SOC 3® REPORT

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

May 10, 2022 to april 30, 2023

accept®

TABLE OF CONTENTS

I. ACCEPT'S MANAGEMENT STATEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Accept's transportation management system (system) throughout the period May 10, 2022 to April 30, 2023, to provide reasonable assurance that Accept's service commitments and system requirements relevant to security, availability, and confidentiality 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 May 10, 2022 to April 30, 2023, to provide reasonable assurance that Accept's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (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). Accept'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 organisation may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Accept uses subservice organisations to provide housing and hosting (Microsoft Azure), database hosting (MongoDB Atlas) and office IT (Accept Systems) services. 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 organisation are suitably designed and operating effectively. The description of the boundaries of the system of Accept also indicates the complementary subservice organisation controls assumed in the design of Accept's controls. The description does not disclose the actual controls at the subservice organisation.

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 Accept's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents Accept's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Accept's controls.

We assert that the controls within the system were effective throughout the period May 10, 2022 to April 30, 2023, to provide reasonable assurance that Accept's service commitments and system requirements were achieved based on the applicable trust services criteria.

Accept Hosting B.V.
Accept Development B.V.
Etten-Leur, June 29, 2023

Frank van Nielen,
Director

II. Independent service auditor's assurance report

To the Management of Accept Hosting B.V. (hereinafter: Accept)

II.1 SCOPE

We have examined Accept's accompanying assertion titled 'Accept's Management Statement' (assertion) that the controls within Accept's SBR application services system (system) were effective throughout the period May 10, 2022 to April 30, 2023, to provide reasonable assurance that Accept's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (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).

II.2 SUBSERVICE ORGANISATIONS

Accept uses subservice organisations Microsoft Azure, MongoDB Atlas and Accept Systems to perform housing and hosting, database hosting and office IT services, respectively. 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 organisation are suitably designed and operating effectively. The description of the boundaries of the system of Accept also indicates the complementary subservice organisation controls assumed in the design of Accept's controls. The description does not disclose the actual controls at the subservice organisation. Our examination did not include the services provided by the subservice organisation, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

II.3 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 Accept's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents Accept's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Accept'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.4 SERVICE ORGANISATION'S RESPONSIBILITIES

Accept 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 Accept's service commitments and system requirements were achieved. Accept has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Accept 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.5 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 organisation'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 organisation's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Accept'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 Accept'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.6 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 organisation'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.7 OPINION

In our opinion, management's assertion that the controls within Accept's SBR application services system were effective throughout the period May 10, 2022 to April 30, 2023, to provide reasonable assurance that Accept's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Amstelveen, June 29, 2023

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

Digitaal ondertekend door:
Marco Francken
29 juni 2023 10:14 +02:00...

drs. M.A. Francken RE RA CISA CRMA
Partner

III. ATTACHMENT A - ACCEPT'S DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

III.1 Background

Accept was founded in 1994. The organisation provides a range of solutions for handling various SBR processes in the Netherlands. Up until the launch of the first SBR application (the SBR Viewer) in 2014, Accept's activities primarily centred on the development of an accounting program (Accept Financieel) and a financial reporting tool (Accept Rapportage). In the past decade, the organisation's focus has shifted to SBR. In that time, Accept has grown into a leading party on the Dutch market with extensive knowledge of XBRL and SBR.

SBR (Standard Business Reporting) is a national standardised method for the digital compilation and provision of (financial) reports to government institutions and banks. XBRL (eXtensible Business Reporting Language) is used as part of the SBR program. XBRL is an international open standard used for the exchange of data. With its wide range of solutions, Accept strives to make SBR more accessible to all involved parties, without necessarily requiring in-depth knowledge of SBR and/or XBRL.

Accept's list of clients primarily consists of accountancy firms that are among the thirty largest of such firms in the Netherlands. Several members of that group belong to the global 'Big Four' (Deloitte, PwC, Ernst & Young and KPMG). Furthermore, Accept works closely together with umbrella organisations such as SBR Nexus and SBR Wonen, and Accept's solutions are purchased by software suppliers from myriad sectors. Several of Accept's employees are actively involved in the development and adaptation of Standard Business Reporting and the XBRL standard in general. To that end, they are members of various national and international working groups, panels and forums.

III.1.1 Service scope

This report covers virtually all of Accept's SBR solutions. These solutions can be used to convert, generate, present, validate, edit, sign and submit SBR documents, among other things.

Accept's solutions are versatile and offered in the form of a web application or system-to-system web service, depending on the client's wishes. SBR solutions in the form of web services are primarily used by external software suppliers and large(r) accountancy firms with software platforms of their own. They can easily integrate Accept's web services into their existing software package or access it via an API. When a client opts to purchase Accept's SBR solutions in the form of a web application, Accept will create an online environment for the party in question.

