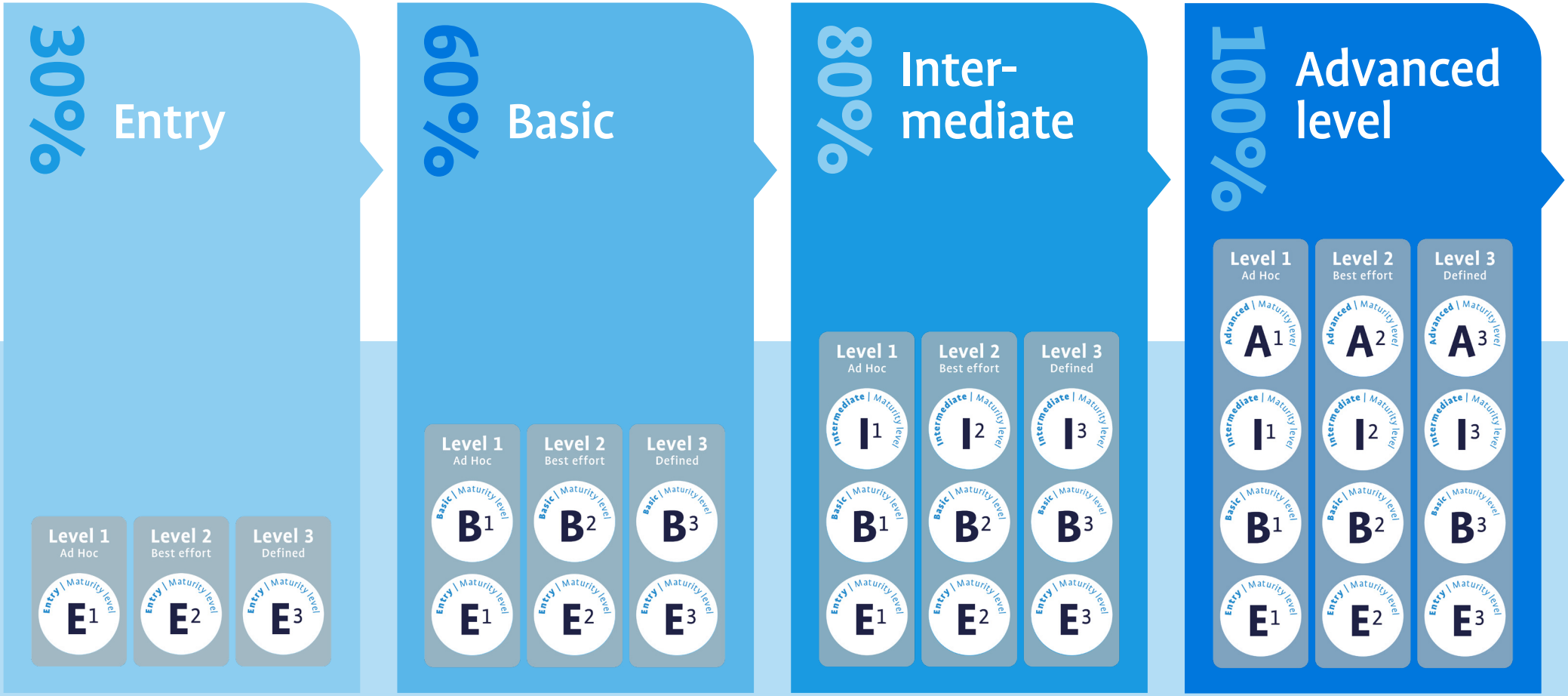
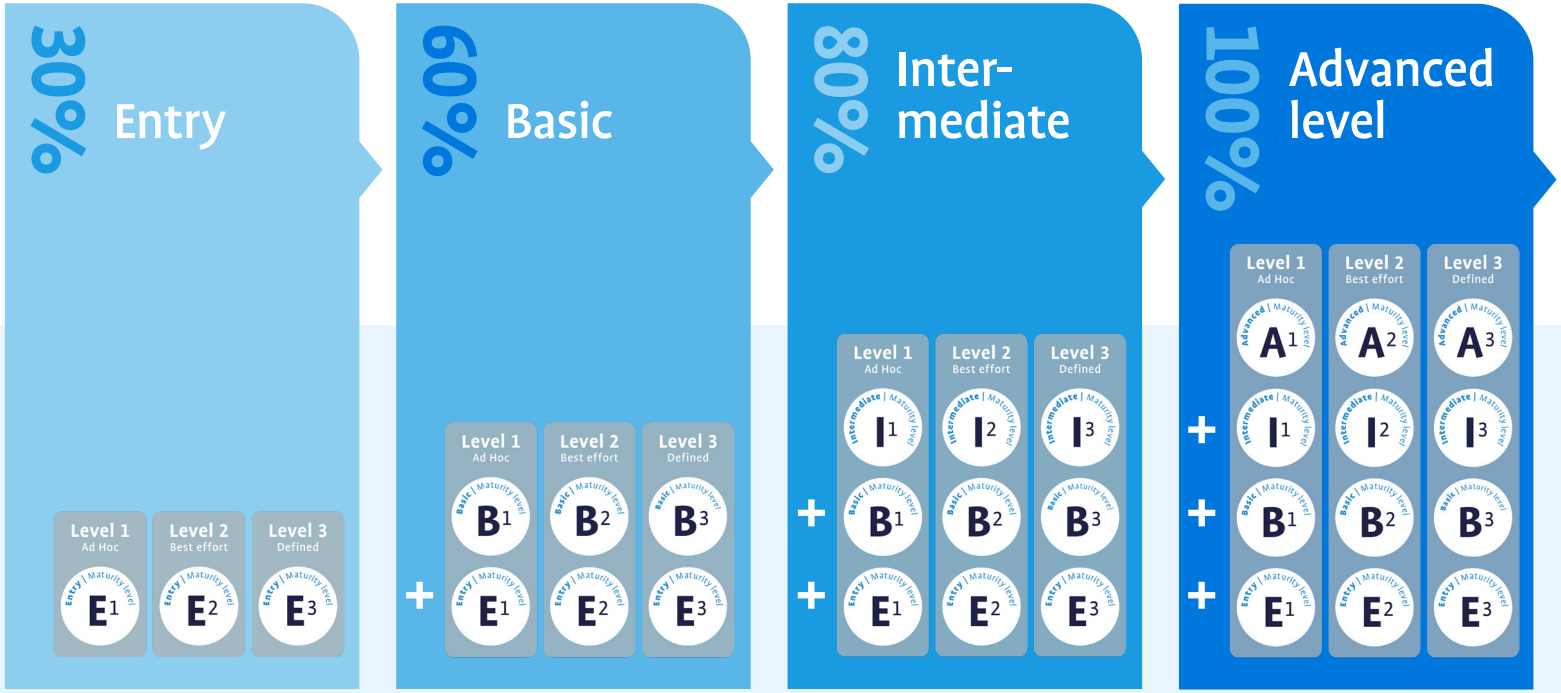
CYRA-OT

Based on IEC 62443



CCV centrum voor criminaliteitspreventie en veiligheid

The CCV CYRA method



Explanation of the CYRA Levels

The CYRA method follows a step-by-step approach. Each higher level builds upon the lower levels, and these lower levels are therefore a mandatory part of the assessment.

For example, if you choose to achieve the **Intermediate level** (80%), this means you are required not only to answer the questions corresponding to that level (the 'I' questions), but **also the questions from the Entry level (E) and Basic level (B)**.

The structure is as follows:
- **Entry level (30%)**: you only complete the E questions.
- **Basic level (60%)**: you complete both the B and E questions.
- **Intermediate level (80%)**: you complete the I questions, as well as the B and E questions.
- **Advanced level (100%)**: you complete the A questions, plus all questions from the underlying levels (I, B and E).

The different levels also consist of three maturity levels:
Level 1 (Ad hoc), Level 2 (Best effort), and Level 3 (Defined). These indicate how well-organised and structured the security measures (controls) are.

- **Ad hoc**: Security measures are either not applied or only applied occasionally. There are no formal policies, procedures, or structured practices in place. Activities depend on individuals and are not standardised.
- **Best effort**: Security measures exist in principle. There is often informal policy or partially documented procedures. Implementation is recognisable but not yet consistent or formally secured.
- **Defined**: Security measures are fully and demonstrably implemented. Policies, processes, and responsibilities are documented and consistently applied and maintained.

