QWOATER

cloud document management

SOC 3® Report

Relevant for the trust services criteria security, availability, confidentiality and privacy.

January 1, 2021 to December 31, 2021

TABLE OF CONTENTS

I. QWOATER'S MANAGEMENT STATEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Qwoater's management system (system) throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Qwoater's service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Qwoater's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Qwoater's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Qwoater uses subservice organizations Microsoft Azure to provide housing and hosting services, SignRequest for digital signing services and Amazon for user authentication services (AWS Cognito). The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Qwoater also indicates the complementary subservice organization controls assumed in the design of Qwoater's controls. The description does not disclose the actual controls at the subservice organization.

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Qwoater's controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents Qwoater's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Qwoater's controls.

We assert that the controls within the system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Qwoater's service commitments and system requirements were achieved based on the applicable trust services criteria.

Qwoater B.V.
Ernesto Lopez Vega
Director

Digitaal ondertekend door:
Ernesto Lopez Vega
10 maart 2022 08:55 +01:00...

Tilburg, March 10, 2022

II. Independent Service Auditor's Assurance Report

To the Management of Qwoater B.V.

II.1 SCOPE

We have examined Qwoater's accompanying assertion titled "Qwoater's Management Statement" (assertion) that the controls within Qwoater's management system (system) were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Qwoater's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Subservice organizations

Qwoater uses Microsoft Azure as a subservice organization to provide housing and hosting services, SignRequest for digital signing services and Amazon for user authentication services (AWS Cognito). The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Qwoater also indicates the complementary subservice organization controls assumed in the design of Qwoater's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Complementary User entity controls

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Qwoater's controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents Qwoater's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Qwoater's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

II.2 SERVICE ORGANIZATION'S RESPONSIBILITIES

Qwoater is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Qwoater's service commitments and system requirements were achieved. Qwoater has also provided the accompanying assertion about the effectiveness of controls within the system.

When preparing its assertion, Qwoater is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

II.3 SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Qwoater's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Qwoater's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

II.4 INHERENT LIMITATIONS

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

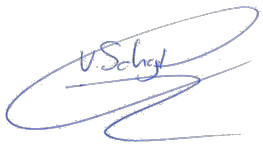
Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

II.5 OPINION

In our opinion, management's assertion that the controls within Qwoater's system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Qwoater's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Amstelveen, March 10, 2022

BDO Audit & Assurance B.V.
On behalf of,



J. van Schajik RE CISA
Partner

ATTACHMENT A - QWOATER'S DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

III.1 BACKGROUND

Qwoater is a professional service provider offering innovative document management services to accountancy and related organisations and to SaaS-providers in the accountancy line.

Qwoater is an efficient and agile company. From 2019 on Qwoater has started employing own personnel on its own payroll. Qwoater's services are sold to customers active in the accountancy branche and related branches. Qwoater's ambition is to become the number one solution for client dossiers management from customer's perspective and get integrated in all major SaaS-platforms used in the accountancy branche. From start Qwoater is integrated within the Loket.nl-platform. Since 2021 new SaaS services are added.

III.1.1 SERVICE SCOPE

This report covers the following Qwoater's services:

Qwoater SaaS integration services:
Consisting of transparent integrations between Qwoater and SaaS suppliers for adding and retrieving documents beside other document management functionality.

Qwoater applications: QwoaterDIRECT and QwoaterRAPPORTEN:
QwoaterDIRECT is Qwoater's main internally developed software solution with rich document management functionality to maintain client dossiers and support document based processes within Qwoater's customers.

QwoaterRAPPORTEN is Qwoater's specific solution to facilitate accountancy report distribution between auditor, customers and report applicants.

III.1.2 SUBSERVICE ORGANIZATIONS

Qwoater runs on the Microsoft Azure platform for delivering and maintaining Qwoater's SaaS-infrastructure. For legallly binding digital signing functionality, Signrequest services are integrated within Qwoater's solutions. Amazon (AWS) delivers professional authentication services to the users of Qwoater's frontend applications. With respect to these sub-service organizations the carve-out method is applied. To guarantee it's service and quality, Qwoater has defined procedures and service levels according to which Qwoater's partners have to deliver. Qwoater's operational processes monitor and manage the service delivered by its partners.

