C Y	N	Control	Evaluation Level	TWN		
				2023	2024	Comment
01	CY-IT101 (Updated)	**Cybersecurity governance** Do you have an appropriate cybersecurity organization within your entity? Ensure that: - the role(s) Cybersecurity Manager or Cybersecurity Correspondent are defined to manage and be responsible for cybersecurity functions. - the Cybersecurity Manager is involved in the CSEC community, by taking part in the regular meetings organized by the group and by being part of the associated mailing list. - Cybersecurity actions are followed up at least twice a year with the entity's management. - a proactive approach is initiated with the Group Cybersecurity department and the CSEC community, and best-practices are shared. Calculate the cyber FTE/employee ratio (approximately). Supporting Document (SD) - Organizational chart - CISO job description / CISO appointment note	**Not-applied:** No cybersecurity organization is in place within the entity (in particular, no CISO). **Ad-hoc:** A CISO appointed to a cybersecurity organization is involved throughout the entity's perimeter. The CISO is involved in the VEOLIA CSEC community. The FTE ratio is 1 cyber FTE per 1,000 employees or more. **Defined:** Measures from previous levels are applied FTE Ratio is 1 cyber FTE per 1000 or less An action plan (roadmap) is shared with the BU's management at least twice a year, and communicated to the Group Cybersecurity Department (application of the copy & adapt approach). **Optimized:** The measures of the previous levels are applied A proactive approach is initiated with the Group Cybersecurity Department and the CSEC community. Best practices are proactively shared with the Group Cybersecurity Department and the Veolia security community.	3	3	cyber security organization is set up with CISO appointed
02	CY-IT102 (Updated)	**Roadmap and dedicated cybersecurity budget** Do you have a cybersecurity roadmap and an associated annual budget within your entity? Check the existence of: - a cybersecurity roadmap - a budget plan associated with the roadmap SD - Latest detailed annual cybersecurity budget (Google Sheet format) - Cybersecurity roadmap	**Not-applied:** Cybersecurity is not a project: there is no specific roadmap or budget allocation. **Ad-hoc:** Roadmap formalized and validated with the Cybersecurity Department and associated budget. **Defined:** measures from previous levels apply A budget is available and sufficient for critical projects. The budget represents 5 to 10% of the budget allocated to the IT Department. The Cybersecurity Department is informed of planned actions and associated requirements. **Optimized:** Measures from the previous levels apply There is a detailed action plan with budgets covering the entire scope of the entity. The budget represents more than 10% of the budget allocated to the IT department. The roadmap and budget are proactively presented to the Cybersecurity Department for approval. The Group Cybersecurity Department is regularly consulted on actions to be implemented.	3	3	cyber security roadmap defined with budget allocated
03	CY-IT105 (Updated)	**Security dashboard** Do you maintain an up-to-date dashboard, including cybersecurity KPIs from the roadmap, to track the progress of action plans and cybersecurity maturity of your entity? Ensure: - cybersecurity key performance indicators (KPIs) are available - cybersecurity KPIs are tracked on a Dashboard - communicate cybersecurity KPIs to the Group cybersecurity department SD - Dedicated cybersecurity dashboard (dedicated document or tool) - List of cybersecurity KPIs monitored (dedicated document or in a tool)	**Not-applied:** Cybersecurity KPIs are not tracked. **Ad-hoc:** A dashboard is set up for some of the roadmap KPIs. **Defined:** A dedicated dashboard is set up to monitor the entity's cybersecurity roadmap KPIs. This dashboard is communicated to the entity's security sponsor and to the Group's cybersecurity department. An analysis of the dashboard identifies deviations from the roadmap, enabling the action plan and the next roadmap to be adapted. **Optimized:** Measures from previous levels are applied, Best practices are shared with the Group Cybersecurity department.	3	3	Group security KPI dashboard is used, monitored and followed up

04	CY-IT107 (New)	**Inventory of critical business process assets** Are business processes (finance, HR, IT, industrial, etc.) and their critical assets identified in an inventory? Is a plan in place to secure these assets? Verify the existence of an inventory of business processes and their critical assets, including: - criticality and assessed impacts, - Business owner, - stakeholders (and third parties) Verify: - Existence of an asset security plan - Application of security measures on assets in accordance with the plan SD - Inventory, register of critical business processes (BIA) - Proof of latest annual inventory update	**Not-applied:** No inventory of business processes and their critical assets. **Ad-hoc:** Inventory in progress or complete, but not associated with a roadmap and budget. **Defined:** Measures from previous levels apply. The roadmap and budget address critical assets. Risks are prioritized by asset criticality. **Optimized:** Measures from previous levels apply The inventory of business processes and their critical assets is updated annually. Best practices are shared with the Group Cybersecurity Department.		2	asset inventory in place for Taho; not applied to Apollo
05	CY-IT103 (Updated)	**Asset inventory** Do you have a regularly updated list of all physical assets (servers, workstations, smartphones, firewalls, switches, VPN concentrators, etc.) and application assets (software, applications, etc.), including identification of related business processes and an assessment of the criticality of each of these assets in your organization? Ensure that: - a documented guide(s) or procedure(s) specifying the scope covered and describing how the inventory is compiled and updated (sources, person responsible) is available - an up-to-date inventory of physical assets (servers, workstations, smartphones, firewall, switch, VPN concentrator, etc.) and application assets (software, applications, etc.), with identification of related business processes and an assessment of the criticality of each asset is available SD - Inventory of physical and application assets with their level of criticality - Identification of related business processes - Proof of last update (annual) and monitoring of criticality level - Proof of sharing the above information with the Group Cybersecurity Department	**Not-applied:** No inventory of assets has been carried out. **Ad-hoc:** An ongoing or complete inventory of technical assets, but only partially linked to business processes. **Defined:** The technical asset inventory is complete, including business process linkage and criticality assessment. **Optimized:** Measures from the previous levels apply. the inventory is updated annually and monitored for criticality level Inventory is shared with Group Cybersecurity Department	2	2	asset inventory partially maintained
06	CY-IT104 (Updated)	**Risk management** Is cybersecurity risk mapping carried out transversally for the entity? Are risk analyzes carried out on critical assets as well as new projects (security by design)? Are the identified cybersecurity risks the subject of an action plan to address them? Ensure that: - a cross-functional risk map is available. - a risk analyses for critical assets and new projects (security by design) is conducted. - risk management plans for critical assets and new projects are in place. SD - Risk analysis with completion date - Associated action plan with completion date - Any other recent risk analyses - Risk mapping	**Not-applied:** No risk mapping is established **Ad-hoc:** A risk map of critical assets is built on the basis of an assessment. **Defined:** Measures from previous levels apply. Risk mapping is documented with risk analyses on the most critical assets and projects, with annually updated risk monitoring and an associated action plan. Risk mapping is validated with the Group Cybersecurity Department. **Optimized:** Measures from the previous levels apply, Cross-functional risk mapping, with annually updated risk monitoring and associated action plan. Sharing of best practices with the Group Cybersecurity Department.	2	3	risk management process in place for Taho; risk assessment performed for both project entities

