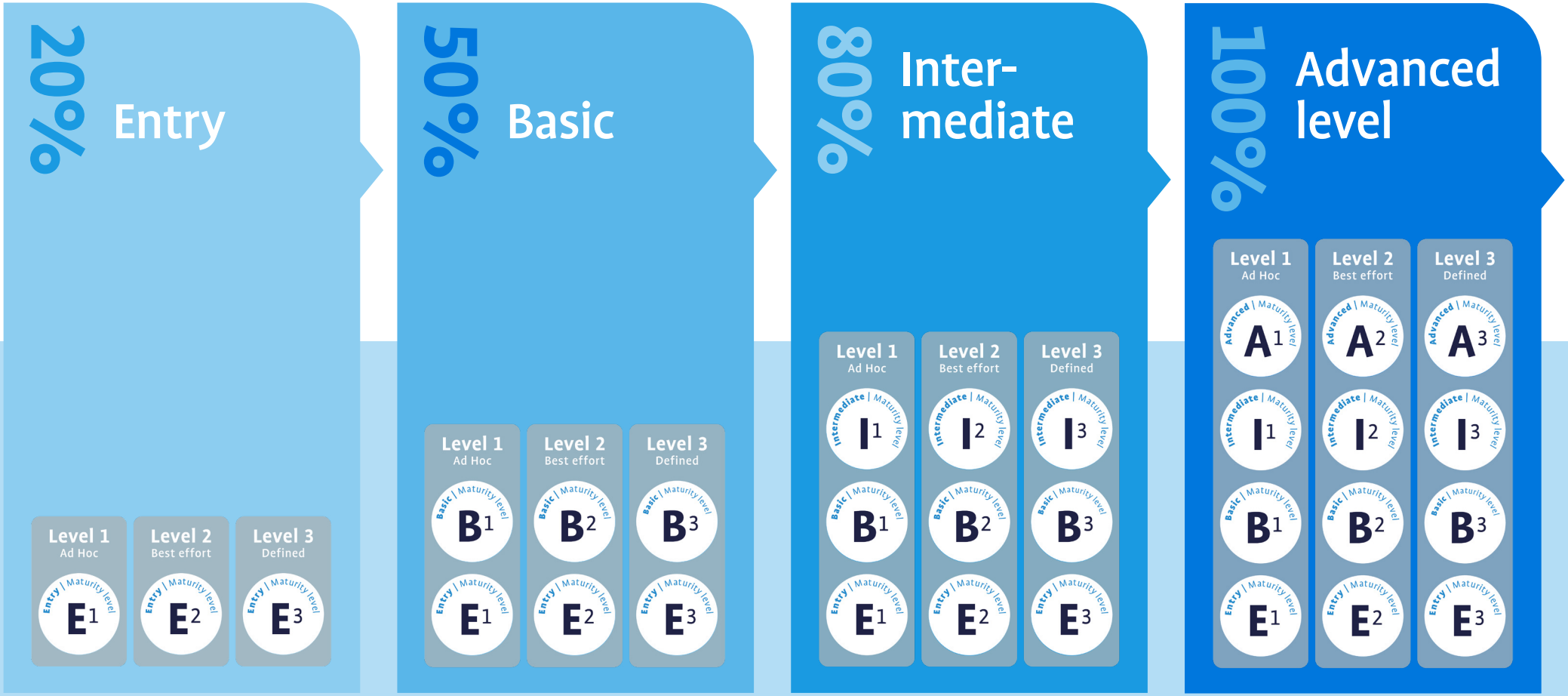
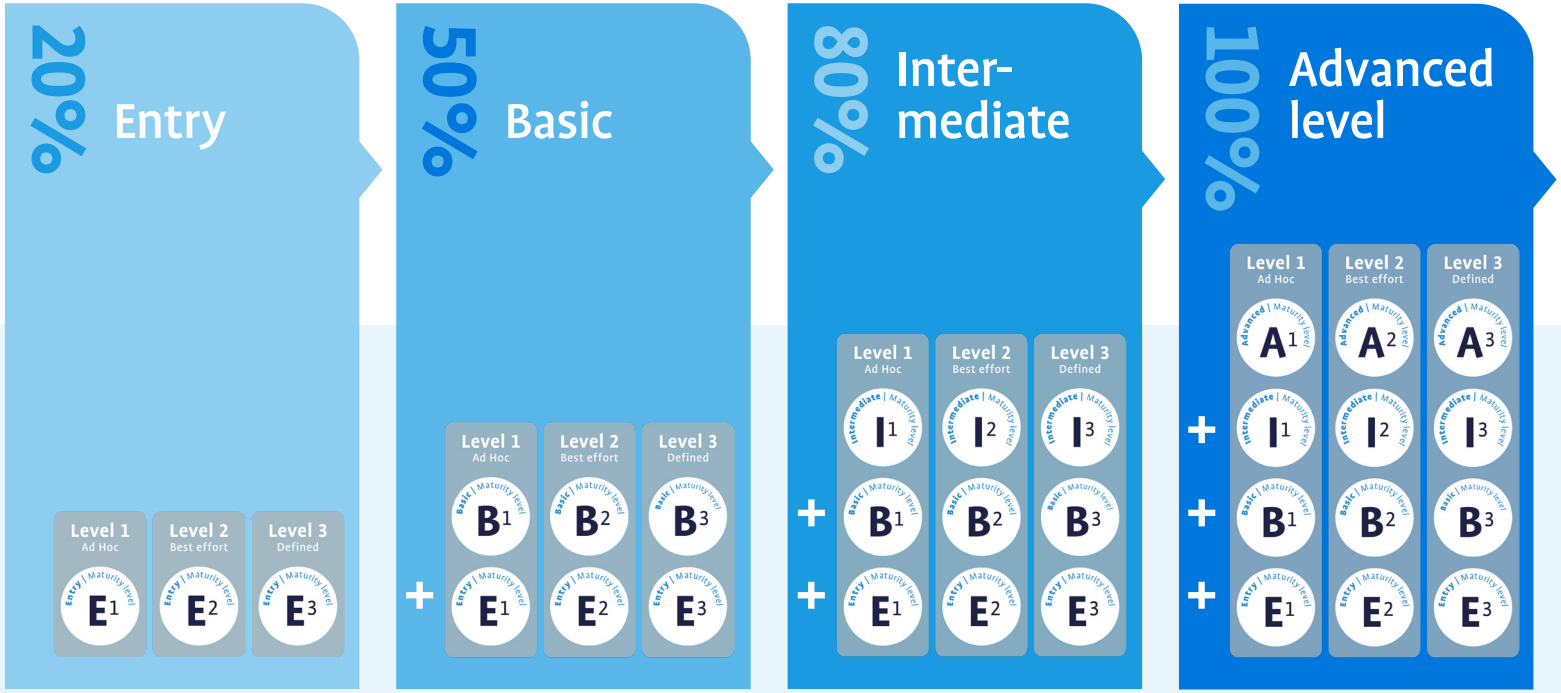
CYRA-Health Care

Based on NEN 7510



CCV centrum voor criminaliteitspreventie en veiligheid

The CYRA method



Explanation of the CYRA Levels

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

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

The structure is as follows:
- **Entry level (20%)**: you only complete the E questions.
- **Basic level (50%)**: you complete both the B and E questions.
- **Intermediate level (80%)**: you complete the I questions, as well as the B and E questions.
- **Advanced level (100%)**: you complete the A questions, plus all questions from the underlying levels (I, B and E).