III.2 SYSTEM OVERVIEW

III.2.1 INFRASTRUCTURE

Qwoater's technical infrastructure runs on Microsoft Azure.

Microsoft Azure

Microsoft Azure delivers a leading global cloud platform. Qwoater's entire infrastructure is hosted in the EER with its primary region being The Netherlands and its secondary region in Ireland.

Qwoater makes preferably use of Microsoft Azure's platform as a service (PaaS) solutions where possible and relies on the security and availability measures that apply for these Microsoft Azure services. Some parts of Qwoater's infrastructure still consist of virtualized systems which are hosted on a high available and extensive scalable environment options in order to meet Qwoater's commitments regarding performance and availability. To extend flexibility, scalability and security Qwoater uses multiple servers that are assigned dedicated tasks and functions. Back-ups are created according to a fixed schedule and are stored on the primary and secondary regions to guarantee data availability after incidents or disasters.

To ensure quality of service Qwoater makes use of industry standard applications as basis for her service delivery e.g., operating systems, databases, anti-virus software and proven technology. Qwoater's infrastructure is strictly secured and only accessible through encrypted connections. Only authorized systems and users are able to connect through these encrypted connections to the systems.

III.2.2 SOFTWARE

Qwoater's SaaS solution consist out of the following major software components:

- A Commercial of the Shelf (COTS) Enterprise Document Management System to store, encrypt, retrieve documents and to execute document-related processes.
- Qwoater Business Layer
  The Qwoater Business Layer is Qwoater's proprietary software layer which exposes Qwoater's functionality to its customers. Important functions of Qwoater's Business Layer are:
  - creating and maintaining client dossiers including HR dossiers;
  - storing documents;
  - retrieving documents;
  - generating documents;
  - digital signing of documents via its signing partner SignRequest.

III.2.3 PEOPLE

Qwoater's flat and flexible organization structure allows the organization to communicate direct and fast between all people involved. The management of Qwoater plays an important role in establishing and carrying out the company's tone and attitude regarding professional service delivery, risk management and towards privacy. Qwoater's operational processes, communication- and escalation lines ensure fast and direct information exchange between the operational level and board and management. Qwoater has adopted the agile working method: "SCRUM" .

All resources involved with Qwoater must have signed confidentiality agreements to guarantee that all knowledge obtained about Qwoater and Qwoater's customers is only used for fulfilling their professional tasks and responsibilities regarding Qwoater. Access to systems is only granted to people with tasks and functions, which require access.

Qwoater has procedures in place to manage system access for new and leaving personnel to ensure system access is permitted to the right persons at any time.

As part of the onboarding procedure of new personnel all resources are trained to acquire all relevant knowledge that's required to carry out the resource's tasks and responsibilities. Training involves business perspectives as well as Qwoater's operational processes, procedures and Qwoater's general perspectives and attitude on professional service delivery.

III.2.4 PROCEDURES

The primary business focus of Qwoater consists out of providing a SaaS-service to its customers, making sure the right service is delivered and service levels regarding i.e. availability and performance are met. Qwoater's secondary focus is to extend its business and to provide new functionality and to enlarge its user base. For the major part of Qwoater's operational activities, the ITIL-processes and procedures are applied and connected to the SCRUM methodology together with a structured development process. Qwoater has tailored these procedures to its own purpose. Changes in the procedures are managed through the Quality Management processes.

III.2.5 DATA

Qwoater handles all productive data with utmost care and confidentiality. Physical access to the data limited to the resources that need to have access. Audited internal processes and procedures of Qwoater's infrastructure partners guard physical access. Logical access is only possible through secured connections. These connections are only available to resources and systems that need to have access. On top of the secured connections, data is also send encrypted through HTTPS-protocols. Even when an unauthorized party compromises the access procedures, information will still be encrypted. All documents stored in the system are AES-256bits encrypted.

III.3 RELEVANT ASPECTS OF INTERNAL CONTROL

This section provides information about the five interrelated components of internal control as defined by the American Institute of Certified Public Accountants (AICPA) at Qwoater:

1. Control Environment. Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
2. Risk Assessment. The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.
3. Control Activities. The policies and procedures that help make sure that management's directives are carried out.
4. Information and Communication. Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
5. Monitoring. A process that assesses the quality of internal control performance over time.

