KEURMERK

ZEKER-ONLINE

Zeker-OnLine is an independent, transparent Quality Mark for online services (also referred to as 'cloud solutions').

Section 5
Framework of Standards
Legal requirements
Infrastructure
Application – Generic and Specific accounting services

English version based on Normenkader versie 3.1

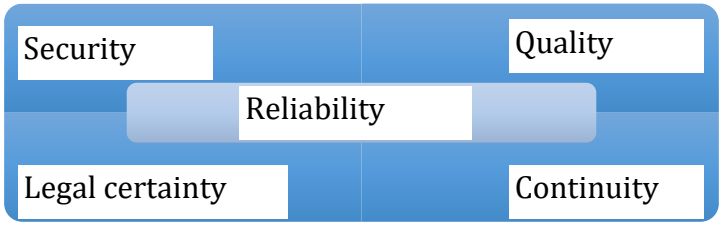
KEURMERK ZEKER-ONLINE

Contents

5. Quality requirements and framework of standards

5.1 Introduction

The award of the Quality Mark is governed by stringent requirements on the reliability of the Participant's service.
The Quality Mark is synonymous with reliability, security, continuity, functional quality and legal certainty.



A system of quality requirements and standards has been developed on the basis of the aforementioned principles.
These are specified in Section 5, “Quality requirements and framework of standards”.
A distinction can then be made between 3 quality elements:

- The technical infrastructure (IT Management and Security);
- The application structure (the generic and specific measures implemented in the application);
- The legal infrastructure.

Standards have been adopted for each of these quality elements. The relationship between these elements is laid down in a framework, i.e. the conceptual model.

The framework pivots on 'the environment', as paramount importance is attached to a reliable and secure infrastructure: the functionality is not then of decisive importance. A number of online services can be constructed within the infrastructure and data can be exchanged between the services in an effective manner. For this reason the system is a scalable concept that can be expanded in the near future. The pace and nature of any such expansions will depend on developments in the market, when the wishes of the community and the clients will, self-evidently, play an important role. The framework of standards will evolve with the system: the system is, in other words, designed as a dynamic entirety as the developments in the cloud are of a nature that will give cause to the need for continual changes.

Although the framework is designed to promote innovation, it will simultaneously need to be robust and as compatible as possible with existing, generally-accepted standards. This is then also applicable to the framework of standards. Nevertheless, the composition of the system is unique, firstly because there are not as yet any comparable concepts and, secondly, because it links the various elements.

The system is principle-based whenever this is feasible. However, the technical security measures, in particular, are more of a rule-based nature as there is a need for comparable levels of security and for a standard against which a given service can be reviewed. Nevertheless, the framework of standards never prescribes the use of specific technologies.

5.2 The system of quality requirements

5.2.1 Diagrammatic representation of the system

The various elements that can be distinguished within online services were reviewed above. Quality requirements have been specified for each of these elements. These requirements have in turn been incorporated in a framework of standards, thereby completing one of the important pillars on which the *Zeker-OnLine* Quality Mark is based.

A diagrammatic representation of the system – a 'stratified model' – containing the elements and their mutual relationships is shown below:

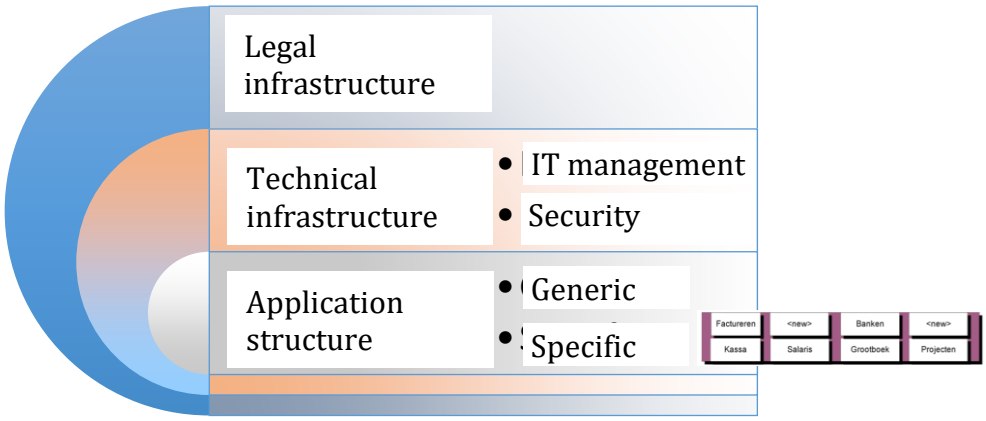


Fig. 1

The *legal infrastructure* encompasses the legal components of the quality requirements as the services offered by service providers not only need to incorporate accountancy, IT assurance engagement and information security best practices but also need to offer service providers and their clients an explicit legal position. This is also the reason why the legal infrastructure forms the foundations of the system, as the legal standards support the other elements that can be distinguished within online services.

The distinction between the *technical infrastructure* and *application structure* is based on the distinction between the Service and the Application (the software that is employed) within the online service. This provision of the application as part of a total package distinguishes online services from installable software packages, as online solutions encompass both the application *and* the full range of specialist IT management and the technical infrastructure.

5.2.2 The service and application

The service (the technical infrastructure)

A distinction can be made between two elements within the service, namely the *IT management* and the *technical security measures*.

IT management focuses on the IT policy and organisational measures, whereby the technical measures implemented in the hardware and infrastructure and the use of secure Internet links force the level of the IT management to the degree that is technically and economically feasible. This, in IT terminology, is referred to as 'hardening'. The IT management needs to be of an appropriate design and performance. The combination of the organisational and technical measures needs to result in a reliable, secure and continuously available service. When viewed from this perspective, these needs result in the allocation of the position of both the IT management and technical security measurements within the (diagrammatic representation of the) framework, as they lay the foundations required for the application to achieve an adequate performance.

The application specific

The 'application' pivots on the software, whereby the client's experience of the software is of essential importance. The application encompasses the software and the functional helpdesk. A distinction can, once again, be made between two elements that require the necessary attention, namely the *generic functionality* and *specific functionality*. The generic functionality encompasses all the general measures relating to the software application.

