| **Set of ICS Security Standards - Operation Management** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Control item** | **Risk mitigation action** | | | **Validation of actions** | | | | **Standard Recommendation (IEC 62443)** | **Objective(s)** | **Goals to be achieved (expected score)** | **Possible problem(s) in Re-validation (Control Action has already been implemented)** |
|  | **Expected weight** | **Validated weight** | **Actions** | **Validation performed** | **Expected weight** | **Validated weight** | **Negative weight** |
| **Management (Weight 10)** | 100 | 0 | Asset inventory |  | 10 |  |  | Policies | a) Definition of which assets are critical   b) Improving the level of knowledge about the assets | 1) There is an inventory (3.0)  2) The list is up to date (2.0)  3) The asset has an expiry date (2.0)  4) The asset has an assigned value (2.0)  5) The asset has a maintenance check (1.0) |  |
| Prioritisation of critical assets |  | 10 |  |  | Policies | a) Define which assets can most severely impact the ICS   b) Validate list and communicate to all involved | 1) There is an up-to-date inventory (1.0)  2) There is a criticality criterion for assets (2.0)  3) There is a survey of critical assets (3.0)  4) There is a list of assets and prioritization (3.0)  5) Frequency of reviews of the list (1.0) |  |
| Definition of implementation policy |  | 10 |  |  | Policies | a) Definition of goals   b) Definition of necessary resources (personnel, tools and investments)   c) Definition of rules for implementing Management | 1) Based on the list, define the main objectives (2.0)  2) Define and approve goals with managers (3.0)  3) Define and approve resources with managers (2.0)  4) Documentation and history of decisions (2.0) 5) Creating an implementation policy (1.0) |  |
| Change management |  | 10 |  |  | Policies | a) Predictability   b) Stability for the operation of the ICS | 1) Is there a committee for evaluating changes (3.0)  2) Frequency of committee meetings (2.0)  3) Change management documentation (2.0)  4) Change history (2.0)  5) Change planning model (1.0) |  |
| Monitoring access to equipment |  | 10 |  |  | Policies | a) Definition of users and access profiles   b) Having a history of access to assets | 1) Access privileges matrix (2.0)  2) Process for creating users (2.0)  3) Process for deleting users (2.0)  4) Access review process (2.0)  5) User audit trails implemented (2.0) |  |
| List of trainings |  | 10 |  |  | Policies | a) Have users trained and aware of their responsibilities | 1) Definition of relevant training (2.0)  2) Resources needed (internal and external) to carry out the training (2.0)  3) General training controls (2.0)  4) Periodic review process  (2,0)  5) Simulations and aptitude tests after training (2.0) |  |
| Training monitoring |  | 10 |  |  | Policies | a) Ensure that new technologies/assets are subject of new training programs | 1) Process for implementing new assets (3.0)  2) Definition of those responsible for new (2.0) implementations (2.0)  3) Alignment with the change committee (2.0)  4) Periodic reports (2.0)  5) Definition of action plans for non-compliance (1.0) |  |
| Documentation management and control |  | 10 |  |  | Policies | a) Up-to-date documentation | 1) Ensure existence of documentation (3.0)  2) Define reviewers and review frequency (2.5)  3) Storage and access process (2.0)  4) Control of printed documentation (2.5) |  |
| Contracting services |  | 10 |  |  | Policies | a) Definition of scope and guarantees   b) Medium/short-term planning | 1) Definition of business partners - costs and level of specialization (2.0)  2) Definition of scope of services (2.0)  3) Alignment of guarantees and service levels (2.0)  4) Definition of services with internal and external execution (2.0)  5) Definition of costs involved and financial planning - expenses and investments (2.0) |  |
| Risk management |  | 10 |  |  | Policies | a) Conducting risk assessments   b) Reports and actions | 1) Creating the list of risks (2.0)  2) Conducting the risk assessment (2.0)  3) Documenting existing risks (2.0)  4) Treating residual risk (2.0)  5) Final report (2.0) |  |
| **Architecture (Weight 3)** | 60 | 0 | Definition of reference architecture |  | 10 |  |  | Reference Architecture | a) Define the strategy for implementing ICS in the Organization | 1) Identify references used - manufacturers and/or literature (3.0)  2) Design of the available architecture (3.0)  3) What critical factors were used to define the architecture (2.0)  4) Model for contracting services and equipment - appropriate to the current architecture (2.0) |  |
| Documentation of the implemented architecture |  | 10 |  |  | Reference Architecture | a) Reference for operation and support teams | 1) Level of knowledge of the architecture among the operations and support teams (10) |  |
| Definition of hardening (Baseline) |  | 10 |  |  | Reference Models | a) Increasing the level of security   b) Make it more difficult for intruders | 1) Manufacturers recommend hardening activities (3.0)  2) Prior evaluation of the effectiveness of countermeasures (3.0)  3) Documentation available for implementing countermeasures (2.0)  4) Configurations have been tested (2.0) |  |
| Definition of communication protocols |  | 10 |  |  | Reference Models | a) Making the environment homogeneous | 1) Definition of a single protocol (2.0)  2) Alignment between different suppliers - is it the best protocol (2.0)  3) Protection actions for the selected protocol (2.0) 4)  Exception handling (2.0)  5) Criteria used to approve an exception (2.0) |  |