III.3.1 CONTROL ENVIRONMENT

As a professional service provider, handling sensitive information, Qwoater takes risk management seriously. The board of Qwoater considers thorough risk management as one the company's primary responsibilities and carries this out throughout the organization. In all layers of the organization and all resources working for Qwoater awareness exists and is continuously stimulated to identifying and assess potential risks.

In order to ensure a high level of operational excellence and flexibility Qwoater's implemented a flat organization structure with a low level of hierarchy, with all roles identified and assigned to individuals. On all aspects of risk regarding security, availability, confidentiality and privacy Qwoater's attitude is very defensive and preventive. Qwoater aims at identifying every risk before it can become relevant. In case when issues occur the continuous learning- and risk management cycle of Qwoater must prevent happening issues of the same kind again. In all relevant operational processes the organization is alert on identifying risk and assessing impact and possible preventive measures. In general Qwoater prefers prevention of risk to mitigation. Whenever a risk might become reality, Qwoater's flexible and flat organization facilitates direct communication and decision-making between the operational organization and Qwoater's management and board. On yearly basis Qwoater reassess all formerly identified risk to ensure risks are rated on the right level of impact and are completely identified. Each year the risk assessment and operational procedures are also audited by an external auditor to ensure compliance with processes, procedures and policies.

III.3.2 RISK ASSESSMENT PROCESS

Qwoater is highly committed to provide high quality to its customers and therefore is aware of the importance of having a solid risk management process in place. The risk management process of Qwoater aims at prevention of risks becoming actual incidents and there for has processes in place to identify, register and mitigate risks in a transparent and appropriate way.

Qwoater takes a proactive approach to risk management following AICPA directives to ensure that:

- Security: Systems are protected against unauthorized access
    - Logical
    - Physical
- Availability: Systems are available for operation and used as committed or agreed with contracting parties
- Confidentiality: Information designated as confidential is protected as committed or agreed with contracting parties
- Privacy: Personal information is collected, used, retained, disclosed, and disposed as committed or agreed with contracting parties

Qwoater has integrated the risk management process as an continuous process in its operational activities, following the next steps:

- Risk identification
- Risk (impact) analyses
- Risk mitigation
- Monitoring and evaluation

III.3.3 CONTROL ACTIVITIES

Qwoater has implemented several control activities in order to make sure the personnel carries out the management's directives. Qwoater's control activities cover the following functions of the organization:

- Human resource management
- Security management
- Vendor management
- User management
- Business continuity management
- Service delivery management

Onboarding of personnel

All personnel working for Qwoater is checked on relevant experience and needs to have a confidentiality statement signed which is applicable to Qwoater. New personnel are informed about processes, procedures and policies. Additionally personnel are trained in-depth in the matter, which is relevant for the specific tasks and responsibilities that are assigned to the resource.

Application development and maintenance

To guarantee the quality and availability of Qwoater's services, Qwoater has several processes in place:

- Incident management: process to identify, register and act upon all incidents that may occur in Qwoater's service delivery. This process aims at restoring a normal service operation as soon as possible after an incident happens. Processes and procedures are in place to identify root causes and to take measures to prevent happening incidents with the same nature again.
- Change management: Qwoater's change management process identifies the impact of every change that's intended to by implemented in the system in order to guarantee system availability. The change management process enables Qwoater to implement changes in a highly managed way in the productive environment, minimizing negative impact on its service delivery.
  The development process is part of the change management process. Every code change is approved by another developer (4-eyes principle) before the new code can be released.
- Capacity management: multiple metrics are in place to measure capacity occupation on several aspects on the system e.g., disk-space availability, memory usage, CPU-usage and bandwidth usage. On regular basis the available capacity is evaluated and tested against expected capacity demand, in order to safeguard sufficient capacity.
- Availability management: as extension of the capacity management process, Qwoater has implemented relevant metrics to measure the service's availability and to trigger action when unavailability might occur.