The specific functionality relates to the measures implemented to offer certain options or, on other words, what the client can actually *do* with the application.

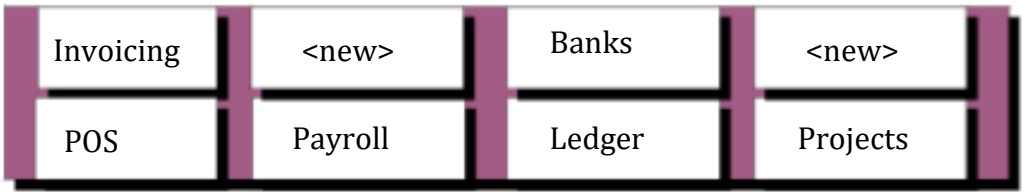


Fig. 2

The framework's generic functionality is supported by the legal infrastructure, IT management and technical security measures: the generic functionality in turn supports the application's specific functionality.

It may not be necessary to duplicate part of the assurance engagement of the service as it may be feasible to make use of work that has been carried out earlier, thereby resulting in a cost advantage. This non-duplication is feasible as identical instances in applications and services managed by or on behalf of one service provider are regarded as *one* environment. Consequently, in addition to multi-tenancy solutions, scope is also offered for multi-instancing.

5.2.3 Further explanatory notes to the system

General

The system is based on responsibilities. The service provider bears the responsibility for the service's management measures (the IT management and technical security measures). This responsibility is applicable, for example, to the provision of (delegated) user access to the correct accounts within a

multi-tenancy environment. However, as the clients retain the responsibility for their accounts the clients bear the responsibility for the delegation of authorisations for their accounts.

Service providers who outsource tasks to third parties continue to bear the responsibility for the overall online service (cloud solution): outsourcing may not, for example, result in a situation in which the auditor is unable to form an opinion on the complete solution. Consequently, service providers will need to take account of this issue when selecting suppliers.

IT management

Service providers are expected to tailor their IT to the service they provide to their clients. The service is focused on assisting clients with their business processes and with the associated records they need to keep in their accounts. This is feasible solely when service providers are thoroughly familiar with their clients' needs and problems, where relevant. The service provider's management bears the explicit responsibility for the appropriate organisation of the IT management process: the management may, once again, be expected to set an example with their behaviour when designing and managing the organisation and processes. The service must be provided in a manner that ensures that clients always receive the agreed service.

The working party selected 'COBIT' to serve as the basis for the formulation of the IT management standards. This generally-accepted framework of standards that has been tailored to the specific nature of cloud services for *Zeker- Online*.

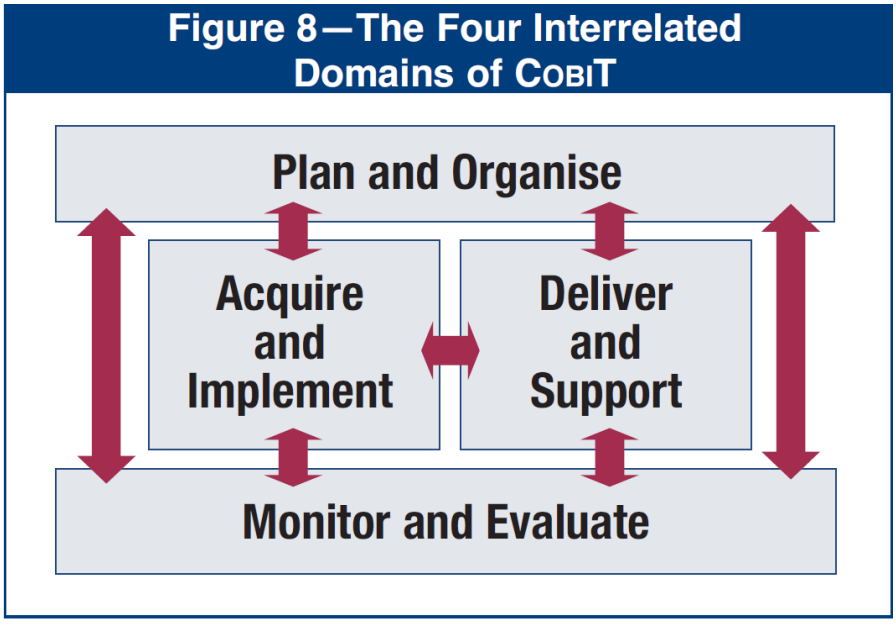


Fig. 3

Security

Service providers must implement up-to-date, secure IT solutions that are compatible with the IT management. As the technology is undergoing continual development the standards committee sought a dynamic framework of standards and found the Netherlands' National Cyber Security Centre's security guidelines suitable for its purposes. As a result, the Foundation's framework of standards is closely in line with an authoritative and practicable framework of standards and provides the necessary assurances for the future maintenance of the framework. The *Zeker- Online* framework of standards and ICT security guidelines are mutually enhancing.

Generic functionality

The generic functionality encompasses all general measures relating to the software application. As a result, this is a broad area for attention. The issues included under generic functionality include the logical access security, isolation of data, processing and recording of all transactions offered to the service, measures to provide for data integrity, the creation of an adequate audit trail, logging by the user, the creation of opportunities to monitor the processing of transactions, change management and documentation. These issues also extend to the measures governing the manner in which links with external systems such as other cloud solutions are made, as well as the creation of the documents and reports that may need to be reviewed during audits.

Specific functionality (separate frameworks)

The specific functionality relates to the options offered by the software or, on other words, what the client can actually *do* with the application. Examples of the specific functionality include keeping the accounts, the electronic creation, roll-in and processing of invoices, and the automatic roll-in and processing of bank statements. Users can maintain reliable accounts solely when they have access to software that enables them to make correct, complete and timely records of transactions: this is assured by implementing specific measures in the application. Paramount importance is attached to the quality of the data and compliance with the provisions of the relevant legislation and regulations.

