharing, expert center working on the future state of Physical & Cyber Protection and Resilience. CRC-ICS goals are to inform industries / critical infrastructures about the fast changing threats they are facing and the measures, controls and techniques that can be implemented to be prepared to deal with these cyber threats.