TECHNICAL & ORGANIZATIONAL MEASURES FOR DATA PROTECTION

The objective of this document is to provide an overview of the technical and organizational measures in place in Questback to ensure the protection of personal data processed in Questback Group (hereinafter: Questback). Please note that this is not a complete documentation on all Questback Technical & Organizational measures.

Document owner: Niklas Olsson
Document version: 1.71
Confidentiality classification: Public

Table of Contents

1. Introduction 4
1.1 Software as a Service 4
1.2 Questback data centres 4
1.3 Questback offices 4
1.4 Fulfilment of the General Data Protection Regulation (GDPR) 5
2. PHYSICAL ACCESS CONTROL 5
2.1 Data centres in Frankfurt, Germany 5
2.2 Questback offices 6
3. DATA ACCESS CONTROL 6
3.1 Data centres in Frankfurt, Germany 6
3.2 Questback Offices 7
3.3 Software / Questback Essentials 7
4. Logging of the processing of Personal data 7
4.1 Data centres in Frankfurt, Germany 7
4.2 Software / Questback Essentials 7
5. TRANSFER CONTROL 7
5.1 Data centres in Frankfurt, Germany 7
5.2 Offices and Software 8
6. INPUT CONTROL 8
6.1 Data centres in Frankfurt, Germany 8
6.2 Questback offices 8
6.3 Software / Questback Essentials 8
7. ASSIGNMENT CONTROL 8
7.1 Data centres 8
7.2 Questback Offices 8
7.3 Software / Questback Essentials 8
8. Confidentiality control 9
8.1 Data Centres 9
8.2 Questback offices 9
8.3 Software / Questback Essentials 9
9. Integrity control 9
9.1 Data Centres 9
9.2 Questback offices 9
9.3 Software / Questback Essentials 9
10. AVAILABILITY CONTROL 9
10.1 Data centres in Frankfurt, Germany 9
10.2 Questback Offices 10
10.3 Software / Questback Essentials 10
11. Resilience of processing systems and services 10

11.1 Data Centres in Frankfurt, Germany 10
11.2 Questback Offices 10
11.3 Software / Questback Essentials 10
12. SEPARATION RULE 10
12.1 Software / Questback Essentials 10
13. Pseudonymisation and encryption of personal data 11
13.1 Data Centres in Frankfurt, Germany 11
13.2 Software / Questback Essentials 11
14. Retention and deletion 11
14.1 Data centres in Frankfurt / Germany 11
14.2 Software / Questback Essentials 11
15. Incident management 11
15.1 Detection 11
15.2 Communication 12
15.3 Notification 12
16. Internal control 12
16.1 Monitoring 12
16.2 Security Audits 12

1. INTRODUCTION

1.1 Software as a Service

Questback provides the software Questback (also known as Questback Essentials) as a Service to its customers.

Questback is a leader in experience management solutions with customers world-wide using its solutions for data collection and analysing as well as acting on business-critical information. The company was founded in 2000 and is headquartered in Oslo, Norway.

Questback makes its software platforms for feedback management available to its customers as software as a service (SaaS) from externally operated data centres, as described in this document.

Personal data relating to Questback's customers, and respondent data collected and processed as part of the feedback process, is processed in accordance with Questback's Group Code of Privacy and the descriptions in this document.

In this document, the sections named "**Software**" demonstrate how protection of personal data is ensured in Questback's Software.

This document is continuously updated and gives an overview but not a complete documentation of Questback's organizational and technical measures.

This document has been updated to only provide information on the Questback / Questback Essentials product together with significant updates in languages for clarity as of version 1.7.

1.2 Questback data centres

Questback makes its software platform for feedback management available to its customers as software as a service (SaaS) from data centres in Germany operated by Oracle.

In this document, the sections named "**Data Centres**" demonstrate how protection of personal data in Questback's software is ensured in accordance with these standards implemented at **Oracle** data centres. For more detail on how Questback is hosted in Oracle's data centres, please refer to the document 'Questback hosting in Oracle Cloud Infrastructure' that can be provided on request.