07	CY-IT106 (Updated)	**Third party management** Is cybersecurity integrated into the management of business and technical third parties (security clauses in contracts, maturity assessment)? Ensure that: * a list of third parties and corresponding interconnection(s) is available * security clauses are contractually agreed with critical business and technical suppliers * third-party security assessment for critical business and technical suppliers (prior to contract signature/renewal) with one or more validated interconnections, including but not limited to remote access, third-party device connecting our on-site network, site-to-site connection, application-to-application connection, etc - is avalable. * records of accepted remediation actions or compensatory mitigation measures for at least the high/medium risk associated with critical third parties is available. (Cybervadis-type assessment) SD - Process for validating cybersecurity maturity prior to contractualization, based on the criticality of suppliers' businesses - Proof of classification of businesses according to their criticality - Example of a critical business contract containing cybersecurity clauses	**Not-applied**: No adaptable security clauses in contracts. No cybersecurity maturity validation process in place prior to interconnection or contractualization. **Ad-hoc**: Contracts for critical technical assets are in the process of being covered or are covered by cybersecurity clauses (including audit clauses). A cybersecurity maturity validation process is carried out before any interconnection or contractualization for the most critical technical suppliers. **Defined:** Measures from the previous levels apply, Contracts for critical business assets are covered by cybersecurity clauses (including audit clauses). A cybersecurity maturity validation process is carried out prior to any interconnection or contractualization for the most critical business suppliers. **Optimized**: Measures from the previous levels apply, The choice of suppliers in the context of consultation is prioritized according to their cyber maturity. sharing of best practices with the cyber group	2	2	Apollo: third party management process in place; Taho: 資訊委外管理說明書&軟體供應鏈資安風險管理參考規範 in place
08	CY-IT201 (Updated)	**Secure management of the information system** Do you apply a patch management process to manage the obsolescence of your equipment (servers, workstations, firewalls, switches, VPN concentrators, mobile devices, etc.) and applications? - Ensure to have (a) guide(s), document(s), procedure(s) describing obsolescence management, - Check the existence of a list of : ° obsolete equipment and applications, and planned treatments ° tools or records maintaining the patch status of equipment (should cover servers, workstations, network and security appliance and mobile devices, where applicable) and applications, including those that are obsolete - Verify the existence of a traceability and tracking tool for equipment and applications. -Verify the implementation of remediation actions or accepted compensation measures for derogations, particularly for obsolete equipment and applications that are still in use. SD - Document presenting the patch management process - Proof that patches have been applied to the installed systems - Inventory with date of last asset update - Action plan for obsolete equipment and software - Evidence of a patch management clause in contracts	**Not-applied:** No patch management process in place. Obsolete assets are not identified. **Ad-hoc:** A formalized and applied patch management process exists for critical assets. **Defined:** A formalized patch management process is applied to the entire fleet. Obsolete equipment and software are identified and an action plan is drawn up. A patch management clause is included in contracts. **Optimized:** Measures from previous levels are applied. Best practices are shared with the Group Cybersecurity department, and a process for anticipating obsolescence is in place.	2	2	Apollo: patching record provided; Taho: 資通安全事件管理說明書 provided

09	**CY-IT202 (Updated)**	**Account and password management** Do you have a process for managing user accounts and privileged accounts, and for securing passwords? Is it applied throughout your perimeter? Are administration tasks only performed from a dedicated account? Ensure: - to have a documented guide(s) or procedure(s) specifying the scope covered (Account and password management process/strategy) - to integrate the life cycle of accounts into HR procedures for managing employees of new arrivals, people on mobility and departures (JML) - to have a password management policy (in accordance with the Group's password policy) - the deployment of the password policy in systems (Servers & workstations) and on applications - the existence of a process for managing user accounts, Service accounts and privileged accounts - the use of dedicated accounts for administration tasks - that exceptions are traced - that a regular review of all user and high-privilege accounts is carried out SD - Account management process/strategy (life cycle) - Password complexity policy - Evidence of configuration of Active Directory (AD) password policy enforcement tool (e.g. Password Policy Enforcer, SecOps) - Evidence of configuration of an Active Directory (AD) password hardening tool (e.g. Password Policy Enforcer, SecOps) - Evidence of use of an IAM solution - Evidence that all administration tasks are performed via a dedicated account - Evidence of exception logging and tracking - Evidence of regular (6-month) review of user and high-privilege accounts - Evidence of MFA on administration accounts - Evidence of awareness-raising among administrators and all staff	**Not-applied:** No process in place for user or privileged account management. No password policy enforced. Administration tasks are not performed via a dedicated account. **Ad-hoc:** A process for managing user accounts and privileged accounts has been defined, but is only partially applied (situations of non-compliance with imposed practices not traced). A password policy is applied to all accounts Not all administration tasks are performed via a dedicated account **Defined:** A process for managing user accounts and privileged accounts is defined and applied throughout the account lifecycle. The Group password policy is technically applied to all accounts. All administration tasks are performed via a dedicated account. All exceptions are traced and monitored over time. A regular review (6 months) is carried out on all user and high-privilege accounts. Administrator awareness is raised. **Optimized:** The Measures from the previous levels apply. MFA on administration accounts and regular awareness-raising action for all staff.	2	2	Apollo: account lockout policy and password GPO provided; account inventory provided; Taho: 資訊內部稽核報告-存取、通行密碼及特殊存取控制 & 密碼控制 process documents in place; AD account inventory maintained and regularly reviewed
10	**CY-IT203 (Updated)**	**Access Control and Authentication** Is authentication of services exposed on the Internet done using SSO with the Google account, and only with a strong authentication mechanism process? - Verify the integration of Single Sign On (SSO) in authentication - Check the existence of a documented guide(s) or procedure(s) (onboarding a new SaaS solution, reviewing Google account statistics with 2FA, etc.) - List systems and services exposed to the Internet, with associated authentication type - Ensure that 2FA is deployed on all Google accounts - Ensure that Google SSO is applied to system access (PaaS, IaaS, servers, workstations, appliance management, etc.) and applications (SaaS) where applicable - Ensure that a strong alternative SSO with 2FA is applied - Monitor the number of Google accounts with and without 2-factor authentication (2FA) SD - Statistics on the number of Google accounts with and without 2 Factor Authentication (2FA) - Percentage of SSO coverage compared to services exposed on the internet - Evidence of integration by design of SSO for any new service exposed	**Not-applied:** No Google SSO in place **Ad-hoc:** Authentication via Google SSO for critical services exposed on the internet **Defined:** Measures from previous levels apply. Authentication via Google SSO for all services exposed on the internet **Optimized:** Measures from previous levels apply. Authentication via Google SSO integrated by design for any new exposed service	2	2	Apollo: SSO implemented for Cyberreason and hub-V; Taho: MFA enabled for CrowdStrike and Azure

11	CY-IT204 (Updated)	**Access Control and Authentication** Do you use an Active Directory (AD) or LDAP authentication directory? Do you apply the recommendations for secure directory architecture? Do you regularly audit your directory? - Verify the implementation of a three-tier architecture - Check that regular directory scans and technical audits are carried out - Check that action plans have been implemented following the results of audits and directory scans. SD - AD environment architecture diagram - Evidence of AD scan (e.g. AD analyzer) - Evidence of AD audit report - Evidence of AD action and remediation plan	**Not-applied:** No measures applied (no 3-tier architecture, no audit, no scan) **Ad-hoc:** Audits and scans performed on directory(ies) **Defined:** Measures from previous levels applied. Implementation of action plans to remediate identified vulnerabilities. **Optimized:** Measures from previous levels are applied. 3-tier architecture in place, regular scans to identify gaps and new vulnerabilities. **N/A:** No AD	3	3	AD Analyzer scan performed and results followed
12	CY-IT206 (Updated)	**Network** Do you have an Internet Access Point (IAP) inventory? Have you implemented a secure architecture for outputs to the Internet? Ensure to have: - a documented guide(s) or procedure(s) specifying the scope covered (organization for validating new accesses, controls, etc.) - a complete inventory of Internet access points (IAPs), updated regularly - network protection via firewalls and proxies (for all applications) - secure architecture for output to the Internet SD - List/schema showing outgoing flows (flow matrix) to the Internet for all environments (on premise / GCP / AWS / etc) - Proof of regular review of rules - Proof of network protection via firewalls and proxies (for all applications).	**Not-applied:** No inventory of internet access points is carried out **Ad-hoc**: An inventory is partially completed Network protections are implemented in a basic way via firewalls. The rules are revised with best effort. **Defined:** The inventory is complete and reviewed regularly Network protections are put in place via firewalls and proxy (for some applications). The rules are reviewed regularly. **Optimized:** Measures from previous levels apply. Implementation of network protections via firewalls and proxies (for all applications)	2	3	Apollo: 連外網路流程 in place; Taho: IAP maintained in network diagram; IAP protected by firewall
13	CY-IT207 (Updated)	**Network** Do you have a network architecture document indicating the segmentations of your information system? - Verify the existence of documented guide(s) or procedure(s) with defined scope (define the organization to validate the implementation of flows or services, in the appropriate areas. Governance must specify the review of services within network zones, and specify the evolution of filtering rules if necessary). - Make sure you have an updated network architecture diagram, with interconnections between IT and OT (if applicable), a flow matrix and security controls. SD - Global architectural diagram presenting the segmentations of the information system - Flow matrix between the IT and OT environments (if existing) of the information system - Document indicating security controls	**Not-applied**: Neither architecture diagram nor flow matrix have been implemented **Ad-hoc**: The flow matrix and architecture diagram are being implemented or complete **Defined**: The flow matrix and architecture diagram are complete. Network segmentations are defined and controlled **Optimized**: Measures from previous levels apply. The flow matrices and architecture diagram are updated regularly. Best practices are shared with the Group Cybersecurity department	2	3	Network diagrams provided; network segmentations defined and controlled

