Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

Part 1 - NEN 7510-1: Information security management system requirements

The NEN 7510-1 requirements below correspond closely with ISO 27001. Additionally, health-specific controls where necessary should be implemented as well pursuant to norm 6.1.3.

#	**NEN 7510-1 controls**	Google Cloud Services - Google's own analysis indicates that Google Cloud Services (GCP) conforms with the ISO 27001 norms marked by '✓' below, which closely correspond with the NEN 7510-1 information security management system requirements.
4	**Context of the organization**	
4.1	Understanding the organization and its context	✓
4.2	Understanding the needs and expectations of interested parties	✓
4.3	Determining the scope of the information security management system	✓
4.4	Information security management system	✓
5	**Leadership**	
5.1	Leadership and commitment	✓
5.2	Policy	✓
5.3	Organizational roles, responsibilities and authorities	✓
6	**Planning**	
6.1	Actions to address risks and opportunities	✓
6.1.1	General	✓
6.1.2	Information security risk assessment	✓
6.1.3	Information security risk treatment	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

6.2	Information security objectives and planning to achieve them	✓
7	**Support**	
7.1	Resources	✓
7.2	Competence	✓
7.3	Awareness	✓
7.4	Communication	✓
7.5	Documented information	✓
7.5.1	General	✓
7.5.2	Creating and updating	✓
7.5.3	Control of documented information	✓
8	**Operation**	
8.1	Operational planning and control	✓
8.2	Information security risk assessment	✓
8.3	Information security risk treatment	✓
9	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	✓
9.2	Internal audit	✓
9.3	Management review	✓
10	**Improvement**	

10.1	Nonconformity and corrective action	✓
10.2	Continual improvement	✓

Part 2 - NEN 7510-2: Comprehensive list of control objectives and controls, implemented in relation to norm 6.1.3 above

The NEN 7510-2 controls and health-specific controls below correspond closely with ISO 27002 and ISO 27799. Please note that the implementation guidance, health-specific implementation guidance, other information and other health-specific information which are also part of the controls are not included in this schedule. Please check the NEN 7510-standard for further detail.

#	**Information security policies**	**NEN 7510-2 controls, similar to the ISO 27002-standard**	**NEN 7510-2 health-specific control translated to English (and abbreviated), similar to the ISO 27799-standard**	**Google Cloud Services** (Google's own analysis indicates that Google Cloud Services (GCP) conforms with the ISO 27002 and ISO 27799 norms marked by '✓' below, which closely correspond with the NEN 7510-2 controls below.)
A.5.1	**Management direction for information security**			
	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Organizations shall have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.	✓
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	The policies for information security should be subjected to a continuous phased review that enables a review of the complete policies at least once a year, and the policies should be reviewed after each serious security incident.	✓
A.6	**Organization of information security**			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.6.1	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.			
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Organisations should define and designate clear responsibilities regarding information security and have an information security management platform to guarantee that there is clear direction and support from the management for security initiatives that relate to the security of health data. At least one individual should be responsible for the security of health data within the organisation. The health data security forum should have meetings at least (almost) every month. A formal declaration should be produced in which the benchmarks for compliance activities regarding people, processes, places, platforms and applications are defined.	✓
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	To the extent possible, organisations should segregate duties and responsibilities in general, to decrease the chance of unauthorized or unintentional modification or misuse.	✓
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.		✓
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.		✓
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Patient safety should be incorporated in the management of all projects associated with the processing of personal health data.	✓
A.6.2	**Mobile devices and teleworking**			
	Objective: to ensure the security of teleworking and use of mobile devices.			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.		✓
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.		✓
A.7	**Human resource security**			
A.7.1	**Prior to employment**			
	Objective: to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.			
A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification on the information to be accessed and the perceived risks.	Organisations should at minimum verify the identity, current address and previous working circle of employees (including freelancers and volunteers) during the application process. For future employees for which qualifications for health care providers apply (such as doctors and nurses, who should be registered), qualifications should be checked. If people are hired for positions relating to security, the organisation should make sure that the candidate has sufficient competencies to fulfil such a position, and can be trusted with such a role, particularly if such a role is crucial within the organisation.	✓
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	For positions associated with the processing of personal data, the job descriptions should contain information on this topic. A similar demand exists for security roles and positions. Specific attention should be paid to the roles	✓