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

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

CCV centrum voor criminaliteitspreventie en veiligheid

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
1	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.1	Policies for information security and privacy	Does the organisation have up-to-date policies regarding information security and privacy?	Although there are some policy guidelines, actions are primarily based on common practice rather than policy.	The policy has not been formally approved. A high-level policy has been published with objectives and principles. Responsibilities have been assigned and processes for handling deviations and exceptions have been defined. The high-level policy has been further elaborated into subject-specific policy rules that mandate the implementation of control measures for information security and privacy. The purpose and necessity of information security have been described, as well as the rights and obligations of employees within the healthcare organisation. Requirements related to legislation and regulations are included in the policy.	The published overarching policy has been approved by management and communicated to staff and relevant external parties. The policy is periodically reviewed for relevance and whenever a serious incident occurs. The policy is approved by top management at least annually.
2	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.2	Information security roles and responsibilities	Has the organisation defined responsibilities concerning information security and privacy?	Some specific roles are known within the organisation, even though they are not formally established.	Crucial roles and responsibilities regarding information security and privacy have been defined and assigned, including those related to risk management (including the acceptance of residual risks), and the protection of facilities and assets. Responsibility for information security is assigned to a single individual.	All responsibilities for information security and privacy are defined and assigned. It is documented which individuals are appointed for which areas. Responsibilities and authorities are clear at every organisational level. Management visibly directs the protection of health information and thereby patient safety. Management holds responsibility for ensuring appropriate (technical) expertise.
3	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.15	Access control	Is access managed?	Access is granted to company assets, networks, and network services, but this is not based on policies aligned with business and information security/privacy requirements.	Although an authorisation matrix is in use, access policy remains informal. Access to personal health information is restricted to roles that require this information in order to provide care or to support the provision of care.	An access control policy has been established, documented, and assessed based on business and information security/privacy requirements. Users are granted access only to assets, networks, and services for which they are specifically authorised. There must be a policy and a process that enable employees to obtain access to information in emergency situations, even where this would not normally be permitted (breaking the glass). This policy allows the usual access control rules to be temporarily adjusted.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
4	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.16	Identity management	Are user accounts utilised?	User accounts are linked to individuals; shared accounts are managed in a way to prevent unauthorized access.	There are procedures in place describing how accounts are managed. Only authorised individuals have demonstrable access to accounts, whether personal or shared. Access rights to these accounts are periodically and demonstrably reviewed. There is a record of users who have access to personal healthcare information and other confidential information.	Personal user accounts are only active for individuals who require access to the relevant systems or information. Shared accounts are managed to ensure that only authorised individuals have access. All rights are periodically reviewed. When third-party accounts are used, the associated risks are considered in a risk analysis. All of the above is documented in procedures and demonstrably applied. The registration process includes verification of the individual's identity, verification of the individual's qualifications, and the assignment of a unique user identity.
5	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.18	Access rights	Are access rights granted and controlled?	There is no policy for user accounts and related privileges, nor an administrative procedure for users and access groups (roles). Access rights are granted and revoked on an ad-hoc basis, depending on individual persons. Users may have access to more information than the 'need-to-know/have' principle dictates.	There is an informal policy covering all accounts and access rights (internal, external, administrative) under all circumstances (normal, emergency). A procedure for managing accounts and related privileges has been defined but not formalised. Accounts and associated access rights are blocked or revoked when a user resigns or is dismissed.	A formal user access provisioning procedure is implemented to assign or revoke access rights for all types of users and for all systems and services. Asset owners regularly review user access rights. The access rights of all employees and external users are removed upon termination of their employment, contract, or agreement, and adjusted upon changes.
6	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.22	Monitoring, review and change management of supplier services	Is supplier service delivery managed?	Monitoring and evaluation of services occur on an ad-hoc basis or reactively when incidents/conflicts arise.	Monitoring and assessment of service delivery takes place in a structured and periodic manner. There is a focus on improvement and reassessment of risks.	The services provided by suppliers are regularly monitored, reviewed, and audited. Changes in supplier services, including enforcement and improvement of existing policies, procedures, and security controls, are managed, taking into account the importance of business information, involved systems and processes, and reassessment of risks.
7	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.29	Information security during disruption	Is the organisation prepared to manage the availability, integrity, and confidentiality of information during incidents?	Some adverse situations (crises/ disasters) are recognized but not formalized in processes, procedures, or control measures. The organisation acts reactively in such cases and relies on specific individuals.	Information security requirements have been established and translated into processes, procedures, and control measures, of which at least the highest-impact scenarios are periodically tested or demonstrably effective.	Requirements for information security and for the continuity of information security management in adverse situations are established. Processes, procedures, and controls are established, documented, implemented, and maintained to ensure the required continuity level. Implemented controls are regularly verified to ensure they remain sound and effective during adverse situations.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
8	**Organisational**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	5.38	Analysis and specification of information security requirements	Are information security requirements included in the requirements for new information systems or improvements to existing information systems?	Information security requirements are determined and requested on an ad hoc basis for new information systems.	Information security requirements are defined in advance and are included in the requirements for new information systems.	Information security requirements are also taken into account when making improvements to existing information systems.
9	**Staff**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	6.1	Screening	Are personnel backgrounds verified prior to employment?	This occurs on an ad-hoc basis.	A recruitment process for (IT) personnel has been established and implemented, incorporating business requirements. Background verification may take place, but this is not formalized. Screening is performed. A Certificate of Conduct (VOG) is available and, where applicable, BIG registration is verified.	Background verification of all candidates for employment is conducted in accordance with relevant legislation and ethical considerations, and is proportionate to business requirements, the classification of the information being accessed, and the identified risks. Verification of VOG and BIG registration is repeated periodically.
10	**Staff**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	6.3	Information security awareness, education and training	Is staff knowledge maintained and updated?	Training and education occur on an ad-hoc basis. There is little to no personal certification.	There are processes in place concerning certification, training, and education for staff, and personal development plans are maintained.	All employees of the organisation and, where relevant, contractors receive appropriate awareness education and training, as well as regular updates on the organisation's policies and procedures, insofar as these are relevant to their role.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
11	**Staff**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	6.7	Remote working	Is information accessed via remote working secured?	The organisation has provided an environment that supports remote work. Agreements have been made regarding the use of resources for this purpose and the conditions under which this option may be utilised.	The organisation supports remote working and has provided an environment for this purpose. Outside of this environment, no other remote working methods are used. A remote working procedure exists, which outlines at minimum (as far as legislation allows): • What users should consider when working remotely. • Which digital environment is to be used. • The risks of working in public spaces. • Protections against malware and the use of firewalls, etc. • The responsibility for the secure storage of organisational assets.	The organisation supports remote working and has provided an environment for this purpose. Apart from this environment, no other methods for remote working are allowed. There is a remote working procedure in which the following points are documented (as far as legislation allows): • Requirements for the physical environment used for remote work. • What the user must consider when working remotely. • Requirements for the connection used. • Which digital environment is used. • Risks associated with, for example, family members gaining access to business information. • Risks of working in public spaces. • Protections against malware and use of firewalls, etc. • The vulnerability of single-factor access where this is used. • Responsibility for secure storage of organisational resources. • Which document classification may be used. • Availability of training for secure remote working.
12	**Staff**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	6.8	Information security event reporting	Are information security events reported?	Incidents are handled pragmatically. Within the organisation, it is widely known whom employees can contact in the event of an information security incident. In line with the GDPR, healthcare recipients are informed about incidents relating to their personal health information that may have adverse consequences.	A formal incident management process is in place, which includes prioritisation and escalation paths, with roles and responsibilities clearly defined. All staff are made aware that they must report incidents as soon as possible and are familiar with the procedure and the appropriate point of contact.	Information security events are reported as quickly as possible through the appropriate management levels. Employees and contractors using the organisation's information systems and services are required to record and report any observed or suspected information security weaknesses.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
13	**Physical**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	7.1	Physical security perimeter	Are physical security zones implemented?	Physical security measures have been scarcely implemented, and there are no formal policies. The organisation is unable to quickly detect theft or attacks on buildings and company assets. It relies on the alertness and skills of individual persons.	Zones have been created based on the security requirements of the assets located within them. Barriers and boundaries are based on a risk assessment and are physically adequate. Although coverage may not be complete and compliance is not always monitored, control measures are in place, such as physical access control to locations/buildings, fire doors equipped with alarms, and detection systems on external doors and windows. The zoning plan specifically takes into account care-related risks, such as predictable or irrational behaviour related to the healthcare organisation or treatment.	Security zones are defined and used to protect areas containing sensitive or critical information and information processing facilities.
14	**Technological**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.5	Secure authentication	Is it verified that users accessing information systems are who they claim to be?	For various systems, users log in with a password. However, there is no formal policy that defines the relationship between the value of the information and the login method. Shared accounts may also be used. At least two-factor authentication is in place for systems that process personal health information.	A policy is in place for identifying users, for example through the use of two-factor or multi-factor authentication (via authenticator apps, biometric data, or tokens). When authentication means (logins, keys, tokens) are issued, identity verification takes place, possibly including managerial confirmation.	Policies ensure that user actions and access can always be traced to individuals. Controls guarantee that sensitive information is never visible until identity is confirmed, which forms the basis for authorization. Monitoring is in place to detect and/or block (un)successful login attempts (including brute force attacks). The interception of logons (sniffers, cameras, keyloggers) is prevented. Inactive sessions are terminated.
15	**Technological**	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.7	Protection against malware	Is the organisation protected against malware?	Ad-hoc virus scanners may be set up, but there is no policy governing installation, maintenance, and control. End users are not familiar with procedures when malware is detected or how to actively prevent malware installation. Patch management is ad hoc (often based on default settings). Vulnerable/older versions of operating systems may have direct contact with the internet. Data carriers may be freely used/connected by (end) users.	There is a policy in place for the selection, installation and maintenance of antivirus software, patch management, and the prevention of malware installation. Policies and staff awareness are not always demonstrably present. The effectiveness of the implemented measures is not always verified, in part due to reliance on the chosen suppliers and/or products. Patch management may not be fully watertight. All externally provided data carriers are scanned and approved before they may be used. The functionality of medical devices must not be disrupted by security software. Where the use of security software is not possible, risk-based control measures must be implemented.	There is control over malware protection. Installation and updates of virus scanners and patches are centrally managed. Users are informed on how to prevent malware installation and report incidents in time. Monitoring/scanning of internet and external network access (web pages, email attachments, downloads/FTP uploads) is performed. Infected systems can be isolated in time. The effectiveness of measures is regularly evaluated.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
16	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.8	Management of technical vulnerabilities	Are technical vulnerabilities prevented?	Vulnerabilities are identified on an ad-hoc or intuitive basis, and there are no defined procedures to identify them in a structured way. The measures taken are not demonstrably effective. During software development, the existence or emergence of new vulnerabilities is not systematically considered.	A procedure is in place to establish as complete an overview as possible of vulnerabilities, based on a full inventory of information systems and identified threats. A policy has been formulated regarding the handling and prevention of new vulnerabilities.	Roles and responsibilities are defined for identifying, updating, and handling vulnerabilities. Vulnerabilities are actively monitored (e.g., by scanning or penetration testing) especially when software or infrastructure changes. Vulnerability reporting and evaluation of mitigation effectiveness are in place. Vulnerabilities that cannot be remediated immediately through patching are mitigated on a risk-based basis.
17	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.15	Logging	Are log files utilised?	Log files are not actively used. When logs are generated, this usually happens unconsciously ('default settings'), and they are rarely or never actively reviewed.	There is a policy defining which activities must be logged. Access to log files is restricted to (system) administrators. Access to personal data is recorded where possible.	Log files are purposefully generated and protected. Regular reviews are carried out to detect and report deviations from normal use/functioning. Log files are considered potential evidence, with administrator access and file integrity being controlled. Technical or organisational measures prevent or compensate for manipulation. It is recorded who accessed which personal data and what modifications, if any, were made. A procedure is in place to ensure that personal data in log files is erased or anonymised as specified in the retention schedule.
18	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.20	Network controls	Is information on the network managed?	The organisation uses network components (routers, firewalls, switches, Wi-Fi routers) without having formulated policies on how they should grant access to the network. Settings are not, or only minimally, used to actively protect the network against misuse (default settings). Protocols (DHCP) may be configured in such a way that access can be easily obtained to any system.	There is structured documentation available describing the network architecture. Based on this and relevant policies, it is determined how different systems and network components are allowed to communicate. For example, VPN and/or IP whitelisting is used.	Policies/documentation are available on how network components and infrastructure should be configured. Firewall settings and VPN connections are actively managed, updated, logged, and monitored. Systems are hardened to be as resilient as possible. Active monitoring for unauthorised access (Intrusion Detection) may take place.
19	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.21	Security of network services	Is the security of network services established?	The organisation uses network services (e.g., internet connections, VoIP) without a clear understanding of the service content or security requirements. Network usage by (external) users is not monitored.	There is a policy concerning supplier access to the network and the use of VPN connections. Security aspects were taken into account when selecting a network services provider, but these are not demonstrably documented or enforced.	The organisation has service contracts with network service providers that define the security aspects applicable to a specific service. Examples include reporting, incident notifications, audit rights, and access logs. Monitoring takes place on VPN connections (internal and external). Redundancy may be in place for critical network services.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
20	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.24	Use of cryptography	Is encryption (cryptography) applied?	The organisation uses ad-hoc encryption (e.g., of hard drives of PCs and laptops and HTTPS) based on default settings or vendor-configured options. There is no targeted policy.	A policy is in place regarding the use of cryptographic applications. For information systems, the required level of protection has been defined. However, the policy may only cover the most obvious applications.	The organisation has a complete overview of encryption use and actively manages encryption keys. Encryption is applied to information at rest and in transit. In an international context, the organisation has also identified relevant laws and regulations beyond the national level.
21	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.25	Secure development lifecycle	Is security by design applied in software development?	There is no demonstrable policy regarding the approach to information security in the development lifecycle of information systems. The organisation relies on the professionalism of developers, architects, etc., for whom this is self-evident.	The organisation has demonstrably implemented measures concerning: • Security of the development environment • Security within the development methodology • Coding guidelines and conventions • Version control • Knowledge and capability to avoid, detect, and remedy vulnerabilities	The organisation has demonstrably established rules for the secure development of software and systems within the organisation, which include the elements from level 2, and applies them to outsourcing as well.
22	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.26	Application security requirements	Is information security considered in the procurement/ development of (new) applications?	In the development and/or procurement of new applications, the focus is primarily on functional requirements, user-friendliness, and costs. Information security is of secondary importance.	When developing or procuring new applications, information security requirements are considered and included among the requirements. However, the focus is primarily on the more obvious aspects such as login, roles and rights, and availability. Supplier selection does take into account aspects such as certifications, but not necessarily known or potential vulnerabilities in the technologies used. Meeting information security requirements may have economic implications, but partial non-compliance is not a knock-out criterion.	Before acquiring or developing applications, requirements are determined, usually based on a (comprehensive) risk analysis, to establish security requirements. Requirements include: • Applicable legal and/or contractual requirements, e.g., regarding logging • Processing of personal data • Processing of payment data • Level of authentication and trust • Classification of information in the (new) application • Need for separation of roles and rights • Protection of the confidentiality of information at rest and in transit • Use of encryption • Secure connections • Resistance to external attacks (SQL injection, etc.), especially when applications are accessible via the internet Failure to meet information security requirements results in a negative implementation recommendation