CCV centrum voor criminaliteitspreventie en veiligheid

CYRA-OT Level

Entry | Basic | Intermediate | Advanced

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
1	**SPE 1 Organisational security measures**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	ORG 1.2	Background checks	Has the organisation ensured that background checks are carried out for (internal, external, temporary) staff, suppliers and other service providers who require access to the OT environment before such access is granted?	Some form of background check is performed for personnel and suppliers working within the OT environment. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that background checks are carried out for all personnel, suppliers, and other service providers requiring access to the OT environment, and there are documented procedures for performing these checks before access is granted.	Policies and/or procedures state that background checks are carried out in advance for personnel, suppliers, and service providers who are granted access to the OT environment. This is done in accordance with documented procedures. Periodic checks are carried out to verify that policies and/or procedures function effectively and are improved where necessary.
2	**SPE 1 Organisational security measures**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	ORG 1.3	Security roles and responsibilities	Has the organisation ensured that security roles and responsibilities are defined and assigned for internal and external staff, (sub)contractors and consultants?	Informal security roles and responsibilities have been assigned. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that security roles and responsibilities are defined and assigned for internal and external staff, (sub)contractors and consultants, and these are documented and communicated within the organisation.	Policies and/or procedures state that security roles and responsibilities are defined and assigned to internal and external staff, (sub)contractors and consultants. These are documented and communicated. Periodic checks are carried out to verify effectiveness and adjustments are made where necessary.
3	**SPE 1 Organisational security measures**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	ORG 1.4	Security awareness training	Has the organisation ensured that periodic cybersecurity awareness training is provided to all personnel (internal and external), (sub) contractors and consultants working within the OT environment?	Cybersecurity awareness training is occasionally provided to personnel and suppliers. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that periodic cybersecurity awareness training is provided to all personnel (internal and external), (sub) contractors and consultants working within the OT environment. Training is documented and delivered according to an established schedule.	Policies and/or procedures state that periodic cybersecurity awareness training is provided to all personnel (internal and external), (sub) contractors and consultants working within the OT environment. Training is carried out and documented according to a set schedule. Periodic reviews are performed to verify effectiveness and make improvements where necessary.
4	**SPE 1 Organisational security measures**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	ORG 2.1	Security risk mitigation	Has the organisation ensured that cybersecurity risks are managed, including identifying, documenting, mitigating and determining acceptable risk levels, and that action is taken for risks exceeding these levels?	Some risk management for OT systems is applied, but the process is informal and there are no documented procedures for identifying, documenting, mitigating and determining acceptable risk levels. Risks exceeding acceptable limits are not consistently addressed. This is not defined in policies or procedures.	Policies and/or procedures state that cybersecurity risks for OT systems are managed systematically, including identification, documentation, mitigation and determination of acceptable risk levels. Documented processes and procedures exist, and the organisation acts on risks exceeding the established levels.	Policies and/or procedures state that cybersecurity risks for OT systems are managed systematically, including identification, documentation, mitigation and determination of acceptable risk levels. The organisation acts on risks beyond these levels. Periodic checks are performed to verify effectiveness and improvements are made where necessary.
5	**SPE 2 Configuration management**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	CM 1.4 SR 3.4	Change control Software and information integrity	Has the organisation ensured that changes in system and network configurations follow a change management process?	Changes are always made in consultation with the administrator. However, formal policy or procedure for validation and approval is missing.	Policies and/or procedures state the steps to be followed when implementing and documenting changes. Wherever possible, the engineering role is separated from the control role.	Policies and/or procedures state that changes follow a formal change management process, ensuring the engineering role is separated from the control role. Periodic checks are conducted to verify correct application and improvements are made where necessary.

CCV centrum voor criminaliteitspreventie en veiligheid

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
6	SPE 3 Network and communications security	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 1.1 SR 5.1	Segmentation from non-IACS zones Network segmentation	Has the organisation ensured that the OT network is logically separated from other networks (such as IT or internet networks)?	The OT network is separated from other networks, but formal policy or procedure is missing. It is unclear how strictly the separation has been implemented in practice.	Policies and/or procedures state that the OT network is logically separated from other networks. Measures have been implemented to achieve physical or logical network segmentation.	The network segmentation defined in policies and/or procedures is periodically evaluated. Checks are performed to detect unwanted connections, and corrective actions are taken where necessary.
7	SPE 3 Network and communications security	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	NET 1.2	Documentation of zones and network zone interconnections	Has the organisation ensured that a network diagram with zoning is maintained, showing connections, conduits, trust levels and security risks?	A network diagram with zoning exists, but it is incomplete or not up to date. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that a network diagram with zoning is maintained, showing connections, conduits, trust levels and security risks. The diagram is maintained, but checks on completeness and accuracy are limited and not systematic.	Policies and/or procedures state that a network diagram with zoning is maintained, including connections, conduits, trust levels and security risks. Periodic checks are conducted to verify effectiveness, currency and coverage, and improvements are made where necessary.
8	SPE 3 Network and communications security	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 1.7 SR 1.2	Network accessible services Software process and device identification and authentication	How does the organisation prevent unauthorised devices or software processes from connecting to the OT network?	Devices are allowed or denied access to the OT network based on experience, e.g. by manually disabling or covering ports. This is done ad hoc and is not defined in policies or procedures.	Policies and/or procedures state that only authorised devices and software processes may connect to the OT network. Technical controls such as MAC address filtering or port-based access control are implemented to limit unauthorised access.	The policy is actively enforced and supported by automated access control measures (such as NAC or device authentication). Measures are periodically evaluated and adjusted where necessary.
9	SPE 3 Network and communications security	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	NET 2.1	Wireless protocols	Has the organisation ensured that wireless communication within the OT environment occurs only via approved protocols, following industry practice, and is adequately documented?	Expectations regarding the use of wireless communication within the OT environment are known within the organisation. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing. Policies and/or procedures state that wireless communication within the OT environment takes place only via approved protocols, following industry practice, and is adequately documented.	Policies and/or procedures state that wireless communication within the OT environment takes place only via approved protocols, following industry practice, and is adequately documented.	Policies and/or procedures state that wireless communication within the OT environment occurs only via approved protocols, following industry practice, and is adequately documented. Periodic checks are conducted to verify effectiveness and currency, with improvements made where necessary.
10	SPE 3 Network and communications security	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 2.2 SR 5.2	Wireless network segmentation Zone boundary protection	Are wireless networks within the OT environment separated from other OT network segments?	Wireless networks are used within the OT environment but are not deliberately logically or physically separated from other network segments. It is assumed that standard configurations provide sufficient protection. Segmentation is neither defined nor verified. No policy or procedure exists for wireless network separation.	Policies and/or procedures state that wireless networks within the OT environment are (logically or physically) separated from other network segments.	Wireless networks within the OT environment are (logically or physically) separated from other OT networks according to defined policies and/or procedures. Separation is demonstrably implemented at all relevant locations and periodically verified. Improvements are made where necessary. New wireless connections are assessed in advance for compliance with segmentation requirements.

CYRA-OT Level

Entry | Basic | Intermediate | Advanced

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
11	**SPE 3 Network and communications security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	NET 2.3	Wireless properties and addresses	Has the organisation ensured that any wireless networks are configured in such a way that accessibility to this information by potential attackers is minimised?	Wireless networks are configured to limit accessibility to information for potential attackers. Policies and/or procedures defining the roles, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that wireless networks are configured so that accessibility of information to attackers is minimised, and the necessary measures are implemented and documented.	Policies and/or procedures state that wireless networks are configured to minimise accessibility of information to attackers. Measures are documented, and periodic reviews are carried out to ensure configurations remain effective and are improved where necessary.
12	**SPE 3 Network and communications security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 3.1 SR 1.13	Remote access applications Access via untrusted networks	Is secure use of remote access enforced through measures such as strong authentication (e.g. MFA), encrypted connections, controlled access (e.g. VPN), and time restrictions?	The mentioned measures are used but are not documented in policies or procedures.	Policies and/or procedures state that remote access may only be applied using the mentioned measures.	Periodic reviews are conducted to ensure that remote access complies with established policies and/or procedures, and corrective actions are taken where necessary.
13	**SPE 3 Network and communications security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 3.2 SR 1.13	Remote access connections Access via untrusted networks	Is it recorded and ensured that all remote access connections are documented, logged, and monitored, including their purpose, duration, and the technologies used?	Remote access is used in practice with some security measures, but there is no structured record of who has access, when, and for what purpose. This is not documented in policies or procedures.	Policies and/or procedures state that every remote access connection must be authorised, logged, monitored, and documented. For each connection, details such as purpose, duration, technologies used (VPN, encryption, MFA), and user identity are recorded.	Policies and/or procedures are fully implemented. There is an up-to-date overview of all active and historical remote access connections. Logging and monitoring take place continuously, and regular reviews verify completeness and compliance with agreed standards. Deviations are immediately addressed.
14	**SPE 3 Network and communications security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	NET 3.3 SR 2.6	Remote access termination Remote session termination	Are remote sessions terminated after a specified period of time?	Remote sessions are automatically terminated after a defined period of (in)activity. This is not documented in policies or procedures.	Policies and/or procedures state that remote sessions are automatically terminated after a certain period of time and under defined conditions.	Policies and/or procedures state the period and conditions under which remote sessions are automatically terminated. OT systems are periodically assessed to verify compliance with the policies and procedures, and corrected where necessary.
15	**SPE 4 Component security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	COMP 1.1 SR 7.7	Component hardening Least functionality	Has the organisation ensured that components and systems in the OT environment are hardened before being deployed, and that this is maintained throughout their lifecycle?	Systems and components are hardened. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that systems and components are hardened and maintained throughout their lifecycle. Unnecessary functions, ports, protocols, and services are disabled.	Periodic reviews are carried out to verify compliance with hardening policies and procedures. Assessments ensure that unwanted functions, ports, protocols, and services remain disabled and that hardening is maintained throughout the lifecycle. Improvement actions are taken as necessary to ensure effectiveness and currency of policies.

