Statement of Applicability.

(version 121 – July 17th 2024 – 00:01AM CET)

CHILI publish

All controls marked by “YES” are implemented.

ISO/IEC 27002:2022 Control	Applicability and justification
5 Organisational controls	
5.1 Policies for information security	YES Policies are a best practice to distribute clear and concise agreements on how information must be handled. Information security objectives and principles to guide the activities relating to information security must be defined. Roles and responsibilities must be defined. Processes for handling deviations and exceptions must be defined. This can be described in policies or components linked to these policies. Business strategy, regulations, legislations contracts and related security objectives, threat environment may change, as can the environment of CHILI publish be changed. This results in the need for policies to be reviewed at planned intervals or at any timeframe. This is best practice and reduces information security events in a fast-evolving world.
5.2 Information security roles and responsibilities	YES Information security is a responsibility for every staff member. But depending on the staff context (handled assets, authorisation levels, training requirements for handling assets, connection with suppliers, customers, used tools, different roles in the organisation, staff handling multiple roles), the responsibilities must be described in an explicit way to make sure: • All related responsibilities are explicitly described • Segregation of responsibilities is implemented where possible This best practice reduces risks on faulty information handling or escalation in case of an event.
5.3 Segregation of duties	YES Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organisation’s asset.
5.4 Management responsibilities	YES To reduce risks in information security handling, management requires all staff to apply the applicable policies and procedures in the organisation.

5.5 Contact with authorities	YES Organisation under attack from the Internet may need authorities to take action against the attack source. Having contact with the authorities are also useful to anticipate and prepare for upcoming changes in laws and regulations which have to be implemented by the organisation, enabling the organisation to prepare for events and act more effective in case an event occurs. Contact with other authorities include utilities, emergency services, electricity suppliers, health and safety, telecommunication providers.
5.6 Contact with special interest groups	YES Control is included to reduce risks by being up to date by acquiring knowledge on best practices, understanding the current completeness of the information security environment, receiving early warnings of alerts, advisories and patches to prevent damage by attacks and exploits of vulnerabilities. Having contacts defined to gain faster specialist and information security advice. Also sharing and exchanging information about new technologies, products threats or vulnerabilities supports CIA of information.
5.7 Threat intelligence	YES • Information related to information security threats are collected and analysed to produce threat intelligence and awareness to create appropriate actions to address them when required.
5.8 Information security in project management	YES • Information security is integrated in the processes executing projects to reduce the risk of information security events during the execution of these projects. • Used information systems must be qualified to protect the information used and handled by those tools, and to reduce risk of information breaches.
5.9 Inventory of information and other associated assets	YES • Inventory of assets help to ensure effective protection of the assets take place and reduces risks on faulty information handling. • It is a good practice to have an accountable person for each asset, so that the assets can be protected and managed.

5.10 Acceptable use of information and other associated assets	YES • It is a good practice to have the acceptable use of each asset made explicit, so that each organisation member knows how to handle the information asset in a secure way. Having acceptable use of assets clear and trained, reduce risk of faulty information handling. • Procedures and related training on handling labelling information is in place to reduce risk of faulty handled information.
5.11 Return of assets	YES It is a good practice to formally manage return of assets where appropriate to reduce risk of abuse of confidentiality, integrity and availability of the involved information.
5.12 Classification of information	YES It is a requirement and good practice to classify information, so it can be labelled and handled the correct way by the staff. When information can be classified clearly, the risk of abusing the information is reduced.
5.13 Labelling of information	YES It is a requirement to label information, so it can be handled the correct way by the staff. When information is labelled, the risk of abusing the information is reduced.
5.14 Information transfer	YES • Since company internal information or more strict classified information is transmitted via communication facilities, the mentioned procedures and controls must be in place, also in the communication between the company and external parties, to reduce the risk of information security breaches. • Since company internal information or more strict classified information is transmitted via electronic messaging, the mentioned procedures and controls must be in place to prevent information security breaches
5.15 Access control	YES • An access control policy must be in place to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to use basis, but make sure the information is available where required. This is a good practice.