14	CY-IT216 (New)	**Network** Does your network architecture follow security best practices? Are there interconnections between IT and OT if there is an industrial information system in your area? - Verify the application of good security practices on the network architecture: * segmentation between IT, OT and internal network * definition and implementation of security zones with filtering, with control. - Verify that the interconnections between IT and OT are clearly identified SD - Evidence of network segmentation between IT and OT - Evidence that segmentation is implemented according to a level of sensitivity - Evidence of filtering of different types of environments (test, pre-prod, prod, ...). - Evidence of segmentation control	**Not-applied**: No segmentation between networks, especially between IT and OT networks. **Ad-hoc**: Network segmentation between IT, OT and Internet **Defined**: Network segmentation into security zones defined and implemented according to a sensitivity level, with filtering. This segmentation is controlled for the most critical assets. **Optimized**: Measures from the previous levels apply. Different types of environment are also filtered (test, pre-prod, prod, etc.). This segmentation is controlled on all network segments.		3	Apollo: network digram provided; Taho: 資訊通訊與作業管理說明書; IT-OT Network; network diagrams
15	CY-IT208 (Updated)	**Protection of exposed assets** Do you have an action plan in place to reinforce security and surveillance on services exposed on the Internet? - Ensure that all assets on the internet are listed and subject to an annual update and monitoring of their level of criticality - Check the deployment on the exposed assets: ° supervision tools and services (e.g.: EDR, CTI, SOC) ° vulnerability scans ° security patches - Verify targeted exposure analyzes and audits on services exposed on the internet. SD - Inventory and declaration to the cyber group of assets exposed on the Internet, patch status per asset and date of last update of the document - Status of the deployment of scanning and detection agents (e.g.: EDR, vulnerability scanning tool) - Proof of audit of exposed services	**Not-applied**: No inventory of assets exposed on the internet is carried out. **Ad-hoc**: A current or complete inventory of assets exposed on the internet is available. Partial deployment on these exposed assets of: - supervision tools and services (e.g.: EDR, CTI, SOC) - vulnerability scans - security patches **Defined**: All assets on the internet are listed with identification of the profession and the associated criticality. Complete deployment on these exposed assets of: - supervision tools and services (e.g.: EDR, CTI, SOC) - vulnerability scans - security patches **Optimized**: All assets on the internet are listed and are subject to an annual update and monitoring of their level of criticality. Complete deployment on these exposed assets of: - supervision tools and services (e.g.: EDR, CTI, SOC) - vulnerability scans - security patches Carrying out targeted exposure analyzes and audits on services exposed on the internet.	3	3	Apollo: 互聯網資產清單 provided; Vulnerability scan report provided; Taho: list of hosts provided

16	**CY-IT209 (Updated)**	**Security by design** Is cybersecurity integrated from the design stage (security by design) and at each key stage of business and technical projects? (expression of needs, definition of architecture, validation before putting into production) Ensure: - to have documented guide(s) or procedure(s) specifying the scope covered, describing how security is included in a project from start to finish - to have defined a methodology for integrating cybersecurity into projects and integrating all IT projects - to share this methodology with all stakeholders (project managers, IT stakeholders, etc.) SD - Proof of cybersecurity participation in key stages of IT projects (process, report, meeting, validation request, validation, etc.) - Methodology for integrating cybersecurity into projects	**Not-applied**: Lack of integration of cybersecurity into projects **Ad-hoc**: Cybersecurity in business and technical projects is partially monitored. **Defined**: The most critical business and technical projects integrate security by design. Security requirements are shared with business stakeholders and MOEs, an action plan is defined and risks are addressed. **Optimized**: Measures from previous levels apply. A methodology for integrating cybersecurity into business and technical projects is defined and integrates all IT projects. This methodology is shared with all stakeholders (project managers, IT stakeholders, etc.). This methodology is based on proven tools (e.g.: market tool, Google template file). Cybersecurity requirements are followed by design in all business and technical projects, followed by an action plan and management of residual cybersecurity risks. This data feeds the roadmap and risk mapping. Best practices are shared with the Group Cybersecurity Department.	2	2	Apollo: not applied; Taho: 資通安全目標達成計畫 provided
17	**CY-IT210 (Updated)**	**Awareness and training** Do you have a cybersecurity awareness and training program and do you carry out cybersecurity awareness actions on a regular basis among employees within your scope? - Ensure that the awareness & training plan is approved by management and aligned with the Group roadmap. - Verify the existence of awareness and training actions (e.g.: communications, events, phishing tests, e-learning, etc.) - Ensure that employee training rates are monitored. - Verify that exercises are carried out in order to check the effectiveness, progress of awareness and training (e.g. fun quiz, phishing test, etc.). SD - Document presenting the awareness and training program - Support, deliverables and/or proof of awareness actions (documents, emails, meetings, etc.) - KPIs of the training rate and awareness of employees	**Not-applied:** Lack of specific awareness or training **Ad-hoc**: Awareness or training actions on an ad hoc basis and without formal intervention (email, etc.). No awareness and training plan defined or approved by management. **Defined**: Cybersecurity awareness and training plan, which is part of the Group cybersecurity plan, defined and shared with management. Communications (e.g.: emails, notes, documents), awareness and training sessions (e.g.: via event or e-learning). Monitoring the training rate of employees over 2 years with the objective of 80% achieved **Optimized**: Measures from previous levels apply. Carrying out exercises to check the effectiveness, progress of awareness and training (e.g.: fun quiz, phishing test, etc.). Sharing best practices with the Group Cybersecurity Department	3	3	Security awareness training as a service delivered from Asia CSEC team
18	**CY-IT211 (Updated)**	**Sever hardening** Are you implementing server and application hardening (including mobile applications)? - Check the implementation of basic hardening rules and rules targeting specific technologies (e.g. hardening of Linux servers, Windows) by design from installation - Control the application of these rules SD - Minimum hardening process - Evidence of hardening for Linux and Windows environments - Tool for checking hardening rules	**Not-applied**: No hardening rules defined and applied. **Ad-hoc**: Basic hardening rules are defined and implemented without specific control. **Defined:** Basic hardening rules and rules targeting specific technologies (e.g. hardening of linux, windows servers) are defined and implemented with control. **Optimized**: Basic hardening rules and rules targeting specific technologies (e.g. hardening of linux, windows servers) are defined and implemented by design upon installation with control. Sharing best practices with the group	2	3	patching requirements defined in 資訊通訊與作業管理說明書; patching performed