A detailed list of the in-scope software solutions, including the programming languages used and the platform on which the solution in question runs, is described in section III.2.2 of this report.

III.1.2 Boundaries of the system

A system is created, implemented, and maintained with the aim of achieving specific business goals as per the requirements specified by management. The purpose of the system description is to define the system's boundaries, which encompass the services briefly outlined in the previous

section (III.1.1) and the five components detailed in section III.2 (infrastructure, software, people, procedures and data).

III.1.3 Subservice organisations

Accept uses subservice organisations Microsoft Azure and MongoDB Atlas to provide the components that are used for the hosting and security of the (online) web applications and services that are accessible to Accept's clients. The services of subservice organisation Accept Systems are used to host most of the components that are used internally by Accept's employees (e.g. to develop new or maintain existing solutions). A comprehensive explanation of the services provided by each sub-service organisation is described in section III.2.1 of this report.

III.2 System overview

III.2.1 Infrastructure

Accept's digital infrastructure can be broken down into external and internal components. The external infrastructure includes the components that are used for the hosting and security of the (online) web applications and services that are accessible to Accept's clients. The internal infrastructure includes the components that are used by Accept's employees and which are therefore not accessible to third parties.

Without exception, the components that form part of the external infrastructure are hosted by Accept's primary service providers: Microsoft Azure and MongoDB Atlas. The components that form part of the internal infrastructure are hosted by Accept Systems or managed by Accept itself.

Microsoft Azure
Various resources in Microsoft Azure are used to host Accept's SBR solutions for affiliated parties and end users. Microsoft Azure is a leading cloud platform that offers a wide range of high-quality digital solution components. The resources used by Accept are hosted in the Azure region of Western Europe. The data centres that belong to this region are located on Dutch soil.

The Azure Kubernetes Service (AKS) is one of the most essential Azure components in Accept's external infrastructure. AKS represents a fully managed and scalable Kubernetes environment that is used to host all individual SBR solutions. An AKS Kubernetes cluster being 'fully managed' means that the maintenance and management of the cluster are handled by Microsoft Azure itself. This also includes the installation of system updates.

An AKS cluster consists of multiple Virtual Machines (VMs) that are combined into a Virtual Machine Scale Set (VMSS). A VMSS makes it possible to run several instances of a single application on multiple VMs at the same time. If there is an issue with one of the VMs, the application will still be accessible via the other VMs with minimal disruption of service. The adequate setup of the AKS ensures that both deploying a solution update and rolling back to a previous version occur without any downtime (rolling).

All external requests sent to Accept's AKS production cluster are monitored and secured using a connected Azure Application Gateway (AAG) with active Web Application Firewall (WAF) functionality before actually reaching the environment. If the WAF flags a request as potentially harmful, it will be preventatively blocked. The rules defined in the Core Rule Set (CRS) version 3.1 of the Open Web Application Security Project (OWASP) are used for this indication process.

MongoDB Atlas
Atlas is the MongoDB database platform that - together with Microsoft Azure - forms the heart of Accept's external infrastructure. All persistent data that are processed in Accept's production environment are stored in a scalable and fully managed MongoDB cluster. A MongoDB Atlas cluster being 'fully managed' means that the maintenance and management of the cluster are handled by Atlas itself. This also includes installing system updates, replicating data, encrypting data (at rest and in transit) and creating backups.

A MongoDB Atlas cluster consists of multiple nodes that are combined into a Replica Set. This structure means that all data in an Atlas cluster are stored in duplicate on all nodes that form part of the cluster in question. If there is an issue with one of the nodes, the data will still be accessible via the other nodes with minimal disruption.

Various Microsoft Azure resources are used for the hosting of Accept's Atlas clusters. Atlas is responsible for their generation and maintenance. The Azure components that form part of Accept's MongoDB Atlas clusters are hosted in the Azure region of Western Europe. The data centres that belong to this region are located on Dutch soil.

All data in Accept's Atlas clusters are structurally backed up in accordance with a fixed schedule and can be restored in little time if necessary. Access to the Atlas clusters is secured with a firewall and limited via IP restriction and verification of a user's username and password.

Accept Systems
The services of Accept Systems are used to host most of the components that are used internally by Accept's employees. Accept Systems is an independent organisation based in Wateringen that specialises in low-level IT consultancy.

III.2.2 Software

The overview below shows all in-scope solutions including the programming languages used and the platform on which the solution in question runs.

As the table shows, this report only concerns Accept's SBR solutions that are developed in Node.js, Angular or RUST. Although the accounting program Accept Financieel and the financial reporting tool Accept Rapportage are both still being actively maintained, they are out of the scope of this report.