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
23	Technological	**Entry** *Answer the questions from:* • *Entry*	NEN 7510	8.32	Change management	Are changes to information processing facilities and systems controlled?	Changes are implemented when practical. Potential problems are considered, but they are generally resolved ad hoc when they occur.	Some form of planning and inventory takes place prior to implementing significant changes. Authorisation is often obtained, but not all potential consequences are fully assessed, nor is communication with all stakeholders always ensured, resulting in potentially inadequate safeguards. Not all significant changes are necessarily tested or formally accepted prior to implementation. Patient safety is taken into account when identifying and assessing all potential consequences.	Procedures are established for software installation (8.19), as well as for other major changes (e.g., technical access security or network infrastructure). These procedures include: a. action plan, b. dependencies and impact, c. approval, d. communication, e. fallback, f. documentation, and g. proof of testing and acceptance prior to implementation. Changes relating to the processing of personal health information are explicitly included in the risk assessment.
24	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.7	Threat intelligence	Are information security threats assessed?	Potential information security threats are taken into consideration.	Potential threats to the organisation's information security are monitored and lessons are learned from them. Specifically for the healthcare sector, threats related to healthcare-specific equipment, including medical devices, are monitored and lessons are learned from them.	Potential threats to the organisation's information security are monitored. These threats are gathered and analysed to reduce the likelihood of such incidents or to minimise their potential impact. This process takes into account the types of attacks, attacker profiles, as well as the methods, tools, and indicators that may be used to detect an attack.
25	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.9	Inventory of information and other associated assets	Are information-related organisational assets recorded?	Some assets are included in an inventory that is kept up to date on an ad hoc basis.	Identified assets are assigned owners, and the inventory is kept up to date. Assets on which personal health information is stored are included in an overview that is kept up to date.	All assets relevant to the information lifecycle are identified and maintained in an inventory, with an owner assigned to each (category of) asset(s). The inventory is systematically kept up to date. All digital information flows relating to health information (both within and between organisations) and their interfaces (including integration platforms) are included in the inventory and assigned appropriate owners.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
26	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.12	Classification of information	Does the organisation employ a classification mechanism?	Information and the assets in which it is stored or otherwise processed are (partially) classified. A classification scheme with uniquely named levels is used for this purpose.	Information and the assets in which it is stored or otherwise processed are classified and provided with corresponding controls per classification level. Asset owners are responsible for the classification. The classification scheme includes rules for classification and criteria for re-evaluation. Classification is incorporated into organisational procedures and aligns with access security requirements. Personal health information is classified as at least confidential in all cases.	Information is classified with regard to legal requirements, value, importance, and sensitivity to unauthorized disclosure or modification.
27	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.19	Information security in supplier relationships	Are information security requirements applied to suppliers with access to organisational assets?	Information security requirements do not arise proactively from risk prevention or reduction but are addressed reactively or on an ad hoc basis following incidents.	Controls are mandatory specifically for suppliers with access to organisational information, such as the categorisation of supplier types, a standardised supplier relationship management process, standard requirements, and/or compliance monitoring. The rights of healthcare recipients are protected, even when a third party with potential access to personal healthcare information is located in a different country (jurisdiction; for example, outside the EU) than the country (jurisdiction) to which the healthcare recipient or healthcare organisation belongs.	Information security requirements to reduce supplier-related risks are agreed upon and documented.
28	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.20	Addressing information security within supplier agreements	Are information security requirements included in agreements with suppliers who access the IT infrastructure or process or manage data on behalf of the organisation?	Information security requirements may be included in supplier agreements, but this is not done structurally and usually only consists of general clauses on confidentiality and/or data breaches.	Agreements have been drawn up with suppliers including obligations to comply with information security requirements, covering aspects such as classification, legal requirements, access, and/or procedures.	All relevant information security requirements are defined and agreed upon with each supplier that (a) has access to IT infrastructure for the organisation's information, or (b) processes, stores, communicates, or provides the organisation's information.
29	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.21	Managing information security in the ICT supply chain	Does the organisation include security requirements in supplier agreements concerning the supply chain?	Does the organisation include security requirements in supplier agreements concerning the supply chain?	Supplier agreements address topics such as requirements for the acquisition of products or services and the transfer of information security requirements in cases of further subcontracting.	Supplier agreements include requirements addressing the information security risks associated with the supply chain of ICT services and products.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
30	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.23	Information security for use of cloud services	Are cloud services utilised?	Information security is taken into consideration when using cloud services.	It is clear how information security is managed when using cloud services. Selection criteria are applied and exit strategies are known. The scope of the service, management of the environment, involved roles/ responsibilities, and incident handling procedures have been agreed with suppliers.	Processes are established for acquiring, using, managing, and terminating cloud services in accordance with the organisation's information security requirements.
31	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.27	Learning from information security incidents	Are lessons learned from information security incidents?	Such incidents are documented, and lessons are learned at the individual level.	Such incidents are recorded, the cause is investigated, and appropriate measures are taken where necessary to prevent recurrence or to reduce potential impact. Trends in the (types of) incidents are reviewed periodically.	There is a procedure for recording information security incidents and handling them. Lessons learned from incidents are used to: • Provide appropriate scenarios for the contingency plan. • Assess the risk of such incidents. • Raise user awareness.
32	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.34	Privacy and protection of personally identifiable information	Does the organisation comply with privacy legislation?	A privacy policy has been established and staff have received one or more privacy training sessions. The organisation strongly relies on the professional conduct of its employees.	Policy has been developed and implemented for privacy and the protection of personal data. Demonstrable knowledge of privacy exists within the organisation. Appropriate technical and organisational measures have been taken to safeguard personal data.	Privacy and personal data protection policies have been developed and implemented. These have been communicated to data subjects. A governance structure is in place, and a privacy officer has been appointed. Appropriate technical and organisational measures have been taken to protect personal data.
33	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.37	Documented operating procedures	Does the organisation ensure operational procedures for information processing and communication facilities?	There are one or more locations where relevant operational procedures can be found. These are placed at one's own discretion and are not systematically controlled.	Operational procedures are managed and published, including installation/ configuration instructions, start-up/ recovery procedures, and guidelines.	Operating procedures are documented and made available to all users who need them.
34	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.39	Uniquely identifying healthcare recipients	Can every healthcare recipient be uniquely identified within the system?	There is a policy ensuring that every healthcare recipient uniquely registered within the information processing system can be identified.	There are processes for identifying healthcare recipients. Information systems support the unique registration of healthcare recipients. This includes merging duplicate or multiple registrations when they exist for the same healthcare recipient.	Processes for the unique identification and registration of healthcare recipients are carried out within the organisation.
35	Organisational	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	5.41	Publicly available health information	Is there a policy regarding publicly available health information?	The organisation has a policy for publishing publicly available health information.	A policy is in place for the entire lifecycle of publicly available health information. This includes protecting and retaining the information.	Publicly available health information is protected, retained, and managed throughout its entire lifecycle.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
36	Staff	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	6.2	Terms and conditions of employment	Are responsibilities for information security/ privacy included in employment contracts?	Employment terms have been agreed upon. Responsibilities regarding information security and privacy may be included, but this is not always the case.	Employment conditions have been agreed with employees, including responsibilities for information security and privacy. This is not done, or not done systematically, for contractors.	The contractual agreement with employees and contractors specifies their responsibilities for information security and privacy, as well as those of the organisation. Ensuring the confidentiality of personal health information is explicitly stated.
37	Staff	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	6.6	Confidentiality or non-disclosure agreements	Are confidentiality/ non-disclosure agreements used?	Confidentiality or non-disclosure agreements are applied on an ad hoc basis and generally cover the protection of confidential information and personal data.	Confidentiality or non-disclosure agreements are aligned with the organisation's information security and privacy requirements, and include elements such as required actions upon termination, ownership of information, and/or agreements on notifications and return. Ensuring the confidentiality of personal health information is explicitly stated in confidentiality or non-disclosure agreements.	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for protecting information and personal data have been established, are regularly reviewed, and documented.
38	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.2	Physical entry controls	Is physical access to secure areas restricted to authorised personnel?	No procedures have been established for registering physical access. Any additional measures to protect physical IT assets are either absent or briefly defined.	Informal procedures are in place to grant, restrict, and revoke access to specific areas within buildings. Observable elements include, for example, visitor registration/ supervision, visible identification, and additional restrictions for areas where confidential information is processed. The organisation has established guidelines for the use of information displays. The placement of large information boards, such as waiting room information or room layouts, is carefully considered. Displays are not directly visible to visitors and patients, while still meeting the functional requirements of healthcare professionals.	Secure areas are protected with appropriate access control to ensure that only authorized personnel have access. Access points like loading and unloading bays or other potential entry points are controlled and, where possible, shielded from information-processing facilities to prevent unauthorized access.
39	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.3	Securing offices, rooms and facilities	Are office spaces and other facilities within the location secured?	Not all areas are accessible to everyone. Access is restricted by locks and/or limitations imposed by (supervising) personnel. Common sense is primarily relied upon.	Policies are in place and demonstrable physical security measures have been implemented that do not rely on (accompanying) personnel. Confidential information and activities are not visible or audible from outside. Address/telephone directories indicating locations where confidential information is processed are not accessible to unauthorised individuals.	There is a formal policy regarding the security of (office) spaces and facilities, incorporating level 2 measures. From the outside, there are minimal indications of information-processing activities (where applicable).