19	CY-IT213 (Updated)	**Mobile devices** Is a mobile device security policy in place? Ensure: * To have an active company-owned or BYOD mobile device inventory, if applicable * MDM deployment on mobile devices. * Security policies and configuration are applied to access Veolia resources with mobile applications SD - Mobile device security monitoring document (inventory, dedicated cybersecurity KPIs, etc.) - Sharing security settings configured on mobile devices - Evidence of mobile device management via local or group MDM	**Not-applied**: Lack of MDM for mobile device management **Ad-hoc**: Users are aware of good cybersecurity practices regarding the use of mobile terminals. Mobile device management enforces cybersecurity best practices **Defined**: Management of mobile devices in a local MDM with application of a security policy securing access to Veolia resources **Optimized**: Mobile device management with Group MDM	2	3	Mobile device management with Group MDM
20	CY-IT214 (Updated)	**Data classification and protection** Do you apply the requirements of the Key 19 procedure? Do you have a regularly updated data inventory? - Verify that the requirements of Key 19 are known and that they are applied - Verify the existence of a regularly updated data inventory, where data is labeled according to its criticality - Verify that regular analysis and reporting is carried out - Verify that a DLP solution with a security level adapted to the type of data is implemented within the perimeter SD - Local procedure for classification, labeling, protection and retention of data - Evidence of the application of Key 19 across the entire BU - Inventory of data and their labeling according to their criticality - Proof of regular updating of the data inventory and their labeling according to their criticality - Evidence of regular analyses/reporting - Proof of the implementation of a DLP solution with a level of security adapted to the types of data	**Not-applied**: No local classification, labeling and data protection procedure is in place. No data inventory is carried out **Ad-hoc**: Knowledge and application of Key 19 is partial, a data inventory is in progress or available. The data is only partially classified and labeled **Defined**: Knowledge and application of Key 19 throughout the BU. The Data Inventory is regularly updated. The data is labeled according to its criticality **Optimized**: Measures from previous levels apply. Regular analyses/reporting are carried out. A DLP solution is implemented on the perimeter with a level of security adapted to the types of data.	2	2	data security requirements mentioned in 瑞昶科技資訊技術安全政策
21	CY-IT215 (Updated)	**Data encryption** An encryption policy for data at rest and in transit is defined and applied ? - Ensure the existence of a formalized encryption policy and its systematic application - Ensure that : * all terminals are encrypted * Web application flows are all encrypted * Sensitive databases are encrypted - Verify that encryption assessments and analyses are carried out regularly, resulting in security level reports and action plans SD - Encryption policy - Proof of the application of the encryption solution used on the different perimeters - Encryption status report: terminals, web application flows, remote access, sensitive databases - Reports on security levels and action plans resulting from regular encryption assessments and analyses	**Not-applied**: No encryption policy. Encryption is not applied **Ad-hoc**: An encryption policy is formalized but partially deployed * less than 80% of terminals are encrypted * Only critical web application flows and remote access are encrypted **Defined**: An encryption policy is formalized and globally applied * more than 80% of terminals are encrypted * Web application flows and remote access are all encrypted **Optimized**: An encryption policy is formalized and systematically applied. Regular evaluations and analyzes of encryption are carried out, resulting in reports on the level of security and action plans. * all terminals are encrypted * Web application flows and remote access are all encrypted * Sensitive databases are encrypted	2	3	資訊通訊與作業管理說明書; bitlocker enabled

22	CY-IT301 (Updated)	**Deployment of detection tools and services** Is a Security Operation Center (SOC) in place? Is an Endpoint Detection Response (EDR) solution deployed across the entire perimeter? Ensure: - that a SOC team in charge of supervising IS security is in place - that an incident processing report by the SOC / a monitoring table of incident processing KPIs is in place - that an Endpoint Detection Response (EDR) solution is deployed across the entire perimeter - that the installation of the EDR is effective on the workstations and servers - that an EDR administration console exists SD - Contract with a SOC - Email, document for processing an alert/incident by the SOC - Contact organization chart between the SOC and the BU - Onboarding in the GSOC - List of equipment covered by the EDR - EDR configuration compliance dashboard	**Not-applied**: No local SOC is implemented. Detection tools are not or are rarely deployed **Ad-hoc:** Detection tools are put in place and are subject to regular monitoring by the GSOC or the historic local SOC. A review of use cases is carried out at least once a year. Events and incidents are reported to the Group Cybersecurity Department. EDR is deployed on the most critical technical assets. Deployment across the entire fleet is planned. **Defined**: The Measures from the previous levels apply, Detection tools are set up and configured according to Group recommendations. Regular analyses give rise to action plans. EDR tools are deployed across the entire fleet. **Optimized**: Measures from previous levels apply The SOC is integrated into the Group Federation, a proactive and continuous improvement approach is put in place for the detection and processing of alerts. Best practices are shared with the Group's Cybersecurity department in terms of EDR detection. ***: BUs fully integrated into the GSOC are at least level Defined**	3	3	Asia EDR and SOC utilized
23	CY-IT302 (Updated)	**Audits, tests and vulnerability detection** Do you carry out vulnerability scans regularly (at least every month) and apply the associated patches as part of a patch management process? Ensure to have: - a patching process - proof of regular scans - remediation monitoring SD - Inventory of vulnerability scans carried out on their perimeter, the date of completion, and the results found - Presentation of the remediation actions carried out following these scans - Evidence of remediation follow-up - Formalized patching process - Evidence of patching automation (via tools)	**Not applied**: No vulnerability scans performed. No patching process. **Ad-hoc**: Formalized patching process. Vulnerability scans performed on some of the assets, with patches partially applied. Critical patches partially implemented. **Defined**: Formalized patching process. Vulnerability scans are performed on more than 90% of the assets (100% of critical tests). Critical patches all implemented. **Optimized**: The patching process is formalized and automated using off-the-shelf tools. Vulnerability scans are performed on all assets, with patches applied (patching rate = 100%). All critical patches are implemented. Best practices are shared with the Group Cybersecurity department.	3	3	VM as a service delivered by Asia CSEC and vulnerabilities followed up
24	CY-IT303 (Updated)	Audits, tests and vulnerability detection Do you regularly (at least every 3 years) carry out intrusion tests (application pentest), audits (information system security audit) and/or red teams on a regular basis and carry out the identified remedial actions resulting from this? - Ensure that technical audits have been carried out over the last 3 years, that follow-up and remediation actions have been defined with a completion date. - Ensure that Pentests / red teams exercises have been carried out over the last 3 years, that follow-up and remediation actions have been defined with a completion date. SD - Evidence of the completion of intrusion tests, audits and/or red team with the date of completion (report, summary of results, etc.) - Presentation of the actions carried out following these intrusion tests, audits and/or red team - Evidence of intrusion tests on all the most critical technical assets and the most sensitive projects before going into production - Evidence of completion of a red-team in the last 3 years - Evidence of participation in a bug bounty program	**Not-applied:** No technical audits, no penetration tests **Ad-hoc**: Technical audits, penetration tests on some of the most sensitive projects before going into production. **Defined**: Technical audits, penetration tests on all the most sensitive projects before going into production. The most critical vulnerabilities resulting from the checks are corrected before going into production. **Optimized:** Technical audits, penetration tests on all the most critical technical assets and the most sensitive projects before going into production. A Red-team has been organized over the past 3 years. All vulnerabilities resulting from these checks are corrected before going into production. Participation in a bug bounty program	2	2	audit performed for Apollo and Taho in 2024; no pentest conducted