The same goes for those SBR solutions that Accept developed in the past in Visual Dataflex. These are: the on-premise SBR Viewer.exe, the on-premise SBR Communicator.exe and the on-premise SBR Webserver.exe. These solutions are still being actively maintained, yet they are out of the scope of this report. For all three aforementioned out-of-scope on-premise SBR solutions (*.exe), alternative in-scope solutions are available in the form of a web service or application.

Name	Description	Programming Languages Used	Platform
SBR Viewer	Generic solution that allows users to quickly and easily consult and validate the contents of an SBR document. The clear manner of presentation ensures no specific knowledge of the complex SBR taxonomy is required.	Node.js Angular RUST	Linux Debian

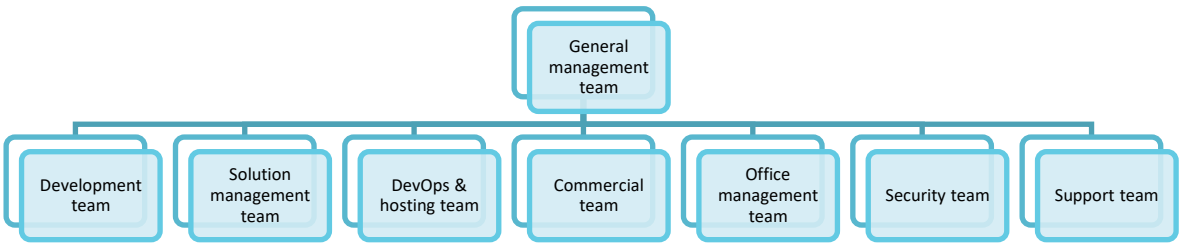
Name	Description	Programming Languages Used	Platform
SBR Processor (SBR Verwerker)	Web application that allows users to create, import, edit, validate and export SBR documents via a digital form.	Node.js Angular RUST	Linux Debian
SBR Signing	Web application that allows users to digitally sign a wide range of SBR documents. Depending on the type of document to be signed, an auditor's report can be included.	Node.js Angular	Linux Debian
SBR Communicator	Generic solution that can be used to send virtually all types of SBR documents. The application communicates directly with the requesting authorities (e.g. banks, the CoC (KvK), the UWV, Statistics Netherlands (CBS) and the Tax and Customs Administration (Belastingdienst).	Node.js Angular	Linux Debian
SBR Exchange server	Web server that allows clients to manage their own SBR communication. This makes it possible to send a large number of SBR documents via a single PKI government certificate (PKIoverheid-certificaat).	Node.js	Linux Debian
SBR Connector	Web application that makes it possible to link external data structures to SBR via an easy-to-understand user interface, without requiring any in-depth knowledge of SBR and/or XBRL.	Node.js Angular RUST	Linux Debian
SBR Converter	Web service that makes it possible to convert a data transport file (XML, JSON or CSV) that meets certain predefined requirements into a valid SBR document. This conversion process can also be performed in reverse to generate a data transport file based on an SBR document.	Node.js	Linux Debian
SBR Auditor	Web application that allows users to form a considered opinion of the contents, the presentation and the technical composition of an ESEF deposit that uses inline XBRL.	Node.js Angular RUST	Linux Debian
SBR Portal	Web application that can be used to activate and access a wide range of SBR solutions, depending on the client's wishes.	Node.js Angular	Linux Alpine
SBR Workflow	Generic digital platform in which various (SBR) processes can be handled sequentially.	Node.js Angular	Linux Debian

III.2.3 People

Accept is a relatively small organisation with fifteen to twenty permanent employees or self-employed staff. The company has a flat and flexible organisational structure in which internal and external responsibilities are divided between eight functional teams. In practice, the distinction between the various teams is relatively fluid. For example, an employee may perform tasks for various teams at any given time.

The General management team plays an essential role in the realisation and execution of the services, the risk management and the information security. The team charts the organisation's

overall course and holds final responsibility for its business operations. All other teams report to the General management team and have the opportunity to communicate directly with the General management team if necessary.



Accept's organisational structure

Responsibilities per team
What follows is a general description of (the primary responsibilities of) each team:

- **General management team:** holds final responsibility for the organisation's business operations, charts the organisation's overall course and is responsible for the recruitment and hiring of new employees.

- **Development team:** focuses on the (further) development of new and existing solutions and collaborates closely with the Security team and the Solution management team.

- **Solution management team:** decides how an application is to be developed further (course), taking into account the client's wishes.

- **DevOps & hosting team:** responsible for the launch of updates and the setup and structure of the various components that form part of the production environment and the various development/acceptance environments (development, test, stage, preproduction).

- **Commercial team:** focuses on the recruitment of new clients, price setting and contract negotiations.

- **Office management team:** is responsible for human resource (HR) management and handles a variety of administrative tasks.

- **Security team:** oversees compliance with the security policy and procedures and is responsible for (the setup and maintenance of) internal and external security measures.