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
40	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.4	Physical security monitoring	Is there monitoring for unauthorised physical access to the organisation?	Some security measures have been taken to protect the organisation's physical location(s) against unauthorised access. There is no structural supervision or monitoring of physical access.	A security system is in place to protect the physical location(s) against unauthorised access. Some form of supervision or monitoring of physical access has been implemented.	A security system is in place to protect physical locations against unauthorized access. Locations housing critical systems are equipped with continuous video surveillance and detection systems. Measures are periodically reviewed.
41	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.5	Protecting against physical and environmental threats	Is physical protection provided against external threats?	There is some pragmatic protection against natural disasters, malicious attacks, and/or accidents, including fire protection, based on individual judgement.	Specialist advice has been sought for protective measures to avoid damage from fire, flooding, earthquakes, explosions, civil unrest, and other forms of natural or man-made disasters.	Physical protection against natural disasters, malicious attacks, or accidents is designed and applied based on specialist advice.
42	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.6	Working in secure areas	Is working in secure areas controlled?	Working in secured areas relies on common sense and the professionalism of the individuals involved.	Some non-formalised rules are in place for working in secured areas.	Procedures have been developed and applied for working in secure areas. Personnel are only informed on a need-to-know basis; vacant rooms are locked; recording devices are prohibited; and unsupervised work in secure areas is avoided.
43	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.7	Clear desk and clear screen	Is a Clear Desk and Clear Screen policy implemented?	Staff are expected to lock their system when leaving their workstation.	A clear desk policy for paper documents and removable storage media, and a clear screen policy for information processing facilities, has been established. Level 1 practices are incorporated within this. A policy is in place for time-outs and automatic log-off based on inactivity, including documented exceptions. Exceptions are made for specific healthcare environments, such as operating theatres or intensive care units, where time-outs or automatic log-off could introduce safety risks.	A 'clear desk' policy for paper documents and removable media and a 'clear screen' policy for information-processing facilities are established. Level 2 practices are included. Time-outs and automatic log-off are configured in line with policy, taking into account the requirements of specific areas such as operating theatres and intensive care units.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
44	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.8	Equipment siting and protection	Is equipment physically protected and shielded?	Equipment has been placed to the best of one's knowledge and ability, without explicitly considering external threats or the risk of unauthorised access/viewing.	There is a culture in which some of these practices are applied: securing storage facilities against unauthorised access; positioning of information processing facilities (such as monitors) to prevent unauthorised viewing; implementation of controls that reduce the risks of physical threats and external threats (theft, fire, smoke, dust, water, etc.); and established guidelines for eating, drinking, and smoking near facilities.	Equipment is positioned and protected to reduce risks from external threats and hazards, as well as to minimize the chance of unauthorized access. Level 2 practices are part of this. When positioning equipment, due consideration is also given to data integrity and the safety of healthcare recipients and staff. This includes, for example, radiation shielding, climate control, aggressive behaviour, and emergency provisions.
45	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.9	Security of assets off-premises	Are organisational assets secured when off-site?	Employees are expected to handle company assets with care when using them off-site, and the organisation relies on this expectation.	There is a culture in which certain practices are followed: not leaving equipment unattended, adhering to manufacturer instructions, and following defined controls for remote and temporary work locations. A policy is in place for the use of medical equipment by (healthcare) staff and healthcare recipients off the organisation's premises.	Assets located off-site are secured, taking into account the various risks of working off the organisation's premises. Level 2 practices are included. Where medical equipment is used by (healthcare) staff and healthcare recipients off the organisation's premises, such use is authorised.
46	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.12	Cabling security	Are information processing cables protected?	Power and telecommunications cables have been professionally installed, but their protection is handled on an ad hoc basis. Measures are mainly taken after something has gone wrong.	There is no formal policy, but cables are routed underground or otherwise protected, and power cables are separated from communication cables. Other measures are implemented pragmatically. Measures to prevent unauthorised use of network wall outlets (network ports) are applied pragmatically.	Power and telecommunications cables transmitting data or supporting information services are protected against interception, disruption, or damage. For sensitive/critical systems, level 2 measures are supplemented with, for example, enclosed cable ducts/rooms, secured switch panels/cable rooms, and technical cleaning and checks for unauthorized devices. There is a policy for network wall outlets (network ports) in publicly accessible areas, and measures are in place to prevent and/or detect unauthorised use. To prevent physical damage, specific healthcare recipients, such as children and confused persons, must be taken into account.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
47	Physical	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	7.14	Secure disposal or re-use of equipment	Are storage media disposed of or reused securely?	There are no formal procedures for data deletion. Data is removed on an ad hoc basis.	Informal procedures are in place to ensure that equipment is checked for storage media prior to disposal or reuse. Responsibilities for data removal are partially defined. Medical equipment is also checked for storage media.	All equipment components containing storage media are verified to ensure that sensitive data and licensed software are removed or securely overwritten prior to disposal or reuse. Additionally, media containing confidential or copyrighted information are physically destroyed or the data is technologically destroyed so it cannot be recovered.
48	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.1	User endpoint devices	Is user equipment (laptop, PC, tablet, smartphone) functioning as part of the workplace protected?	There is no formal policy outlining what users may or may not do when using (mobile) information systems. System registration is handled on an ad hoc basis, and employees may use personal devices for work purposes without any governing policy.	Responsibilities regarding systems used by end-users are documented and, in principle, known by the end-users. There is no need for active monitoring. The organisation has policies and a methodology in place that determine which systems have access to its information. However, there is no structured (remote) management of these systems. This also applies to (portable) medical devices used by (healthcare) staff and healthcare recipients.	Users are aware of procedures and requirements when using information systems, including shutting down when not in use and conduct in public spaces. Where applicable, there is controlled policy for BYOD (Bring Your Own Device). The status of systems (e.g., regarding patches and encryption) is recorded, and software installation on workstations is managed by the organisation. There is technical and organisational control over all end-user equipment.
49	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.2	Privileged access rights	Is the allocation and use of special access rights (system administrators, super users, etc.) restricted?	Although not precisely inventoried, there are certain roles with special privileges. The staff involved are aware of their responsibilities and are trusted.	The organisation knows exactly which special access rights are used. These are limited to necessity, in line with the access policy. Special access rights are only granted after the authorization procedure has been followed. Where possible, these are personal accounts with no more rights than necessary to perform the tasks.	In addition to level 2: Users have the minimum rights needed to perform their tasks. Users are aware of the rights they are currently working with. There is a process for granting and revoking rights. This process is recorded. Main accounts (e.g., root) are extra secured, and measures are taken to limit their use as much as possible. Personal accounts are used, and where not possible, shared accounts can be traced back to a user. Competencies of users with special access rights are regularly assessed.
50	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.3	Information access restriction	Is access to information and system functions of applications restricted?	Access is pragmatically restricted in the absence of a formal access control policy. Access is granted on an ad hoc or individual basis, potentially even to third parties (suppliers).	Access is restricted in accordance with an informal and/or incomplete access control policy. Policy components, such as an authorization matrix, are applied but not formally used. There is no guarantee that more access is granted than necessary to fulfill a role or function.	Access management is in place, where access is restricted/controlled according to formal and current access policies, related to functions/ roles and the value of information. Access is based on 'no access, unless...'. Where necessary, read, write, and execute rights are distinguished.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
51	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.10	Information deletion	Is information deleted when there is no longer a need to retain it?	Information that is no longer needed is deleted on an ad hoc basis. There is no structured approach in line with formal policy, nor are there supporting tools in place.	Periodically, information that is no longer needed is cleaned up. No tools are available to support this. Retention periods for key information sets have been mapped out.	Information that is no longer needed is systematically deleted in line with the organisation's established policy. Retention periods have been identified and are (where possible) applied automatically. When deleting, agreements with clients, logging as evidence, and old versions or temporary files are considered. If a supplier is used for deletion, evidence is recorded, and the supplier's authority is documented.
52	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.12	Data leakage prevention	Are measures in place within the organisation to prevent information security breaches?	Some measures have been taken within the organisation to reduce the likelihood of breaches. These rely heavily on the awareness and vigilance of employees.	Within the organisation, measures have been taken to reduce the likelihood of breaches. This has been achieved by securing systems and raising user awareness of their personal responsibility to work securely.	Measures have been taken within the organisation to reduce the risk of breaches. This is done by securing systems and raising user awareness of their responsibility to work safely. Agreements have been made in the form of a policy. Information within the organisation is classified. Common communication channels are monitored for possible breaches. Common methods that may cause breaches are blocked, such as copying database data into Excel.
53	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.13	Information backup	Is information backed up within the organisation?	A backup policy is in place within the organisation. Periodic testing is part of this policy. Back-ups of personal health information are encrypted.	The organisation has a backup policy that addresses the following: • What is included in the backup • How a backup can be restored • How the storage location of the backup is ensured to be secure and reliable, with minimum requirements matching the actual storage location • A test schedule which is demonstrably executed and covers the requirements of a recovery action in an emergency.	The organisation has a backup policy that covers: • What is included in the backup • How a backup can be restored • How the backup storage location is ensured to be safe and reliable, meeting at least the same requirements as the original storage location • A test schedule demonstrably performed covering a recovery action in an emergency • Applying encryption to the backup in line with the classification of the information types concerned • Ensuring a backup is not triggered when unintentional data loss occurs. When using cloud services, it must be determined to what extent the supplier's facilities meet the organisation's requirements according to the applicable information classification.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
54	Technological	**Basic** *Answer the questions from:* • *Entry* • *Basic*	NEN 7510	8.19	Installation of software on operational systems	Is software installed in a controlled manner on systems that are essential to operational processes?	Software is installed, whether by a supplier or otherwise, in a manner and at a time deemed appropriate. No thorough analysis is carried out regarding the potential consequences for processes dependent on the system.	There is a documented process for the installation of software on operational systems, designed to minimize disruptions to operational processes. Depending on the situation, this process is followed to varying degrees. Consideration is given to medically certified systems. Where changes cannot be made, mitigating measures are implemented. Identified vulnerabilities and the associated mitigating measures are documented.	There are well-defined processes and procedures for installing software on operational systems. This is done only • in accordance with organisational requirements and policies • after authorisation from the system owner or management • by qualified personnel • after successful testing • with a rollback strategy in case of failed installation • by keeping a log of updates and changes • with maintaining the ability to process still-relevant historical data. Where possible, hardening of (operational) systems is performed.