CCV centrum voor criminaliteitspreventie en veiligheid

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
16	**SPE 4 Component security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	COMP 1.2	Dedicated portable media	Has the organisation ensured that the use of portable media within the OT environment is recorded?	It is known how portable media should be used within the OT environment. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that the use of portable media within the OT environment is permitted only under defined conditions and with explicit approval.	Periodic reviews are conducted to verify that policies and/or procedures related to portable media use in the OT environment function correctly, remain current, and cover the appropriate aspects. Improvements are implemented where necessary.
17	**SPE 4 Component security**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	COMP 2.3	Malware protection software validation and installation	Has the organisation ensured that only supplier-approved anti-malware solutions are used, and that changes such as signature updates are compatible with the OT environment?	Agreements have been made with the OT environment supplier regarding which anti-malware solutions may be used and how they may be applied. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that only supplier-approved solutions are used, and that any changes or updates are checked for compatibility before being deployed to production.	Periodic reviews verify that policies and procedures for the use of anti-malware solutions and implementation of signature updates function correctly, are complete and current, and are followed in practice. Deviations or deficiencies are identified, and concrete improvement actions are implemented to ensure effectiveness. The cooperation with the supplier is also reviewed to confirm updates are applied on time and in line with compatibility and approval agreements.
18	**SPE 5 Protection of data**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.4 SR 4.2	Data retention policy Information persistence	Has the organisation ensured that the retention period of OT-related information is aligned with business needs, and that confidential data is removed from equipment being decommissioned or sent for repair?	When retaining or deleting data, practicality and risks are considered, but this is not defined in policies or procedures.	Policies and/or procedures state how long data must be retained and define which information must be removed from equipment, and under what conditions this should occur.	Periodic reviews verify that policies and/or procedures function correctly, retention periods are complied with, and confidential data is properly removed from equipment being decommissioned or sent for repair. Audit logs of data removal are maintained, and improvements are implemented where necessary.
19	**SPE 5 Protection of data**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.6 SR 1.5	Key management Authenticator management	How is the use and protection of cryptographic keys organised?	There is no policy or procedure for the use and protection of cryptographic keys. Keys are used or stored on an ad hoc basis.	Policies and/or procedures state that the use and protection of cryptographic keys are based on recognised industry standards, and describe how keys are generated, shared, stored, and destroyed.	Policies and/or procedures state the use and protection of cryptographic keys based on recognised industry standards. These are actively applied and periodically reviewed. Additionally, it is technically ensured that: • Default keys or passwords are changed during installation. • Keys or authenticators are renewed regularly. • Authenticators are stored and transmitted securely, protected against unauthorised viewing or modification. Technical measures for secure storage, distribution, and periodic renewal are tested and improved.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
20	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.1 SR 1.1 RE(1)	User identity assignment Human user identification and authentication - Unique identification and authentication	Has the organisation ensured that all user accounts within the OT environment are personal, that users are uniquely identified and authenticated, and that roles are formally assigned during account management?	There is no formal policy or procedure regarding personal accounts, role assignment, authentication, or access rights management. While the use of personal accounts is encouraged, a structured approach is lacking. Roles are not formally assigned, and authenticators are managed ad hoc.	Policies and/or procedures state that: • All user accounts must be personal. • Shared accounts are not permitted. • Roles are formally assigned to users during account creation. • Authenticators are managed securely and in a controlled manner (including initial setup and replacement). This policy is documented and actively communicated within the organisation, but compliance is not yet systematically or periodically verified.	Policies and/or procedures are systematically enforced. A centrally managed system for user identities and role assignment exists. Compliance with policies and/or procedures is periodically verified, including the prevention of shared accounts and the secure management of authenticators. Improvements are implemented and policies updated where necessary.
21	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.1 SR 1.3	User identity assignment Accountmanagement	Is the management of user accounts in the OT environment carried out systematically throughout their entire lifecycle, from creation to removal, including the management of access rights?	Policies and/or procedures do not define how account lifecycle management and access rights administration within the OT environment are performed. Account management is done ad hoc without standardised processes.	Policies and/or procedures state how user account and access rights management must take place throughout the full lifecycle. This policy has been communicated, but compliance is only sporadically verified.	Policies and/or procedures state that account management is consistently performed and periodically reviewed. All changes to accounts and access rights are logged and assessed, and findings lead to improvements where necessary.
22	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.2 SR 1.3	User identity removal Accountmanagement	How is it ensured that users within the OT domain are assigned the correct user identity, authentication method (such as password or token), and role (access rights)?	Users are assigned accounts and access rights based on experience or need, but there is no formal policy or procedure for assigning user identities, authentication methods, and roles.	Policies and/or procedures state how user accounts, authentication methods (such as passwords or tokens), and roles are assigned. This includes who is responsible for requesting, evaluating, and assigning access rights within the OT domain.	Policies and/or procedures state the process for assigning accounts, authentication methods, and roles. This policy or procedure is consistently applied by authorised personnel. Periodic reviews are conducted to ensure that accounts and roles remain appropriate for users' job functions and are modified or removed where necessary. Periodic reassessment of access and mandatory removal of unused accounts are required.
23	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.4 SR 2.1	Access rights assignment Authorization enforcement	How is the review and revocation of access rights organised within the OT domain?	User accounts are revoked when the user leaves the organisation. This is not defined in policies or procedures.	Policies and/or procedures state the responsibilities for revoking user accounts within the OT domain, including how long accounts remain active, who initiates the request, and when a user account must be blocked.	Policies and/or procedures state the responsibilities for revoking user accounts within the OT domain, including account retention periods, request procedures, and blocking triggers. Access rights are periodically reviewed against the personnel list and corrected where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
24	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.5 SR 1.3	Least privilege Accountmanagement	How is the granting of access rights for user accounts within the OT domain organised?	It is unclear whether user accounts are granted only those rights strictly necessary for their function and whether rights are revoked when users leave the organisation. This is not defined in policies or procedures.	Policies and/or procedures state the responsibilities for granting rights within the OT domain, including which roles are permitted specific access rights.	Policies and/or procedures state the responsibilities for granting rights within the OT domain, including which roles are permitted specific access rights. Access rights are periodically reviewed against account holder roles and corrected where necessary.
25	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.8 SR 1.1	Human user authentication Human user identification and authentication	Is it ensured that all users accessing OT systems, regardless of the interface (e.g. local login, application, web service, file transfer, OPC server, or remote desktop), are identified and authenticated before access is granted, and that OT system functions can only be operated after successful login?	In practice, a login is usually required to use OT systems, but this is not formally documented in policies or procedures. Authentication is not applied consistently across all interfaces, and shared accounts exist.	Policies and/or procedures state that users must be identified and authenticated on key OT access interfaces (such as local login and remote desktop). Exceptions are limited and demonstrably controlled.	All OT access interfaces are inventoried and equipped with consistent, up-to-date identification and authentication methods aligned with the security policy. Shared accounts are prohibited or strictly controlled. Monitoring and periodic testing of the implemented measures are in place.
26	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.15 SR 1.11	Consecutive login failures Unsuccessful login attempts	How is access blocked after a number of failed login attempts?	Technical blocking after several failed login attempts is intended but not defined in policies or procedures.	Policies and/or procedures state after how many failed login attempts access is blocked. Technical controls have been implemented for this. There are policies and/or procedures in place to manage exceptions for specific OT systems.	Policies and/or procedures state after how many failed login attempts access is blocked. Technical measures are implemented accordingly. Periodic checks are performed to verify that user accounts are blocked as required and corrected where necessary. policies and/or procedures state how exceptions are handled for specific OT systems.
27	SPE 6 User access control	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.18 SR 2.5	Screen lock Session lock	Is a Clear Desk and Clear Screen policy applied?	Personnel understand they are expected to lock system access when leaving their workstation, but this is not defined in policies or procedures.	Policies and/or procedures state that Clear Desk and Clear Screen principles are applied, specifying the period of inactivity after which the screen lock activates, and ensuring the policy is technically enforced on all OT systems.	Policies and/or procedures state that Clear Desk and Clear Screen principles are applied, specifying the inactivity duration for automatic screen lock activation, and ensuring technical enforcement across all OT systems. Technical settings are centrally managed, deviations are automatically reported, and periodic audits verify adherence by personnel. Corrections are made where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
28	**SPE 6 User access control**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 1.19 SR 1.2	Component authentication Software process and device identification and authentication	How is identification and authentication of all networked/logical components within the OT network organised and enforced?	Devices and software processes within the OT network are recognised technically or permitted based on experience. Policies and/or procedures do not define how identification and authentication of networked/logical components should be implemented or enforced. Some components are granted access without verification.	Policies and/or procedures state how identification and authentication of networked/logical components must be implemented and enforced. If systems cannot meet these requirements, mitigation such as restricted access or isolation is applied.	Policies and/or procedures state how identification and authentication of networked/logical components must be implemented and enforced. Unknown devices are automatically blocked or quarantined. Periodic checks verify that components comply with defined requirements, and non-compliant systems are corrected or removed.
29	**SPE 6 User access control**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	USER 2.1 SR 1.6	Authorization Wireless access management	Is wireless communication used within the OT environment, and is access restricted to specific users and devices?	Wireless communication is used within the OT environment, but there is no clear overview of which users or devices have access. Access is granted and monitored ad hoc by individual staff members. Knowledge resides with individuals rather than processes. This is not defined in policies or procedures.	Policies and/or procedures state that wireless communication is used and that access is restricted to specific users and devices. A general list of authorised users and devices exists, but it is not always up to date and checks are partly manual.	Access control for wireless communication is fully defined in policies and/or procedures. Current, documented information exists on which users and devices have access. Access is technically controlled (e.g. via whitelists, certificates, or authentication) and periodically reviewed for effectiveness. Unauthorised devices or users are automatically detected and blocked.
30	**SPE 7 Event and incident management**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.5 SR 2.8	Log entries Auditable events	Are (cyber)security-related events within the OT domain recorded and analysed in such a way that they are suitable for time-correlated analysis and non-repudiation, including sufficient detail on source, type, and outcome of the event?	No policy or procedure has been established for analysing events based on log data. Analyses are performed ad hoc using available information, without structured recording or guarantees for non-repudiation or cross-system correlation.	Policies and/or procedures state which log data must at minimum be collected for event analysis (including timestamp, source, event type, user, and result). This information supports traceability and time-correlated analysis. Staff are familiar with the policy or procedure and apply it during incident analysis.	The organisation periodically verifies that log data are sufficient for time-correlated analysis and non-repudiation. Policies and/or procedures are regularly reviewed and improved based on incident experience, audit results, or technological developments. Event correlation and analysis are systematically supported by tooling or SIEM solutions where possible.
31	**SPE 7 Event and incident management**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	EVENT 1.9	Vulnerability handling	Has the organisation ensured that existing and newly identified OT vulnerabilities are identified, addressed, and, where possible, mitigated in a timely manner?	Existing and newly identified vulnerabilities are identified, addressed, and resolved. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that existing and newly identified OT vulnerabilities are identified, addressed, and resolved in a timely manner.	Policies and/or procedures state that existing and newly identified OT vulnerabilities are identified, addressed, and resolved in a timely manner. Periodic reviews ensure that policies and/or procedures function correctly, remain current, and cover all relevant aspects. Improvements are implemented where necessary.
32	**SPE 8 System integrity and availability**	**Entry** *Answer the questions from:* • *Entry*	IEC 62443-2-1	AVAIL 1.1	Continuity management	Has the organisation ensured that a disaster recovery plan (DRP) and/or a business continuity plan (BCP) exists, setting out scenarios, procedures, and processes to ensure operational continuity?	Consideration has been given to actions required in the event of an incident to maintain operational continuity. However, no formal policy or procedure defining a BCP or DRP, including tasks, responsibilities, and authorisations, exists.	Policies and/or procedures state that a disaster recovery plan and/or a business continuity plan must exist. These plans include defined scenarios, response procedures, and processes for maintaining operational continuity.	Periodic reviews are conducted to ensure that policies and/or procedures related to the disaster recovery and business continuity plans are up to date and function effectively. Improvements are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
33	SPE 1 Organisational security measures	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1	ORG 1.6	Supply chain security	Has the organisation ensured that cyber-security requirements are imposed on its suppliers?	Some cybersecurity requirements are imposed on suppliers, but these are not formally documented or consistently applied across all suppliers. This is not stated in policies or procedures.	Policies and/or procedures state that cybersecurity requirements must be imposed on all suppliers. These requirements are documented and integrated into contracts or agreements, and a process exists to monitor compliance.	Policies and/or procedures state that all suppliers must comply with cybersecurity requirements. These are documented, included in contracts or agreements, and a monitoring process ensures compliance. Periodic reviews confirm that policies and/or procedures are effective and improvements are made where necessary.
34	SPE 1 Organisational security measures	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1	ORG 3.1	Physical access control	Has the organisation ensured that physical access to the OT infrastructure is managed in line with cybersecurity objectives?	Measures exist to manage physical access to the OT infrastructure, but they are not formally documented or aligned with the organisation's broader cybersecurity objectives. This is not stated in policies or procedures.	Policies and/or procedures state that physical access to the OT infra-structure is managed in accordance with the organisation's cybersecurity objectives. Documented procedures govern access control and the security of physical OT infrastructure, and are regularly evaluated and updated.	Policies and/or procedures state that physical access to the OT infra-structure is managed according to cybersecurity objectives. Documented procedures govern access control and protection, are periodically reviewed for effective-ness and currency, and improvements are implemented where necessary.
35	SPE 2 Configuration management	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	CM 1.1 SR 7.8	Asset inventory baseline Control system component inventory	Has the organisation ensured that an asset management system exists in which hardware and software components are recorded with the necessary information?	Asset management is in place. The organisation is aware of which equipment, hardware, software, communication protocols, and open ports are used and their details. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that throughout the entire lifecycle of the OT environment, an asset manage-ment system provides visibility of all equipment, hardware, software, communication protocols, and open ports. At minimum, it records: responsible person, supplier, model, version numbers, serial numbers, network interfaces, communication address, patch levels, and history.	Periodic reviews verify that asset management policies and/or procedures are followed and that the system remains current. Improvements are implemented where necessary.
36	SPE 2 Configuration management	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1	CM 1.2	Infrastructure drawings/documenta-tion	Has the organisation ensured that diagrams and documentation for the physical and logical connections of OT equipment and software components remain current?	Network diagrams and documen-tation on the physical and logical connections of OT components exist. However, policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that all documentation and network diagrams must be maintained and updated, and that the tasks, responsibilities, and authorisations for this are clearly defined.	Periodic reviews confirm that policies and/or procedures stating the maintenance and updating of documentation and network diagrams are up to date and functioning effectively. Improve-ments are implemented where necessary.

