Cyber Security Checklist

REV	DATE	APPROVED	DESCRIPTION OF CHANGE
	19/02/2021		

Automatically generated by exSILentia® version 4.10.0.0.

Table of Contents

1 Cyber Security Checklist

This document, automatically generated by the exida exSILentia® software, documents the project cyber security assessment. The assessment is based on IEC 62443-2-1 and industry best practices.

1.1 General Project Information

Project Identification:

Project Name:

Project Description:

1.2 References

Document ID	Title	Revision	Revision Date
IEC 62443-2-1	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	1.0	10-Nov-2010

2 Cyber Security Checklist

2.1 Cybersecurity Risk Assessment

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES
The organization has developed a high-level business rationale as a basis for its effort to manage IACS cyber security	C.3.2			
The organization has selected a risk assessment methodology	C.3.3.3.4			
Likelihood and consequence scales have been calibrated for the organization	C.3.3.3.7.3			
High level risk assessment has been conducted	C.3.3.3.7			
Key Industrial Automation and Control Systems (IACS) and their devices have been identified and placed into logical groups	C.3.3.3.8.2;C. 3.3.3.8.3			
Simple Network Diagrams have been created for the IACS's identified	C.3.3.3.8.4			
Detailed Risk Assessments have been conducted for each logical IACS identified	C.3.3.3.8.5			
An IACS asset management program for ongoing asset tracking of hardware (physical), software (electronic) and administrative (procedures, policies, training) components on process control system networks	Best Practice			
Risk assessments have been made part of the IACS lifecycle such that they are planned to occur at key times such as during the development of a new or updated IACS, during implementation of a new or updated IACS or during retirement of an IACS	C.3.3.3.8.10			

2.2 Cybersecurity Policy, Organization, and Awareness

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES
A cyber security policy document has been approved by management, published and communicated to all relevant stakeholders	5.1.1			
The cybersecurity policy document includes a scope statement defining to what the policy applies	5.1.1			
The cybersecurity policy is reviewed at planned intervals or if significant changes occur	5.1.2			
Management support of cybersecurity is demonstrated by: Defined roles and responsibilities for cybersecurity across the organization, Plans and programs to maintain cybersecurity awareness, Sufficient resources provided to carry out cybersecurity policy, Implementation of cybersecurity controls coordinated across the organization	6.1.1,6.1.3			
Cyber security activities are coordinated by representatives from different parts of the organization with relevant roles and job functions	6.1.2			
Requirements for confidentiality or non-disclosure agreements are identified and regularly reviewed.	6.1.5			
The organization's approach to managing cyber security and its implementation is reviewed independently at planned intervals or when significant changes to the security implementation occur.	6.1.8			
Risks are identified and controls implemented before granting third party access (including physical, logical or network connectivity both on and off site)	6.2.1			
Security requirements are identified before giving customers access to the organizations IACS	6.2.2			
Agreements with third parties involving accessing, processing, communicating or managing the organization's IACS cover all relevant security requirements	6.2.3			

2.3 Asset Management

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
All IACS assets have been clearly identified and an inventory of all important assets have been drawn up and maintained. These assets consist of physical, logical and informational objects that have value to the organization and are associated with the IACS.	7.1.1			
All IACS assets are clearly owned by a designated part of the organization	7.1.2			
Rules for acceptable use of assets associated with the IACS have been documented and implemented.	7.1.3			
Information is classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.	7.2.1			
Procedures for information labeling and handling in accordance with the classification scheme are implemented.	7.2.2			

2.4 Human Resources Security

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Security roles and responsibilities are documented and enforced for employees, contractors and third party users.	8.1.1,8.2.1			
Validation of identity and background checks are performed for all candidates for employment, contractors, and third party users with access to the IACS (both physical and cyber)	8.1.2			
Employees, contractors and third party users with access to IACS assets are required to agree and sign terms and conditions which document their and the organization's responsibilities for IACS security.	8.1.3			
All employees, contractors and third party users of the IACS system receive awareness training and regular updates in the organizational policies and procedures as relevant for their job function.	8.2.2			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
There is a disciplinary process in place for employees, contractors and third party users who have committed a security breach	8.2.3			
Responsibilities are in place to ensure an employee's contractor's or third party user's exit from the organization is managed, that the return of all equipment and controlled items and the removal of all access rights are completed	8.3.1, 8.3.2, 8.3.3			