55	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.3	Segregation of duties	Are duties within the organisation segregated?	The organisation does use roles and aims to follow the principle of least privilege, but there is no formal segregation of conflicting duties and responsibilities. Tasks that pose risks of errors or fraud can be performed by the same individuals without oversight.	There is awareness of the importance of segregation of duties, and roles are designed to separate conflicting tasks as much as possible. However, this is not yet consistently applied and is not systematically monitored. Where it is not possible to separate conflicting functions and responsibilities, additional measures are defined.	Segregation of duties has been formally implemented: conflicting tasks and responsibilities are separated across different individuals. An automated process monitors changes in tasks and responsibilities to prevent conflicts of interest. Particular attention is given to the segregation of duties and responsibilities in situations where roles change regularly.
56	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.4	Management responsibilities	Is there an information security policy within the organisation?	This policy is accessible to all employees and is demonstrably adhered to.	This policy describes the organisation's guidelines for information security, including a whistleblower procedure. This policy is demonstrably adhered to.	Management ensures and demonstrates that staff: • Have access to information security guidelines, understand their responsibilities in this regard, and have the necessary rights, resources, and time to fulfil them. • Have access to a whistleblower procedure allowing anonymous (or safely disclosed) reporting of information policy violations that may harm the organisation.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
57	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.8	Information security in project management	Is information security addressed in projects, and are security requirements considered in the procurement/ modification of systems?	Information security is addressed in some projects. Security requirements are considered on an ad hoc basis. In some cases, risk assessments are conducted as part of the project plan. Much depends on individual competencies. In projects where personal health information plays a role, information security is addressed.	In all projects, information security implications are addressed and assessed. Risk assessments are conducted at an early stage of the project as part of the risk management process, where risks are identified. Concrete requirements (logging, etc.) and risks are determined based on general criteria and are not always fully aligned with business objectives. In addition to information security, safety and privacy are also an integral part of project management.	Information security objectives are incorporated into project objectives, and information security is integrated into all phases of projects. Information security requirements reflect the value of the information and the potential business impact, are documented, and reviewed by stakeholders. Product acceptance criteria are applied, and a formal testing and acquisition procedure is used when procuring new products. Agreed security requirements are included in contracts with suppliers.
58	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.10	Acceptable use of information and other associated assets	Does the organisation manage acceptable use of information and organisational assets?	General instructions have been given to staff on the proper use of information (assets). These are also included in an awareness programme.	There are concrete rules for acceptable use. Procedures for handling business assets have been developed and implemented.	Acceptable use rules have been identified, documented, and implemented. Procedures for handling company assets have been developed and implemented in accordance with the information classification scheme established by the organisation.
59	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.11	Return of assets	Is there a fixed process within the organisation for role changes or employee departures?	There is a process in place to ensure that assets issued to employees are retrieved when they are no longer entitled to them due to a role change or termination.	A process is in place to ensure that issued resources are retrieved from employees who are no longer entitled to them due to a change or termination of their position. A record of the retrieval is kept.	A process is in place within the organisation to ensure that the following items are demonstrably returned upon role change or termination of employment: • End-point devices (laptops, smartphones, etc.) • Storage media (USB sticks, hard drives, etc.) • Specialised equipment • Authentication hardware (smartcards, etc.) • Physical documents Records are maintained for both issuance and return, indicating mutual agreement between issuer and recipient.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
60	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.13	Labelling of information	Is information within the organisation labelled?	Information within the organisation is occasionally labelled.	A procedure exists that outlines the classifications used within the organisation, and information is labeled accordingly. Users of health information systems must be aware when the data to which they gain access contains personal health information.	Information within the organisation is labelled, and it is clearly described: • When exceptions are made. • How the label is applied and what it signifies. • How to handle situations where labelling is not possible due to technical limitations. Procedures describe how to manage the classification of information, such as secret, confidential, public, etc. All relevant parties must be familiar with these procedures.
61	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.17	Authentication information	Does the organisation implement a password policy?	There is a password policy in place within the organisation that outlines: • The minimum required password complexity. • The user's responsibility regarding passwords.	Within the organisation, there is a password policy that specifies: • The minimum complexity of a password. • The responsibility of users regarding passwords. • Passwords are unique. Alternative authentication technologies are considered for situations where using passwords is impractical due to the time pressure experienced when delivering healthcare.	The organisation has a password policy that includes the following: • Minimum password complexity. • Use and description of strong passwords (to prevent use of easily guessed passwords). • User responsibilities within the process. • Use of unique passwords. • Passwords are securely stored in an agreed location. • For traditional systems (without hardware key or MFA), passwords must be changed at fixed intervals.
62	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.24	Information security incident management planning and preparation	Are management responsibilities and procedures established to respond adequately to information security incidents?	No formal procedures have been established, but everyone knows whom to contact in the event of an incident.	There are various procedures in place for incident response, monitoring, and reporting. A contact point within the organisation and competent personnel are involved. Definitions are established and standard forms are used.	In addition to level 2: Appropriate contacts are maintained with authorities, interest groups, and forums. Procedures for forensic evidence handling are in place. Disciplinary procedures are referenced, and feedback is provided to the incident reporter.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
63	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.25	Assessment and decision on information security events	Are incidents within the organisation recorded?	Incidents are recorded within the organisation, and information security incidents are specifically identified as such.	Incidents are recorded within the organisation, and information security incidents are marked as such. Each incident is assigned a priority, and solution times associated with these priorities are defined. Incident registration is detailed enough to clarify cause and effect, as well as what has been done to resolve the issue. A distinction is made between incidents involving personal health information and those that do not.	Incidents are recorded within the organisation, with information security incidents specifically identified. Each incident is assigned a priority, and associated resolution times are defined. A designated person is responsible for information security incidents, who evaluates, classifies, and monitors their progress. These incidents are documented in detail, including root cause analysis, progress, and resolution, for future learning.
64	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.26	Response to information security incidents	Are incidents within the organisation addressed?	Information security incidents are handled and resolved within the organisation.	Information security incidents are handled and resolved within the organisation such that there is always: • A root cause analysis. • A clear description of the incident's impact. • What has been done to resolve the incident. • What the structural solution is.	Information security incidents are handled within the organisation, covering the following points: • What is the impact of the incident on the organisation? • Which systems were affected and what was the impact? • What evidence is available and where is it securely stored? • Is crisis management required and has escalation taken place as per agreed procedures? • Does the documentation provide a clear picture of the actions taken? • Stakeholders are provided with necessary information on a need-to-know basis. • The incident is formally closed and archived once resolved. • Depending on the type of incident, forensic investigation may be carried out. • Each incident includes a root cause analysis and a resolution. If a trend or overarching risk is identified, it is documented and addressed as per organisational procedures.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
65	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.31	Identification of legal, statutory, regulatory and contractual requirements	Are contractual information security requirements and relevant legal/regulatory requirements considered?	It is known which parties (legislation, clients, insurers, etc.) impose information security requirements on the organisation.	It is clear which parties (e.g. legislation, clients, insurers) impose information security requirements on the organisation, and an approach has been established to comply with them.	The organisation complies with information security requirements imposed by legislation and contractual obligations. The following elements are included in the relevant procedures: • Control measures for information security are developed and modified with these requirements in mind. • These requirements are also considered when classifying information and assets, conducting risk analyses, and assigning roles and access rights. • Cryptographic controls and tools are applied in compliance with legal and contractual requirements.
66	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.32	Intellectual property rights	Is intellectual property respected by the organisation?	The organisation only works with legal software and information. Self-developed products (e.g., by software developers) are accompanied by a licensing agreement.	The organisation only works with legal software and information. Monitoring is conducted to ensure correct usage (no more installations than allowed, no illegal software) and it can be demonstrated that the organisation is the rightful owner. In-house developed products (e.g. software developers) are provided with a license agreement.	The organisation ensures that licensing agreements and intellectual property matters comply with applicable requirements. Items developed and offered by the organisation itself are also covered by such agreements. The following aspects are in place: • Procedures exist for managing rights related to software and information products. • Software may only be obtained from trusted sources approved by the organisation. • The organisation has a policy on intellectual property. • Ownership can be demonstrated. • Monitoring of licensing agreements regarding maximum use (e.g. CPU, user count) is in place. • Software installations on systems are monitored. • Licensing usage is controlled. • Procedures exist for retiring or transferring licences. • Copying is not permitted unless otherwise stated in the agreement.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
67	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.33	Protection of records	Does the organisation maintain records as evidence of compliance?	The organisation has insight into its data flows and has secured logging in compliance with legislation, contractual agreements, and its own policies.	A processing register exists within the organisation, which identifies the different types of information. Agreements have been made regarding the use and retention period of this information.	A processing register exists within the organisation that identifies the various types of information handled. For each type, agreements are in place and demonstrably adhered to concerning storage and management. Storage and handling are in accordance with the recommendations of relevant vendors. For long-term storage, provisions are made to ensure data can still be accessed in the future, especially for media that may become obsolete. Guidelines exist for each media type concerning: • The type of storage. • How it should be handled. • How it should be destroyed. • The required retention period.
68	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.36	Compliance with policies and standards for information security	Does management assess compliance with information processing and procedures based on its own policies, standards, and security requirements?	Compliance with internal policies, standards, and requirements occurs on an ad hoc basis and/or when prompted by specific events.	Compliance with the organisation's policies, standards, and requirements takes place periodically, for which a monitoring and reporting instrument is used.	The organisation audits compliance with its information security policies. Measures are in place to ensure that all requirements of internal policies, legislation, and other stakeholders are met. In case of deviations, the following information is recorded: • What the deviation is. • The cause of the deviation. • The necessity for corrective action. • Implementation of corrective action. • Effectiveness testing and identification of any residual risks. • The time frame for handling all the above.