	• Access to networks and network services must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice.
5.16 Identity management	YES • User registration and de-registration must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice.
5.17 Authentication information	YES • Allocation of secret authentication information must be controlled since this user specific information is directly linked to the information this user has access to and should be on need-to-know and need-to-use basis. This is a good practice and reduces risks on information security breaches. • Staff signs an agreement, agreeing to the organisation's practices on handling information, to reduce risk of faulty handling of information. • It is a good practice to have a password management system and related policy in place, including the necessary password requirements and login procedure, to reduce risk of unauthorised access to information.
5.18 Access rights	YES • User access provisioning must be managed to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. This is a good practice. • To make sure user access needs to remain on need-to-know and need-to-use basis, and next to the user access management, an extra regular review of access controls reduces the risk of unallowed or blocked information access. This is a good practice and reduces risks on information security breaches. • There is a formal procedure in place to make sure that in case staff leaves, access is revoked. This to reduce risk of leaking information.
5.19 Information security in supplier relationships	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure

	handling of information security must be handled depending on the access to the organisation's assets.
5.20 Addressing information security within supplier agreements	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure handling of information security must be handled depending on the access to the organisation's assets.
5.21 Managing information security in the ICT supply chain	YES To make sure information is handled securely by suppliers, and reduce the risk of information security breaches, agreements with suppliers on secure handling of information security must be handled depending on the access to the organisation's assets.
5.22 Monitoring, review and change management of supplier services	YES • To reduce risk in faulty handling of information by a supplier, suppliers are monitored and regularly reviewed. • When services by suppliers change, the scope of the information accessed by the supplier may change, hence the related risk may change. In that case, also the related risk must be managed.
5.23 Information security for use of cloud services	YES • There is a process for acquisition, use, management and exit from cloud services in accordance with the organisation's information security requirements to specify, control and manage information security for the use of cloud services.
5.24 Information security incident management planning and preparation	YES To handle information security incidents effective and efficient, a formalised procedure, including management responsibilities is in place. This is a good practice.
5.25 Assessment and decision on information security events	YES To have an inclusive effective and efficient response, all information security events are logged, and classified. This is a good practice and helps to prevent other future information security events.
5.26 Response to information security incidents	YES There is a formal procedure in place explaining on how to handle information security events and incidents. This is a good practice and

	enables the organisaztion to learn and prevent other future information security events.
5.27 Learning from information security incidents	YES For continuous improvement purposes, and detect if related information security incidents could occur, post-mortem analysis is done on information security incidents. This reduces the risk of future information security events.
5.28 Collection of evidence	YES Forensic gathering is part of the information security handling process. This reduces the risk of future information security events and enables the organisaztion to take appropriate actions. This is a good practice.
5.29 Information security during disruption	YES • To ensure continuity of information security management during adverse situations, a formallised trained and tested policy is in place. This is a good practice. • To make sure an adverse situation is handled well, and continuous improvement purposes, formal processes are in place to warrant the required level of continuity for information security during such situations. This is a good practice. • To make sure an adverse situation is handled well, a formal information continuity exercise is regularly held, of which the outputs lead to verification, review and evaluation of the existing controls in place, and for continuous improvement purposes. This is a good practice.
5.30 ICT readiness for business continuity	YES • ICT readiness is planned, implemented, maintained and tested to ensure availability of the organisation’s information and other associated assets, as well as the organisation’s operations during disruption.
5.31 Legal, statutory, regulatory and contractual requirements	YES • To remain in line with contractual, legal and regulatory obligations, the company must remain up-to-date and manage the applicable contractual, legal and regulatory obligations. This is a good practice. • Relevant legislation, regulations and contractual obligations related to cryptographic controls must be followed, to reduce risks on not