2.5 Physical and Environmental Security

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Security perimeters are used to protect areas that contain IACS. This includes combination of barriers such as walls, card controlled entry gates or manned reception desks.	9.1			
Secure areas are protected by appropriate access controls to ensure that only authorized personnel are allowed access	9.1.2			
Guidelines for working in secure areas have been established (e.g. unsupervised working in secure areas should be avoided, vacant secure areas should be physically locked and periodically checked, photographic, video, audio or other recording equipment should not be allowed)	9.1.5			
Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and if possible isolated from IACS.	9.1.6			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Equipment is sited or protected to reduce risk from environmental threats and hazards as well as opportunities for unauthorized access. This includes items such as: Equipment is sited to minimize unnecessary access, IACS with sensitive data is positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons, Controls are adopted to minimize the risk of potential physical security threats such as theft, fire, explosives, smoke, water, dust, vibration, chemical effects, overheating, etc.	9.2.1			
Critical Equipment is protected from power failures and other disruptions caused by supporting utilities	9.2.2			
Power and telecommunications cabling equipment carrying data or supporting information services is protected from interception or damage. This includes IACS distribution and communications lines within local organizational facilities.	9.2.3, 9.2.10			
Equipment is maintained in accordance with the suppliers recommended service intervals and specifications. Records are kept of all suspected or actual faults and all preventative and corrective maintenance	9.2.4			
Controls to protect sensitive information should be taken when equipment is scheduled for maintenance by personnel unauthorized to view that information.	9.2.4			
Equipment containing storage media is checked to ensure that any sensitive data and licensed software is removed or securely overwritten prior to disposal.	9.2.6			
Procedures are in place to ensure that equipment, information or software is not taken off-site without prior authorization	9.2.7			
Organization keeps a current list of personnel with authorized access to the facility where the IACS resides and issues and assigns appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials	9.2.8			

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES
Organization controls all physical access points to the facility where the IACS resides and verified individual access authorizations before granting access to the facility.	9.2.9			
Organization controls physical access to the IACS independent of the physical access controls for the facility. Identity verification is required for entry to the most secured IACS spaces	9.2.9			
Organization controls physical access to IACS devices that display information to prevent unauthorized individuals from observing the display output.	9.2.11			
Physical access to the IACS is monitored to detect and respond to physical security incidents	9.2.12			
Visitors are escorted and their activity monitored	9.2.13			
The organization maintains a record of all physical access, both visitor and authorized individuals for a minimum of one year	9.2.14			
Physical security of the plant is observed to determine if IACS systems are well secured and in accordance with documented procedures. These observations should not be announced in advance so they are done in the plants normal alert level.	Best Practice			
Network cabling is neat, organized and color coded for function.	Best Practice			

2.6 Communications and Operations Management

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES
Documented procedures exist for system activities associated with the IACS (e.g. control's station start-up and close down, backup, equipment maintenance, media handling, control room and network management, system migration and updates, and safety)	10.1.1			
Changes to IACS facilities and systems are controlled by a change management system	10.1.2			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
The change management system follows separation of duty principles to avoid conflict of interest as well as unauthorized or unintentional modification or misuse of the organizations assets.	10.1.2, 10.1.3			
Development, test, and operational facilities are separated to reduce the risks of unauthorized access or changes to the operational system	10.1.4			
Hard copy documents output from the IACS are marked using standard naming conventions to identify any special dissemination, handling, or distribution instructions	10.1.5			
Procedures are in place to ensure that security controls, service definitions and delivery levels are included in third party service delivery agreements.	10.2.1			
The services, reports and records provided by third parties are regularly monitored, reviewed and audited.	10.2.2			
Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures are implemented	10.4.1			
The use of mobile code (software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction) must be authorized	10.4.2			
Controls are in place to prevent unauthorized mobile code from executing	10.4.2			
Controls are in place to ensure that authorized mobile code operates according to a clearly defined security policy	10.4.2			
Malicious code protection mechanisms are updated whenever new releases are available in accordance with organization configuration management policy and procedures	10.4.3			
The organization receives IACS security alerts and advisories on a regular basis and takes appropriate actions in response	10.4.4			
Back-up copies of information and software are taken and tested regularly in according with an agreed backup policy	10.5.1			