69	**Organisational**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.40	Validation of displayed/printed data	Are all displayed or printed data provided with information that allows identification of the healthcare recipient to whom these data apply?	Before healthcare professionals use personal health information from an information system, they verify that this information relates to the correct healthcare recipient.	Printed health information includes data that identify the healthcare recipient.	Displayed or printed health information includes data that identify the healthcare recipient.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
70	Organisational	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	5.43	External reporting of information security incidents	Are information security incidents externally reported where applicable?	Information security incidents are reported externally on an ad hoc basis.	A policy has been established for the external reporting of information security incidents. This policy includes at least: • Roles and responsibilities • An overview of authorities • Reporting methods • Reporting criteria • Process description	The policy for external reporting is demonstrably applied, and management is informed when external reports are made.
71	Staff	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	6.5	Responsibilities after termination or change of employment	Does the organisation consider the impact on information security following a role change or employee departure?	The organisation takes information security-related roles and responsibilities into account when making changes to staffing.	The organisation considers roles and responsibilities in information security when changes occur in the workforce. Employees are aware that upon termination they must adhere to the information security policy, including confidentiality obligations. When roles change within the organisation, access rights for the former role are removed. Only the access rights required for the new role are granted.	As part of job change and offboarding procedures, employees are reminded that they remain bound by the information security policy even after leaving the organisation. Information security-related roles are maintained, ensuring continuity even during staff changes.
72	Staff	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	6.9	Management training	Are training sessions specifically provided for management in the field of information security?	Management is informed on an ad hoc basis about their tasks and responsibilities in the field of information security.	Training objectives for management are specified in advance. Management has received at least one training session. The training primarily focuses on risk management and awareness.	A training programme for management is in place. Training sessions are formally documented and maintained.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
73	**Physical**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	7.10	Storage media	Is unauthorised disclosure, modification, deletion, or destruction of information stored on media prevented?	Measures have been taken within the organisation to ensure the security of company information or access to information processing activities on physical storage media.	There are procedures in place within the organisation to secure business information or information processing processes on physical storage media. There is a procedure in place that defines how to handle removable media; the following requirements must be met: • Those involved know that this procedure must be used. • The information on the medium or the media itself must be encrypted in a way appropriate to the classification of the information. • If retention periods are relevant, they must be taken into account. • If loss of information on the medium poses a risk, multiple copies must exist. Personal health information must be encrypted. Guidelines are in place for internal storage within equipment, such as printers.	Procedures are in place within the organisation to secure business information or information-processing activities on physical storage media. There is a procedure detailing how to handle removable media, including: • Stakeholders know this procedure must be used. • All media must be stored according to the classification of the information on the medium. • Information on the medium or the medium itself must be encrypted appropriately to the classification. • Retention periods must be considered if applicable. • If the loss of information on the medium poses a risk, multiple copies must exist. • Hardware ports (USB, card readers, etc.) are only available for organisational reasons. • If there is a reason to store information on removable media, this must be included in an audit trail. Equipment is screened and cleared prior to maintenance and at the end of its lifecycle in accordance with procedures.
74	**Physical**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	7.11	Supporting utilities	Are utilities protected against disruptions?	Utilities (electricity, tele-communications, water supply, gas, sewage, ventilation, and air conditioning) are professionally installed. Any disruptions are handled on an ad hoc basis.	To protect equipment from disruption of utilities, the installation (where necessary and applicable) meets the manufacturer's technical description and legal requirements, is periodically assessed for capacity, inspected, and tested, and is equipped with detection and/or multiple power supplies. Emergency power supplies are in place to continue providing power to essential medical or ICT equipment and devices in the event of a power failure. Measures have also been taken to manage the quality (voltage and frequency) of the power supply. A continuity plan for power supply is in place, in which the required power capacity is also assessed.	Equipment is protected against power failures and other disruptions caused by utility disturbances, including the measures from level 2, at least supplemented with emergency lighting, communication means, and emergency switches/buttons to shut down utilities such as power, water, and gas. Emergency power supplies are periodically tested.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
75	Physical	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	7.13	Equipment maintenance	Is equipment maintained to ensure the availability, integrity, and confidentiality of information?	There is no defined process for maintenance. Changes are made without a formal strategy or overall plan and without explicit attention to availability, integrity, or confidentiality. Maintenance is carried out based on incidents and/or short-term needs.	An informal maintenance process has been implemented that is not aligned with business requirements or strategy. Maintenance is carried out by authorised maintenance personnel in accordance with supplier-recommended guidelines and intervals for service visits, as well as any maintenance requirements in insurance policies. Attention is given to availability and integrity, but confidentiality is not systematically ensured. When maintaining equipment that is part of healthcare processes, patient safety is taken into account. This also includes consideration of the consequences of not performing maintenance.	Equipment is properly maintained to ensure its continuous availability, integrity, and confidentiality. To this end, there is a clearly defined and generally understood maintenance process, where aspects from level 2 are supplemented with the recording of suspected and actual faults, commissioning after inspection, and appropriate measures for data confidentiality. A risk assessment is in place for equipment that forms part of the healthcare process. Measures are in place to ensure that no unexpected issues arise that could affect systems and equipment dependent on the equipment being maintained. Additional attention is required when maintenance is performed remotely or by a third party.
76	Technological	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.6	Capacity management	Is the capacity of resources within the organisation monitored?	The capacity of (some) information processing systems is monitored, and mechanisms are in place to detect (impending) overages. The organisation is reactive and has been able to manage this (so far).	There are policies for capacity management, which also define (future) capacity requirements. These take into account how business-critical systems are and the type of resources involved.	There is a formal policy in place for managing resource capacity, covering: information processing systems, human capacity, office space, and other potentially disruptive facilities. Provisions include: hiring extra staff, expanding or purchasing new space, acquiring more powerful systems, freeing storage, removing data beyond retention periods, decommissioning redundant applications and systems, and optimising automated processes and queries.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
77	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.14	Redundancy of information processing facilities	Are measures in place within the organisation to maintain the desired level of service availability?	The organisation has considered the requirements from legislation and contractual agreements with clients regarding the availability of the organisation's services. Measures have been taken to comply with these requirements.	Within the organisation, it is clear which legal requirements and contractual agreements must be met regarding availability. Measures taken are in line with these requirements. A procedure exists to document this. For critical processes, contracts are in place with two or more suppliers, such as internet providers. Processes and systems are configured to use redundant solutions, suitable for the required availability.	The organisation is aware of the legal and contractual availability requirements it must meet. Measures in place are appropriate for these requirements. The relevant procedure includes: • Contracts with two or more suppliers for critical processes (e.g. ISPs) • Use of redundant networks • Use of two mirrored data centres at separate locations • Use of redundant power supplies and circuits • Use of parallel software processing supported by a load balancer • Redundant hardware Failover events (e.g. failures triggering redundant systems) occur automatically and are logged.
78	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.16	Monitoring activities	Is anomalous behaviour in networks, systems, and applications monitored?	Networks, systems, and applications are checked on an ad hoc basis for abnormal behaviour.	Networks, systems and applications are monitored for abnormal behaviour and appropriate measures are taken to assess potential information security incidents. Monitoring is performed in real-time or at regular intervals.	Networks, systems, and applications are monitored for abnormal behaviour, and appropriate measures are taken to assess potential information security incidents.
79	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.17	Clock synchronization	Is clock synchronisation considered on systems processing information?	The assumption is that systems are synchronised to the same time as professionals have installed and configured them. The organisation is not certain, but this has (so far) not led to problems.	The organisation is aware of which systems process information and clock synchronisation is active on these systems. It can be demonstrated which clock is being used as reference.	The organisation has identified which systems process information, and time synchronisation is active on these systems. If multiple time synchronisation services are used (e.g. cloud services), differences between them are monitored.
80	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.22	Segregation in networks	Are information processing systems separated from each other?	Measures have been taken to separate information processing systems in such a way that unnecessary connections do not exist. Examples include network segmentation and separating such systems from the internet by using a firewall.	Information-processing systems that do not need to be interconnected are separated from each other and from the outside world. Network segmentation is applied where possible.	Information processing systems that do not need to be connected are separated from each other and from external networks. Where possible, network segmentation is applied. Wireless networks do not directly connect to these systems. Access is separated and, where necessary, an additional security layer is used to establish contact.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
81	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.29	Security testing in development and acceptance	Is security testing conducted during or after the development process?	Security testing is part of the development process and/or delivery. Clinical users should be involved in testing clinically relevant system functions.	As part of the development and lifecycle process, security testing is carried out. The organisation has guidelines covering: • Security requirements the application must meet • Frequency of re-evaluation during operational use • Methods of testing during and after development, both on code and environment • When code reviews or a four-eyes principle apply • When code goes live	Security testing is part of the development and lifecycle process. Organisational guidelines include: • Security features such as authentication and cryptography • Secure coding practices • Security configurations, including the environment and peripheral measures like firewalls A test plan is executed before software goes live, covering: • Activities involved in testing • Input used and expected output • Criteria for result evaluation • Decision-making in specific scenarios For internally developed software, an independent person outside the development team must: • Conduct a code review to verify compliance and detect anomalies • Perform vulnerability scans to assess system security • Execute a penetration test for insecure code and design flaws
82	**Technological**	**Intermediate** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate*	NEN 7510	8.30	Outsourced development	Are software development activities outsourced?	Software development activities are outsourced, and agreements have been made with the supplier regarding ownership and work tasks.	Software development activities are outsourced. Agreements with the supplier include: • Licence agreement / ownership • Security requirements of the supplier's development environment • Security and privacy by design • The organisation remains responsible for compliance with laws and regulations	Software development tasks are outsourced. Agreements with the supplier cover: • Licensing/ownership • Security and privacy by design, secure coding, and testing requirements • Application risk analysis • Final testing by the organisation before going live • Evidence that the supplier's delivery meets organisational standards • Escrow agreement to secure software in case of supplier issues • Right to audit • Supplier development environment security requirements • The organisation remains responsible for legal and regulatory compliance