1.2.1 Oracle

Processing in software platforms in the data centres in Frankfurt, Germany - personal data of Questback's customers as well as respondent data collected and processed as part of the feedback process are hosted on external servers in Oracle controlled data centres in Frankfurt.

Oracle holds various certificates and attestations. Exact details about existing certificates can be found on the information pages provided by Oracle at https://www.oracle.com/cloud/cloud-infrastructure-compliance/.

Data Centre provider	Address	Country
Oracle Deutschland B.V. & Co. KG	Riesstraße 25, 80992 München	Germany

1.3 Questback offices

Processing in Questback's Offices and systems - Personal data relating to Questback's employees, customers, visitors and suppliers is processed in accordance with Questback's internal privacy policies.

In this document, the sections named "**Questback offices**" demonstrate how protection of personal data is ensured in Questback's offices and systems.

Further information about the structure of the data storage process as well as contact information concerning the data protection officers of Questback group are available on Questback.com.

Name of Questback entity	Office address	Country
Questback AS	Bogstadveien 54, 0366 Oslo	Norway

Questback OY	Keilaranta 1, 02150 Espoo	Finland
Questback Sweden AB	Sveavägen 59, 113 59 Stockholm	Sweden
Questback Nederland B.V.	Radarweg 29, 1043NX Amsterdam	Netherlands
Questback UK		United Kingdom
Questback Deutschland GmbH	Kurfürstendamm 30, 10719 Berlin	Germany

1.4 Fulfilment of the General Data Protection Regulation (GDPR)

This document describes how Questback fulfils its obligations for processing Personal data on behalf of its customers in accordance with the requirements in the GDPR for Technical and Organizational Measures. The relevant requirements are found in the GDPR articles 5, 17, 19, 24, 25, 28, 29, 32, 33, 35 and 39.

The technical and organizational measures described in this document are set out by Questback, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of natural persons, ref. GDPR article 32.

The data centre operator (Oracle) provide further information in various formats.

1.4.1 Oracle

Oracle has implemented and will maintain appropriate technical and organizational security measures for the processing of personal data to prevent the accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to personal data.

These security measures govern all security areas applicable to the Services, including physical access, system access, data access, transmission and encryption („Encryption in Transit“ & „Encryption at Rest“), input, data protection, data separation and security oversight, enforcement and other security controls and measures.

Oracle provides extensive information through the Oracle Web site.

https://www.oracle.com/applications/gdpr/

2. PHYSICAL ACCESS CONTROL

This section describes Questback's measures that are in place to prevent unauthorized individuals from physically accessing the data processing systems that are employed to process or use personal data:

2.1 Data centres in Frankfurt, Germany

Oracle's layered approach to the physical security of data centres starts with the building itself. The company builds and works with partners to build data center facilities durably with steel, concrete, or comparable materials, and that are designed to withstand impact from light-vehicle strikes. The data centres use perimeter barriers to secure site exteriors, and security guards and cameras monitor vehicle checks. Every person who enters a data center must pass through security checkpoints at the site entrances. Anyone who doesn't have a site-specific security badge must present government-issued identification and have an approved request that grants them access to the building.

Employee and third party access to the data centres

All employees and visitors must always wear visible official identification badges. All sites are staffed with security guards. Additional security layers between the site entrance and the server rooms vary depending on the building and risk profile. Server rooms themselves are required to have more security layers, including cameras, two-factor access control, and intrusion-detection mechanisms. Physical barriers that span from the floor to the ceiling create isolated security zones around server and networking racks. These barriers extend below the raised floor and above the ceiling tiles, where applicable. All access to server rooms must be approved by authorized personnel and is granted only for the necessary time period. Access is audited, and access provisioned within the system is reviewed periodically and updated as required. For more details, please refer to Oracle, https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

2.2 Questback offices

2.2.1 All offices

All Questback offices adhere to the requirements in the IT Governance Policy. The following sections describe some specific elements in place for each office.