25	CY-IT304 (Updated)	**Centralization of logs** Are qualified security event logs containing relevant security information (source, date, user and timestamp) implemented on critical systems? Are these qualified security event logs collected in a SIEM and analyzed by the GSOC or a local SOC? - Ensure that the processing of security events is followed, specifying their source, date, user and timestamp - Verify that security event logs are collected and qualified in a SIEM - Verify the generation of security event logs by critical systems - Verify the existence of (a) documented guide(s) or procedure(s) specifying the scope covered (for example: local logging policy) SD - Sample evidence of group policy application (firewalls, servers, AD, etc.) - Sample of security logs generated by critical systems - Evidence of associated Group Policy Objects (GPO) - Log well architecture file (log centralization) - View of event indexing in the SIEM - Verification of contract with SOC or onboarding in GSOC	**Not-applied:** No logging is performed. **Ad-hoc:** Certain events are collected locally on the entity's most critical assets, integrating monitoring of these logs. **Defined**: All events are collected on all the entity's critical assets, centralized and supervised. **Optimized**: Measures from previous levels apply. A supervision action plan is put in place to improve the collection of security events.	2	2	logs are partially retained
26	CY-IT401 (Updated)	**Incident management** Do you apply the group procedure for managing cybersecurity alerts and incidents? Do you have a local cybersecurity incident management procedure? Is this procedure updated and tested at least every 3 years as part of an exercise? - Verify that cybersecurity incident escalation contacts are identified - Check the existence of documented guide(s) or local procedure(s) with defined scope (e.g. local procedures for managing cybersecurity incidents) - Check that the cybersecurity incident management procedure is updated at least every 3 years - List the main cybersecurity incidents recorded over the last 18 months - Check that the processing reports for major cybersecurity incidents (file kept for 18 months) are kept - Check the evidence of exercises and/or tests dedicated to the management and response to cybersecurity incidents carried out. Specify the date of these exercises and/or tests. (report, minutes, summary of results, emails, etc.) SD - Local cybersecurity incident management procedures (Business Continuity Plan - BCP and/or Business Resumption Plan - BRP) with the date of the last update of the document - Evidence of updating the local incident management procedure at least every 3 years - Evidence of carrying out exercises and/or tests dedicated to the management and response to cybersecurity incidents. Specify the date of these exercises and/or tests. (report, minutes, summary of results, emails, etc.) - Evidence of processing of all alerts - Evidence of implementation of a continuous improvement process	**Not-applied**: no incident management procedure **Ad-hoc**: Critical incidents are managed without clear organization **Defined**: All alerts are processed. Alerts concerning areas subject to regulatory requirements (e.g. NISv2 in Europe) are qualified and notified to the authorities within the allotted time frame. Critical alerts and incidents are notified to the Group cybersecurity department and follow the Group procedure. **Optimized**: Measures from previous levels apply. a continuous improvement process is in place (evolution of detection rules based on alerts, new pattern of attacks observed with implementation of new use cases)	3	3	資訊安全事件調查方法 & 資訊安全事件回應流程 in place; incident records provided

27	CY-IT402 (Updated)	**Crisis management** Do you apply the group alert and crisis management procedure adapted to your scope? Is this procedure regularly tested as part of cyber crisis management exercises? Ensure: - that a person is designated for cybersecurity crisis management - that the Group alert and crisis management procedure is known and applied - that the procedure is regularly tested as part of cybersecurity crisis management exercises SD - Local crisis management procedure with the date of the last update of the document - Proof of carrying out exercises and/or tests dedicated to cybersecurity crisis management. Specify the date of these exercises and/or tests. (report, minutes, summary of results, emails, etc.) - Monitoring of the action plan following each exercise	**Not-applied**: Not following the alert and group crisis management procedure. **Ad-hoc:** Adaptation of a local procedural policy when necessary based on the group crisis management procedure, formalized crisis reports, crisis exercises involving the entity's management every 3 years at least, with monitoring of the action plan following each exercise. **Defined**: Adaptation of a local procedure when necessary based on the group crisis management procedure, formalized crisis reports, crisis exercises involving the entity's management every 2 years at least, with monitoring of the action plan following each exercise. **Optimized:** Measures from the previous levels apply. Crisis exercises every year with one or more exercises in order to involve the entire hierarchical chain of the entity: management, operational actors, cybersecurity stakeholders, with monitoring of the action plan following each exercise.	3	3	- 瑞昶科技災害應變計畫; - IT contingency plan-硬體-網路及軟體; - 資通安全事件管理說明書; - contact list
28	CY-IT501 (Updated)	**Backup and Restore** Is there a documented and implemented backup management procedure that takes into account full equipment backup, recovery testing, offline data storage and on-premises or Cloud data retention time? Is this procedure consistent with the Recovery Point Objective (RPO) associated with the activity? Make sure you have: * data backup and recovery plan meeting the need for RPO * Data backup media is encrypted, stored securely and separated from the source system. * recovery exercise execution records and validated regularly. * Data backup retention enforced as per policy. * High availability and/or disaster recovery plan for critical applications/systems respecting the SLA. *Proof of recovery testing. Specify the date of these exercises and/or tests. (report, minutes, summary of results, emails, etc.) SD - Proof of backups stored securely and disconnected from the network - Process and technical means of restoring systems - Proof of carrying out restoration tests. Specify the date of these exercises and/or tests. (report, minutes, summary of results, emails, etc.)	**Not applied:** No backup strategy. **Ad-hoc**: Backup strategy defined but not aligned with the RPO, without covering all perimeters, without frequency. No restoration tests. **Defined**: Backup strategy defined and aligned with the RPO, including the perimeters to be covered and the associated frequency. Restoration tests as part of the campaign on the most critical areas. Protection of backups (e.g. against a ransomware threat). The backups are stored on a site other than hosting production but in the same region and with the same supplier. **Optimized**: Measures from the previous levels apply. Restoration tests as part of campaigns across all areas. Protection of backups (e.g. against a ransomware threat). Backups are stored on a site other than the hosting production, with another supplier.	3	3	Backup procedure defined with backup records provided
29	CY-IT502 (New)	**Business continuity** Does the business continuity plan (BCP) include a plan to manage cyber events? Is an IT business recovery plan (DRP) applied to all activities? Ensure: - to have RTO (Recovery Time Objective), RPO (Recovery Point Objective) by activity and services - to have continuity and recovery documents (BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan)) - that recovery and continuity tests are carried out (with evidence) - that this is carried out on business scopes supported by third parties SD - RTO and RPO for critical activities and services - Proof of disaster recovery plan (DRP) and communication of elements to the Business owner to integrate into the BCP and Business continuity plan (BCP) - Proof of follow-up of the action plan following the tests - Proof of regular frequency tests (< 3 years) with followed action plan.	**Not applied**: No identification of the RTO and RPO of activities and services. No definition of a Business continuity plan (BCP) and a Disaster recovery plan (DRP) adapted to cyber crisis scenarios by the BO, in line with the RTO and RPO. **Ad-hoc**: Identification of the RTO and RPO for some activities and services. Definition and implementation of a Disaster recovery plan (DRP) and Business continuity plan (BCP) adapted to crisis scenarios of cyber origin by the BO, in line with the RTO and RPO but on a partial scope of activities and services. **Defined:** Identification of RTO and RPO for critical activities and services. Definition and implementation of a Disaster recovery plan (DRP) and communication of elements to the Business owner to integrate into the BCP and Business continuity plan (BCP) adapted to cyber crisis scenarios by the BO, in line with the RTO and RPO and taking into account a risk of long disruption. **Optimized**: Measures from the previous levels apply. These elements are tested regularly (< 3 years) with a monitored action plan."		2	IT contingency plan-硬體-網路及軟體 in place