	following legislations, regulations and contractual obligations and protect information as required. This is an obligation by law.
5.32 Intellectual property rights	YES • To remain in line with contractual, legal and regulatory obligations, and to keep IP as valuable asset in the company, IP rights and usage of proprietary software products are regulated. This is a good practice.
5.33 Protection of records	YES • Records must be protected to be in line with needs and expectations of interested parties of the CHILI publish information security management system. This is a good practice and required for the availability and integrity of the related records.
5.34 Privacy and protection of PII	YES • Relevant legislation and regulations related to PII must be followed, to protect confidentiality, integrity and availability of personal identifiable information. This is an obligation required by law.
5.35 Independent review of information security	YES • To avoid conflict of interests, internal and external audits are executed by parties not having responsibility on building and maintaining the ISMS. To reduce risks in unwanted interpretations and implementations of the standard.
5.36 Compliance with policies, rules and standards for information security	YES • To make sure the scope of the current ISMS keeps being up-to-date with the ever changing context of the world we live in, components of the ISMS must be reviewed regularly to reduce information security risks. • Security demands and hacking technology evolve as well as security policies and standards. The organisation must be regularly reviewed for compliance with these evolutions to reduce risks and events.
5.37 Documented operating procedures	YES • Formally approved standard operating procedures reduce the risk of faulty information handling during operations.
6 People controls	

6.1 Screening	YES • Depending on the role of a staff member, the CIA of the handled information must be handled. To prevent abuse of handling information and reduce risks of hiring not trustworthy staff, a background verification check must be executed on potential new staff members.
6.2 Terms and conditions of employment	YES • To reduce risks in information security, new staff members must formally agree with the CHILI publish Information Management System procedures, responsibilities, use of assets and disciplinary actions in case information is not handled correctly.
6.3 Information security awareness, education and training	YES • To reduce risk in information security handling, all staff receive regular and timely security awareness training.
6.4 Disciplinary process	YES • To further reduce risk in information security handling, communicate and enforce the (a policy) commitment for the staff, so a formal disciplinary process is in place.
6.5 Responsibilities after termination or change of employment	YES • To reduce risks in information security handling, after termination or change of employment, the rule of having access and need to know and need to use basis must be established.
6.6 Confidentiality or non-disclosure agreements	YES • It is good practice, and for the sake of good information security to have this control in place.
6.7 Remote working	YES • Information of stakeholders is handled during remote working. This invokes a possible information security risk. these risks must be handled. To reduce these risks, a mobile device policy, agreed by the staff is in place.
6.8 Information security event reporting	YES • To handle information security incidents effective and efficient, a formalised procedure, including management responsibilities is in

	place. This includes communication through appropriate management. This is a good practice. • All staff is regularly trained to report information security weaknesses to be able to respond effectively and efficiently. This is a good practice.
7 Physical controls	
7.1 Physical security perimeters	YES • The logical and organisational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
7.2 Physical entry	YES • The logical and organisational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters. • It is good practice to make clear agreements on how packages, delivered to the company address, are handled. This to reduce risks of unauthorised access within specific perimeters and related information for unauthorised visitors.
7.3 Securing offices, rooms and facilities	YES • The logical and organisational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
7.4 Physical security monitoring	YES • Premises are monitored according to the information security risks for the specific premises to reduce the risks on unauthorised access to information.
7.5 Protecting against physical and environmental threats	YES

	• It is good practice to assess the external and environmental threats to the locations where information is handled, assess the risk, and manage it.
7.6 Working in secure areas	YES • The logical and organisational split and availability of information might be linked to specific zones inside and outside the company. It is good practice to also have physical different security perimeters, which are linked to the confidentiality of the information located in the specific perimeters.
7.7 Clear desk and clear screen	YES • To prevent unauthorised access to information, users are trained and formally agree upon the clear desk and clear screen policy. This is a good practice and reduces the risk on information breaches.
7.8 Equipment siting and protection	YES • It is good practice to protect the equipment where information is managed on to reduce risks from several threats and opportunities for unauthorised access.
7.9 Security of assets off-premises	YES • In times of remote working it is good practice to have a formally trained policy in place which is formally agreed upon by the staff, this to reduce the risk of leaking information.
7.10 Storage media	YES • A formal procedure is in place on how to handle removable media that might contain information. It is a good practice to train the staff on this and have them formally agree to decrease risk of faulty information handling. • To reduce risk on leaked information, it is a good practice to have a formal procedure in place to dispose of the media • To reduce risk on leaked information, it is a good practice to have a formal procedure in place to dispose of the media • As part of asset management, to control access, and to prevent leaking of information on assets, it is good practice to have this control in place, and the formal agreement of the staff handling the information.