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
83	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.5	Contact with authorities	Is contact maintained with relevant government authorities?	Contact is maintained with these institutions where necessary.	There is an overview of relevant government bodies and the purposes for which they are contacted.	A list of relevant government agencies is maintained. For each agency, it is specified who to contact, under what circumstances, how to make contact, and applicable response times.
84	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.6	Contact with special interest groups	Are relevant information channels monitored?	Information channels relevant to the organisation are monitored.	The organisation stays informed via information channels and by actively participating in other interest groups that discuss matters relevant to the (security of the) organisation.	The organisation is a member of interest groups or forums to: stay informed about best practices and security trends, validate the effectiveness of security measures, be alerted early to potential threats (e.g., available updates), access experts, exchange security information, and gain incident support when needed.
85	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.14	Information transfer	Is information exchange conducted in accordance with business rules?	When exchanging information, company policies exist to safeguard its associated confidentiality and integrity. Information ownership is demonstrable. It is clear who is authorised to access the relevant information.	When exchanging information, business rules are in place to ensure its confidentiality and integrity. Information ownership is demonstrable. It is clear who is authorised to access the relevant information.	The organisation has procedures, which are demonstrably followed, for information exchange. These procedures describe: the type of media (digital, physical, etc.), who is responsible, who has access, how information is transferred and secured (including attachments), the reliability of the exchange method (availability, integrity, confidentiality), how labels are applied, and how consistent application is ensured. E-mail containing personal health information is sent in a secure manner. Personal health information that is transported by other means is secured using cryptographic techniques. Non-digital transmission of personal health information is also protected during transport.
86	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.28	Collection of evidence	Is evidence collected in the event of an information security incident?	In the event of such an incident, evidence is collected, including system log files, etc.	When such an incident occurs, evidence is gathered regarding the entire incident.	When such an incident occurs, evidence is gathered by qualified personnel, at a level suitable for potential legal proceedings. Personnel qualifications are demonstrable via certifications or diplomas.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
87	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.30	ICT readiness for business continuity	Are business continuity requirements and ICT continuity requirements aligned?	In the event of a disruption to business services, the organisation acts to ensure information security remains operational. Organisations identify processes, systems, and other relevant equipment that are vital for healthcare delivery. Processes, systems, and other relevant equipment that are vital for healthcare delivery have been identified.	Business continuity objectives and ICT continuity requirements are known and based on a business impact analysis (BIA). Recovery time objectives (RTOs) are assigned as input for ICT readiness strategy. In view of the stringent availability requirements in healthcare, the organisation has given particular attention to measures for resilience and redundancy, covering technology, processes, and personnel.	ICT readiness is planned, implemented, maintained, and tested based on business continuity goals and ICT continuity requirements. The ICT continuity plan for healthcare processes is integrated within the business continuity plan (e.g., managing power outages, implementing infection control, and handling other clinical emergencies).
88	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.35	Independent review of information security	Is the management and implementation of information security independently assessed?	The organisation has its information security assessed ad hoc by an independent party with respect to the area being evaluated (internal auditor, independent manager, or external organisation).	The organisation periodically and after major changes assesses information security through an independent party not involved with the area being assessed (internal auditor, independent manager or external party).	In addition to level 2: This assessment includes: relevant laws and regulations, incidents, changes in organisational strategy or new initiatives, and changes to information policy that may pose risks.
89	**Organisational**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	5.42	Emergency communication	Is there an emergency communication plan in place in the event of ICT failure?	Emergency communication facilities are in place. In the event of a failure, critical functions can reach each other and key external partners can be contacted.	An emergency communication plan has been established in which emergency communication processes are defined. The emergency communication plan is known within the organisation.	The emergency communication plan is periodically tested and reviewed. Where applicable, changes are implemented.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
90	Staff	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	6.4	Disciplinary process	Are there sanctions for employees who breach information security?	Employees who act contrary to the organisation's information security policy can be held accountable, even if they were not informed of this possibility or if no formal sanctions policy has been established.	When employees act contrary to the information security policy, they may face sanctions. They have been informed of this possibility, even if it is not clear which specific sanctions may apply or to which standard or policy they relate.	There is a sanctions policy within the organisation. When employees act in violation of the information security policy, they may be subject to sanctions under this procedure. These sanctions are in accordance with applicable laws and regulations. This procedure includes the following aspects: • How, what, when, and how the violation was committed, the severity of the situation, and the impact on the organisation. • Whether the violation was intentional. • Whether it was the first time the employee committed such a violation. • Whether the employee was experienced enough to avoid making the mistake. In the event of serious violations, external bodies are informed, such as the training institution or registration authorities.
91	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.4	Access to source code	Is access to programme source codes controlled?	Access to source code is restricted to a designated group of employees.	Access to source code is restricted to a protected group of employees with no more rights than necessary to perform their duties. Source code changes are centrally tracked.	Access to source code within the organisation is managed exclusively via company-approved tooling. Users granted access are restricted to systems and functionalities necessary for their work. Changes are centrally registered in a version control system with logs detailing access and code modifications. Where possible, precautions are taken to ensure the integrity of the source code.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
92	**Technological**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.9	Configuration management	Are configurations within the organisation documented?	System configurations are documented within the organisation.	Within the organisation, configurations of systems relevant to information security are documented and kept up to date. It is known who is responsible for making changes when needed.	Within the organisation, configurations of systems (software, hardware, and services) relevant to information security are recorded in such a way that the following points are ensured: • Where applicable, references to public templates and best practices. • Alignment of the provided security level with what is deemed necessary. • Consideration of external and internal developments when establishing configurations. • Limiting the number of users who can make changes to a practical minimum. • Assessment and revision of access rights on a regular basis. • Clock synchronisation. • Changing default login credentials provided by vendors. • Automatic logout after a certain period. • Identifying the system owner. • Logging changes with details of what was changed, when, by whom, and any other relevant information. Connections of healthcare systems with other internal and/or external systems are implemented according to the appropriate (medical) standards, and these connections are also managed. When establishing management processes, the different responsibilities of ICT and medical process owners (such as a clinical physicist) are taken into account.
93	**Technological**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.11	Data masking	Is (personal) sensitive information within the organisation masked, pseudonymised, and/or anonymised?	Masking, pseudonymisation and/or anonymisation is carried out at the initiative of the employees involved.	Access to sensitive personal data is restricted and techniques such as pseudonymisation and anonymisation are used to limit the number of authorised employees as much as possible.	Access to (personal) sensitive information is restricted in line with the relevant policy using techniques such as masking, pseudonymization, and/or anonymization. The methods used are tested and approved by the organisation. In case of anonymization, individuals cannot be traced back, either directly or indirectly. If hash functions are used, they are combined with a salt function. References to sources (such as internet addresses) are avoided.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
94	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.18	Use of privileged utility programs	Is the use of programmes/systems that can bypass control measures restricted and monitored?	Use of such measures is discouraged but not forbidden. Employees are considered professional enough and are not monitored for this.	Such solutions are not used, or there is oversight in place that provides traceability of what has occurred. Medical technicians may sometimes require the same system tools as IT staff. This must be defined in the (access) policy.	The organisation has established a baseline of normal behavior and monitors for deviations. Continuous monitoring is used via a tool. Monitoring is done in real-time or at periodic intervals. Monitoring data is retained for the duration of defined retention periods. The logical access policy is demonstrably enforced for system utilities.
95	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.23	Web filtering	Is access to external websites controlled?	Employees are instructed on which types of websites they may and may not visit. The organisation relies heavily on employees' professional conduct.	The organisation has identified and communicated which types of websites employees are or are not allowed to access. At least some of these have been made technically inaccessible. There is a policy in place to prevent the incorrect blocking of content relevant to healthcare.	The organisation has identified which types of websites employees are allowed or not allowed to access. Employees are trained on such risks. Websites are blocked in accordance with the policy, considering platforms that may host illegal content or allow data uploads that conflict with company rules. The platform responsible for detection and blocking keeps itself up to date.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
96	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.27	Secure system architecture and engineering principles	Are principles applied for the engineering of secure systems?	When setting up servers, services, and developing in-house applications, attention is paid to secure deployment and ongoing security of these environments.	When setting up servers, services and developing in-house applications, attention is paid to secure deployment and maintenance of such environments. Best practices such as segmentation are taken into account where applicable.	Security by design is a fixed component when setting up servers, services, and developing custom applications. Before starting such projects, a risk analysis is performed that considers the following points: • What risks the project is exposed to. • What forms of logging and monitoring are needed to gain insight into threats. • What options are needed to intervene if a crisis is about to occur or occurs. • What needs to be done to minimize the chance of an incident and limit the impact. All measures must take into account: • Integration into the security landscape. • The organisation must be capable of developing and deploying it. • Cost, time, and complexity must be clear. • Wherever possible, based on best practices. • Security review of the project. • Documentation must be complete, and if functionality is used that bypasses the organisation's rights system, it must be stated and approved by management. Organisational information must be protected in such a way that access is granted with the assumption: • Systems may already be compromised. • Never trust, always verify principle. • Verify the sender of each request. • Apply the least privilege principle.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
97	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.28	Secure coding	Are principles applied for writing secure code?	Programming activities are carried out in a secure manner. There is no fixed process or defined set of coding standards; reliance is placed on the professionalism of the staff.	Programming is carried out by qualified staff in a way that is considered secure. One or more (coding) standards and practices (such as code reviews and/or the use of tools) are applied.	Programming is carried out by qualified personnel in a manner that can be considered secure. Before starting programming, the following points are taken into account: • Security requirements regarding the methods used and expectations set by the organisation for both internal and outsourced development. • Situations to be avoided based on experience, in order to minimise the risk of vulnerabilities. • Use of guidelines. • Use of an up-to-date development environment. • Use of qualified personnel. • Secure design and architecture that considers potential threats. • Use of secure coding standards. • Use of isolated development environments. During programming, work is carried out in accordance with a documented procedure. This describes how the OTAP (development / testing / acceptance / production) environment is used and managed. The following elements are included: • Which development techniques/ standards are used. • How and where documentation is maintained. • Prevention of insecure code. • Integration of a review process by other team members. • Implementation of updates in all forms, including third-party libraries. • Logging. • Licences. • Handling of discovered vulnerabilities. • Long-term availability. • Changes in ownership where applicable (e.g. internal to external) and how to handle them. • Compatibility.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
98	Technological	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.31	Separation of development, test and production environments	Are separate environments used during development and production in software development activities?	A separate environment from the live production environment is used during development.	Software development follows an OTAP (Development, Test, Acceptance, Production) environment and process. All phases from development to production take place in their respective environments. Measures are in place to prevent confusion between test and production data. There is a procedure for development within the OTAP framework, including agreements on control and test moments.	Software development is conducted using an OTAP environment and process. Each stage from development to production takes place in a separate environment. These environments are isolated to ensure no information is shared between them. Procedures are in place to ensure a consistent method is used for the OTAP process. Testing is not conducted in production environments unless specifically agreed upon. Development tools and access to relevant environments are not available unless necessary. Measures are in place to mitigate the risk of sensitive information in code being published to production, including use of labels in menu structures and agreements on not copying sensitive data. The OTAP environment is kept up to date according to the organisation's policy, which includes libraries, operating systems and development software. All systems used in the OTAP process are configured to be considered secure by the organisation and are monitored for deviations. There is a policy for testing with personal health information. Test patients are used for this purpose. Only where unavoidable may testing be performed using real patient data; in such cases, appropriate mitigating measures must be implemented.