CYRA-OT Level

Entry | **Basic** | Intermediate | Advanced

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
37	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.1 SR 5.1 RE(1)	Segmentation from non-IACS zones Physical network segmentation	Has the organisation implemented policies and measures to achieve physical network segmentation ensuring that OT networks are strictly separated from non-OT networks, and that critical OT systems are strictly separated from non-critical OT systems to minimise the risk of unwanted connections?	In practice, physical separation of OT systems exists, but it is applied ad hoc. Formal policies and/or procedures on physical network segmentation are missing.	Policies and/or procedures state that physical network segmentation is mandatory for all OT systems. Critical OT systems must be physically separated from non-critical systems and from non-OT networks, with only authorised and controlled physical connections permitted. This segmentation is documented, including physical layout diagrams and authorised connections.	Policies and/or procedures state that physical network segmentation is periodically tested and verified. Unauthorised or unintended physical connections are detected and removed, and improvements are made to ensure the effectiveness and relevance of physical separation.
38	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.1 SR 5.4	Segmentation from non-IACS zones Application partitioning	Has the organisation stated policies and measures to logically separate applications, data, and services within OT systems according to their criticality to the OT process?	There is no formal policy or procedure, but in practice attempts are made to separate critical and less critical functions within systems.	Policies and/or procedures state that OT applications, data, and services must be logically separated according to their importance and role within the OT environment. This separation is applied during design, implementation, and maintenance.	Policies and/or procedures for logical separation of applications and data are periodically reviewed. Improvements are implemented based on evaluations or changing risks.
39	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.6 SR 1.13	Internal network access control Access via untrusted networks	How is internal segmentation between the OT network and the IT office network technically managed, and how is unauthorised communication between segments and via untrusted networks prevented?	OT segmentation exists, but there is no formal policy or procedure. Segmentation between OT and IT, and between OT segments, is applied ad hoc. Access via untrusted networks is not systematically controlled.	The OT network is separated from the IT office network, and further segmentation within the OT network is implemented. Policies and/or procedures state that access via untrusted networks must be explicitly approved by an authorised role.	The OT network is separated from the IT network, and segmentation within the OT domain is described in detail in policies or procedures. Periodic assessments determine whether segmentation and access remain adequate based on risk, and verify that access via untrusted networks is explicitly approved. Corrective actions are taken where required.
40	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.6 SR 5.2	Internal network access control Zone boundary protection	Has the organisation segmented the OT network based on risk, considering system function, ownership, or physical/logical location?	Different segments exist within the OT network, but there is no policy or procedure for this.	Policies and/or procedures state that the OT network must be segmented based on risk, considering system function, management/ownership, physical or logical location, technology used, or other relevant factors.	Periodic reviews verify that policies and/or procedures function correctly, ensuring that risk-based segmentation of the OT network is applied in accordance with the stated criteria. Improvements are made where necessary.
41	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.6 SR 5.2 RE(1)	Internal network access control Zone boundary protection - Deny by default, allow by exception	Has the organisation ensured that security risks arising from communication between internal networks are managed?	The risks are partly understood, but this is not stated in policies or procedures. No defined risk level or plan exists for adjustment when risks increase.	Policies and/or procedures state that security risks are managed, that the acceptable level of risk is determined, and that actions are defined for addressing risks that exceed this level.	Policies and/or procedures state that security risks are managed. The acceptable level of risk is determined, and actions are defined for responding to risks that exceed this level. Periodic reviews verify that policies and/or procedures function correctly and that risks remain within the established level. Improvements are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
42	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.7 SR 2.3	Network accessible services Use control for portable and mobile devices	Has the organisation ensured that the use of portable and mobile devices within the OT network is controlled and monitored?	No policy or procedure exists regarding the use of portable and mobile devices (such as USB sticks, laptops, or tablets) within the OT network. Devices are used occasionally without formal guidelines or technical restrictions.	Policies and/or procedures state that the use of portable and mobile devices within the OT network is permitted only with explicit approval and with appropriate security measures in place.	Policies and/or procedures state that the use of portable and mobile devices within the OT network is regulated. The policy or procedure is supported by technical measures (such as whitelisting or device control software), is actively enforced, and is periodically reviewed and strengthened where necessary.
43	**SPE 3 Network and communications security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	NET 1.9 SR 2.11	Network time distribution Timestamps	Has the organisation ensured that OT systems use clock synchronisation and that this process is secure and controlled?	It is assumed that OT systems use the same time because professionals have configured them correctly, but this is not systematically verified. This is not stated in policies or procedures.	Policies and/or procedures state that OT systems must use clock synchronisation. The organisation maintains visibility of the systems to which this applies, and internal time synchronisation is actively maintained.	Clock synchronisation is technically implemented and governed by policies and/or procedures. When multiple time sources are used (such as cloud environments or GPS), deviations between them are actively monitored. Time sources are protected against unauthorised modification, and synchronisation frequency is configurable.
44	**SPE 4 Component security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	COMP 2.1	Malware free	Has the organisation ensured that if the use of portable media is permitted, such media are free from malware?	Where the use of portable media is permitted, it is checked for malware before use. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that, where the use of portable media is permitted, the media must be checked for malware prior to use. A procedure describes how this verification is to be performed and who is responsible for it.	Periodic reviews confirm that policies and/or procedures for checking portable media for malware function correctly, remain current, and cover all relevant aspects. Improvements are implemented where necessary.
45	**SPE 4 Component security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	COMP 3.1	Security patch authenticity/integrity	Has the organisation established policies and measures to verify that patches are authentic and unaltered before installation?	No formal policy or procedure has been established, but in practice patches are verified to ensure they originate from a trusted source and have not been modified.	Policies and/or procedures state how patches are to be verified for authenticity and integrity before installation. These checks are performed in practice.	Policies and/or procedures for verifying the authenticity and integrity of patches are periodically evaluated. The effectiveness of these controls is tested and adjusted as needed.
46	**SPE 4 Component security**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	COMP 3.2	Security patch validation and installation	Has the organisation implemented policies and measures to test patches for compatibility, approve them, and install them in a timely manner?	No formal policy or procedure has been established, but in practice patches are often tested before installation. Installation occurs regularly but not always within a defined timeframe.	Policies and/or procedures state how patches are tested for compatibility, who must approve them, and within what timeframe they must be installed. This process is followed in practice.	Policies and/or procedures for testing, approving, and installing patches are periodically reviewed for completeness, timeliness, and accuracy, and updated as required. Improvements are implemented where necessary based on evaluation results.
47	**SPE 5 Protection of data**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.1 SR 3.9	Data classification Protection of audit information	Has the organisation ensured that confidential OT-related information is classified accordingly and protected in line with its classification?	It has been agreed that confidential data will be treated as such, but classification and protection are not stated in policies or procedures.	Policies and/or procedures state which information must be classified as confidential and how it must be protected against unauthorised access, alteration, or deletion.	Periodic reviews confirm that policies and/or procedures function correctly, ensuring that confidential information is properly classified and protected in line with its classification against unauthorised access, alteration, or deletion. Improvements are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
48	SPE 5 Protection of data	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.4 SR 7.4	Data retention policy Control system recovery and reconstitution	Has the organisation ensured that the retention period for OT backups is appropriate and that the organisation can restore systems to a known safe state after an incident?	When setting up backup systems, the desired retention period was determined, and the system can be restored to a safe state. However, no policy or procedure has been established for one or both aspects.	Policies and/or procedures state how long backups must be retained and that systems can be restored to a known safe state. This is aligned with a risk assessment.	Backup archives are periodically reviewed against policies and/or procedures. The effectiveness of restoration procedures is tested periodically (e.g. through recovery tests or simulations). Corrective measures are implemented where necessary.