			and responsibilities of temporary workers such as interns.	
A.7.2	**During employment**			
	Objective: to ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.		✓
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Training on information security should be provided to new employees, and updates should be provided regularly to existing employees and if applicable interns, volunteers, etc. Employees should be made aware of disciplinary proceedings and consequences of breaching information security.	✓
A.7.2.3	Disciplinary process	There shall be formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.		✓
A.7.3	**Termination and change of employment**			
	Objective: to protect the organization's interests as part of the process of changing or terminating employment.			
7.3.1	Termination or change of employment responsibilities.	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.		✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.8	**Asset management**			
A.8.1	**Responsibility for assets**			
	Objective: to identify organizational assets and define appropriate protection responsibilities.			
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Organisations should have a register of assets, designate an owner of these assets, and have rules on how to use the assets. Such rules must be documented and implemented.	✓
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.		✓
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified documented and implemented.		✓
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	All employees should return all non-electronic personal health data in their possession when their contract ends, and make sure that all electronic personal health data that they possess is updated on all relevant systems and then securely deleted from their own devices.	✓
A.8.2	**Information classification**			
	Objective: to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.			
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	All personal health data should be uniformly classified as confidential.	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Systems should remind users of the confidential nature of the information on the system, and should label paper output as confidential when it contains personal health information.	✓
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.		✓
A.8.3	**Media handling**			
	Objective: to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.			
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Media containing personal health data should be physically protected or encrypted; the location of non-encrypted media should be monitored.	✓
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	All personal health information should be safely deleted, or the medium itself should be destroyed, if it is no longer used.	✓
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.		✓
A.9	**Access control**			
A.9.1	**Business requirements of access control**			
	Objective: to limit access to information and information processing facilities.			
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	This additional control contains additional details on what an access control policy in healthcare should	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

			contain. For more information, please check NEN 7510-2 and/or NEN's checklist.	
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.		✓
A.9.2	**User access management**			
	Objective: to ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Procedures for registering users should guarantee that the required level of authentication of identities of users matches their access levels. Registration data should be regularly reviewed to assess whether it is complete and whether access rights are still requisite.	✓
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.		✓
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.		✓
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.		✓
A.9.2.5	Review of user access rights	Asset owners shall review user's access rights at regular intervals.		✓
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment contract or agreement or adjusted upon change.	Access rights must be withdrawn as soon as possible upon the termination of a contract of an employee.	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.9.3	**User responsibilities**			
	Objective: to prevent unauthorized access to systems and applications.			
9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.		✓
A.9.4	**System and application access control**			
	Objective: to prevent unauthorized access to systems and applications.			
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Health information systems that process personal health data should verify users' identities using two factor authentication. Access to such systems should be isolated and separated of (access to) information processing infrastructures that are not associated with the processing of personal health data.	✓
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.		✓
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.		✓
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.		✓
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.		✓
A.10	**Cryptography**			
A.10.1	**Cryptographic controls**			

	Objective: to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.		✓
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.		✓
A.11	**Physical and environmental security**			
A.11.1	**Secure areas**			
	Objective: to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.			
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Physical security perimeters should be used to protect information processing facilities that support health care applications, and these areas should be protected through appropriate security measures for physical access to ensure that only authorized personnel have access to these perimeters.	✓
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		✓
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.		✓
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.		✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.		✓
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.		✓
A.11.2	**Equipment**			
	Objective: to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations			
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		✓
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.		✓
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.		✓
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.		✓
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Organisations that supply or use assets that are used for health purposes and process personal health data may not allow that such assets are relocated without the consent of the organization.	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Off premise use of equipment and assets that is used to register or report data should be authorised. This should include equipment used by remote works, even where such usage is perpetual.	✓
A.11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Media with applications for health data or personal health data on it should be safely deleted or destroyed when they are no longer used.	✓
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.		✓
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.		✓
A.12	**Operations security**			
A.12.1	**Operational procedures and responsibilities**			
	Objective: to ensure correct and secure operations of information processing facilities.			
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.		✓
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Organizations processing personal health information shall by means of a formal and structured change control process control changes to information processing facilities and systems that process personal health information to ensure the appropriate control of host applications and systems and continuity of patient care.	✓