- **Support team:** is responsible for supporting end users and external parties who have questions about how to use the software or who have encountered a problem with one of Accept's solutions.

III.2.4 Procedures

Accept has implemented various procedures that contribute to the security, performance and availability of its solutions and the systems on which these solutions are active. All policy documents and procedures are internally available to employees on Accept's intranet (SharePoint). These documents are periodically reviewed and amended if necessary.

Access, authentication and authorisation
Accept has implemented an access policy that defines the applicable rules regarding access to its various in-scope systems and solutions. The number of Accept employees who are authorised to launch updates or make other changes to the production environment is kept to an absolute minimum.

In order to launch updates or make other changes to Accept's production environment, an authorised member of the DevOps & hosting team must be connected to Accept's internal office network (attack surface reduction). This connection can be established indirectly via VPN or on site at the office in Etten-Leur. Furthermore, they must periodically authenticate themselves by completing a multi-factor authentication procedure (MFA), which requires the team member to enter their username and password and go through an additional authentication step (receiving an access code via a text message or confirming the login request via a smartphone app).

Change management
An overarching DTAP procedure is available for assessing, implementing, testing, releasing and registering changes. The abbreviation DTAP stands for 'Development, Testing, Acceptance and Production.' This procedure is intended to help Accept's employees implement changes in a correct and uniform manner. Depending on their qualification, changes are registered in the form of issues in GitHub Enterprise's DTAP repository and followed up on by the Development team and/or the DevOps & hosting team. An expedited hotfix procedure is in place for changes with limited impact.

Before a change is taken to production, it will be extensively tested. Depending on the change qualification, this testing process consists of various stages. Following the (successful) implementation of a change, the issue created for the change in question will be closed. If necessary, the relevant stakeholders will be informed.

Release management
Accept's in-scope solutions and systems are regularly expanded and updated. To safeguard the quality, security and availability of new versions, Accept has implemented a structured release procedure. This process forms part of the overarching DTAP procedure. The DevOps & hosting team is responsible for compliance with the release procedure to ensure that only authorised and tested updates are implemented in the production environment. The adequate setup of the production environment (AKS) ensures that both deploying a new version and rolling back to a previous version occur without any downtime.

Incident management
An incident management procedure is available for reporting, evaluating, handling and registering (security) incidents and (potential) data leaks. This procedure is made available to all employees via Accept's intranet (SharePoint) and is intended to help them respond to incidents in a correct and standardised manner. Incidents are registered in the form of issues in GitHub Enterprise's incident repository and - depending on their impact - followed up on within the time frame defined in the agreement that the client has signed.

Monitoring and capacity management
All external requests sent to Accept's production environment are monitored and logged using a Web Application Firewall (WAF). If the WAF flags a request as potentially harmful, it will be preventatively blocked. Improvements to the security of the production environment are periodically implemented based on the collected information (e.g. request duration, request size, http response code, http method, client IP, etc.).

In addition to external requests, the capacity utilisation of the individual in-scope solutions and systems is also monitored and logged. If the available capacity of one of the system components exceeds a predefined limit, an automated alert will be sent via email to the members of the DevOps & hosting team. After conferring with the General management team, they will then initiate an appropriate up- or downscaling measure.

III.2.5 Data

All persistent data that are processed in Accept's production environment are replicated and stored in a MongoDB Atlas cluster. These data include the logs of web applications, services and systems, user data and user profile data. Accept handles all these data with the utmost care and confidentiality. The principle of least privilege is used to control access to these data. This means that only employees or systems that were explicitly granted permission may access these data.

The contents of the Atlas cluster are structurally backed up in accordance with a fixed schedule and can be restored in little time if necessary. All data traffic to and from the Atlas cluster (in transit) is encrypted using Transport Layer Security (TLS) v1.2 or higher. Lastly, all data are encrypted when stored in the cluster (at rest). The encryption method used for this is 256-bit AES.

Logs of web applications, services and systems
All external requests sent to Accept's production environment are logged. The same goes for the capacity utilisation and the API requests that are processed by Accept's solutions and systems. When registering an API request, the following information is recorded: the API user in question, the name of the requesting party (intermediary), the CoC number (identifier), the time of the request, the file size and the entry point. Under no circumstances will the logs of web applications, services or systems contain any substantive XBRL data.

User data
The term ‘user data’ refers to the records that a user has created in or using one of the SBR solutions developed by Accept. Think of e.g. a specific workflow in the SBR Workflow app, a document in the SBR Verwerker, a record in the SBR Signing app, a report in the SBR Auditor or a submitted SBR document in the SBR Communicator (web application). To store user data, a separate database is used per client. The sensitive contents of all these client databases are encrypted using a unique encryption keypair (mechanism = mongoose encryption/crypto (Node.js)). By design, this structure prevents users from ‘environment x’ from accessing the contents of the database of ‘environment y,’ e.g. in the event of a configuration error.