7.11 Supporting utilities	YES • It is good practice to support utilities against power failures and other disruptions to prevent undesired loss of information. CHILI publish has a server room for which this is applicable.
7.12 Cabling security	YES • It is good practice to manage cables carrying data or supporting information services to prevent interception, interference or damage. This is applicable to CHILI publish.
7.13 Equipment maintenance	YES • It is a good practice to have a maintenance policy in place for continuous availability and integrity of information.
7.14 Secure disposal or re-use of equipment	YES • To prevent unauthorised access to information which is on need-to-know and need-to-use basis, a formal policy describes how equipment is either securely disposed or re-used. This is a good practice and reduces risk on faulty information sharing.
8 Technological controls	
8.1 User endpoint devices	YES • Information of stakeholders is handled on mobile devices. This invokes a possible information security risk. This risk must be handled. To reduce these risks, a mobile device policy, agreed by the staff is in place. • To prevent unauthorised access to information, users are trained and agree upon a way of working which ensures unattended equipment has appropriate protection. This is a good practice and reduces the risk on information breaches.
8.2 Privileged access rights	YES • Privileged access must be restricted and controlled to e.g. guarantee confidentiality of information, to manage access to staff on need-to-know and need-to-use basis, but make sure the information is available where required. Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or

	breaches of systems. Managing of privileged access is therefore a good practice.
8.3 Information access restriction	YES • It is a good practice to restrict user-based information access on need-to-know and need-to-use basis.
8.4 Access to source code	YES • CHILI publish develops source code, which is part of the IP of the company, and which must be protected. Hence access to this source code must be restricted. This is a good practice and reduces risk on leaking information.
8.5 Secure authentication	YES • It is a good practice to have secure log-on procedures in place to give users access to information.
8.6 Capacity management	YES • Capacity management ensures availability of information by ensuring sufficient capacity.
8.7 Protection against malware	YES • It is crystal clear that the control of malware reduces risks in confidentiality, availability and integrity of company and customer dat2013 A. One of the best practices is also to give formal security awareness training where this topic is emphasised.
8.8 Management of technical vulnerabilities	YES • To prevent exploits of vulnerabilities that impact information of security, the organisation must remain knowledgeable about actual and future vulnerabilities to handle related information security risks in a timely fashion. • Security demands and hacking technology evolve as well as security policies and standards. Information systems must be regularly reviewed for compliance with these evolutions to reduce risks and events.
8.9 Configuration management	YES • To prevent the risks associated with uncontrolled changes in the configuration of IT components, including security infrastructure, all

	changes to the configuration of the IT infrastructure must be managed following the policies and procedures of the company.
8.10 Information deletion	YES • To specific assets, a deletion period is defined to delete data when no longer required. This asset management handling is reviewed periodically to enforce information deletion when required.
8.11 Data masking	No • All the uses of information in the company processes require the use of unmasked data • The use of production information in non-production contexts such as testing is forbidden by the company security policies
8.12 Data leakage prevention	YES • Identification and classification of information is in place to protect against unauthorised sharing of information • Sensitive data is protected accordingly to reduce risks of leaking of information
8.13 Information backup	YES • Secure back-ups, related procedures and testing these procedure is a way to mitigate risk of data loss in case of an event resulting in data loss on active systems.
8.14 Redundancy of information processing facilities	YES • To ensure availability of information, sufficient redundancy in information facilities must be provided. This reduces the risk of information being unavailable when required.
8.15 Logging	YES • Event logging and review of logs is a means to trace-back anomalies, execute root cause and post-mortem analysis, helping to prevent information security breaches or act on them in case an event occurred. • The integrity of logged events is a condition for the logged events to have value during the trace-back anomalies, execute root cause and post-mortem analysis, disciplinary cases and helping to prevent