5.3 Legal infrastructure

5.3.1 Legislation and regulations

Control objective:

Controls provide reasonable assurance that the Dutch legislation and regulations govern the service.

Controls:

1. The service provider declares Netherlands law applicable to the service and to any disputes about the service that may arise with entrepreneurs.
2. The service provider complies with the statutory obligations, including the information obligations prescribed by articles 3:15d, 6:227b and 6:227c of the Civil Code.
3. The service provider supplies the service in a manner that ensures that entrepreneurs can comply with the provisions of articles 47 to 53 inclusive of the State Taxes Act (Algemene Wet Rijksbelastingen).

5.3.2 Terms and conditions

Control objective:

Controls provide reasonable assurance that the client can take cognisance of the service provider's terms and conditions.

Controls:

1. The service provider publishes the terms and conditions governing the service on the service provider's website and issues these terms and conditions to entrepreneurs in time and in the appropriate manner.
2. The service provider implements adequate version management for the terms and conditions governing the service. The service provider publishes the various versions, together with a statement of the version number and the date, on the service provider's website.
3. The service provider adopts a notice-and take-down policy which is compatible with the Notice-and-Take-Down code of conduct published by the ECP[1] governing the approach to wrongful conduct and content that infringes third-party rights in some other manner.
4. The service provider incorporates an appropriate confidentiality clause in the terms and conditions governing the service.

[1] http://www.ecp.nl/werkgroep-notice-and-takedown

5.3.3 Privacy

Control objective:

Controls provide reasonable assurance that the service provider respects and provides assurances for the client's right to privacy.

Controls:

1. The service provider complies with the Personal Data Protection Act when processing personal data.
2. The service provider publishes a privacy statement on the service provider's website.
3. The service provider's privacy statement states the objective of the service provider's processing of the details of entrepreneurs and third parties.
4. The service provider's privacy statement states how entrepreneurs and third parties can inspect, amend and delete their personal data.
5. The service provider concludes a processor's agreement in the sense of the Personal Data Protection Act with all suppliers that receive personal data for which the service provider is responsible.
6. This processor's agreement includes provisions that grant the service provider the right to conduct audits of suppliers who receive personal data.
7. This processors agreement includes provisions on how to report dataleaks so that the responsible party can timely report a dataleak to the supervising authority and the persons concerned. It should be clear who is responsible for the duty to report. The agreement includes provisions regarding appropriate technical and organizational control measures for personal data.
8. In case personal data are processed by a third party the service provider only supplies these data only to organisations outside of the European Union if the European Commission decided that either the organization has adequate privacy protection, a model agreement has been concluded or the person concerned has given permission.
9. The service provider implemented an emergency plan with procedures how to handle in case of a dataleak.
10. This emergency plan includes provisions on who is responsible for reporting a dataleak to either the supervising authority or the responsible party concerned.

5.3.4 Data

Control objective:

Controls provide reasonable assurance that the client has and retains the title to the client's data that are entered and collected in connection with the online service. Agreements on data management and the retention period for data are reached between the service provider and client which are applicable in the event that the service agreement is terminated.

Controls:

1. The service provider's terms and conditions governing the service include a provision stating that entrepreneurs retain the title to all data entered by or on behalf of the relevant entrepreneur.
2. The service provider offers an option for the export of the data in a common format.
3. The service provider, on receiving the entrepreneur's notice of termination of the service agreement, draws the entrepreneurs' explicit attention to their obligation to retain records. The service provider then offers to store and file their data or to transfer the data before the data are deleted from the service provider's records.
4. The service provider files an entrepreneur's data for a period of at least six months after the termination of a service agreement due to the bankruptcy of the relevant entrepreneur. The six month period starts on the day of subscription in the solvency register. Solely (investigating) officials possessing the requisite competence and the receiver are granted access to the data during this period. The service provider includes a provision making the necessary arrangements in the service agreement.

5.3.5 Continuity

The service provider provides assurances for the continuous availability of the relevant online service.

Controls:

1. The intellectual property rights to the application are vested in an entity other than the service provider's operating company, or other measures have been implemented to provide assurances for the continuous availability of the online service.
2. The service provider implements provisions that ensure that the service can continue to be provided for a period of at least six months after the service provider's bankruptcy or the occurrence of another situation that results in the service provider's inability to continue to supply the service. These provisions are intended to enable entrepreneurs to transfer their accounts to another service provider.
3. The service provider's terms and conditions governing the service include a provision stating that the service provider may unilaterally terminate the service solely with due regard for a six-month period of notice unless the user of the service has failed to fulfil the user's obligations.

5.4 Technical infrastructure: IT management

5.4.1 Planning and organisation

5.4.1.1 Keeping records of the service process, the organisation and the dependencies:

Control objective:

Controls provide reasonable assurance that the service provider's organisation is of an adequate design and that explicit responsibilities are formally and clearly assigned within the organisation. This includes responsibilities for risk management, compliance and information security.

Controls:

1. The service provider's management bears the overall responsibility for the risks associated with the service and is the owner of those risks.
2. The service provider has assigned explicit responsibilities within the organisation for risk management, information security and compliance.
3. The organisation has implemented a policy for risk management, information security and compliance. The policy is documented and is actively conveyed by the management.
4. The service provider draws up explicit specifications of the roles and responsibilities related to the service and communicates these within the organisation.
5. The service provider draws up explicit specifications of duties and powers to ensure that all staff can perform the duties assigned to their position without hindrance.
6. Modifications to the organisation result in the commensurate modifications of the roles, responsibilities, duties and powers. The aforementioned specifications are reviewed at least once every year to verify that they are in agreement with practice.
7. The duties and powers are divided in a manner which minimises the risk that a member of staff can disrupt or abuse a critical process. The management carries out periodic reviews of the critical processes to verify that staff act within their powers.
8. The service provider has identified the key officers involved in providing the service. The organisation's dependency on individuals is minimised.