Platform- and data security

The technical infrastructure is hosted on the Microsoft Azure platform. As one of the global cloud provider Microsoft Azure holds multiple certifications e.g. ISO 27001:2013 and SOC 2 for the following Trust Services Criteria: Security, Availability, Processing Integrity, and Confidentiality. The SOC 2 report is yearly checked whether the certification is prolonged and if the services that are relevant for Qwoater are still in scope.

Privacy
Qwoater takes privacy serious. Not only due to the sensitive personal information stored by customers in the system but also because customers may expect that Qwoater can relieve them partly from their obligations concerning privacy. The role of Privacy Officer is responsible for all privacy related matters. All people involved with Qwoater are aware of the importance of privacy and how to deal with it in their daily jobs. Some measures have been taken to ensure the privacy within the system and to ensure that basic principles like privacy by default and privacy by design are followed. These principles are checked by the Privacy Officer before each update of the system. Furthermore controls are in place to guarantee that documents of employees within the system are timely destroyed and the data breach procedure is yearly checked.

Regarding to the GDPR, the customers of our clients can be designated as the controller of the data, Qwoater's customers as processors and Qwoater as sub-processor for the personal data of the Controller. As part of the agreement between our customer and Qwoater, a data processing agreement (DPA) is signed.

III.3.4 INFORMATION AND COMMUNICATION
For the internal communication within Qwoater and the external communication with its customers multiple systems are in place.

Internal communication
As part of the SCRUM methodology multiple meetings are fixed and joined by the scrum team consisting of the Devops Team and Product Owner e.g. Daily Scrum meeting, Sprint planning, Refinement meeting, Sprint Review and Retrospective. During these meetings the ongoing business on operational level is addressed to ensure service is on the right level and all open issues are getting the follow-up needed. The product owner informs the board monthly about the operation, address potential issues and risks and to define the business development roadmap.

External communication
Since the introduction of QwoaterDIRECT and QwoaterRAPPORTEN a direct support line is implemented. For customers that only use Qwoater via Saas integration services the customer's channels of the service are in use and for support or registration of incidents these customers use primary the helpdesk that's provided to them by the service. Whenever new functionality is introduced in Qwoater the customers are informed through the digital newsletter of Qwoater and Loket.nl depending on the type of feature. QwoaterDIRECT or QwoaterRAPPORTEN features are always communicated via Qwoater's newsletter.

III.3.5 MONITORING OF CONTROLS
Qwoater's technical platform is continuously monitored by automated tools on key elements that are essential for the availability of the platform. Whenever disruptions occur, the responsible resources are informed to take action and an incident will be raised.

During the scrum meetings issues and changes are evaluated to verify whether they are handled according in compliance to the defined processes and procedures. The delivered service by vendors is continuously evaluated and when necessary service level meetings are planned. Whenever necessary measures are implemented in order to meet the agreed service levels.

Controls are added or improved whenever this is beneficial to the quality of Qwoater's service.

III.4 COMPLEMENTARY USER ENTITY CONTROLS

Qwoater's system was designed with the assumption that certain complementary user controls would be operating effectively at user entities. User entities should consider the following controls:

- Physical and logical security to the end-user's hardware is in place.
- Appropriate functionality in the front-end / application that's used to access Qwoater via a connected SaaS service is enabled / authorized. Enabling / authorizing the appropriate functionality determines which functionality is available for the end-users.
- Users are the owners of the data they store in Qwoater. This includes the responsibility for the disposal of data when users decide to end the contractual relationship with Qwoater.
- Authorization and authentication on end-user level to the SaaS application that's used to access Qwoater is in place.
- On employer-level the applicable permissions are defined for each combination of document type and role in Qwoater's authorization matrix if available within the connected SaaS service.
- Internal procedures are in place regarding saving of documents within the correct document type with special attention towards retention and destruction periods.
- Incidents are being reported as quickly as possible and by using the correct processes and communication paths.
- All incidents, issues and risks are discussed with Qwoater.
- Data is encrypted by the user entity in case physical transport of data takes place.

III.5 COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Qwoater's cloud system was designed with the assumption that certain complementary subservice organizations controls would be operating effectively at the subservice organizations. This paragraph describes the subservice organizations including the nature of the services provided by the subservice organizations. In addition, each of the applicable trust services criteria that are intended to be met by controls at the subservice organizations and also the types of controls that service organizations management assumed, in the design of the service organizations system, would be implemented by the sub-service organizations are described.