A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.		✓
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Development and testing environments should be (physically or virtually) separated of operational systems in which health information systems are hosted. Rules for migrating software and development to operational status should be defined and documented by the organisation that hosts these systems.	✓
A.12.2	**Protection from malware**			
	Objective: to ensure that information and information processing facilities are protected against malware.			
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Organizations processing personal health information shall implement appropriate prevention, detection and response controls to protect against malicious software and shall implement appropriate user awareness training.	✓
A.12.3	**Backup**			
	Objective: to protect against loss of data.			
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Organisations should make back ups of all personal health data and securely store them in a physically protected location to guarantee availability. To protect its confidentiality, such back ups should be encrypted.	✓
A.12.4	**Logging and monitoring**			
	Objective: to record events and generate evidence.			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.		✓
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Audit reports and tools for audits of systems and audit procedures should be secured to prevent manipulation, misuse or compromise.	✓
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.		✓
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Health information systems that support time critical activities for shared care should foresee in time synchronisation services to trace and retrace the timelines for activities when required.	✓
A.12.5	**Control of operational software**			
	Objective: to ensure the integrity of operational systems.			
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.		✓
A.12.6	**Technical vulnerability management**			
	Objective: to prevent exploitation of technical vulnerabilities.			
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.		✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.		✓
A.12.7	**Information systems audit considerations**			
	Objective: to minimise the impact of audit activities on operational systems.			
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.		✓
A.13	**Communications security**			
A.13.1	**Network security management**			
	Objective: to ensure the protection of information in networks and its supporting information processing facilities.			
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.		✓
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.		✓
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.		✓
A.13.2	**Information transfer**			
	Objective: to maintain the security of information transferred within an organization and with any external entity.			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.		✓
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.		✓
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.		✓
A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Organizations processing personal health information shall have a confidentiality agreement in place that specifies the confidential nature of this information. The agreement shall be applicable to all personnel accessing health information.	✓
A.14	**System acquisition, development and maintenance**			
A.14.1	**Security requirements of information systems**			
	Objective: to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.		✓
A.14.1.1.1	Unique identification of recipients of health care	N/A	Health information systems that process personal health information should verify that every client can be uniquely identified in the system, and should be able to merge double or multiple registrations of one client if	N/A

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

			they have been made unintentionally, or during a medical emergency.	
A.14.1.1.2	Validation of output data	N/A	Health information systems that process personal health information should provide in personal identification information that helps health care providers that the requested electronic health care registration matches the client that receives treatment.	N/A
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.		✓
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		✓
A.14.1.3.1	Publicly available health information.	N/A	Publicly available health information (not being personal health information) must be archived. Its integrity must be protected to prevent unauthorized changes. The source/authorship of such information must be recognised and its integrity protected.	N/A
A.14.2	**Security in development and support processes**			
	Objective: to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.		✓
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.		✓
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.		✓
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.		✓
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.		✓
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.		✓
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.		✓
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.		✓
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Organizations processing personal health information shall establish acceptance criteria for planned new information systems, upgrades and new versions. They shall carry out suitable tests of the system prior to acceptance.	✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.14.3	**Test data**			
	Objective: To ensure the protection of data used for testing.			
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.		✓
A.15	**Supplier relationships**			
A.15.1	**Information security in supplier relationships**			
	Objective: To ensure protection of the organization's assets that is accessible by suppliers.			
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Organizations that process health information must assess the risks associated with access by external parties to these systems or data they contain, and subsequently implement security controls that match the identified risk levels and applied technologies.	✓
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information.		✓
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.		✓
A.15.2	**Supplier service delivery management**			

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.		✓
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.		✓
A.16	**Information security incident management**			
A.16.1	**Management of information security incidents and improvements**			
	Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.		✓
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	This additional control contains additional details on how information security events should be reported.	✓
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.		✓

Google Cloud Services (GC) conformance mapping with NEN 7510

Google Cloud Mapping

A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.		✓
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.		✓
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.		✓
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		✓
A.17	**Information security aspects of business continuity management**			
	Information security continuity			
	Objective: Information security continuity shall be embedded in the organization's business continuity management systems.			
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.		✓
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.		✓
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at		✓

		regular intervals in order to ensure that they are valid and effective during adverse situations.		
A.17.2	**Redundancies**			
	Objective: To ensure availability of information processing facilities.			
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		✓
A.18	**Compliance**			
A.18.1	**Compliance with legal and contractual requirements**			
	Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.			
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.		✓
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.		✓
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.		✓

A.18.1.4	Privacy and protection of personal data	Privacy and protection of personal data shall be ensured as required in relevant legislation and regulation where applicable.	Organisations that process personal health data should manage the informed consent of clients. Insofar as possible, informed consent should be acquired before personal health information is communicated to external parties.	✓
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.		✓
A.18.2	**Information security reviews**			
	Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation [i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.		✓
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.		✓
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.		✓