2.2.2 Oslo, Norway

- The entrance doors are equipped with a key card access control system and surveillance camera. Entrance door are opened by employee key cards while office doors require key card and employees personal pin code. The Office Manager has the list of activated keys used by employees.
- Allocation and collection of key cards are done in accordance to Questback's onboarding and offboarding routines.
- Visitors must report to an employee with which they have an appointment and are accompanied in the building by an employee.
- Server room has surveillance cameras and key card access control system. Entrance to the server room requires personal pin code.

2.2.3 Stockholm, Sweden

- The building entrance doors are equipped with an rfid reader and opened with rfid chip. The office doors are opened with rfid chip and mechanical key.
- Allocation and collection of key cards are done in accordance to Questback's onboarding and offboarding routines.
- Visitors must report to an employee with which they have an appointment and are accompanied in the building by an employee.

2.2.4 Helsinki, Finland

- Visitors must report at the reception or to an employee with whom they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Finance Manager has the list of activated keys used by employees.
- Allocation and collection of key cards are done in accordance to Questback's onboarding and offboarding routines.
- Quesback has cameras located inside the office at the entrance doors.

2.2.5 Amsterdam, Netherlands

- The entrance doors are equipped with a keycard access control system and surveillance camera. Entrance door are opened by employee keycards while office doors require keycard and mechanical key. The Office Manager has the list of activated keycards as well as mechanical keys used by employees.
- Allocation and collection of key cards are done in accordance to Questback's onboarding and offboarding routines.
- Visitors must report to an employee with which they have an appointment and are accompanied in the building by an employee.

2.2.6 Berlin, Germany

- Visitors must report at the reception or to an employee with which they have an appointment, and are accompanied in the building by an employee.
- The entrance doors are equipped with a digital locking system, opened by employee key cards only. The Office Manager has the list of activated keys used by employees.
- Allocation and collection of key cards are done in accordance to Questback's onboarding and offboarding routines.

3. DATA ACCESS CONTROL

This section describes Questback's measures, including identification and authentication, that are in place to prevent unauthorized persons from accessing and using data processing systems, and from accessing and using removable devices.

3.1 Data centres in Frankfurt, Germany

Oracle employees have access to personal data only to the extent necessary to carry out the processing. Oracle imposes confidentiality obligations on employees who have access to personal information. Oracle employees have no access to the data stored in Questback's 'tenant' inside Oracle's hosting solution.

Access to systems by employees (IT staff) is role-based. Access is encrypted (SSH, SFTP, SSL) via VPN software with 2-factor authentication. Access is logged (keystroke logging).

3.2 Questback Offices

All Questback offices will adhere to the requirements in the Questback Group IT Governance Policy, where it is stated that portable storage devices should be encrypted.

Authentication to the operating system and the applications is by means of individual user IDs and passwords. Employees are required to lock the workplace client whenever they leave the room (“Clear Screen”).

Employees also are required to keep their passwords secret and not to divulge them to anybody, even for support purposes. There are password conventions that are implemented technically (system configuration) and organizationally (password policy). According to these conventions, all passwords must fulfil the defined minimum requirements.

3.3 Software / Questback Essentials

Customers can only gain access to and authentication for the licensed software via user-specific accounts.

- The password must be changed after the first login
- Account names are not case sensitive
- Passwords are case sensitive
- Passwords must have at least 8 characters, but no more than 20
- Passwords must contain characters from all of the following three groups: lower case letters (a-z), capital letters (A-Z) and numbers (0-9)
- Other printable ASCII characters are accepted, but not required
- Passwords may not contain spaces
- To protect itself against brute-force attacks (10 failed attempts within 30 minute window), the system blocks access to the user account, until opened by Questback support or responsible user in the account
- Passwords are not saved as plain text

4. LOGGING OF THE PROCESSING OF PERSONAL DATA

This section describes Questback’s measures for logging and documenting the access to and processing of personal data processed on behalf of its customers.