REQUIREMENT	REFERENCE IEC 62443-2-1	COMPLETE	COMPLIANCE ARGUMENT	OPEN ISSUES
USB ports are either: Disabled in software (e.g. via group policy), Disable in hardware (e.g. physical USB locks), Enabled but with a strict access policy and security measures in place to enforce the policy	ISA-TR99.00.02-2004			
Audit logs recording user activities, exceptions and information security events are produced and kept for an agreed upon period documented in a policy or procedure.	10.10.1			
Log files are examined periodically to find system intrusions	10.10.2			
Log files are protected against tampering and unauthorized access	10.10.3			
Security Information & Event Management (SIEM) tools are used to assist in monitoring system log files	Best Practice			
Intrusion Detection or Prevention Systems are used to detect attacks on the system and alerts are sent to appropriate personnel when such attacks are detected.	Best Practice			
Intrusion Detection or Prevention systems are deployed behind ICS firewalls with ICS specific signatures	Best Practice			
A policy exists covering the use of laptops and portable	Best Practice			
Whitelisting techniques are used to ensure that only approved devices are connected to the network	Best Practice			
A policy exists to ensure that approved devices have been scanned with up to date virus scanners.	Best Practice			
All portable media must be run through an anti-virus scanner prior to connecting to the IACS. A dedicated anti-virus scanning computer is available to perform this task	Best Practices			
A policy is in place for management of removable media including tapes, disks, flash disks, removable hard drives, CDs, DVDs and printed media	10.7.1			
A policy is in place to securely and safely dispose removable media when no longer required	10.7.2			

2.7 Network Security Management

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Network segmentation strategies employing security zones have been developed and implemented	10.6.1			
Controls are in place to safeguard confidentiality and integrity of data passing over public networks or wireless networks	10.6.1			
High risk IACS are isolated from or employ a barrier device to separate it from other zones with different security levels or risk	10.6.1			
The network is analyzed to determine if there are any redundant network loops. Unnecessary redundant loops are removed.	Best Practice			
Isolated networks are analyzed to determine if there are any unintended connections. If so such connections have been removed	Best Practices			
If the network crosses trust boundaries, DMZ's are created to connect multiple networks of different trust levels.	Best Practice			
All network switches are configured with strong unique passwords	Best Practice			
Dual homed servers have been eliminated. DMZ's are instead used to accomplish data transfer between two networks.	Best Practice			
A Management of Change (MoC) process is in place for all network changes include changes to the configuration of switches and routers	Best Practice			
Best practices for switch configuration are documented and used. The NSA best practice or equivalent document is used.	Best Practice			
Non-industrial grade switches are not used	Best Practice			
All switches are configured and have strong unique passwords	Best Practice			

2.8 Access Control: Account Administration, Authentication, and Authorization (including Network Segmentation)

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
An access control policy for IACS has been developed and implemented	11.1.1			
There is a procedure in place for user registration and de-registration which includes assigning users unique ID's and granting them the minimum level of access control needed in order to perform their job function.	11.2.1			
Access to configuration settings and cybersecurity settings of all control system products should be limited to the most restrictive mode that is consistent with the manufacturer's recommendations and operational requirements	Best Practice			
User access rights are reviewed periodically by management at regular intervals	11.2.4			
Policies are in place to ensure that users follow good security practices in the selection and use of passwords	11.3.1			
A policy exists for specifying password strength, usage time, and complexity	Best Practice			
A policy exists specifying unique accounts for non-operator logins	Best Practice			
A policy exists to restrict access to Windows desktop and other unnecessary applications for devices that are part of the IACS	Best Practice			
Unattended equipment security policies are in place such as the following: Users are advised to terminate active sessions when finish, Users are advised to logout of systems when activity is complete, Unattended equipment is prevented from unauthorized use by a key lock or an equivalent control such as password access	11.3.2			
Clear desk and screen policies are in place to protect sensitive information	11.3.3			
Appropriate authentication methods are used to control access by remote users	11.4.2			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Best practices for remote access are documented and followed. Examples include the following: Change TCP port numbers for well-known remote access protocols from their defaults; Configure VPN such that split tunneling is not allowed by technical policy; Monitor and log (log user ID, time and duration of remote access) all remote access sessions; Require multi-factor (e.g. two-factor or greater) authentication for any remote access sessions.	Best Practice			
Physical and logical access to diagnostic and configuration ports is controlled.	11.4.4			
For critical systems, inactive sessions are configured to shutdown after a defined period of inactivity	11.5.5			
Guidance and best practices for secure usage of wireless technologies have been developed if such technologies are allowed	11.7.3			