49	SPE 5 Protection of data	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.5 SR 4.3	Cryptographic mechanisms Use of cryptography	Has the organisation ensured that the encryption technology used complies with current standards and is free from known vulnerabilities?	The use of modern encryption standards is encouraged, but this is not stated in policies or procedures.	Policies and/or procedures state that encryption technology must comply with current standards and be free from known vulnerabilities.	Periodic reviews confirm that policies and/or procedures function correctly, ensuring that the encryption technology used complies with current standards and is free from known vulnerabilities. Outdated or vulnerable encryption is phased out in a timely manner. Improvements are implemented where necessary.
50	SPE 5 Protection of data	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.7 SR 3.1	Data Integrity Communication integrity	Has the organisation ensured that the confidentiality and integrity of data flows from OT systems (such as sensor data or control signals) are protected during communication with untrusted networks, in accordance with the importance and sensitivity of the information?	Confidential data are encrypted before transmission. This is not stated in policies or procedures.	Policies and/or procedures state that appropriate security measures must be implemented based on the importance and sensitivity of the data, to prevent loss or alteration of integrity during transmission via external network connections or when using portable media.	Policies and/or procedures describe suitable measures to ensure the integrity of data flows from OT systems during communication via untrusted networks and when using portable media. The effectiveness of these measures is periodically tested and improved where necessary.
51	SPE 6 User access control	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	USER 1.1 SR 1.6 RE(1)	User identity assignment Wireless access management - Unique identification and authentication	Has the organisation ensured that unique identification and authentication of users (human, software, or devices) are enforced when accessing OT systems via wireless connections?	Wireless access occasionally occurs within the OT domain, but unique identification and authentication are not consistently applied or recorded. This is not stated in policies or procedures.	Policies and/or procedures state that all users (including software processes and devices) accessing OT systems via wireless connections must be uniquely identified and authenticated. This policy is known within the organisation, but compliance is checked only occasionally.	Periodic reviews confirm that wireless access is correctly configured according to policies and/or procedures. Technical or procedural improvements are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
52	**SPE 6 User access control**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1	USER 1.3	User identity persistence	Has the organisation ensured that login credentials, authenticators, and access rights are configured so that they are not automatically disabled?	Some measures are in place to manage login credentials, authenticators, and access rights, but no formal policy or procedure ensures that these are not automatically disabled or that unwanted automatic blocking does not occur.	Policies and/or procedures state that login credentials, authenticators, and access rights must be configured so that they are not automatically disabled without proper authorisation or process. Documented procedures and configurations ensure controlled and deliberate actions when disabling access, to prevent unwanted blocking.	Policies and/or procedures state that login credentials, authenticators, and access rights must not be automatically disabled without proper approval. Documented processes and configurations exist to prevent unintended automatic blocking. Periodic tests confirm that no unwanted automatic blocking occurs, and deviations are reported and addressed. Regular reviews verify that policies and/or procedures are effective, and improvements are implemented where necessary.
53	**SPE 6 User access control**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	USER 1.16 SR 3.8	Session integrity	Has the organisation ensured that unauthorised access to another user's session on OT systems is prevented?	Login is required to access system functions. Staff are expected to log out or lock their screen when leaving the workstation, but this is not stated in policies or procedures.	Policies and/or procedures state that systems must be configured so that functions are available only after login, and that user sessions are technically protected against misuse by others.	Policies and/or procedures state that systems provide access to functions only after login, and that user sessions are technically protected against misuse by others. Periodic reviews verify that policies and/or procedures function correctly and are improved where necessary.
54	**SPE 7 Event and incident management**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.4 SR 2.8	Logging Auditable events	Has the organisation ensured that cyber-related (system) events within the OT domain, including timestamp and username, are recorded in protected log files and retained as long as reasonably necessary for incident investigation (preferably at least nine months)?	No policy or procedure exists for collecting and retaining logs and log content. System logs are retained for some time if they are part of automatic backups. The backups are protected.	Policies and/or procedures state that logs of cyber-related (system) events must be traceable to the time of the event and, where possible, to the system or user involved. Critical logs are protected and retained for at least three months.	Policies and/or procedures for log registration and retention are periodically reviewed. Improvements are implemented where necessary to ensure log protection and retention periods remain adequate.
55	**SPE 7 Event and incident management**	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.4 SR 2.9	Logging Audit storage capacity	Has the organisation ensured that the growth of log files within the OT domain does not exceed storage capacity?	Log growth has been considered, but no formal policy or procedure is in place to manage this effectively.	Policies and/or procedures state that storage capacity must be configured to accommodate expected log growth.	Policies and/or procedures state that available storage capacity is periodically evaluated based on expected log growth. Measures are taken where necessary to ensure timely capacity management.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
56	SPE 8 System integrity and availability	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 2.1 SR 7.3	Backup Control system backup	Has the organisation ensured that backups are made periodically to enable restoration of OT systems after an incident?	Backups are made, but formal backup policies or procedures are missing.	Policies and/or procedures state that periodic backups must be made of OT systems to allow restoration after an incident. This includes backups of backup servers, infrastructure configurations, licences, master data, and historical data where applicable.	Periodic reviews confirm that backup-related policies and/or procedures are followed correctly. Reviews verify that all required backups, including those of backup servers, configurations, licences, master data, and historical data, are made. Improvements are implemented where necessary.
57	SPE 8 System integrity and availability	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 2.2 SR 7.3 BR	Backup non-interference Control system backup	Has the organisation ensured that backup processes do not interfere with normal OT operations?	Backups are performed for OT systems, but there is no formal policy or procedure to ensure that these processes do not affect normal operations. The operational impact of backups is not systematically assessed.	Policies and/or procedures state that backup processes must be executed in such a way that they do not negatively affect normal OT operations. Documented procedures and controls ensure that backups are performed safely and optimally, without disrupting OT operations.	Policies and/or procedures state that backup processes must be executed in a way that does not interfere with normal OT operations. Documented procedures and controls ensure this. Regular reviews assess the effectiveness of policies and/or procedures, and improvements are made where necessary.
58	SPE 8 System integrity and availability	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1	AVAIL 2.4	Backup media	Has the organisation ensured that backups are handled securely to maintain integrity, authenticity, and availability?	Backups are stored securely, and integrity, authenticity, and availability are tested regularly. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that backups must be handled securely to maintain integrity, authenticity, and availability.	Policies and/or procedures state that backups must be handled securely to maintain integrity, authenticity, and availability. Examples include backup encryption, offsite storage, access control, and logging of backup access. Regular reviews assess the effectiveness of policies and/or procedures, and adjustments are made where necessary.
59	SPE 8 System integrity and availability	**Basic** *Answer the questions from:* • *Entry* • *Basic*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 2.5 SR 7.4 BR	Backup restoration Control system recovery and reconstitution	Has the organisation ensured that backups of OT environments can be restored in a stable and timely manner?	Backups can be restored in a timely manner, but policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that backups of OT environments must be restorable in a stable and timely manner.	Policies and/or procedures state that backups of OT environments must be restorable in a stable and timely manner. Periodic reviews assess whether policies and/or procedures are effective and improved where necessary.
60	SPE 1 Organisational security measures	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	ORG 2.2 SR 3.3	Processes for discovery of security anomalies Security functionality verification	Has the organisation ensured that security measures continue to function correctly, vulnerabilities are detected and resolved, and unauthorised software and/or systems within the OT domain are identified?	Action is taken when unfamiliar devices or malfunctioning security functions are observed. Security updates are regularly installed on computers and firewalls, but it is unclear whether this is done comprehensively. Policies and/or procedures to actively oversee this are missing.	Policies and/or procedures state that security measures must function correctly, and that the use of unauthorised systems or software must be prevented. Security updates are installed on computer systems, firewalls, and other systems. The urgency of updates is determined based on risk severity.	Policies and/or procedures state that security measures, updates, and detection of unauthorised systems are periodically reviewed. Improvements are implemented where necessary to ensure continued effectiveness.