For the in-scope solutions that do not use persistent data, such as the SBR Viewer, the SBR Converter, the SBR Exchange server and the SBR Communicator (web service), only general monitoring data are being stored. In these cases, the processed data transport file or SBR document is only temporarily available in the working memory of the solution in question (= stateless).

User profile data
This category includes information related to individual user accounts, including access rights and user activity. The user profile data also includes passwords. Within Accept's in-scope solutions and systems, user passwords are additionally and irreversible encrypted using a cryptographic salt. The encryption method used for this is pbkdf2Sync. This makes it impossible for anyone - even Accept's own employees - to deduce the entered value.

III.3 Relevant aspects of internal control

This section provides information about the manner in which the following five components of internal control - as defined by the American Institute of Certified Public Accountants (AICPA) - have been implemented by Accept:

1. **Control Environment:** sets the tone of an organisation, 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:** policies and procedures that help ensure 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

The effectiveness of control measures is inextricably tied to the integrity and ethical awareness of the employees responsible for the implementation of and compliance with these measures. Accept's General management team is fully aware of this and therefore considers the integrity and ethical awareness of its employees to be of the utmost importance.

The organisation's ethical core values are recorded in the staff handbook. At the start of their employment, employees are required to sign a confirmation form that states they were given access to this document and that they understand the responsibility they have to comply with the code of conduct outlined in the handbook. Furthermore, employees are invited to take part in a security awareness training once per year. This training gives them insight into their obligations and responsibilities with regard to information security.

In addition to the integrity of employees, the organisational structure also plays a significant role in the determination, planning and realisation of Accept's goals. Accept has a flat and flexible organisational structure in which internal and external responsibilities are divided between eight functional teams. An organisational chart with role descriptions is available that outlines the responsibilities of these teams, as well as the (limited) hierarchical relations and the reporting structure. This organisational chart is made available to all employees via Accept's intranet (SharePoint). This ensures everyone understands what their tasks and responsibilities are and knows what is expected of them and their colleagues.

Accept's flat organisational structure allows employees to quickly and directly confer with each other and make decisions. A positive consequence of this is that (security) incidents or bugs are generally resolved in a short time frame. The short lines of communication between the General management team and the various subordinate teams make Accept a highly effective and productive organisation.

As a supplier of solutions for handling a wide range of SBR processes, it is incredibly important to retain and attract competent and knowledgeable staff. The composition and structure of an XBRL taxonomy or the SBR standard in general are relatively complex affairs. Learning processes regarding SBR, XBRL and XBRL taxonomies take a lot of time and effort. For that reason, only a limited number of people actually possess the requisite knowledge. To verify whether new potential employees possess the required qualifications, Accept has implemented a standardised recruitment procedure. A limited background check forms part of this process.

III.3.2 Risk assessment process

Identifying, evaluating and managing risks to the services provided by Accept and its goals is of essential importance to the organisation. The organisation's (current) goals and the associated risks are continuously assessed, revised and (if necessary) addressed during digital or physical meetings in which members of the various functional teams take part. The General management team will generally take the initiative to organise these meetings and ensures that the members of other subordinate teams are informed about possible new goals or changes to the company's existing services. This approach ensures that everyone understands where potential risks may manifest (in the future).

At least once per year, the General management team will perform an extensive formal risk analysis. Optionally, this can be done in collaboration with members of other subordinate teams (e.g. the Security team, the Office management team or the DevOps & hosting team). As part of this risk analysis, all current risks including the risk of fraud are identified and (re)evaluated. Risks are identified using a number of main categories, namely: end users and API users (1), employees and self-employed staff (2), web services and applications (3), digital infrastructure DTAP environments (4), digital infrastructure internal (5), office environment (6) and business continuity, integrity and organisation (7).

Within each of these categories, both internal and external risk factors are taken into consideration. The following table contains a few examples of this. For each factor, it has been indicated in what risk category it manifests:

Examples of internal risk factors	Cat.	Examples of external risk factors	Cat.
Incorrect use of solutions	1	Technological developments	3,4
(Too) limited quality of staff	2	Changing needs of clients	3,4,7
System disruptions	4,5	Changes to laws and regulations	3,4,7
Security vulnerabilities	3,4,5	Natural disasters	4,5,6
Faltering performance of solutions	1,3	Economic changes	6,7
Possibilities of fraud	2		

Once a risk has been identified, the General management team will determine what risk strategy, follow-up and control measures to utilise. Identified risks can be handled in a number of ways. Accept employs the following strategies: accept, manage, avoid and transfer. Managing a risk involves mitigating the risk in question by reducing the odds of its occurrence or minimising its impact. This can be done by amending an existing control measure or by implementing a new one.