| Types of encryption |  | 10 |  |  | Reference Models | a) Make the environment homogeneous   b) Avoid conflicts between manufacturers and solutions | 1) Reason for using encryption (2.0)  2) Existing documentation (2.0)  3) Criteria for choosing the type of encryption used (2.0)  4) Exception handling (2.0)  5) Criteria used to approve an exception (2.0) |  |
| Management of manufacturer documentation |  | 10 |  |  | Reference Models | a) Ensure the ICS is up to date | 1) Documentation is stored (2.0)  2) Process in place for updating (2.0)  3) Frequency of revisions (2.0)  4) Definition of those responsible (2.0)  5) Execution process (2.0) |  |
| **Updates (Weight 5)** | 30 | 10 | Defining the frequency of updates |  | 10 | 10 | -2 | Policies | a) Keeping systems up to date b) Dealing with legacy systems | 1) Documentation on updates (2.0)  2) Update history (2.0)  3) Update and rejections and description of reasons (2.0)  4) Frequency criterion used (2.0)  5) Implementation schedule (2.0) |  |
| Implementation windows |  | 10 |  |  | Policies | a) Define updating strategy | 1) Update plan by asset criticality (10) |  |
| Exception handling |  | 10 |  |  | Policies | a) List of exceptions   b) Impact assessment   c) Definition of actions | 1) Criteria used to define exceptions 2 ) Existing analysis and documentation - impacts and risks (2.0)  3) Approval to include the exception (2.0)  4) Palliative measures (2.0)  5) Evaluation of actions taken (2.0) |  |
| **Network segregation (Weight 8)** | 60 | 0 | Segmentation OT and IT network |  | 20 |  |  | Security zones | a) Protect the OT and IT environment respectively   b) Ensuring the Organization’s operation | 1) Definition of security zones (2.0)  2) Firewall rules implemented (2.0)  3) Real-time evaluation of rules (2.0)  4) Cabling and physical structure implemented (2.0)  5) Action plans for handling incidents (2.0) |  |
| Firewall implementation |  | 20 |  |  | Security zones | a) Evaluating and protecting network traffic   b) Ensuring ICS security | 1) Equipment and support and maintenance strategy in place (3.0)  2) Procedures available (3.0)  3) Process for implementing new rules (2.0)  4) Process for maintaining existing rules (2.0) |  |
| Defining traffic rules |  | 10 |  |  | Security zones | a) Reduce exposure to risks | 1) Evaluation of systems involved (2.0)  2) Definition of basic requirements (2.0)  3) Traffic monitoring to evaluate rules (2.0)  4) Immediate blocking process implemented (2.0)  5) Definition of responsibility matrix (2.0) |  |
| Monitoring firewalls |  | 10 |  |  | Security zones | a) Ensuring the operationalization of security   b) Proactivity | 1) Monitoring system in place (2.0)  2) Status definition and communication plan (2.0)  3) Matrix of responsibilities and contacts (2.0)  4) Process for updating events and procedures (2.0)  5) Change history (2.0) |  |
| Threat treatment |  | 10 |  |  | Security zones | a) Root cause analysis of events   b) Improving the security strategy | 1) Evaluation process and consultation sources (3.0)  2) References and knowledge bases (3.0)  3) Definition of indicators (3.0)  4) History of events (1.0) |  |
| Periodic review of rules |  | 10 |  |  | Security zones | a) Constant monitoring of the ICS for new threats | 1) Updated documentation (2.0)  2) Frequency of reviews (2.0)  3) Analysis and control process (2.0)  4) Updating documentation (2.0)  5) History of reviews and analyses (2.0) |  |
| **Users (Weight 10)** | 60 | 0 | Change standard passwords for equipment |  | 10 |  |  | Policies | a) Minimising attacks | 1) Asset commissioning procedures (3.0)  2) Equipment manuals and documentation (3.0)  3) Standardized access review process (2.0)  4) Documenting change history (2.0) |  |
| Active Directory (AD) implementation |  | 10 |  |  | Policies | a) Network integration   b) User traceability   c) Definition of access groups and segregation of duties   d) Maintenance of the user lifecycle | 1) Active Directory implemented (2.0)  2) Definition of specific policies (2.0)  3) Configuration of audit trails and logs (2.0)  4) Permission and access control process (2.0)  5 Updated documentation (2.0) |  |
| Password policies |  | 10 |  |  | Policies | a) Access control | 1) Process for individualizing users (2.0)  2) Process for notifying users (3.0)  Password policy implemented and known to users (2.0)  3) Alignment of the policy with the organization’s rules (1.0)  4) Access testing (2.0) |  |
| Integration of equipment with Active Directory (AD) |  | 10 |  |  | Policies | a) Access control   b) Maintenance of the user lifecycle   c) Avoiding parallel and compensatory controls | 1) Documentation of assets suitable for integration (2.0)  2) Documentation of assets unsuitable for integration (2.0)  3) List of exceptions (2.0)  4) Mitigation actions and access control process (2.0)  5) Password change history for exceptions (2.0) |  |
| Password review and change process |  | 10 |  |  | Policies | a) Additional control for processes | 1) Configurations implemented in Active Directory (3.0)  2) Configuration implemented in exceptions (3.0)  3) Documentation (1.0)  4) Evaluate audit trails and logs (3.0) |  |
| Documentation |  | 10 |  |  | Policies | a) History and reference source | 1) Procedures available (3.0)  2) Level of knowledge of end users (3.0)  3) References used (3.0)  4) History of changes (1.0) |  |