CYRA-OT Level
Entry | Basic | **Intermediate** | Advanced

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
61	**SPE 1** **Organisational security measures**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1	ORG 2.4	SP reviews	Has the organisation ensured that the OT security programme is periodically reviewed and adjusted?	The OT security programme is reviewed from time to time, but there is no formal process or fixed frequency for periodic assessment and adjustment. This is not stated in policies or procedures.	Policies and/or procedures state that the OT security programme is reviewed and adjusted periodically. A documented process exists for evaluating the programme, and action is taken to update it based on evaluation results.	Policies and/or procedures state that the OT security programme is reviewed and adjusted periodically. A documented process exists for evaluation and amendment. Regular checks verify that policies and/or procedures are current and effective, with improvements implemented where necessary.
62	**SPE 3** **Network and communications security**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	NET 1.1 SR 5.2	Segmentation from non-IACS zones Zone boundary protection	Has the organisation established policies and measures to keep OT (IACS) networks separated from other networks, with inter-network traffic controlled and limited to what is necessary?	Efforts are made to keep OT networks separate from office networks and to limit connections as much as possible. Policies and/or procedures for this are missing.	Policies and/or procedures state how OT networks are separated from other networks (such as IT or the internet) and how traffic between them is limited to what is necessary. These measures are applied in practice.	Policies and/or procedures for network segmentation and controlling communications between zones are reviewed periodically. Measures are adjusted or improved as needed based on these reviews.
63	**SPE 3** **Network and communications security**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	NET 1.8 SR 5.3	User messaging General purpose person-to-person communication restrictions	Has the organisation ensured that e-mail or other instant-messaging systems are excluded from the OT domain to prevent the spread of malicious software or links?	E-mail (and similar) is not used in the OT domain, but this is not recorded in policies or procedures.	Policies and/or procedures state that the use of e-mail and instant messaging in the OT domain is prohibited, except for automated, outbound messages for (status) signalling.	Policies and/or procedures state that the exclusion of e-mail and instant messaging in the OT domain is monitored via technical controls and reviewed periodically. Improvements are implemented and the policy updated where necessary.
64	**SPE 4** **Component security**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	COMP 2.2 SR 3.2	Malware protection Malicious code protection	Has the organisation ensured that servers, workstations, and (engineering) laptops in the OT domain are equipped with an up-to-date anti-malware solution?	As far as is known, all systems have an anti-malware solution, but this is not stated in policies or procedures and is not monitored.	Policies and/or procedures state that computer systems must be equipped with up-to-date malware protection.	Policies and/or procedures state that systems must have up-to-date malware protection with updates installed promptly and automatically. Compliance is checked periodically and corrected where necessary.
65	**SPE 4** **Component security**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	COMP 3.5	Security patch mitigation	Has the organisation ensured that the risks of not installing patches are assessed and addressed?	The risks of not installing patches are taken into account, and action is taken if risks are deemed unacceptable. Policies and/or procedures defining tasks, responsibilities, and authorisations for this are missing.	Policies and/or procedures state that the risks of not installing patches must be assessed. If risks are unacceptable, they are mitigated and the solution is documented.	Policies and/or procedures state that the process for assessing and documenting risks of not installing patches must function correctly, including the execution of mitigating measures and the associated documentation. Periodic reviews confirm effectiveness and improvements are implemented where needed.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
66	**SPE 5 Protection of data**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.2 SR 4.1	Data confidentiality Information confidentiality	Has the organisation established policies and measures to protect confidential OT data against unauthorised access, both at rest and in transit?	No formal policy or procedure exists yet, but there is attention to protecting sensitive data and avoiding unauthorised access.	Policies and/or procedures state how confidential OT data are protected against unauthorised access, based on data type and risk. These arrangements are applied in practice.	Policies and/or procedures for protecting confidential OT data are regularly checked and evaluated. Improvements are implemented where necessary based on the evaluations.
67	**SPE 5 Protection of data**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1	DATA 1.3	Safety system configuration mode	Has the organisation ensured that changes and updates to safety systems are carried out in a secure manner?	Changes to safety systems are made only after enabling configuration mode, and this mode is enabled solely for that purpose. Policies and/or procedures defining tasks, responsibilities, and authorisations are missing.	Policies and/or procedures state that changes to safety systems are made only after temporarily enabling configuration mode, which is enabled solely for that purpose and disabled after use.	Policies and/or procedures state that safe changes to safety systems are enforced and checked periodically, preventing and logging unauthorised modifications. Improvements are implemented where necessary.
68	**SPE 5 Protection of data**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.7 SR 3.9	Data Integrity Protection of audit information	Has the organisation ensured that logbooks and audit tools (audit information and tools) within OT systems are protected against unauthorised access, alteration, or deletion?	No formal policy or procedure exists, but in practice access to logbooks and audit tools is limited to authorised personnel.	Policies and/or procedures state how logbooks and audit tools are protected against unauthorised access, alteration, and deletion. These arrangements are followed in daily operations.	Policies and/or procedures for protecting logbooks and audit tools are periodically reviewed and evaluated. Checks confirm that only authorised access is possible and that changes or deletions are logged. Improvements are implemented to keep protection effective and current.
69	**SPE 6 User access control**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	USER 1.11 SR 1.7	Password protection Strength of password-based authentication	Has the organisation established a password policy for OT systems, and is this policy technically enforced?	Password settings (such as complexity, lifetime, and reuse) are configured per OT system without a documented policy, procedure, or central alignment.	Policies and/or procedures state the requirements that passwords in OT systems must meet. At a minimum: complexity, lifetime, reuse, and the technical means to enforce these settings.	Policies, procedures, and technical alignment are in place. Periodic reviews verify that OT systems comply with password settings (e.g., prevention of reuse, maximum/ minimum lifetime). Corrective measures are taken where necessary.
70	**SPE 6 User access control**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1	USER 1.12	Shared and disclosed/ compromised passwords	Has the organisation ensured that compromised and shared passwords are managed?	Some measures are taken to manage compromised and shared passwords, but there is no formal process or policy. There is no clear procedure for detecting, reporting, or remediating compromised passwords.	Policies and/or procedures state that compromised and shared passwords must be managed in a formal and secure manner. A documented procedure exists for identifying, handling, and remediating compromised passwords, and the organisation ensures shared passwords are avoided as far as possible or managed under security guidelines.	Policies and/or procedures state that compromised and shared passwords are securely managed, with processes for detection and remediation. Detection of compromised passwords is automated (e.g., against breach databases), and the use of shared passwords is actively prevented. Operation is periodically reviewed and improved.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
71	**SPE 6 User access control**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1	USER 1.14	User login failure displays	Has the organisation ensured that failed login attempts do not provide an attacker with information that could assist them?	Some measures are in place to prevent attackers from obtaining information from failed login attempts, but no formal policies or documented procedures ensure that error messages do not contain helpful information for potential attackers.	Policies and/or procedures state that failed login attempts must not provide information that could assist an attacker, such as detailed error messages revealing the type of failure. Documented procedures ensure that error messages are generic and do not disclose valuable information.	Policies and/or procedures state that failed login attempts must not disclose specific information that could assist an attacker, such as details on the nature of the error. Documented guidelines and technical measures ensure that error messages are generic and contain no sensitive data. Logging and error messages are periodically tested to confirm that no unintended information is revealed. Policies and/or procedures are periodically reviewed for effectiveness, and improvements are implemented where necessary.
72	**SPE 6 User access control**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	USER 1.17 SR 2.7	Concurrent sessions Concurrent session control	How is the number of concurrent sessions per user limited on OT systems?	In practice, there are no restrictions set on the number of concurrent sessions a user can open on OT systems. Users can start multiple sessions without limitation. No policies and/or procedures exist on this matter.	Policies and/or procedures state how many concurrent sessions a user is permitted to have on OT systems.	Policies and/or procedures state how many concurrent sessions a user is permitted to have on OT systems. Policies and/or procedures are periodically reviewed and adjusted where necessary.
73	**SPE 6 User access control**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	USER 2.2 SR 2.1	Separation of duties Authorization enforcement	How are the principles of separation of duties and least privilege for OT system users organised?	Authorisations are managed ad hoc: users are assigned tasks and rights based on knowledge or experience. There are no policies and/or procedures for separation of duties or the principle of least privilege.	Policies and/or procedures state that separation of duties and least privilege for OT system users must be applied.	Policies and/or procedures state that separation of duties and least privilege for OT system users must be applied. Automated role validation or periodic cross-checks on segregation of duties are in place. Policies and/or procedures are periodically reviewed and improved where necessary.
74	**SPE 7 Event and incident management**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.1 SR 6.1	Event detection Audit log accessibility	Are log files available in the OT environment, and are they accessible to authorised persons or tools on a read-only basis?	Policies and/or procedures do not state whether and how log files are used within the OT environment. Logging occurs ad hoc or follows default settings, and access to logs is neither limited nor protected. There is no specification of who may view or modify logs.	Policies and/or procedures state which log files must be generated and who has access to them. Access to log files is limited to authorised administrators, with read-only access configured in some cases but not consistently enforced.	Policies and/or procedures state that log files must be generated consistently and are only accessible to authorised persons or tools, always on a read-only basis. The use of log data for detecting and analysing security-relevant events is described and periodically evaluated.
75	**SPE 7 Event and incident management**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.1 SR 2.8	Event detection Auditable events	Has the organisation ensured that detected cyber-related events in the OT domain are logged, analysed, reported, and adequately followed up?	The organisation knows who the contact point is for cyber-related incidents. However, policies and responsibilities are not formally documented in policies and/or procedures.	Policies and/or procedures state that incidents must be recorded and followed up. Roles and responsibilities are clearly defined and communicated. Where third-party dependencies exist, the required service is included in a service level agreement.	Policies and/or procedures for incident registration and follow-up are periodically evaluated. Roles, responsibilities, and third-party agreements are ensured. Improvement measures are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
76	SPE 7 Event and incident management	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.1 SR 6.2	Event detection Continuous monitoring	Has the organisation established policies and measures to actively monitor OT systems and networks so that security incidents can be detected and followed up in a timely manner?	Part of the OT domain is monitored, but there are no policies or procedures defining continuous monitoring or follow-up in case of anomalies.	Policies and/or procedures state that OT systems and networks must be actively monitored to detect violations of security measures in a timely manner. Follow-up is arranged through an Incident Response Plan with clear roles, responsibilities, and steps.	Policies and/or procedures for monitoring and incident follow-up are periodically reviewed. Real-time alerts are tested, and lessons learned are systematically applied. The Incident Response Plan is updated based on operational experience or changing risks.
77	SPE 7 Event and incident management	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.1 SR 2.10	Event detection Response to audit processing failures	How are failures or outages in the audit logging process of OT systems managed?	There are no policies or procedures describing how the operation of audit logging is monitored. Failures or outages are noticed ad hoc, usually only when users or administrators encounter them by chance. There are no structured measures in place to mitigate audit logging failures.	Policies and/or procedures state that technical measures are in place to (partially) detect audit logging failures. Policies and/or procedures also state that administrators are notified in case of failure and that basic procedures for recovery actions are established.	Policies and/or procedures state that the functioning of audit logging must be actively monitored. In case of failure, administrators are automatically alerted, and recovery actions are clearly described. Policies and/or procedures also state that failures must not result in the loss of essential OT functionality. These procedures are periodically tested and improved.
78	SPE 7 Event and incident management	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1	EVENT 1.8	Incident handling and response	Has the organisation established policies and measures to assess and handle OT-related security incidents appropriately?	No formal policies or procedures have been established, but in practice, efforts are made to assess and respond appropriately to security incidents within the OT environment.	Policies and/or procedures state how OT security incidents must be assessed, followed up, and resolved. Tasks, responsibilities, and response times are defined and applied in practice.	Policies and/or procedures for assessing and handling OT security incidents are regularly reviewed and improved where necessary. Lessons learned from past incidents are also taken into account.
79	SPE 8 System integrity and availability	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 1.2 SR 7.1	Resource availability management Denial of service protection	Has the organisation ensured that appropriate measures are in place to protect OT systems against power failures, overload, component failure, and denial-of-service (DoS) attacks?	Critical OT components are configured redundantly and supported by an uninterruptible power supply (UPS) and backup power system, but there are no formal policies or procedures for this.	Policies and/or procedures state that critical OT systems must be protected, to a reasonable degree, against power failure, overload, and component failure. Network measures have been implemented to protect against DoS attacks. A backup power system is in place.	Policies and/or procedures for protecting OT systems against power failure, overload, component failure, and DoS attacks are periodically reviewed to confirm they function correctly. Improvement measures are implemented where necessary, and policies and/or procedures are updated accordingly.