III.3.3 Control activities

To ensure that identified risks to Accept's services and goals are adequately dealt with, various control activities have been implemented. These activities vary in terms of their structure and pertain

to different components within the organisation. Depending on the component to which a control activity pertains, a different functional team is responsible for its execution.

General control activities over technology

A number of general control activities have been implemented to ensure that the technology used by Accept functions properly and contributes to the realisation of the organisation's goals and service obligations. This category of control activities includes both automated and manual control measures. The responsibility for the implementation and functioning of these control activities generally lies with the DevOps & hosting team, the Security team or the Solution management team. The control activities in this category concern e.g. the following aspects:

- **Monitoring:** all external requests sent to Accept's production environment are monitored and logged. The Security team and the DevOps & hosting team use these data to implement improvements to the security, availability and performance of the production environment. In the event of an incident, the Security team can also use the collected data to uncover the cause of the incident in question.

- **Capacity monitoring:** the capacity allocation of the individual components that form part of Accept's production environment is monitored and logged using various integrated systems. If the available capacity of one of these components exceeds a predefined limit, the DevOps & hosting team will take measures to scale up.

- **Updating and patching:** in order to comply with Accept's availability and security obligations, the DevOps & hosting team will keep all systems that form part of the IT infrastructure up to date. To this end, the team will go through a standard procedure every month. Keeping the systems that are managed by Accept's service providers up to date is the responsibility of the respective external parties. The DevOps & hosting team oversees this process.

- **Platform security:** without exception, the components that form part of Accept's production environment are hosted by Microsoft Azure and MongoDB Atlas. The control measures implemented by these primary service providers for the purposes of security, availability and confidentiality are inspected and evaluated every year by the Security team and the Solution management team. This inspection is conducted with the review of the SOC2 type II reports of the service providers in question.

- **Availability management:** in order to comply with the applicable availability requirements, redundancies are in place for the essential components that form part of the digital infrastructure of Accept's production environment. Every year, the DevOps & hosting team will assess to what extent the existing production environment still meets the applicable requirements and current standards.

- **Backup:** all persistent data that are processed in Accept's production environment are replicated and stored in a fully managed MongoDB Atlas cluster. All data in this cluster are structurally backed up in accordance with a fixed schedule and can be restored in little time if necessary.

- **Authentication:** all external parties who access Accept's solutions system-to-system will be given a unique system account (with username and password) for this purpose. To prevent unauthorised access to the environments of Accept's clients, users must authenticate themselves with a unique username and password. The Security team is responsible for the aforementioned security measures and periodically verifies that these all function as intended.

Policies and procedures
In addition to the aforementioned group of general control activities that concern the technology used by Accept, certain policies and procedures are in place to ensure that Accept's risks are adequately managed. These policy documents and procedures are made available to all employees via Accept's intranet (SharePoint).

The General management team holds primary responsibility for compliance with these policies and procedures within the organisation. In the event of non-compliance with the procedures or guidelines outlined in policy documents, the members of the General management team can take corrective measures or impose sanctions. What follows is an overview of Accept's primary policy measures and procedures:

- **Start- and end-of-employment procedure:** a fixed procedure is in place for the start and end of employees' employment. As part of the start-of-employment process, it is verified whether a candidate possesses the requisite qualifications. Furthermore, employees are required to sign a confidentiality agreement and a confirmation form which states that they were given access to the staff handbook and the information security policy. As part of the end-of-employment process, all access rights of the employee in question are revoked.

- **DTAP procedure:** an overarching DTAP procedure is available for assessing, implementing, testing, releasing and registering changes. The abbreviation DTAP stands for 'Development, Testing, Acceptance and Production.' This procedure is intended to help employees implement changes in a secure, correct and uniform manner. By following every step of the DTAP procedure, the risk of bugs or other flaws is mitigated and only authorised and tested changes are implemented in the production environment.

- **Incident management procedure:** an incident management procedure is available for reporting, evaluating, handling and registering (security) incidents and (potential) data leaks. This procedure is intended to help employees handle incidents in a correct and uniform manner. Depending on their impact, incidents are followed up on within the time frames specified in the agreement signed by the client. Incidents are registered and followed up on via a ticket system.

- **Information security policy:** a general information security policy is available. This document outlines a wide range of control measures that Accept uses to safeguard the security, availability and confidentiality of information and data in a general sense. Among other things, the policy document contains provisions pertaining to staff security, the management of company resources, access control, cryptography, physical security, operational security, communication security and supplier relations.

- **Disaster recovery plan:** to recover from situations in which a disaster occurs, Accept has drawn up a disaster recovery plan. This document describes the most critical scenarios to ensure that adequate measures can be taken in the event of a disaster and the affected systems can be restored as soon as possible. The scenarios described in the disaster recovery plan are tested every year and revised if necessary.