	information security breaches or act on them in case an event occurred. • Privileged users might be able to manipulate logs of other information security systems. As preventive action, and for root cause and post-mortem analysis and disciplinary cases, access for system administrators and operators are logged and regularly reviewed.
8.16 Monitoring activities	Yes • Networks, systems, and applications are monitored to prevent information security incidents, early detect ongoing ones, and serve as input for threat assessment.
8.17 Clock synchronisation	YES • The correct setting of computer and system clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. This is a good practice.
8.18 Use of privileged utility programs	YES • In IT environments, it is a good practice to handle access to privileged utility accounts in a restricted and controlled way, to reduce risk of inappropriate information handling.
8.19 Installation of software on operational systems	YES • Faulty risk handling is prevented by having controlled standard operational procedures in place, reducing risks when installing new software. • To reduce risks on information security breaches via software installed by users, rules about the installation of software and related risk handling are in scope of this ISMS.
8.20 Networks security	YES • To protect information sent over networks and prevent information breaches, the networks are managed and controlled to protect the transported information.
8.21 Security of network services	YES • To reduce the risk of non-availability of information where required.

8.22 Segregation of networks	YES • Where appropriate and practically possible, groups of information services, users and information systems are segregated on networks, to reduce limit the impact when a security event takes place.
8.23 Web filtering	YES • To reduce the risk of exposure to malicious content, web filtering for external websites is in place
8.24 Use of cryptography	YES • A policy on the use of cryptographic controls is necessary to maximise the benefits and minimise the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. Cryptographic controls are used in different locations throughout the organisation. Managing these cryptographic controls is a good practice. • The management of cryptographic keys is essential to the effective use of cryptographic techniques and therefore a good practice to have a policy in place.
8.25 Secure development life cycle	YES • To secure information handled by internally developed application, rules for development with attention to information security, are in place. This is a good practice and reduces the risk of developing vulnerable software and systems.
8.26 Application security requirements	YES • Information passing over public networks is protected to reduce risk of interception and abuse of information. • Information passing over public networks is protected to reduce risk of interception and abuse of information.
8.27 Secure system architecture and engineering principles	YES • To secure information handled by internally developed application, and to reduce related information security breaches, rules for development with attention to information security, are in place.
8.28 Secure coding	Yes

	• To prevent security incidents caused by bugs or logical errors in the software developed by the company, secure coding principles are applied and verified.
8.29 Security testing in development and acceptance	YES • To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested, including the security functionality. • To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested.
8.30 Outsourced development	YES • To secure information handled by internally developed application, rules for development with attention to information security, are in place, also for outsourced development. This to reduce the risk on developing vulnerable software and/or systems.
8.31 Separation of development, test and production environments	YES • Segregation of development, testing and operational environments reduces the risk for customers to have a environment in place where information security gaps are present. • Development environments are appropriately protected, protecting company owned and hosted information, reducing the risk on information security breaches.
8.32 Change management	YES • Changes of systems can have impact on the CIA triad of information. A formal process to manage changes reduces risk of a negative impact of changes on information security handling. • To reduce risk of information breach, changes to the systems in the development lifecycle are formally managed. • To reduce risk of information breach, changes to the systems in the development lifecycle are formally tested. • To reduce the possibility of uncontrolled and unknown information security risks.
8.33 Test information	YES • Test data is carefully protected and controlled, to ensure fluent testing of the information security related functionality of the

	product. Test data is also part of the IP, and protection of the test data reduces the risk of loss of this IP.
8.34 Protection of information systems during audit testing	YES • To reduce and avoid impact on operational information systems, audit requirements and activities are planned and agreed upon.

– END OF DOCUMENT --