80	SPE 8 System integrity and availability	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 1.2 SR 7.2	Resource availability management Resource management	Has the organisation ensured that OT system performance is not hindered by security measures?	The aim is to avoid negative impact, but no formal policies or procedures exist for this.	Policies and/or procedures state that security measures must not hinder OT system performance.	Policies and/or procedures are periodically reviewed to ensure that security measures do not hinder OT system performance. Any negative impact is evaluated, and improvement measures are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
81	SPE 8 System integrity and availability	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 1.3 SR 3.6	Failure-state Deterministic output	Has the organisation ensured that processes and/or machines are brought to a defined safe state if normal operation is disrupted by a security incident?	When designing systems, this is taken into account as far as possible, but it is not documented in policies or procedures.	Policies and/or procedures state that control systems must be designed so that, in the event of a security incident (as far as possible), processes and/or machines are brought to a defined safe state. Compliance is monitored during development, testing, and commissioning of control systems.	Policies and/or procedures state that control systems must ensure processes and/or machines are brought to a safe state in the event of a security incident. Compliance with these policies and/or procedures is periodically reviewed, and improvements are implemented where necessary.
82	SPE 1 Organisational security measures	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1	ORG 1.5	Security responsibilities training	Has the organisation established policies and measures to ensure that personnel with OT security responsibilities receive appropriate cybersecurity training relevant to their specific roles?	No formal policies or procedures have been established, but personnel with OT-related security responsibilities sometimes receive training relevant to their role and duties.	Policies and/or procedures state that personnel (including external staff) with OT cybersecurity responsibilities must receive appropriate training suited to their specific role. The training is documented, delivered, and periodically repeated.	Policies and/or procedures for task-specific OT cybersecurity training are periodically reviewed. Based on evaluations, improvements are made where necessary to ensure knowledge and skills remain up to date.
83	SPE 1 Organisational security measures	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1	ORG 2.3	Secure development and support	Has the organisation ensured that a secure development lifecycle process is followed for systems and components within the OT environment?	Some level of secure development is applied for OT systems and components, but there is no formal SDLC process or documented security guidelines for OT system development. This is not captured in policies or procedures.	Policies and/or procedures state that a secure development lifecycle (SDLC) process must be followed for the development of systems and components within the OT environment. The process is documented, integrated into development, and includes security measures throughout the entire lifecycle of OT systems and components.	Policies and/or procedures state that a secure development lifecycle (SDLC) process must be followed for OT systems and components. Security measures are embedded throughout the entire lifecycle. Policies and/or procedures are periodically reviewed for currency and effectiveness, and improvements are made where necessary.
84	SPE 2 Configuration management	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	CM 1.3 SR 7.6	Configuration settings Network and security configuration settings	Has the organisation ensured that configurations of OT equipment and software applications follow vendor recommendations, are documented, and verified?	Configurations follow vendor recommendations and industry best practices. However, policies and/or procedures defining tasks, responsibilities, and authorisations for this are not in place.	Policies and/or procedures state that OT equipment and software applications must be configured according to vendor recommendations and industry best practices, and that such configurations must be documented.	Policies and/or procedures are periodically reviewed to confirm that OT equipment and software application configurations comply with vendor recommendations and industry best practices, and are properly documented. Where necessary, improvements are implemented to maintain the currency and effectiveness of the policies.
85	SPE 3 Network and communications security	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1	NET 1.3	Network segmentation from safety systems	Has the organisation ensured that safety systems used cannot be influenced by other systems and networks?	Checks are carried out to ensure that safety systems used cannot be influenced by other systems and networks. However, policies and/or procedures defining tasks, responsibilities, and authorisations for this are not in place.	Policies and/or procedures state that safety systems used must not be influenced by other systems and networks.	Policies and/or procedures state that safety systems used must not be influenced by other systems and networks. Compliance is periodically reviewed to confirm the policies and/or procedures function correctly, are up to date, and address the right aspects. Improvements are made where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
86	SPE 3 Network and communications security	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	NET 1.5 SR 5.2 RE(3)	Network disconnection from external networks Zone boundary protection - Fail close	Has the organisation ensured that OT systems can be disconnected from external networks in the event of a (suspected) security incident?	The method for disconnecting from external networks is known but this is not documented in policies or procedures.	Policies and/or procedures state that OT systems must be disconnected from external networks in the event of a (suspected) security incident. This requirement is also taken into account when implementing new systems.	Policies and/or procedures for disconnecting OT systems from external networks during (suspected) security incidents are periodically reviewed for currency and effectiveness. They are updated and improved where necessary.
87	SPE 4 Component security	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	COMP 2.2 SR 3.2 RE(1)	Malware protection Malicious code protection on entry and exit points	Has the organisation ensured that all entry points to the OT network are controlled for malware?	It is agreed that portable media must be scanned for malware before use. It is unclear whether network traffic is inspected for malware. This is not documented in policies or procedures.	Policies and/or procedures state that all data must be scanned for malware before being used in the OT domain, regardless of whether it enters via the network, portable media, or other channels. Anti-malware systems are kept up to date.	Policies and/or procedures state that all incoming data must be checked for malware. The effectiveness of these controls is periodically evaluated and improved where necessary.
88	SPE 4 Component security	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	COMP 3.3	Security patch status	Has the organisation ensured that the patch status and installed software/firmware versions of OT components are documented and kept up to date?	No policies or procedures have been established for documenting the installed software/firmware versions and patch status of OT components, but this information is known and maintained where possible.	Policies and/or procedures state how the installed software/firmware versions and patch status of OT components must be documented and implemented.	Policies and/or procedures state how the installed software/firmware versions and patch status of OT components must be documented and implemented, and whether the documentation is current and complete. Compliance is periodically reviewed, and improvements are implemented where necessary.
89	SPE 4 Component security	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	COMP 3.4	Security patching retention of security	Has the organisation ensured that the installation of patches does not reduce the security level?	Measures are in place to ensure that the installation of patches does not reduce the security level. However, policies and/or procedures defining tasks, responsibilities, and authorisations for this are not in place.	Policies and/or procedures state that the installation of patches must not reduce the security level and that this must be tested.	Policies and/or procedures are periodically reviewed to ensure that patch installations do not lower the security level, function correctly, remain current, and address the right aspects. Improvements are implemented where necessary.
90	SPE 5 Protection of data	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.2 SR 4.1 RE(1)	Data confidentiality Information confidentiality - Protection of confidentiality at rest or in transit via untrusted networks	Has the organisation established policies and measures to protect confidential OT data when stored or transmitted via untrusted networks, such as the internet?	No policies or procedures have been established, but there is awareness of the risk that confidential data could be intercepted during storage or transmission. Efforts are made to prevent this as much as possible.	Policies and/or procedures state how confidential OT data must be protected, particularly during transmission via untrusted networks. Encryption or other protective measures are applied, and these agreements are followed in practice.	Policies and/or procedures for protecting confidential OT data during storage and transmission via untrusted networks are periodically reviewed. Based on these evaluations, improvements are implemented where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
91	**SPE 5 Protection of data**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	DATA 1.7 SR 3.4	Data Integrity Software and information integrity	Has the organisation ensured that stored OT-related data, including logs, are protected against unauthorised access and/or modification, in accordance with the importance and sensitivity of the information?	No policies or procedures have been established, but the intention is to grant access to OT data only to authorised persons and systems.	Policies and/or procedures state that, in accordance with the importance and confidentiality of the data, appropriate security measures must be implemented to prevent unauthorised persons from viewing or modifying data. Entered control parameters are verified for validity.	Policies and/or procedures state that stored OT data, including logs, must be adequately protected against unauthorised access and modification. Policies and/or procedures are periodically reviewed to confirm compliance and effectiveness, and improvements are implemented where necessary.
92	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 1.5 SR 2.1 RE(2)	Least privilege Authorization enforcement - Permission mapping to roles	How is role-based access organised within the OT domain?	No policies or procedures have been established, but in practice role-based access is applied to a limited number of OT users. Roles and access rights are partly known within the team but not formally defined.	Policies and/or procedures state that role-based access control must be applied and that the access rights assigned to each defined role must be documented.	Policies and/or procedures state that role-based access control must be applied and that the access rights assigned to each defined role must be documented. Policies and/or procedures are periodically reviewed against the actual assigned rights and corrected where necessary.
93	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 1.6 SR 1.2	Software service authentication Software process and device identification and authentication	Are software services within the OT environment verified and authenticated before they are allowed to run?	No policies or procedures have been established. Software services are executed without verification of source or identity. There is no mechanism to confirm whether a service is legitimate, and no logs or notifications are maintained. Trust relies on the original installation or configuration.	Policies and/or procedures state that visibility must exist regarding which software services operate on OT systems, that critical services must be verified as originating from a trusted source (for example, by signature or approved installation paths), and that the approach for doing so must be documented.	Policies and/or procedures state that all software services operating within the OT environment must be identified and authenticated in advance through a formal process. Digital signatures, whitelisting, or certificate-based controls are applied. Documentation is complete and up to date, and deviations are automatically blocked or reported.
94	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 1.9 SR 1.1 RE(2)	Multifactor authentication (MFA) Human user identification and authentication - Multifactor authentication for untrusted networks	Is MFA enforced for external connections?	No policies or procedures have been established, but the use of MFA is encouraged, although not always implemented.	Policies and/or procedures state that external connections are only permitted when MFA authentication is applied.	Policies and/or procedures state that external connections are only permitted through MFA (Multi-Factor Authentication). The MFA configuration is tested periodically, and any deviations are automatically blocked. The policy or procedure is reviewed periodically and improved where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
95	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1	USER 1.13	User login display information	Has the organisation ensured that users are shown information during login, such as the last successful login or failed attempts, to help them recognise potential misuse?	No policies or procedures have been established, and users receive minimal support in detecting fraudulent logins. There are no formal processes or tools to help users recognise suspicious or fraudulent activity during login.	Policies and/or procedures state that users must be supported with login information (such as warnings, notifications, or logs) to help detect fraudulent logins. Documented procedures and tools inform users of suspicious activities and assist them in recognising and reporting them.	Policies and/or procedures state that users must be shown clear information during login, such as the date and time of the last successful login and any failed attempts. This supports users in recognising potential fraudulent activity. Documented processes and tools are available to identify and report suspicious login attempts. Policies and/or procedures are periodically reviewed to ensure the measures remain effective, and improvements are implemented where necessary.
96	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 1.16 SR 3.8 RE(1)	Session integrity Session integrity - Invalidation of session IDs after session termination	Has the organisation ensured that user sessions on OT systems are automatically terminated and cannot be reused after logout or timeout?	No policies or procedures have been established. Sessions remain active after logout or timeout, and no technical measures prevent accidental or intentional reuse.	Policies and/or procedures state that sessions must be automatically terminated upon logout or inactivity and cannot be reused. Sessions are technically protected against misuse.	Policies and/or procedures are periodically reviewed to confirm that automatic session termination upon logout or timeout functions correctly, including technical protection against reuse. Technical measures are periodically tested to verify that sessions are actually terminated and cannot be reused. Improvements are implemented where necessary.
97	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 1.16 SR 3.8 RE(2)	Session integrity Session integrity - Unique session ID generation	Has the organisation ensured that every user session on OT systems receives a unique session ID, and that unknown or unexpected session IDs are rejected?	No policies or procedures have been established, and no technical mechanism exists to assign unique session IDs. Multiple sessions may share the same ID, or unrecognised IDs may not be detected or blocked.	Policies and/or procedures state that systems must generate a unique session ID for each session and automatically reject unknown or unexpected session IDs. This configuration is technically implemented.	Policies and/or procedures are periodically reviewed to confirm compliance with the requirement that systems assign unique session IDs and automatically reject unknown or unexpected session IDs. Unexpected session IDs are automatically logged and blocked. Improvements are implemented where necessary based on test results or incidents.
98	**SPE 6 User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 2.1 SR 2.1 RE(1)	Authorization Authorization enforcement for all users	How are assigned access rights for users enforced?	No policies or procedures have been established for enforcing assigned access rights for users. In practice, access to systems is usually limited through default settings or manual assignment, but this is neither standardised nor formally documented.	Policies and/or procedures state how assigned access rights for users must be enforced.	Policies and/or procedures state how assigned access rights for users must be enforced. Policies and/or procedures are periodically reviewed to confirm effectiveness and improved where necessary.