4.1 Data centres in Frankfurt, Germany

Data transmission is logged and there are alerts connected to behaviour such as sudden high loads on a server. Scope of the internet logs: Meta Data of internet traffic. (IP address of the connected client, the called domain, date, time and time zone from which the connection came, the concrete request of the client in plain text, the method used, the requested data, the protocol used, the URL called up, the referrer, the HTTP status code returned on the request, the size of the data transmitted, measured in bytes, operating system and version, type of client, browser and version)

4.2 Software / Questback Essentials

Activities, of both Customers and Questback employees, are logged in the system. Customer activity is logged to LogActivity and Questback (support/QBAdmin) activity is logged to QBAdmin logs. Content of the LogActivity are ID, TIMESTAMP, LOGGERNAME, MESSAGE, PARAMETERS, SESSIONID, ACCOUNTID, USERID, UPDATEDUSERID, QUESTID, CONTEXTID, EVENTID, TEMPLATEID, RESPONSEID, INVITATIONID, REMINDERID, FOLDERID, REPORTID. Where contextid and eventid describes what the log is about. Content of the QBAdmin logs are: ADMINUSERID, LOGTYPEID, ACCOUNTID, USERID, QUESTID, ID, DESCRIPTION, TIMESTAMP. Where logtypeid describes the log entry. Some of the LogActivity and QBAdmin logs are available in QBAdmin. The software do not offer an UI of these activity logs in the Essentials service.

5. TRANSFER CONTROL

This section describes Questback’s measures ensuring that personal data cannot be read, copied, changed, or deleted during electronic transmission, transport or storage on data storage media and for checking and determining at which points personal data are to be transferred by means of data transmission equipment:

5.1 Data centres in Frankfurt, Germany

Encryption of data during transmission ("encryption in transit")

Access to databases at **Oracle** is encrypted and via SSH (Secure Shell) and VPN tunnel. Redundancy is in place for all data lines to the Internet, and they are implemented as BGP (Border Gateway Protocol). The entire network infrastructure (firewalls, switches etc.) has complete redundancy in place. Firewalls and DMZ settings are defined by BSI/ISO standards. Any access by Questback employees (especially from Support or Development) to customer data hosted by the data centre for the purpose of administration of the Essentials surveys utilizes TLS encryption (PCI compliance). Logging of data transmissions and ongoing evaluation of the logs.

Encryption for resting data ("encryption at rest")

All data in the Frankfurt data centres at **Oracle** are stored in encrypted form when idle.

5.2 Offices and Software

Data access to all the software components of the survey platform can be provided using TLS encryption. The transmission of personal data is secured using HTTPS/TLS encryption.

6. INPUT CONTROL

This section describes Questback’s measures ensuring that whether and by whom personal data has been entered, changed, or deleted in the data processing systems can be checked and determined:

6.1 Data centres in Frankfurt, Germany

The employees of the data centres of Oracle, who are responsible for remote maintenance measures can neither enter data into the data processing systems nor view, change nor delete personal data of Questback customers.

6.2 Questback offices

Questback offices adhere to the requirements in the IT Governance Policy.

All employees sign a confidentiality clause as an integral part of their employment contracts, hereunder a commitment to maintaining data secrecy, which protects clients even after the employees’ job contracts are terminated or expire. A ticket system in the support and administration area ensures that all tasks are completed correctly and on time. The contractor’s employees are supported by a directory service and may only access such data as is needed for their work within the framework of the respective task area and field of activity.

6.3 Software / Questback Essentials

All activity in the system is stored in an Activity Log in the database. The associated date, time, user, and activity is logged. This log is never deleted.

7. ASSIGNMENT CONTROL

This section describes Questback’s measures ensuring that personal data which are processed on behalf of a client can only be processed in accordance with the client's instructions.