30	**CY-OT101 (Updated)**	**Roles and Responsabilities** At entity level, has a formal OT cybersecurity organization been defined and implemented with the appropriate correspondents across the entity? At sites level, has a local OT correspondent been identified for each site? Ensure: - A local correspondant for cybersecurity exists - The local correspondant participates in exchanges with the entity's cybersecurity team SD - Identification of the local correspondent - Formalization of a job description for the local OT correspondent - Complete Organization Charts (by priority, OT, sites, BU, Zone, IT)	**Not-applied**: No organization is in place at the Business Unit level to identify local contacts at industrial sites. **Ad-hoc**: A member of the BU's cybersecurity team is responsible for industrial cybersecurity. Additionally, a cybersecurity correspondent is identified at critical sites and is tasked with relaying certain industrial cybersecurity issues. **Defined**: Each site has identified a local cybersecurity contact. Critical sites are supported by a business correspondent who is aware of industrial cybersecurity and ensures local liaison and information reporting to the BU reference. **Optimized**: At critical sites, the correspondents monitor the security plan for the sites they oversee and share their best practices with the representative of their entity. Across all sites, the correspondents are trained and ensure communication with the BU.	3	3	Only Taho is assessed for OT. Joy responsible for OT cybersecurity for Taho
31	**CY-OT102 (Updated)**	**Risk Management** Has a risk analysis been conducted, validated by the business, and a budget allocated to deploy the appropriate action plan? - Make sure a risk analysis for the industrial site exists - Check out the OT cybersecurity roadmap, as well as the associated budget Note: A risk analysis should be conducted at the entity level first to define appropriate action plan and budget globally and then site specific risk analysis should be conducted when relevant SD - Risk analysis - Formalization of an OT cybersecurity roadmap with associated costs	**Not-applied**: Cybersecurity is not a project at the BU level: no comprehensive risk analysis is conducted on industrial sites, nor does the BU allocate specific cyber funds, even for ongoing contracts. **Ad-hoc**: A few isolated industrial cybersecurity actions are planned at critical sites, with some human resources allocated. However, these are not linked to a risk analysis. **Defined**: Isolated cybersecurity actions are planned across all sites. A risk analysis is conducted, and a medium-term cyber action plan is defined for critical sites. A global OT cybersecurity budget is allocated at the BU level. The BU is informed of the actions and needs within its scope. **Optimized**: All sites have an action plan based on a risk analysis. Critical sites have a dedicated OT cyber budget, adequate human resources, and regularly monitor their action plan. Moreover, the BU budget covers a minimum level of security across all sites. The BU is involved and consulted.	3	3	- risk evaluation process document; - risk assessment records provided; - budget allocated to deploy the appropriate action plan
	CY-OT201 (Updated)	**Awareness & Training** Is there a dedicated industrial cybersecurity training in place for the OT cybersecurity team and is there an awareness program in place for OT Cybersecurity for plants' staff, visitors and suppliers? - Make sure a awareness raising program exists and aligns with the group's cyber roadmap - Check out the awareness actions and sesssions organised (supports, plannings, lists of people who assisted to a session) SD - OT Awareness material - OT Awareness planning - List of people who have followed the awareness campaign - Sharing of Group documents to sites (entity) - List of people who followed a training (which training and when)	**Not-applied**: No cybersecurity awareness initiatives for industrial cybersecurity are conducted at the BU level. **Ad-hoc**: Local OT correspondents at critical sites are trained in industrial cybersecurity. **Defined**: All OT correspondents are trained in industrial cybersecurity. At critical sites, a portion of the teams are made aware of industrial cybersecurity issues. However, there are still some personnel who need to be made aware. **Optimized**: Across all sites, a comprehensive awareness program is implemented for all individuals accessing the industrial network. Mandatory sessions are regularly held and feedback is incorporated. The BU ensures that best practices are shared within the CSEC network.	2	2	OT cybersecurity awareness training roadmap planned; training records provided
32	**CY-OT103 (Updated)**	**Asset inventory** Are all plant assets tracked in an asset inventory and kept up to date under the responsibility of the CISO with the support of the OT Correspondent? Is there a network diagram for the site? - Verify that there is complete OT documentation available that allows for the identification of equipment, software, critical data, and associated flows, and that it is updated regularly - Ensure that there is an architectural diagram of the entire industrial network, and that it is updated regularly SD - Complete OT asset inventory - OT full cartography (network architecture diagram)	**Not-applied**: No inventory or cartography of the industrial network is formalized at industrial sites. **Ad-hoc:** An inventory of equipment and a partial cartography of the OT (with some mandatory information such as typology, IP address, etc.) are formalized at critical sites. **Defined**: All sites are committed to formalizing an inventory of the industrial network. A complete inventory and network mapping are formalized for critical sites, especially for TICS. **Optimized**: The entire OT is documented for all sites. The equipment inventory and network mapping are regularly updated, and all recommended information is recorded at critical sites.	2	2	asset inventory provided

33	**CY-OT104 (Updated)**	**Sites/contracts inventory** Are all contracts and plants listed with an identification of their criticality based on a self-assessment performed on a regularly basis at the entity level? - Ensure that sites are listed, and that an identification of their criticality is performed regularly at the entity level - Ensure that contracts are listed, and that an identification of their criticality is performed regularly at the entity level SD - List of contracts/sites with their level of criticality	**Not-applied**: The BU does not maintain a list of sites and contracts. **Ad-hoc**: A partial list of contracts and sites has been formalized by the BU. **Defined**: Contracts and sites are fully listed within the BU. **Optimized**: All contracts and sites undergo regular criticality evaluations based on risk analysis conducted by the BU.	2	2	DCS list maintained
34	**CY-OT105 (Updated)**	**Audit & Control** Are there periodic audits and/or self-assessments based on the Fix the Basics including the supplier's managed perimeter? Are results shared to the relevant stakeholders (the Group, clients, etc.)? - Ensure cybersecurity maturity self-assessments including the supplier's managed perimeter are done regularly - Ensure industrial cybersecurity audits are done regularly - Check that results are consolidated and shared with the group Note: An assessment program must be defined at the entity level and implemented at site level SD - Complete self-assessment (site) - Audit report - Consolidation of self-assessment at entity level and communication to the group	**Not-applied**: The BU does not assess the cybersecurity maturity of its sites. **Ad-hoc**: The maturity of critical sites is globally identified based on an initial high-level self-assessment. **Defined**: The maturity of all sites is gobally identified based on an initial high-level self-assessment. All critical sites have been evaluated based on a detailed audit. **Optimized:** The maturity of all sites is evaluated based on a detailed audit. The maturity of critical sites is precisely identified through a third-party evaluation (audit) that is communicated and periodically renewed	2	2	audit performed in 2024, report provided
35	**CY-OT202 (Updated)**	**Security by design** Is OT cybersecurity taken into account from end to end in projects with the involvement of the entity CISO or the local OT correspondent? - Check that cybersecurity is taken into account in projects carried out on the OT - Ensure there is a local/entity cyber follow-up for all projects carried out on the OT Note: projects can be the construction of a new site, the installation of a solution on industrial site, etc. SD - Addition of a cyber clause in all future site/entity projects (new projects and renewals)	**Not-applied**: No industrial cybersecurity manager is involved in the BU's projects. **Ad-hoc**: An industrial cybersecurity manager is consulted on global BU projects and critical site projects that have a cybersecurity dimension. **Defined**: An industrial cybersecurity manager is consulted on projects across all sites. They define cybersecurity requirements and ensure their adherence in critical site projects. **Optimized**: An industrial cybersecurity manager defines cybersecurity requirements and ensures their adherence across all site projects. They are involved in all project phases for critical sites: design, specifications, development, and compliance (FAT/SAT).	2	2	established a guidance document to define the roles & responsibilities of self-assessment operation and remediation actions
36	**CY-OT203 (Updated)**	**Identity and access management** Is there a documented and enforced process for access control, account management and access rights that takes into account the criticality of assets and user authorization ? - Ensure that nominative accounts are used for write access on supervisory applications - Ensure that there are nominative accounts dedicated to administration and remote access - Verify the formalization of a password requirements standard for each type of machine within the industrial scope - Ensure that default, generic, and unused accounts are disabled SD - Accounts inventory - Local procedure for managing accounts and passwords - Extract of password strategy for workstations servers	**Not-applied**: Accounts and passwords are not subject to any specific policy. Default and generic accounts and passwords are predominantly used, and unused accounts remain. **Ad-hoc**: At critical sites, some workstations and servers comply with an account management policy. Basic hygiene principles are respected, at least for administrative tasks: individual accounts, no default passwords, periodic renewal, etc. **Defined**: Across all sites, some workstations and servers comply with an account management policy. At critical sites, all workstations and servers follow an account management policy related to their criticality. Administration account authentication is subject to criteria of length, complexity, and periodic renewal. **Optimized**: Across all sites, all workstations and servers follow an account management policy. At critical sites, all accounts and access are inventoried, reviewed annually, and their authentication complies with the group policy. An entry/exit procedure is applied globally. Exceptions are justified and tracked.	2	2	資訊內部稽核報告-密碼控制 process document in place