5.4.1.2 Risk management

Control objective:

Controls provide reasonable assurance that risks are managed at all levels in the organization including management. Risk management is aimed at ensuring continuous and reliable services through a process of assessing threats to the service and implementing controls to reduce risks to an acceptable level.

Controls:

1. The service provider has implemented a risk management system that identifies and appraises internal and external threats to the service.
2. Significant occurrences that pose threats to the service are identified, recorded and evaluated.
3. Qualitative and quantitative assessments are made of the probability of the materialisation of each risk and its impact.
4. The service provider has adopted a method for the implementation of measures to reduce the consequences of a prevailing risk to an acceptable level.
5. The risk management system has been implemented at all levels in the organisation, is subjected to periodic reviews of its performance and suitability and undergoes continual maintenance.

5.4.2 Procurement, development and implementation

5.4.2.1 Transfer of knowledge

Control objective:

Controls provide reasonable assurance that knowledge about the organisation, required to take ownership of the systems, is transferred to management and that staff have received the training and knowledge they require to provide the service with sufficient quality.

Controls:

1. The management is the owner of the systems.
2. The management is cognisant of the systems and the service that is provided.
3. Training material and/or process specifications and procedures, technical documentation and job and duty descriptions are available for the purposes of the transfer of the necessary knowledge to the staff.
4. The staff has received the training required to perform their duties at the required level of quality.
5. The management and staff communicate at regular intervals on the service that is provided and the changing circumstances.

5.4.2.2 Change Management

Control objective:

Controls provide reasonable assurance that for the implementation of changes a formal procedure is implemented with regard to acceptance, planning, implementation and monitoring.

Controls:

(i) Acceptance

1. Proposed changes shall be systematically classified in terms of their impact.
2. Proposed changes shall be authorised with due regard for the impact analysis.

(ii) Planning

3. Proposed technical changes shall be prioritised and announced to the clients in good time.
4. Proposed functionality changes shall be prioritised and planned in consultation with the staff.
5. Urgent changes that cannot be implemented in full accordance with the regular procedure for changes are governed by an extraordinary procedure that prescribes that regular inspection steps skipped during the implementation shall be carried out after the implementation.

(iii) Process

6. A secure test environment that is representative of the production environment is available.
7. A test plan is drawn up for each significant change. The test plan is approved by the management and staff.
8. The test plan is based on standards governing the entire organisation and pays due regard to the various roles, responsibilities and acceptance criteria.
9. A back out/fall back scenario is drawn up prior to the change and included in the implementation plan. The scenario is drawn up in consultation with the staff and approved by the management.
10. All significant changes are tested independently from the production environment, in accordance with the defined test plan, and the results are approved by the management prior to the ultimate migration to the production environment.
11. Changes which encompass a conversion of data and/or a migration of infrastructure are scheduled as elements of the service development process and the plans include provisions for audit trails and back out/fall back-scenario.
12. The organization has a code review procedure; there is segregation of duties between reviewer and developer.
13. Changes are recorded as being complete only once an inspection has been carried out to verify that all work has been completed and all changes have been recorded.

(iv) Monitoring

14. The progress of proposed changes is monitored to ensure that all work is carried out in time.

5.4.3 Service delivery and support

5.4.3.1 Definition and management of the service that is provided

Control objective:

Controls provide reasonable assurance that clients can comprehend the terms and conditions of the service and that both the service provider and clients can verify that the services provided are in accordance with the agreement.

Controls:

1. The management and staff are involved in the definition of the service and the associated terms and conditions.
2. The management signs the specification of the service and the associated terms and conditions for approval. The specifications of the service and the associated terms and conditions are formulated in a manner which is comprehensible and readily accessible to the client.
3. The specifications of the service and associated terms and conditions are in accordance with the agreement. The management and staff are cognisant with the agreement and endorse its contents.
4. The agreement contains specifications of at least the following elements of the service: its availability, performance, reliability, security and the degree of support, continuity and the preconditions.
5. The service provider and the client conclude an agreement for each service that is to be provided.
6. The service provider provides for the continual measurement and registration of the performance of the provision of the service.
7. The service provider analyses the measurements and any indications that the performance has fallen short of the agreements. The service provider takes appropriate actions when necessary.
8. The service provider submits periodic reports to the clients which contain information about the service levels that have been achieved, the changes that have been implemented and the incidents that have occurred. The report, which is explicit and readily accessible to the clients, contains analyses carried out to identify favourable and unfavourable trends.
9. The service provider and the clients carry out periodic assessments to review the suitability of the agreement as viewed from the perspective of the service currently provided and the developments and/or future developments.

5.4.3.2 Supplier Management

Control objective:

Controls provide reasonable assurance that the service provider assesses the relevant outsourced services on the potential risks for the service, the demand met and if the supplier meets the service agreement.

Controls:

1. The management and staff are involved in the identification of relationships with external suppliers.
2. The relevant relationships with suppliers have been identified. The service provider has a clear insight into the degree to which the supplier is of critical importance to the service, the roles and responsibilities involved in the relationship with the supplier and the objectives that have been formulated for the cooperation. The service provider also has a clear insight into the agreements on the (level of the) provision of service reached with the supplier.
3. Agreements with suppliers are specified explicitly in a contract.
4. The risks associated with outsourced services are identified and analysed at periodic intervals.
5. Performances within the context of outsourced services are measured and recorded continuously.
6. The performance measurements and any indications of transgressions of critical quality limits, where applicable, are analysed and compared with the agreements reached with the relevant suppliers.
7. The service provider assesses reports on the level of services supplied, the achievement or non-achievement of the targets and forecasts of performances in the near future.

5.4.3.3 Performance and capacity planning

Control objective:

Controls provide reasonable assurance that the service provider determines whether sufficient capacity is available to provide the services and that the service provider timely implements additional IT resources if required.