III.5.1 DATA CENTER

III.5.1.1 Nature of the services provided by the data center

The subservice organization Microsoft Azure delivers the housing and hosting service to Qwoater. The following two paragraphs describe the intended Trust services criteria and implemented controls for the data center.

III.5.1.2 Trust service criteria that are intended to be met by controls at the subservice organizations

The following trust service criteria depend on the data center services. Qwoater has implemented several monitoring controls to review the delivered services.

Criteria	Definition
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

III.5.2 DIGITAL SIGNING PARTNER

III.5.2.1 Nature of the services provided by the digital signing partner

The digital signing partner delivers all services needed for digital signing of electronic documents including all legal aspects. Qwoater sends document towards the digital signing partner if a Qwoater user has indicated a document should be digitally signed. Qwoater controls all activities around the document to retrieve it after signing and remove from the environment of the digital signing partner.

III.5.2.2 Trust services criteria that are intended to be met by controls at the subservice organizations

The following trust services criteria depend on the digital signing partner. Qwoater has implemented several monitoring controls to review the delivered services.

Criteria	Definition
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.

III.5.3 USER AUTHENTICATION SERVICE

III.5.3.1 Nature of the services provided by the user authentication service

The user authentication service, authenticates and manages user accounts with direct access to one of Qwoater's frontend applications in a secure way. Before a user can access the backend of Qwoater's services, the user is always authenticated via the authentication service.

III.5.3.2 Trust services criteria that are intended to be met by controls at the subservice organizations

The following trust services criteria depend on user authentication service. Qwoater has implemented several monitoring controls to review the delivered services.

Criteria	Definition
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

III.6 CRITERIA NOT ADDRESSED BY CONTROLS

Qwoater has implemented controls to address all criteria from the SOC2® framework, which are relevant to the organization i.e. criteria related to security, availability, confidentiality and privacy. Multiple criteria are defined for these categories, which are all addressed by one or more controls. One exception is made for multiple criteria regarding the privacy category.

The following privacy criteria have not been addressed by controls:

- P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.
- P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice.

Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

- P3.1: Personal information is collected consistent with the entity's objectives related to privacy.
- P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.
- P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
- P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.
- P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
- P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

Regarding to the GDPR, the customers of our clients can be designated as the controller of the data, Qwoater's customers as processors and Qwoater as sub-processor for the personal data of the Controller. The privacy criteria that have not been addressed by controls are in our opinion only relevant for data controllers. As a result, the privacy criteria that have not been addressed by controls are not included in the scope of the system of Qwoater.

ATTACHMENT B - QWOATER'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

IV.1 SERVICE COMMITMENTS

Qwoater makes service commitments to its customers and has established service requirements as part of Qwoater services. These commitments to customers are communicated via General Agreements, Terms and Conditions and Data Processing Agreements. Service commitments to Qwoater customers are achieved by designing, implementing and operating effective controls within Qwoater.

IV.2 SYSTEM REQUIREMENTS

Qwoater delivers an innovative online document management platform for accountancy firms and related organizations and is specialized in client dossier management. Internal policies of Qwoater's system are developed in consideration of legal and regulatory obligations, to define organizational approach and system requirements. The offering of Qwoater's services depends upon the appropriate internal functioning of system requirements defined by Qwoater to meet customer commitments. Various controls and procedures are implemented to meet Qwoater's requirements and commitments to its customers which includes:

Security: Qwoater has made commitments to its customers related to security of their data by restricting unauthorized access to Qwoater application and systems. These commitments are monitored through the functioning of various internal controls implemented for Qwoater.

Availability: Qwoater has made commitments to its customers to make Qwoater applications available for an average yearly availability of certain percentage for 24 hours a day 7 days a week.

Confidentiality: Qwoater has made commitments to its customers related to maintaining the confidentiality of customers' data through access security, least privilege and other relevant security controls.

Privacy: Qwoater has made commitments to its customers related to privacy of its personal data. Qwoater ensures that objectives and responsibilities regarding data privacy is in line with accepted privacy principles and applicable laws and regulations.