37	**CY-OT205 (Updated)**	**Antivirus/EDR** Is there an Antivirus/EDR deployed on the workstations and servers? - Ensure an antivirus/EDR is deployed on all workstations and servers - Make sure there is a process in place for updating the antivirus daily SD - Installation of an antivirus/EDR	**Not-applied**: The sites do not have antivirus/EDR on servers and workstations. **Ad-hoc**: Some of the workstations and servers at critical sites have an antivirus. **Defined**: Across all sites, at least some of the workstations and servers are equipped with antivirus software. All workstations and servers at critical sites have antivirus installed, with antivirus databases regularly updated at least on critical assets at critical sites. **Optimized**: All OT assets at critical sites have antivirus/EDR with daily updates. At all other sites, antivirus databases are regularly updated.	2	2	Security tools like EDR, firewall, antivirus are utilized by Taho.
39	**CY-OT206 (Updated)**	**USB protection** Are USB keys sanitized before being connected to industrial workstations to avoid the introduction of malware within the ICS environment and disabled for non administrative usage? - Have a formalized procedure detailing how USB devices are managed - Make sure USB usage on stations and servers is disabled, and exceptions are justified SD - Procedure for managing USB removable media - Awareness	**Not-applied**: Removable media are not subject to any security constraints or dedicated procedures. **Ad-hoc**: The use of removable media is only regulated on critical machines at critical sites. Their use is justified by business needs and restricted to identified systems and individuals. Few controls are in place. **Defined**: Across all sites, the use of removable media is regulated on critical machines. At critical sites, the use of removable media is regulated across the entire fleet with control tools (docking stations, software solutions). Their use is justified by business needs and restricted to identified systems and individuals. **Optimized**: The use of removable media is regulated across all sites with control tools. At critical sites, their use is strictly regulated and subject to a security procedure: devices are identified and physically protected, subjected to antivirus analysis (e.g., clean/white station), formatting, etc.	1	2	USB usage on stations and servers is disabled for Taho. Missing the process document
40	**CY-OT207 (Updated)**	**System hardening** Is there an asset configuration hardening in place (workstations, servers, network equipements, PLCs)? - Make sure there is a formalized procedure detailing the local hardening procedure for OT workstations and servers, specific to each technology (linux, windows), and used from set up SD - Hardening procedures (workstation, servers, network devices, PLCs) - Hardening follow-up document	**Not-applied**: The software configuration of OT assets is not listed (open ports, types of traffic, etc.), and no hardening measures are implemented. **Ad-hoc**: A few hardening measures are implemented on some OT assets (non-essential services/protocols are disabled) at critical sites. **Defined**: Across all sites, hardening measures are implemented on at least some OT equipment. Key hardening measures are applied to critical industrial assets (supervisory stations, SCADA systems, main OT switches/firewalls) at critical sites. **Optimized**: Across all sites, key hardening measures are implemented on critical industrial assets. At critical sites, hardening measures are applied to all OT assets, including servers, workstations, network devices, PLCs, and other OT devices, and hardening is controlled/monitored.	2	2	system hardening performed by maintanence team mannually during onsite service
41	**CY-OT301 (Updated)**	**Third-party management** Is the OT security correspondent involved during the projects to provide high level Cybersecurity requirements and ensure that Cybersecurity principles will be applied during the development? - Ensure cybersecurity is considered in current and new contracts - Review the SATs carried out to check contractors' compliance Note: Contracts can be managed at the entity level when the same supplier operates at multiple sites SD - Contracts with cyber requirements	**Not-applied**: Cybersecurity clauses are absent from contracts at industrial sites. At the BU level, no process for validating the cybersecurity maturity of partners is in place before any interconnection or contracting. **Ad-hoc**: At critical sites, maintenance and/or integration contracts for critical systems include cybersecurity clauses (including audit clauses). At the BU level, a cybersecurity maturity validation process is carried out before any interconnection or contracting for some critical technical suppliers. **Defined**: Across all sites, maintenance and/or integration contracts for critical systems incorporate cybersecurity clauses (including audit clauses). At critical sites, all maintenance and/or integration contracts include cybersecurity clauses (including audit clauses). At the BU level, a process for validating the cybersecurity maturity of the most critical business and technical suppliers is performed before any interconnection or contracting. **Optimized**: All contracts across all sites incorporate cybersecurity clauses (including audit clauses). The industrial cybersecurity requirements communicated to suppliers and service providers are subject to verification	2	2	- 承攬商安全衛生及環保管理規則附件六 個人資料保護條款; - Web Service 資訊系統防護基準符合程度控管表; - 達和事業團 供應商關係章程保密條款