Controls:

1. The service provider has an up-to-date, documented availability and capacity plan for the service which has been approved by the management.
2. The service provider ensures that continuous measurements and records are made of the availability of the service, the utilisation of the capacity for the service and the utilisation of the IT equipment.
3. Capacity measurements and availability measurements are analysed at periodic intervals and compared with the stipulated requirements and forecast workload.
4. The service provider carries out periodic trend analyses of the workload and any incidents, where relevant, and draws up periodic forecasts that serve as input for the availability and capacity plan.
5. The service provider submits reports to the clients on the availability and capacity as laid down in the agreements.
6. The availability and capacity plan is evaluated at periodic intervals, updated as required and approved by the management.

5.4.3.4 Continuity Management

Control objective:

Controls provide reasonable assurance that service disruption is minimised in case of a major disaster by means of an IT continuity plan and offsite equipment, software and data.

Controls:

1. The service provider has an up-to-date, documented continuity plan for the service which has been approved by the management. The management evaluates the continuity plan at periodic intervals.
2. The continuity plan contains explicit specifications of the guidelines, roles and responsibilities, procedures, communication processes and test approaches governing the operations in the event that an emergency occurs which threatens the continuity of the service.
3. The continuity plan contains a number of scenarios which are in line with the severity of any incident and its impact on the service.
4. The continuity plan contains explicit specifications of the sequence in which elements of the service are to be restored, together with alternative scenarios.
5. Test plans have been drawn up for the testing of (elements of) the continuity plan. These test plans are tailored to the agreed service levels.
6. The test plans are used to test the continuity plan at periodic intervals.
7. The results from the tests are recorded in documents and reported to the management and all interested parties. The tests may, where relevant, result in the preparation of a plan of action.
8. The clients receive clear and timely communications on the occurrence of any emergency and the restoration of the service.
9. The clients have been issued explicit guidelines informing them of the actions they need to take in the event that the service goes down.
10. Critical back-up media, documentation and other essential IT equipment are stored at another location.
11. The external storage of back-ups and other data is carried out in accordance with the data classification policy (information security policy) and with the provisions of the relevant legislation and regulations.
12. Periodic inventories are made of the data stored at an external location to review whether they are up to date, whether they are secure and whether the facilities at the back-up location are adequate for the restoration of the filed data.
13. Every incident in which the service goes down is recorded, analysed and evaluated by the management.
14. The service provider responds to every emergency by carrying out the activities laid down in the continuity plan, when any alternative scenario that may be necessary is adopted in consultation with and after the approval of the management.

5.4.3.5 Information Security Management

Control objective:

Controls provide reasonable assurance that the service provider translates functional requirements from the contract, risks and relevant rules and legislation into an information security plan and that security measures are continuously tested, monitored and updated.

Controls:

(i) Process

1. Information security is implemented in the form of a process.
2. The management is responsible for the information security.
3. The service provider has an up-to-date, documented information security plan which is approved by the management.
4. The security measures are in line with the contents of the information security plan.
5. The information security plan and the associated procedures and measures are documented and actively communicated to all interested parties.

(ii) Access

6. The service provider has an up-to-date, documented (access) security standard and authorisation matrix which is approved by the management.
7. Unique identity characteristics, such as a user name, are assigned to staff solely after the verification of their identity and approval from the management.
8. Individual, confidential means of authentication are issued to staff solely after approval from the management.
9. Access rights are issued to staff in accordance with their role or position and solely after approval from the management.
10. Changes in job roles and job terminations are monitored to ensure that access rights can be amended accordingly and that, where relevant, identification characteristics and means of authentication can be disabled.

(iii) Generic requirements for IT equipment

11. Patch management is implemented and all current and relevant patches have been completed.
12. Adequate procedures have been implemented to provide for authorised access and the identification of networks.

(iv) Monitoring

13. The security standard and access rights are evaluated at periodic intervals, updated as necessary and reapproved by the management.
14. Operational effectiveness of Information security measures is proactively monitored.
15. Any variances or information leaks are identified and reported to the management.
16. The level of the information security is tested periodically for security leaks. The results from these tests are reported to the management.
17. Periodically security audits are performed. Penetration tests by a third party are part of these audits.
18. Vulnerability assessments (security scans) are carried out at periodic intervals.
19. The characteristics of potential security incidents have been defined and communicated to the staff.

20. An identified potential security incident is classified and dealt with at the appropriate level within the organisation.

5.4.3.6 Service desk

Control objective:

Controls provide reasonable assurance that the service desk process is supported by an adequate system and procedures and management is periodically informed about the quality of the service desk process and the reported incidents.

Controls:

1. At least 95% of the reports, incidents, requests and questions are dealt with under the conditions and within the time limits mentioned on the service providers website.
2. Users have the opportunity to give feedback on the quality of the answer they received.
3. Monitoring and escalation procedures have been drawn up on the basis of the service level laid down in the agreement that provide for the classification and prioritisation of each incident reported to the service desk.
4. Incidents are analysed on a systematic basis to identify any problems, where relevant.
5. Procedures are in place for the classification of problems and their assignment to officers for resolution.
6. Incidents are closed only once the steps taken in arriving at a solution have been recorded and the interested parties concur with the proposed solution.
7. Records are kept of the solutions for incidents. These records are accessible to all service desk staff.
8. Periodic evaluation if reports, incidents, requests and questions are dealt with within time limits.

5.4.3.7 Configuration management

Control objective:

Controls provide reasonable assurance that the service provider has configuration management in place.

Controls:

1. The service provider has a repository containing structured records of the configuration items, their characteristics and their mutual relationships and the associated documentation.
2. A baseline has been specified for each system and service.

3. The configuration management is supported by the requisite procedures. Configuration management is an element of incident, problem and change management.
4. The adequacy of the repository's contents is evaluated at periodic intervals.

5.4.3.7 Data management

Control objective:

Controls provide reasonable assurance that effective procedures are in place for the management of the media library, back up and recovery of data, as well as secure data destruction.