2.9 System Hardening

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Unnecessary functions or features have been removed or disabled from IACS	Best Practice			
IACS components have been locked down so that unnecessary functions or components cannot be added without permission.	Best Practice			
Security best practices provided by vendors are applied	Best practice			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Policy for file sharing should be in place and followed. Insecure practices related to file sharing such as the following should be avoided: Mistake 1: Sharing an entire hard drive, Mistake 2: Letting anonymous people write to your computer, Mistake 3: Sharing folders containing system data, Mistake 4: Giving the "everyone" group permissions on any share.	Best Practice			
Default user accounts are removed or renamed (e.g. Admin, Guest)	Best Practice			

2.10 Vulnerability, Patch Management and Virus Scanning

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Systems are periodically checked for known vulnerabilities	Best Practice			
Unsupported components with known vulnerabilities are updated to supported components	Best Practice			
A register or database of all applications on the ICS system is kept to aid in checking for known vulnerabilities.	Best Practice			
Non-critical applications with known vulnerabilities are removed (e.g. Adobe, Flash, Internet Explorer, Java, MS Office, Games)	Best Practice			
Risk analysis is used to determine whether the benefit of correcting the vulnerability outweighs the risk of deploying patches	Best Practice			
Patches are deployed to machines on a priority basis	Best Practice			
Patches, updates, and virus definition files are not distributed to the IACS directly from the business network.	Best Practice			
A dedicated patch manager and anti-virus server in the DMZ is used to distribute patches and virus definitions to the IACS	Best Practice			
Automated patch management tools and services are used to improve critical patch response time	Best Practice			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Compatibility of Windows patches with major control software suppliers is done before deploying to control system machines	Best Practice			
Patches are tested on non-critical systems before deploying on production machines.	Best Practice			
Anti-virus software is running on all Windows based hosts.	Best Practice			
Virus definition files are regularly updated	Best Practice			
Virus definition updates are staggers so that all computers are not updated at the same time.	Best Practice			
Compatibility of anti-virus software and signatures are verified with major control system software suppliers	Best Practice			
Alert methods from control system vendors are in place to identify anti-virus updates that are NOT appropriate for the IACS	Best Practice			
A rollback procedure is in place in case any anti-virus updates are incompatible with the IACS	Best Practice			
Anti-virus updates are deployed to machines on a priority basis	Best Practice			

2.11 Cybersecurity Incident Management

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
An incident response procedure is in place defining the actions and responsivities for reporting and responding to incidents.	13.1.1, 13.1.2, 13.2.1			
The organization monitors the types, volumes, and costs of security incidents	13.2.2			
Personnel are trained in their incident response roles and responsibilities with respect to the IACS including periodic refresher training	13.2.5			
The incident response procedure documents when external parties (government, local law enforcement) need to be notified and who will make such notifications	13.2.9			

Requirement	Reference IEC 62443-2-1	Complete	Compliance Argument	Open Issues
Failed cybersecurity breaches are investigated as well as successful ones	Best Practice			
Drills are periodically carried out to test the cybersecurity response process.	Best Practice			

3 Abbreviations and Definitions

3.1 Abbreviations

DMZ	Demilitarized Zone (sometimes referred to as a perimeter network or screened subnet)
IACS	Industrial Automation Control System
MoC	Management of Change
SIS	Safety Instrumented System

4 Disclaimer, Assumptions, Equipment Data

4.1 Disclaimer

The user of the exSILentia® software is responsible for verification of all results obtained and their applicability to any particular situation. Calculations are performed per guidelines in applicable international standards. *exida.com L.L.C.* accepts no responsibility for the correctness of the regulations or standards on which the tool is based. In particular, *exida.com L.L.C.* accepts no liability for decisions based on the results of this software. The *exida.com L.L.C.* guarantee is restricted to the correction of errors or deficiencies within a reasonable period when such errors or deficiencies are brought to its attention in writing. *exida.com L.L.C.* accepts no responsibility for adjustments made by the user to this automatically generated report.

4.2 Assumptions

An overview of the specific assumptions made for each of the exSILentia® tool modules, including SILect and SILver, is listed in the user guide as well as in the detailed reports that can be generated for each of these tools.

The cyber security requirements listed in this document are based on a draft copy of IEC 62443-2-1 and industry best practices. The majority of the requirements listed are derived from the standard with little or no additional interpretation. For some requirements additional interpretations were needed. *exida.com L.L.C.* accepts no responsibility for the correctness of the regulations or standards on which the tool is based. In particular, *exida.com L.L.C.* accepts no liability for decisions based on the results of this software. The *exida.com L.L.C.* guarantee is restricted to the correction of errors or deficiencies within a reasonable period when such errors or deficiencies are brought to our attention in writing. *exida.com L.L.C.* accepts no responsibility for adjustments made to this automatically generated report made by the user.