7.1 Data centres

Questback will audit the respective security concepts of providers. Written contracts with the Data Centres are in place to ensure the maintaining of data protection.

At no time do the cloud provider Oracle process personal data without a contract. All employees are subject to confidentiality agreements (NDAs).

7.2 Questback Offices

All Questback employees adhere to Questback privacy policies and receive regular training on how to protect personal data. The assessment of content in any Data Processing Agreement, or in instructions from client are part of such training.

Questback managers, and Questback employees who are in dialogue with customers, are under obligation to ensure that instructions are provided to relevant personnel and adhered to.

7.3 Software / Questback Essentials

When a customer’s subscription to any of Questback’s services is terminated or expired, the account will be deactivated and becomes non-accessible. Information collected through the service will be deleted according to our data retention policies.

8. CONFIDENTIALITY CONTROL

The GDPR section 32 defines confidentiality control as a requirement to ensure security of processing. This section describes Questback's measures ensuring confidentiality control.

8.1 Data Centres

Oracle's data centres, which are responsible for the storage and technical operation of the data, have no access to the data. The operators of data centres do not have an account on Questback's servers. Exceptions to this rule apply only to the creation of backups so that the backup software can back up the data. The backups are stored securely and documented and are subject to strict access rules. Backups are stored in encrypted form.

8.2 Questback offices

Questback offices ensures confidentiality through a variety of measures. This includes visitor management, strong account management, clean workplace rules, encrypted devices, and confidentiality agreements.

8.3 Software / Questback Essentials

Questback's software ensures confidentiality through a variety of measures. This includes access through strong user account management, use of certified data centres, availability of 2 factor authentication for customers, VPN with password protection for Questback administrators, option to mark data as personal inside the solution and overall encrypted transport over internet.

9. INTEGRITY CONTROL

The GDPR section 32 defines integrity control as a requirement to ensure security of processing. This section describes Questback's measures ensuring integrity control.

9.1 Data Centres

Oracle's data centres ensure integrity through a variety of measures. These include various national and international certifications, such as ISO27001 or SOC, which in their form maintain the integrity of all information processing systems and data, as well as encrypted backup tapes and encrypted transport over the Internet.

9.2 Questback offices

Questback offices ensure integrity through a variety of measures. This includes encryption of media, strong access controls and use of encrypted communication.

9.3 Software / Questback Essentials

Questback's software ensures integrity through a variety of measures. This includes ensuring of the integrity of the program modules via checksums/comparison against reference list, URL manipulation mechanisms, secure cookies, specific Web service rights and logging, continuous improvement of current codebase, file integrity checks, change audit logs and input validation controls.

10.AVAILABILITY CONTROL

The GDPR section 32 defines availability control as a requirement to ensure security of processing. This section describes Questback's measures ensuring that personal data is available, while preventing that it is not accidentally destroyed or lost, hereunder routines for backup and recovery.

10.1 Data centres in Frankfurt, Germany

Essentials application is configured to provide nearly full-time availability and it has redundant hardware and software that make it available despite failures.

Multiple components can perform the same task. The problem of a single point of failure is eliminated because redundant components can take over a task performed by a component that has failed.

Essentials resides in Frankfurt Oracle Cloud Infrastructure region - a localized geographic area composed of one or more availability domains (data centres). Frankfurt region has 3 availability domains and each availability domain has three fault domains. The redundancy of fault domains within the availability domains ensures high availability.

Availability domains are isolated from each other, fault-tolerant, and unlikely to fail simultaneously. They don’t share physical infrastructure or the internal availability domain network, so a failure that impacts one availability domain is unlikely to impact the others.

Fault domains let us distribute our instances so that they aren’t on the same physical hardware within a single availability domain. As a result, an unexpected hardware failure or hardware maintenance that affects one fault domain doesn’t affect instances in other fault domains. All the availability domains in a region are connected to each other by a low-latency, high-bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery.