Control	Category	CYRA Level Entry, Basic, Intermediate, Advanced	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
99	**SPE 6** **User access control**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	USER 2.4 SR 2.1 RE(3)	Manual elevation of privileges Authorization enforcement - Supervisor override	Do OT systems have a supervisor-override capability?	No policies or procedures have been established, but the system has a supervisor-override function that can be used by anyone when necessary.	The system has a supervisor-override capability. Policies and/or procedures state in which situations and by whom an override may be used.	The system has a supervisor-override capability. Policies and/or procedures state in which situations and by whom an override may be used. The use of overrides is logged and evaluated for misuse or anomalies. The frequency and users of overrides are periodically reviewed.
100	**SPE 7** **Event and incident management**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.2 SR 6.2	Event reporting Continuous monitoring	Has the organisation established policies and measures to ensure OT security incidents are reported in a timely manner to the appropriate internal or external parties?	No policies or procedures have been established, but incidents are sometimes reported without formal definition of how, when, or to whom they should be reported.	Policies and/or procedures state that OT security incidents must be reported promptly to the appropriate internal and/or external parties. The reporting procedure includes clear steps and responsibilities.	Policies and/or procedures are periodically reviewed to confirm that OT security incidents are reported in a timely manner to the appropriate internal and external parties. Based on incident evaluations, improvements are implemented to maintain reliable and effective reporting, and policies and/or procedures are updated accordingly.
101	**SPE 7** **Event and incident management**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	EVENT 1.3 SR 6.2	Event reporting interfaces Continuous monitoring	Has the organisation ensured that, where possible, standard interfaces are used for communicating OT security-related information?	No policies or procedures have been established, but as far as known, standard interfaces are used for communication.	Policies and/or procedures state that, where possible, standard interfaces must be used for communicating OT security-related information. This is taken into account during the design and development of systems.	Policies and/or procedures state that, where possible, standard interfaces must be used for communicating OT security-related information. Policies and/or procedures are periodically reviewed to confirm that the use of standard interfaces functions correctly. Improvements are implemented where necessary, and policies and/or procedures are updated accordingly.
102	**SPE 7** **Event and incident management**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1	EVENT 1.7	Event analysis	Has the organisation ensured that OT-related security events are identified and analysed in a timely manner?	No policies or procedures have been established, but OT-related security events within the OT environment are identified, analysed, and evaluated in a timely manner.	Policies and/or procedures state that OT-related security events must be identified, analysed, and evaluated in a timely manner.	Policies and/or procedures state that OT-related security events must be identified, analysed, and evaluated in a timely manner. Policies and/or procedures are periodically reviewed to confirm that they function correctly, remain up to date, and cover the relevant aspects. Improvements are implemented where necessary.
103	**SPE 8** **System integrity and availability**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	IEC 62443-2-1 IEC 62443-3-3	AVAIL 2.1 SR 7.3 RE(1)	Backup Control system backup - Backup verification	Has the organisation ensured that OT system backups are reliable by periodically testing their integrity and completeness?	No policies or procedures have been established, but information is occasionally restored from backups when needed. There is no formal policy or procedure for verifying backups.	Policies and/or procedures state that the reliability of backups must be periodically tested for integrity and completeness.	Policies and/or procedures state that the reliability of backups must be periodically tested for integrity and completeness. Policies and/or procedures are periodically reviewed to confirm adherence. Backups are tested to verify that they are reliable, complete, and intact so that OT systems can be restored after an incident. Improvements are implemented where necessary.