Controls:

1. The service provider has drawn up guidelines for the storage, provision and filing of data which are compatible with the provisions of the agreement.
2. The service provider maintains a system that offers the clients an explicit insight into the location at which their data are stored and filed.
3. The service provider has implemented and maintains organisational and technological measures to provide assurances for the continuous integrity and accessibility of the data and which also ensure that the service provider complies with the requirements laid down in the agreement and in the relevant legislation and regulations.
4. The service provider implements measures to protect the clients' data during transport via data communications and on the removal, decommissioning or destruction of hardware and media. These measures are approved by the management and tested at regular intervals.
5. Websites giving access to data that are no longer used are removed within ten days after the decision to use them any longer.
6. The service provider has adopted and implemented procedures for the backup and recovery of systems, applications, data and documentation. These procedures are in line with the requirements laid down in the agreement and continuity plan.
7. The service provider has adopted and implemented guidelines and procedures for the compliance of the processing, storage and distribution of data with the requirements laid down in the information security plan.
8. The service provider implements measures to segregate client environments and accounts.
9. Encryption is used for external backups. The management and backup of the keys is segregated.

5.4.4 Monitoring and evaluation

5.4.4.1 Monitoring of services

Control objective:

Controls provide reasonable assurance that active monitoring contributes to the quality of the services delivered to clients, internal control of the service delivery process, information security and compliance to legislation.

Controls:

1. The service provider has drawn up and implemented a suitable method for the monitoring of the provision of the service, the internal control of the service delivery, information security and compliance with the provisions of the relevant legislation and regulations.
2. The performance indicators are based on the agreement and selected to provide an appropriate insight into the delivery of the service.
3. The service provider periodically reviews client wishes and developments in the technology to determine whether modifications of the service are required.
4. The management adopts an active approach to monitoring developments in the relevant legislation and regulations. The management provides for the integration of the provisions of the relevant legislation and regulations in the process for the provision of the service and their integration in the policy, measures and procedures.
5. All significant variances are analysed in a manner that results in the explicit specification of the underlying cause. Escalation towards the clients and third parties[2] takes place as required. The management implements timely measures to resolve the causes of any variances to prevent their recurrences.

[2] Third parties can be supervisory authorities, regulatory authorities (pursuant to the legislation and regulations) or other relevant parties in the service provider's environment.

5.5 Technical infrastructure: security

5.5.1 Network security

Control objective:

Controls provide reasonable assurance that the security of information in networks and the underlying infrastructure is maintained in order to safeguard the availability of the web application and the confidentiality of the network traffic and the stored data.

Controls:

1. The service provider employs a 'demilitarised zone' (DMZ) based on compartmentalisation and the restriction of the traffic between the compartments to the level that is absolutely necessary.
2. The management and production traffic is segregated.
3. The provisions for network access to the web applications are identical for all user groups.
4. Network compartments do not contain any physical links in the form of shared compartments.
5. Measures have been implemented to combat (d)DoS.
6. Measures have been implemented to ensure that the network does not contain any Single Points-of-Failure (SPOFs).
7. Measures are implemented to ensure that certificates used to gain access to a site/page are valid, i.e. have not expired or been withdrawn.
8. Backend connections are secure connections or use an alternative form of encryption.

5.5.2 Platform security

Control objective:

Controls provide reasonable assurance that security of platforms and operating systems is designed, implemented and maintained in such a way that these systems are better equipped against attacks of malicious parties.

Controls:

1. The service provider uses safe control mechanisms.
2. Hardening is carried out (at network, OS and application level) to secure the system against manipulation and prevent the unnecessary disclosure of information on security settings.
3. System processes are isolated whenever feasible (jailing/sandboxing).
4. The service provider employs firewalls.

5.5.3 Application security

Control objective:

Controls provide reasonable assurance that web applications are secured with respect to vulnerabilities that might be present in the web applications.

Controls:

1. The web application validates the content of a HTTP request before it is used.
2. The web application checks each HTTP request to verify that the initiator is authenticated and has been granted the requisite authorisations.
3. The web application normalises input data for validation.
4. The web application codes dynamic elements of the output.
5. The web application uses solely parameterised queries when consulting and/or amending data stored in the database.
6. The web application validates all input on the server side.
7. The web application does not allow dynamic file includes or limits the available options (whitelisting).
8. The web server sends solely the HTTP headers that are of importance to the functioning of the application.
9. The web server displays solely the information in the HTTP headers that is absolutely necessary for the functioning of the application.
10. The web server minimises the information in a HTTP response sent to the user following the occurrence of an error.
11. Comment lines are deleted from the scripts (code).
12. The web server uses solely those HTTP methods that are absolutely necessary.
13. Directory listings are disabled.
14. The level of the information security is tested regularly for security leaks and the results from the tests are reported to the management.
15. Any variances or information leaks are identified and reported to the management.
16. The 'HttpOnly' and 'Secure' cookie attributes are set.
17. Measures are implemented to prevent the use of cross-site scripting.
18. Measures are implemented to prevent changes of the URL to gain unauthorised access.

5.5.4 Session management

Control objective:

Controls provide reasonable assurance that access to information is denied when the session is terminated until the user is identified and authenticated again.

Controls:

1. The locations at which the user and/or administrator can log in to the web application are also equipped with explicit functionality that can be used to log out and terminate the session.
2. Access to the information is denied when the session is terminated.

5.5.5 Reliability and non-repudiation

Control objective:

Controls provide reasonable assurance that no information is leaked, that non-repudiation is supported and that data are stored and sent by means of common encryption methods.

Controls:

1. The service provider implements measures to prevent the non-secure transmission of keys and non-secure storage of keys on servers.
2. The service provider uses common encryption methods for the encryption of communications between the browser and servers.
3. The service provider ensures that the security is sufficient to protect the data from potential threats.

5.5.6 Monitoring, auditing and alerting

Control objective:

Controls provide reasonable assurance that an environment exists of closely related (network) components that can communicate effortlessly and that new security components can integrate within the existing environment.

Controls:

1. The service provider has implemented adequate procedures and technologies to provide for (solely) authorised access and for the identification of networks.
2. Logging is only accessible for authorized users.
3. Correlations are introduced.
4. System clocks are synchronised.
5. The service provider has implemented measures to be taken in the event that the logging mechanisms go down.
6. The logging retention times have been specified.
7. Logging is secured against retrospective changes.
8. Logging is actively analysed.
9. Measures implemented for information security are actively monitored to review their performance and the results are logged.