42	**CY-OT208 (Updated)**	**Network security** Does the network architecture of the industrial site respect the standard established by the group? - Ensure OT is isolated from the IT , and communications are limited to necessary flows - Make sure a DMZ is properly configured - Ensure that OT assets are not exposed on the internet, and that the core of the OT network is segmented SD - Complete OT architecture diagram - Flow matrix(s) - Implementation of a secure architecture	**Not-applied**: The industrial network at the sites is not isolated: uncontrolled connections exist between industrial assets and the outside (IT or the Internet). **Ad-hoc**: At critical sites, there is a dedicated industrial network and its connections to the outside (IT or Internet) are filtered by a firewall, but some uncontrolled connections remain. **Defined**: At least some connections between OT and the outside (IT or Internet) are controlled across all sites. At critical sites, all connections within the industrial network and with the outside (including IT, Internet, and auxiliary connections) are documented and filtered by a firewall, and a DMZ is used for exchanges with the outside of the OT. **Optimized**: Across all sites, all connections within the industrial network and with the outside (including IT, Internet, and auxiliary connections) are documented and filtered by a firewall, and a DMZ is used for exchanges with the outside of the OT. At critical sites, the OT is segmented into subnetworks by equipment typology. Filtering is performed between the different subnetworks.	2	2	firewall sets in the plants and policy defined
43	**CY-OT209 (Updated)**	**Vulnerability and patch management** Is there a patch management process defined, documented and applied at plant level associated with a vulnerability management process to ensure related-risks are managed appropriately? - Verify that there is a local patch management strategy, taking into account the frequency and application timelines for each type of asset - Ensure there is a security watch of available security patches on sensitive assets - Ensure there is a mechanism for detecting vulnerabilities and alerting SD - Local patch management procedure	**Not-applied**: There is no process for tracking OT vulnerabilities at the sites. No recent patches are installed. **Ad-hoc**: A patch management process exists at critical sites, and an OT vulnerability monitoring system identifies critical patches, which are installed on an ad-hoc basis. **Defined**: A patch management process exists across all sites. At critical sites, the patch management process is broken down by type of assets throughout the OT, it specifies the frequency and deadlines for applying the patches. A monitoring of software updates is performed for critical assets. **Optimized**: Across all sites, the patch management process is tailored by equipment typology across all OT. At critical sites, vulnerability monitoring is enhanced by a mechanism for detecting and alerting anomalies and vulnerabilities within OT (e.g., Nozomi industrial probe). A list of missing patches for each site is formalized.	1	2	monthly vulnerability scan performed and vulnerabilities remediated
44	**CY-OT501 (Updated)**	**Backup & Restore** Is there a documented and implemented backup management procedure that takes into account the complete backup of industrial equipment, recovery tests, offline data storage and business data retention? - Have a formalized procedure detailing the back up plan for all systems in OT scope - Make sure there is an offline copy of each back up - Ensure tests are done regularly to verify the integrity of the backups SD - Local backup & restore backup plan - Operational backup & restore procedure	**Not-applied**: No formal backup and restore process for OT is developed. **Ad-hoc**: A backup process covering part of the critical data and systems (SCADA, PLC programs and configurations, etc.) is applied following changes or during maintenance periods at critical sites. **Defined**: A backup process covering part of the critical assets across all industrial sites is implemented following changes or during maintenance periods. The backup process includes all assets at critical sites. Data is backed up and available offline. Unit tests for restoration are performed. **Optimized**: A backup process covering part of the critical assets across all sites. The backup process is as automated as possible and carried out periodically based on the criticality of the assets at critical sites. The restoration process is regularly tested for improvements.	2	2	Backup and resotre procedure in place; backup records provided; lacking restoration tests

45	**CY-OT210 (Updated)**	**Obsolescence Management** Are obsolete assets formally tracked within the asset inventory? Is there an obsolescence remediation plan? - Make sure there is an up to date list of obsolete devices and software, as well as any related vulnerabilites - Make sure there a renewal plan has been shared and approved by management SD -List of "end of support" dates for devices and software (included in the inventory template, but information could be provided with Nozomi or with a dedicated follow-up file) -Obsolescence remediation plan	**Not-defined**: The obsolescence of assets and software is not subject to specific monitoring, and no renewal is planned. **Ad-hoc**: The obsolescence of critical assets and software at critical sites is broadly identified, and ad-hoc replacement measures are considered. **Defined**: The obsolescence of critical assets and software across all industrial sites is broadly identified. The obsolescence of critical assets and software at critical sites is formally inventoried. A renewal program is defined and resources are allocated to it. **Optimized**: A renewal program is defined and resources are allocated across all sites. Measures to limit the obsolescence of all assets and software at critical sites are anticipated and integrated into contracts: system version upgrades, software updates, support, etc.	1	2	evidence about laptop disposal provided. lacking comprehensive managment of obsolete device and software

46	CY-OT302 (Updated)	**Remote Access** Do you have a secure remote access process? - Verify that the remote access connection: *Is located in a DMZ *Encrypts the data flows *Complies with the account management policy (access reviews, principle of least privilege) - Ensure that users with remote access have individualized accounts, use strong authentication, and that their actions are properly tracked SD -List of stakeholders with a need for remote access to the industrial network present in the inventory -Description of the remote access solution	**Not-applied**: Direct remote access to OT is not controlled: non-validated solutions, simple authentication, extended access, and lack of documentation. **Ad-hoc:** Remote access is rationalized in number, users, and scope at critical sites. Accesses are performed with a protocol break (DMZ). Access is targeted and the process is documented. **Defined**: Remote access is targeted and the process is documented across all sites. At critical sites, any remote access solution to the production network is validated and its various uses are justified by a business need (e.g., remote maintenance). Their accesses are traced and require Multi-Factor Authentication. **Optimized**: Across all sites, industrial remote access is conducted via a solution compliant with the Group's Industrial cybersecurity policy. Sessions are logged, and privileged access is validated at critical sites.	2	2	資通系統存取控制管理說明書 5.7 遠端存取之限制 provided
47	CY-OT401 (Updated)	**Detection - Logging & Monitoring** Are event logs with relevant security information (source, date, user and timestamps) implemented on the systems that support them ? Are these logs collected into a SIEM and analyzed by a SOC? - Make sure the information information is logged from the right assets - Ensure an SOC exists and takes into accounts logs from the OT Note: the SOC should be implemented at entity or Group level SD -Enabling logging on industrial assets -Integration of the industrial scope into the SOC	**Not applied**: Logging is not enabled on the industrial environment. **Ad-hoc**: At critical sites, the main events on the industrial environment are collected locally (connections, administrative actions, etc.). **Defined**: Main events in the industrial environment are locally collected across all sites. The complete set of events to be collected locally on the industrial environment is precisely configured at critical sites. Clock synchronization is performed. **Optimized**: Across all sites, all recorded logs are centralized (e.g., Syslog) and analyzed (e.g., by a GSOC or local SOC) with historical data. Incidents reported are analyzed and enriched with feedback from stakeholders (users, administrators, etc.).	2	2	firewall logs are retained

48	**CY-OT402 (Updated)**	**Incident & Crisis Management** Is there an incident management plan, including reporting of incident to local CISO and Group Cybersecurity, and a crisis management plan, including cybersecurity event scenarios, documented? - Make sure an incident management plan is defined and it is relevant - Ensure crisis exercises are done periodically, and the results are taken into account to improve crisis management procedures Note: the process should be defined at the entity level and then shared to industrial sites and adapted locally when necessary SD -Incident management plan -Crisis management procedure -Crisis exercise debrief	**Not-applied:** No formalized cybersecurity incident and crisis management process is in place for OT. No incident reporting is conducted. **Ad-hoc**: At critical sites, an incident management process is formalized for critical OT assets. **Defined**: Across all sites, an incident management process is formalized for critical OT assets. At critical sites, an incident management process is formalized for all OT assets. The incident reporting procedure appropriately involves the CISO of the BU and the Group. A crisis management process is formalized. Alerts concerning areas subject to regulatory requirements (e.g., NISv2 in Europe) are qualified and notified to authorities within the required timeframe. **Optimized**: Across all sites, an incident management process is formalized for all OT assets. The incident and crisis management process is regularly tested and improved at critical sites. The reporting procedure is regularly updated.	2	2	資通安全事件管理說明書 in place including high-level incident and crisis management requirements
49	**CY-OT502 (New)**	**BCP** Is there a BCP (Business Continuity Plan) / DRP (Disaster Recovery Plan) documentation and processes in place that include industrial cybersecurity aspects? - Have a formalized BCP and DRP procedure including industrial cybersecurity - Ensure crisis exercises are done periodically, and the results are taken into account to improve crisis management procedures SD BCP DRP Systems Rebuild Operational Procedure	**Not-applied**: No DRP/BCP is defined for the BU. **Ad-hoc**: At critical sites, a DRP is defined for critical assets. It determines the degraded mode and the reconstruction or recovery procedures. **Defined**: Across all sites, a DRP is defined for critical assets. At critical sites, a BCP is consolidated and applicable to critical OT assets. It details the roles, objectives, escalation steps, detailed operational procedures, etc. **Optimized**: A complete BCP and DRP are consolidated and applicable to OT across all industrial sites. They are regularly tested and improved at critical sites: reconstruction tests, feedback from stakeholders, etc."		2	I-2-43-13資訊業務永續運作管理說明書 and OT 災難演練記錄 provided. Cyber scenario crisis to be further included.