Essentials multiple components / instances that performs same tasks are distributed over 2 or 3 availability domains (depends on role and count of components).

Storage in Oracle cloud was designed to be highly durable. Multiple copies of the data are stored across servers in the availability domains. Data integrity is actively monitored using checksums. Corrupt data is auto detected and auto healed from redundant copies. Any loss of data redundancy is actively managed by recreating a copy of the data.

Besides high availability we are running policy-based backups to perform automatic, scheduled backups and retain them based on a backup policy. Those backups can be restored across availability domains. As part of our preparation to possible disaster situation we test full restore procedure to ensure that we are aligned to our expectations.

10.2 Questback Offices

Backup strategy:

- Every night, a complete backup of the data is made on an independent backup system. Thanks to this backup, the contractor can immediately commence operations again in the event of an emergency.

10.3 Software / Questback Essentials

Backup strategy:

- Every night, a complete backup of the data is made on an independent backup system. Thanks to this backup, the contractor can immediately commence operations again in the event of an emergency.
- Backups can be precisely restored for each of the previous seven to 60 days depending on how critical the system is.

11.RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

The GDPR section 32 defines resilience of processing systems and services as a requirement to ensure security of processing. This section describes Questback’s measures ensuring resilience of processing systems and services.

11.1 Data Centres in Frankfurt, Germany

Oracle’s Data Centres ensure resilience through a variety of measures. This includes use of scalable network components, on the fly connectable resources, fault-tolerant hardware components, state of the art network infrastructure, provision of sufficient personnel and permanent monitoring of operational health.

11.2 Questback Offices

Questback’s offices ensure resilience through a variety of measures. This includes use of scalable network components, forward-looking planning of needs, provision of sufficient personnel and permanent monitoring of operational health.

11.3 Software / Questback Essentials

Questback’s software ensure resilience through a variety of measures. This includes the use of scalable databases, modern coding, agile development and the use of high-performance software components.

12.SEPARATION RULE

This section describes Questback’s measures ensuring that data that has been collected for different purposes is processed separately.

12.1 Software / Questback Essentials

Segregation of personal data is done logical by ID filtering via code (Essentials is a multi-tenant solution). Test computers are physically separated from live systems and are subject to separate security restrictions. Separate environments for development, staging and penetration testing are in place for test purposes whenever installations are altered. Live/production data is not used in development environments.

13.PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA

The GDPR section 32 defines pseudonymisation and encryption of data as a requirement to ensure security of processing. This section describes Questback's measures ensuring pseudonymisation and encryption of data.

13.1 Data Centres in Frankfurt, Germany

Oracle's Data Centres communicate encrypted with customers, using modern transport encryption. Backups are stored encrypted.

13.2 Software / Questback Essentials

Questback's software store passwords encrypted (hashed). Our GDPR functionality allows customers to have personal data in answers to Quests to be anonymized in the system by means of Quest settings. On pseudonymisation all data fields marked as personal information (such as email address, first name / surname) are replaced by generic information.

14. RETENTION AND DELETION

This section describes Questback's retention time for data, hereunder personal data, processed by Questback on behalf of its customers. Furthermore, the routines for deletion of data are defined.

14.1 Data centres in Frankfurt / Germany

The data centres retain the data for the duration of an existing contractual relationship between Questback and its customers. After a customer contract ends, Questback terminates the customer installation and information in the database in accordance with the terms stated in the customer agreement.

14.2 Software / Questback Essentials

14.2.1 Default setting: retention time for personal data defined by Questback's customer

Questback software is made available for Questback's customers, for them to create surveys and questionnaires that are made available for respondents. Upon creation of a survey or questionnaire, the customer will define retention time for the responses collected. The data will be anonymized automatically when the retention time has passed. Data stored in back-ups will be deleted (over-written) no later than 60 days after the original data has been deleted. Deletion will take place in accordance with Questback then-current deletion routines.