III.3.4 Information & communication

To ensure employees carry out their internal and external responsibilities, it is essential to have access to relevant information. Accept has set up a number of systems in which various streams of information are brought together, processed and made available to the teams for whom the information in question is of value. Several of these information systems function automatically. In these instances, relevant data are mechanically retrieved and processed into valuable information

without any input from employees. This is possible with e.g. an API interface. Among these automatic information systems are:

- The integrated systems that are used to monitor the capacity utilisation of the production environment.

- The Logs analytics system that is used to analyse all external requests sent to the production environment.

- The dashboard that provides insight into the various order requests that are sent to the production environment via a system account.

In addition to these automated information systems, manually recorded information is also used for internal control purposes. This category includes information about policy, processes or developments within the organisation itself (internal information), as well as information about external events such as legislative and regulatory changes or the release of a new XBRL taxonomy (external information).

Internal communication
Within Accept, both the General management team and the other subordinate teams have a number of ways to manually record information and share it with colleagues, such as: GitHub Enterprise (for the registration of changes and incidents), the Intranet (SharePoint) (for sharing various policy documents and procedures), Microsoft CRM (for the registration of client communication), the chat functionality of Microsoft Teams and email.

At least once per year, the General management team will organise a security awareness training for all employees. During this training, every member of the organisation is reminded of their internal and external responsibilities and the importance of the implemented control measures. Despite the hierarchical relationship that exists between the General management team and the other teams, the subordinate teams have the option to communicate directly with the General management team, if necessary. This is done to ensure the General management team remains in touch with what is happening within the organisation.

External communication
Similarly, a number of channels are available for the communication with clients and other external parties such as partners and suppliers. These means of communication are used to e.g. ensure that Accept's clients are aware of their responsibilities with regard to using the provided SBR solutions. Furthermore, clients are given the opportunity to share their wishes and (user) experiences. The General management team takes this information into account when considering future developments. External communication takes place via e.g. manuals and API documentation, physical and digital feedback sessions, the helpdesk (available via telephone and email) and the website.

III.3.5 Monitoring of controls

Accept conducts various monitoring activities to monitor the quality and performances of the internal control measures it has implemented. Among these activities are: evaluating the control design, verifying a measure's effectiveness and implementing possible improvements. The majority of Accept's control measures are continuously or periodically monitored. Furthermore, a control measure may be evaluated separately. A combination of both approaches is also possible.

Continuous monitoring activities
What follows is an overview of the most important continuous monitoring activities carried out within Accept's organisation:

- All external requests sent to Accept's production environment are monitored and logged. At least once per year, the Security team and the DevOps & hosting team will perform a thorough analysis of the collected data. Based on their findings, they will implement improvements to the production environment if possible.

- Every year, the DevOps & hosting team will assess to what extent the existing production environment still meets the applicable requirements and current standards. As part of this assessment process, the production environment's performances, capacity, security and availability are evaluated. Afterwards, it is determined what modifications need to be implemented, if any.

- To identify possible security issues, an independent specialised party will perform a penetration test on Accept's production environment at least once per year. The Security team will assess the results of this test. After this evaluation, the Development team (possibly in collaboration with the DevOps & hosting team) will be tasked with resolving any critical and high-risk issues.

- An overall Common Vulnerabilities and Exposures (CVE) scan will be performed at least once per year. The Security team will assess the results of this scan. After this evaluation, the Development team will be tasked with resolving any critical issues.

- The control measures implemented by Accept's primary service providers (Microsoft Azure and MongoDB Atlas) for the purposes of security, availability and confidentiality are inspected and evaluated every year by the Security team and the Solution management team. If any deficiencies are found, these will be discussed with the General management team. They will then decide what follow-up measures should be taken.

- Every year, the General management team will conduct a risk assessment. Among other things, the production environment, the web services and applications and the business organisation are analysed as part of this assessment. Afterwards, the General management team will decide what risk strategy, follow-up and control measures to utilise.

Separate evaluations
In a number of cases, it may be necessary to evaluate an internal control measure separately. This may be the case following e.g. an organisational change, changing demands from clients, the introduction of a new law or regulation or the launch of a new solution or functionality. The separate evaluation of a control measure is generally initiated and performed by the members of the team that is directly involved in the execution of the control measures in question. During their evaluation, they assess the extent to which the control measure is adequate and whether there are any improvements that can be implemented.

Shortcomings
Any abnormal findings that come to light during an evaluation or the continuous monitoring activities are shared with the General management team. If it turns out that a control measure contains shortcomings, this will also be shared with the General management team. The General management team - possibly in collaboration with the Security team - will ultimately decide if and, if so, how the evaluated control measure is to be amended. Next, all teams involved in the execution of the control measure in question are informed. Implementing the change falls under the

responsibilities of the functional team that is directly involved in the execution of the control measure in question.