5.6 Application structure: generic

5.6.1 Segregation of environments

Control objective:

Controls provide reasonable assurance that the service provider ensures that the accounts are segregated. Users may gain access solely to the accounts they own or to which they have to which they have been granted access by or on behalf the owner of the accounts.

The following quality standards are applicable:

1. The various accounts are logistically and/or physically segregated to an adequate extent.
2. The service provider continually monitors the system to verify that the segregation of the accounts is assured.
3. The user has access solely to the user's accounts. This is achieved by implementing adequate technical measures.
4. The service provider ensures that any breach of the access rights is identified immediately and that appropriate measures are implemented.

5.6.2 Logical access control and management of access rights

Control objective:

Controls provide reasonable assurance that identification and authentication mechanisms for access to the administrations are adequate.

Controls:

(i) Identification and authentication

1. User IDs are unique.
2. Default user IDs for the application and service provider are secured to an adequate extent.
3. The characters of passwords being entered by the user are not displayed on the screen.
4. Passwords are stored in such a way that it is impossible to trace the original password.
5. Passwords are governed by restrictions such as a minimum length and the need for the password to be changed at regular intervals. These restrictions are monitored by the application. Blank passwords are not allowed.
6. The user can change the user's password and receives a confirmation via a preset medium like email or text message. A change in medium is confirmed via the preceding medium.
7. Authentication methods other than methods using passwords must achieve at least the same identification and authentication levels.
8. The number of login attempts is limited to a maximum. The user ID is blocked once the maximum is exceeded. Once the user has logged in the user is displayed information about the date and the duration of the last login.
9. Records are kept of the last login date to enable the administrator of the application to identify user IDs that do not use the application and then block the user IDs.

10. When the service provider makes use of external login facilities the service provider fulfils the service provider's authentication responsibility by reaching agreement with the external party on the login requirements.

(ii) Authorisation management

11. The application forces the adequate segregation of duties within the user's organisation required for control purposes. Authorisation options are available for:
    - the entire application;
    - specific modules or components;
    - specific functions;
    - specific data and/or
    - the creation, reading, amendment and deletion of data.
12. If so required, access to the entire application can be shielded from specific users.
13. The authorisations granted to the application can be classified into categories including user, user group and position. This enables the user's organisations to assess the authorisations granted for the application.
14. The entry, change and deletion of authorisation data has no effect on the intended operational work.
15. When a number of user sessions may be held simultaneously measures are implemented to provide assurances for the integrity of the data processing, for example on the simultaneous amendment of the same data.
16. Inactive users are automatically logged out after a certain period of time.

5.6.3 Critical functions

Control objective:

Controls provide reasonable assurance that the critical functions for the user accounts are properly managed. Users need to be able to assign critical functions to specific job roles.

Controls:

1. It is possible to assign the administrator functionality to a specific user or specific user profile, i.e. a 'superuser'.
2. The superuser can, within the range of options offered by the specific service, enable or disable specific functionality.
3. The superuser can create, amend or delete user IDs. The superuser is responsible for the authorisation management for the relevant account.
4. The fine tuning of the account is reserved for or assigned to the superuser.
5. The superuser can generate a comprehensible report which provides an insight into the design of the accounts and the timeline of successive amendments.
6. Systematic inspections of the cloud solution are carried out to assess whether the deletion of data is in conflict with the statutory seven-year retention of records and/or impedes the smooth processing of the accounts. The user receives information about the potential problems and is

requested to give explicit agreement for the deletion, whereby the user also agrees to accept the consequences.
7. Functionality for cleaning up the logging is not available.

5.6.4. User support

Control objective:

Controls provide reasonable assurance that users working with the application receive appropriate support.

Controls:

1. The user's support is orderly, up to date and readily accessible.
2. Error messages include an explicit description of the error and offer a potential solution for the problem. This does not include technical information about the manner in which the application operates.

5.6.5 Integrity of the accounts

Control objective:

Controls provide reasonable assurance that a transaction can only be processed if it is a logical and consistent unit. The transaction status shows if this is not the case and the transaction cannot be processed. The application must enable the user to check the consistency of his account.

Controls:

1. Transactions can be completed only when they are one logical unity.
2. The processing of a transaction relates solely to one account. However, accounts can be updated in sequence following a given transaction.
3. Transactions and master data are uniquely identifiable.
4. The application validates the input of transactions using logical data enty controls.
5. All transactions are governed by the same set of controls, irrespective of the way they are entered.
6. When the input of transactions is terminated abruptly the transaction is subsequently restored or is re-offered for processing. When this fails the user can see clearly that the relevant transaction has not been processed.
7. The user can establish the integrity of the accounts by transaction, day or financial year. Variances can be traced back to individual transactions.
8. Master data used in a transaction cannot be deleted. Elements with an influence on completed transactions cannot be deleted.

5.6.6 Interfacing and integration with external systems

Control objective:

Controls provide reasonable assurance that it is clear to a user that transmittal of data is performed accurately and completely. The user must be informed and the integrity of the administration must be safeguarded if errors arise. The same validations must be applied no matter how data is entered in the account.

Controls:

1. Technical documentation and user documentation is available for the developers of external systems wishing to create links with the relevant application and are allowed to do so.
2. A check of the content and format of mandatory entry fields is carried out when importing data.
3. The user is able to establish that the import and export of data was carried out correctly, completely and in time and is able to assess whether any corrections need to be made.
4. The import functionality includes a list of check numbers for the data that are rolled in.
5. The consistency of the database is assured in the event that the transfer of data is interrupted due to a malfunction. The user is displayed a specified list of any errors, where relevant, that caused the malfunction.
6. The user can export data in the customary formats.

5.6.7 Logging and audit trail

Control objective:

Controls provide reasonable assurance that for all transactions in an account the user should be able to inspect by whom, when and how they were performed Adequate logging and audittrail that can be accessed by the user are required.