14.2.2 Optional setting: retention time not defined by customer

Should the customer not choose to define a retention time, the data in question will be kept until deleted manually, or until the contract between Questback and the Customer is terminated. Data stored in back-up will be deleted (over-written) no later than 60 days after the original data has been deleted. Deletion will take place in accordance with Questback then-current deletion routines.

15. INCIDENT MANAGEMENT

Breach notification is a mandatory topic between Questback and its customers. A data breach which results in a risk for the rights and freedoms of individuals will be handled according to applicable law. Breach notification must be done within 72 hours of Questback first having become aware of the breach. Questback will notify our customers, the controllers, "without undue delay" after Questback first became aware of a data breach.

While the above statement only indicates the requirement for notification within 72 hours of identifying a data breach and does not say Questback must have an incident response program, it is evident that to meet the 72-hour notification requirement, Questback provides to be able to quickly detect a breach within their networks, systems, or applications.

15.1 Detection

In the event of a detected breach, Questback immediately acts against an adversary within the network, especially if an early detection opens the possibility to stop the attack before the attacker can do any damage.

15.2 Communication

Beside the detection requirements identified above, internal communication between impacted departments and groups is agreed as well, to ensure a smooth response to an incident or breach. A communication plan identifies who is authorized to talk to external entities and customers.

Questback routinely test the response program to ensure effectiveness and timely notification, to comply with regulatory requirements and timeframes.

15.3 Notification

To reduce the risk of not having a complete or thorough response, Questback has developed an incident response program, created policies and procedures, and ensured relevant parties are aware of the program.

Questback has a customer inventory connected to the accounts of Questback Essentials, so the incident response team quickly can access contact information to a customer that has been impacted by a potential security event. Questback's accurate inventory of data is crucial to help with any potential individual notifications in the event of a breach, by pointing to which customer is impacted and support the process to notify the customer in the event of a breach. The then starting communication with the customer describe the nature of the breach and recommendations to mitigate potential adverse effects.

16. INTERNAL CONTROL

This section describes Questback's measures ensuring that its policies, including the policies described in this document, are adhered to through the organization, and the process for regularly testing, assessing, and evaluating the effectiveness of these technical and organisational measures.

16.1 Monitoring

16.1.1 Software / Questback Essentials

- Our hosting system has a monitoring and alarm setup that captures irregular behaviour in our infrastructure with a multitude of different checks
- Alerts are issued 24x7
- Alerts are immediately picked up by Questback's experienced system administrators
- The monitoring system has redundancy in place and is observed by a third-party monitoring tool
- A further monitoring system gives insights to the platforms' performance from places all over the world

16.2 Security Audits

Regular audits of the hosting environment are part of the ISO 27001 certificate requirements as applied to the Oracle data centres.

Apart from the Oracle data centre ISO audit, Questback has been subject to various ad-hoc audits performed by some of our customers who require verification for the highest security compliance. Questback also performs frequent self-audits.

16.2.1 Security Audit

To comply with the high requirement towards the platforms' security Questback hires 3rd party security experts to conduct security tests towards our platforms. The aim is to ensure continuous security when it comes to current and up-and-coming technologies and constant incremental development work.

The tests are conducted as an application test which mainly focus on the following areas:

- OWASP Top 10
- Cross-Site scripting (XSS)
- Session Fixation
- Weak or missing authentication
- Hidden parameters
- Directory browsing
- SQL Injection

16.2.2 Regularity of Security Audits

- 1 - 2 application tests of the service every year.
- 1 Infrastructure test of our hosting environment each year.

16.2.3 Results of Audits

- Results of application and infrastructure tests are presented to Product Management
- Any critical vulnerability is sent to development to be fixed
- Operation department takes care of issues related to infrastructure and server environment
- Issues related to Questback server environment are fixed by IT operations
- Vulnerabilities in our commercial website www.questback.com are fixed by developers responsible for the design of our commercial website