III.4 Complementary user entity controls

Accept's system was designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. This paragraph describes the complementary user entity controls that are necessary to achieve the control objectives stated in the description of Accept's system and also identifies the control objectives to which the complementary user entity controls relate.

User auditors should determine whether user entities have established controls to provide reasonable assurance that:

- Appropriate security measures have been implemented on the hardware used by the end user.
- Appropriate security measures have been implemented on the internal digital infrastructure if a client opts to host and manage Accept's SBR solutions by itself.
- Appropriate security measures have been implemented on the overarching platform or system if a client opts to access Accept's SBR solutions system-to-system as a web service.
- User accounts are registered, managed and distributed in a secure and responsible manner.
- End users are aware of the applicable laws and regulations pertaining to SBR and XBRL and can therefore use the SBR solutions developed by Accept in a correct and secure manner.
- Any incidents, issues and risks related to the purchased solutions are immediately and transparently shared with Accept.
- Client's Azure Active Directory is configured securely and appropriately if the client opts to use Azure Active Directory as authentication system for Accept's SBR solutions.

III.5 Complementary subservice organisation controls

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

Accept's three subservice organisations are extensively described in sections III.1.3 and III.2.1 of this report. These are: Microsoft Azure, MongoDB Atlas and Accept Systems. The components that form part of Accept's external infrastructure (accessible to clients) are exclusively purchased from and hosted by Microsoft Azure and MongoDB Atlas. The components that form part of the internal infrastructure (only accessible to Accept employees) are purchased from and hosted by Accept Systems or managed by Accept itself. The table below presents an overview of the Trust Services criteria that Accept expects to be covered by controls implemented by the aforementioned subservice organisations.

Criteria	Definition	Microsoft Azure	MongoDB Atlas	Accept Systems
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.	x	x	x
A1.2	The entity authorises, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	x	x	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	x	x	
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.	x	x	x
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorises new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorised.	x	x	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorised personnel to meet the entity's objectives.	x	x	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	x	x	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	x	x	x
CC6.7	The entity restricts the transmission, movement, and removal of information to authorised internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	x	x	

Criteria	Definition	Microsoft Azure	MongoDB Atlas	Accept Systems
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.	x	x	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.	x	x	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	x	x	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		x	

Monitoring subservice organisations

The Security team and the Solution management team will conduct an annual audit to verify whether the aforementioned criteria are actually covered by controls implemented by the subservice organisations in question. For Microsoft Azure and MongoDB Atlas, this audit is performed using both organisations' SOC2 type II report. If any deficiencies are found, these will be discussed with the General management team. They will then decide what follow-up measures should be taken. Accept Systems currently does not (yet) have a SOC2 type II declaration or an ISO 27001 certification. In this instance, the presence of the applicable criteria is verified by requesting relevant information from the organisation's management.

IV. ATTACHMENT B - ACCEPT'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

IV.1 Service commitments

Accept does everything it can to safeguard the security, availability and confidentiality of its SBR solutions and the data processed by these solutions. To accomplish this goal, Accept makes service commitments to its customers and has established requirements to its system as part of its service delivery. The security, availability and confidentiality commitments to Accept's clients are documented and communicated via General Agreements, Terms and Conditions, Service Level Agreements and Data Processing Agreements. To fulfil the aforementioned commitments, Accept has implemented effective controls. The operation of these controls is continuously monitored and improved, if necessary.

IV.2 System requirements

Accept has designed and implemented a system to deliver its SBR solutions to its customers in a secure, effective and appropriate way. This system is extensively described and explained in section III.2 of this report. The internal policies of Accept's system are developed in consideration of legal and regulatory obligations, to define Accept's organisational approach and system requirements. The delivery of Accept's services depends upon the appropriate internal functioning of system requirements defined by Accept to meet customer commitments. In order to meet Accept's systems requirements and customer commitments various controls, policies and procedures are implemented. Below is a list of the key measures:

- Policies and procedures regarding information security are documented and made available to all Accept employees.
- Robust authentication is enforced for both client environments and components that are part of Accept's in-scope systems.
- A change management procedure is in place to safeguard the quality, security and availability of new versions.
- An incident management procedure is in place for reporting, evaluating, handling and registering (security) incidents and (potential) data leaks.
- A wide range of security measures are in place to protect client data, both at rest and in transit.
- A penetration test and an overall Common Vulnerabilities and Exposures (CVE) scan are performed periodically in order to identify possible security issues.
- A wide range of monitoring data is collected from client environments and Accept's in-scope systems to analyse and improve system performance, resource utilization and potential security vulnerabilities.