Controls:

1. Every change in relevant master data is logged.[3].
2. For transactions that are part of a statement (e.g. a VAT return) it is recorded by whom, when and how they are registered (audit trail). Changes that effect a statement are tracable. If a transaction effects a statement it is considered to be final.
3. An overview of all transactions in each account is available, together with the associated logging and audit trail.
4. The logging contains records of the identity of the user, the date, the time and the functionality that was used.
5. The user can trace transactions which are generated automatically back to their origin and type.

[3] Information about the prevailing statutory framework governing automated accounts is available on the Tax and Customs Administration's website.

6. The user can trace each transaction readily and explicitly back to the relevant document.

5.6.8 Reports

Control objective:

Controls provide reasonable assurance that a user can obtain insight into his administration by means of reports. It must be clear to the user which information a report provides and from which data collections this information originates. Selection criteria (if any) are clear to the user. The report is readable by the user and displays information accurately and completely

Controls:

1. The report states the data it contains and the origins of the data.
2. The report bears:
   - the title or name of the report
   - the name or number of the accounts
   - the date on which the report was compiled
   - the name of the user who compiled the report
   - page numbers (page x of y).
3. The fields in the report have explicit headers.
4. The report specifies the selection criteria adopted for any selections of data, where relevant.
5. All data in the report is completely legible: the report does not, for example, contain fragments of data or half-columns.
6. Totals in the report are accurate.
7. The user is not able to modify original report formats for standard reports. Other reports may be modified solely by users who have been granted the requisite authorisation.
8. When reports offer a drill down option then the underlying data must be presented correctly and in full.
9. The user can export reports in common formats.

5.7 Application structure: specific for SAAS suppliers Administrative

5.7.1 Financial – basis

Control objective:

Controls within the application provide reasonable assurance that the application provides for the correct accounting substance of the accounts.

Controls:

1. The application includes measures to provide for the correct, complete and timely reconciliation between general ledger and subledgers.
2. The entries of the transactions must always balance.
3. The application ensures that any negative cash balance is always identified.

5.7.2 Audit file

Control objective:

Controls within the application provide reasonable assurance that the application provides for the correct and complete transfer of the financial / administrative data via the audit file.

Controls:

1. The application supports the export of an audit file approved by the Tax and Customs Administration.
2. The audit file contains the correct and complete data contained in the selected account in the relevant period and includes the opening balance sheet.

5.7.3 Entering and processing transactions

Control objective:

Controls within the application provide reasonable assurance that the application safeguards that unique transactions can be entered only once and that postings do not impair the consistency of previous reports.

Controls:

1. The application does not allow the user to make entries that impair the consistency of accounts and tax returns filed at an earlier date.
2. The application safeguards that the user can process unique transactions only once.

5.7.4 Overviews and reports

Control objective:

Controls within the application provide reasonable assurance that the application provides the user an insight into its accounts by means of overviews and reports.

Controls:

1. The balance sheet and profit and loss account are compiled from all ledger accounts in an auditable manner.

2. Standard reports provide an insight into the outlines and at detail level.
3. The user can specify selection criteria for the generation of summaries and reports.
4. The user has at least the following reports available:
   - Accounts payable list
   - Accounts receivable list
   - Age analysis of accounts payable and accounts receivable
   - Balance sheet
   - Trial balance sheet
   - Profit and loss account
   - Transactions not yet processed
   - Authorisation overview

5.7.5 Setup and closure of financial years and period

Control objective:

Controls within the application provide reasonable assurance that the application includes functionality to setup financial years and periods consistently and in accordance with the organisation's needs.

Controls:

1. The user can work in different financial years and periods within the accounts.
2. The user can exercise the user's full discretion in the creation of periods and financial years, such as broken financial years, in the application. The application provides assurances for the reconciliation of the periods and financial years.
3. The user cannot amend created financial years or periods once transactions have been entered.
4. The application provides for controllable and auditable year end procedure.
5. The user can close a period independently of the VAT return.
6. The application ensures that entries of transactions are reconciled with the specified financial years and periods.
7. An option is available whereby financial years and periods can be subjected to an authorisation when they are closed and/or opened or reopened.

5.7.6 Invoicing (when the application includes an invoicing module)

Control objective:

Controls within the application provide reasonable assurance that the application enables the user to with the statutory requirements.

Controls:

1. When the application supports the import of invoices by means of scanning or importing then the application also offers an option for visual inspections.
2. The application enables the user to create invoices that comply with the statutory requirements.
3. The application enables the user to inspect the invoices to verify that at least the statutory information is stated in the invoices.
4. The application ensures that the base amount for VAT and the amount of VAT is always reconciled.

5.7.7 VAT returns

Control objective:

Controls within the application provide reasonable assurance that the application supports the appropriate registration of VAT obligations. A clear and explicit structure and control mechanisms tailored to the structure are available.

Controls:

1. The user cannot amend or delete data (traceably) used to compile the VAT return once the return has been filed.
2. The user must have filled all the mandatory fields of a tax return before the relevant return can be filed. The application displays a message when mandatory fields have not been filled.
3. The application offers an insight into the manner in which tax returns have been compiled from the relevant underlying transactions.
4. SBR/XBRL returns are based on the taxonomy prevailing at the time the tax return was filed.
5. The application is able to identify the need to file a supplementary return pursuant to Article 15 of the *Uitvoeringsbesluit OB* ('VAT (Implementation) Decree').
6. The application ensures that the VAT calculations at journal level and the ultimate VAT return are in agreement.
7. The application offers an insight into the transactions that will result in the need to file a tax return in the future or for periods in which a tax return has already been filed.

5.7.8 Electronic banking and collection (for applications including this module)

Control objective:

Controls within the application provide reasonable assurance that electronic bank transactions are accurately, timely and completely processed in the financial accounts.

Controls:

1. The user has a clear insight into the banks for which exchanges of electronic transactions are supported.

2. The user is offered at least the following summaries:
   - payment advice list
   - current payment orders
3. The application provides for the automatic processing of bank statements.
4. The application provides for completeness checks of bank statements imported in the application.