Control	Category	CYRA Level	Standard	Standard Control Measure	Subject	Question	Level 1 Ad Hoc	Level 2 Best Effort	Level 3 Defined
99	**Technological**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.33	Test information	Is test data handled with care?	Operational databases containing personal or other confidential data are used regularly. No formal policy is in place, but employees have been informed of their responsibility to handle this data with care.	The use of operational databases containing personal or otherwise confidential information is avoided or limited. If necessary, sensitive details are protected and test data is deleted as soon as possible. There is a policy for testing with personal health information. Test patients are used for this purpose. Only where unavoidable may testing be performed using real patient data; in such cases, appropriate mitigating measures must be implemented.	A procedure is in place regarding test data. This procedure ensures the confidentiality of production data while maintaining test results that accurately reflect real scenarios. The guidelines in the procedure describe: • What access to production systems is required to retrieve production data. • Mandatory authorisation each time a link from production to test is established. • Logging of all access to production data. • Possible data sanitisation. • Deletion of data after test completion.
100	**Technological**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.34	Protection of information systems during audit and testing	Are potential disruptions due to verifications/ testing resulting from audits considered?	Audits can be conducted on production systems. Based on staff assessment, it is verified that this does not cause unacceptable disruptions.	Audits can be conducted on production systems. The impact on production is explicitly assessed and minimised.	Audits may be conducted on production systems in a way that limits impact on live operations. The procedure for this includes the following points: • The process of obtaining permission to conduct the audit. • Agreement on the audit scope. • Restricting access to read-only systems. • Ensuring auditor systems meet security requirements, such as having antivirus software. • Requesting permission for the use of any special software. • Arrangements made if the audit might impact production capacity. • Monitoring and logging of all activities.
101	**Technological**	**Advanced** *Answer the questions from:* • *Entry* • *Basic* • *Intermediate* • *Advanced*	NEN 7510	8.35	Zero trust principles	Is the IT environment configured in such a way that no one has access to information unless this is necessary (zero trust)?	Access to network (segments) is restricted based on a risk assessment.	Zero trust principles are defined in policy. At a minimum, the following aspects are considered: • Network segmentation • Identity verification • Device validation • Least privilege principles • Authentication	Groups of users, systems and information services associated with a network are kept as small as possible. They are only granted access to another network if both networks first verify and approve (authenticate) each other.