AccountsIQ

Security & Compliance Overview

Version 4.0

Date: February 2023

Contents

Introduction

AccountsIQ is a software company headquartered in Dublin, Ireland with offices also in London. AccountsIQ is a provider of secure Cloud Accounting Software to our clients and partners.

Our purpose is to simplify how Finance teams capture, process, and report the results of multi-location businesses. AccountsIQ takes the security of our customers, data storage and data processing very seriously.

The following document describes the measures we take to ensure robust security practices are followed at all levels.

The security measures implemented by AccountsIQ and our technology partners can be categorised under the following main headings:

1. Security Governance
2. People & Process Security
3. Data Access Security
4. Software Development Security Methodology
5. Information Backup
6. Business Continuity
7. Security Incident Management

1. Security Governance & Compliance Standards

AccountsIQ has implemented an ISO 27001 based ISMS for security governance and controls. The company is certified by an external accredited certification body (Certification Europe) for its compliance with the standard's requirements.

ISO27001 is the internationally recognised standard for information security and Cloud compliance.

Regarding governance, AccountsIQ has an appointed Chief Information Security Officer (CISO) and Data Protection Officer (DPO).

AccountsIQ is a Saas cloud accounting application and is hosted on Microsoft Azure infrastructure in secure data centres in UK, EU & US. These data centres are independently audited under Microsoft's own SOC and ISO27001 accreditations.

We provide our customers with the choice of where their data should be hosted based on their data residency requirements.

For production site hosting services support including network management, provision of Security Operations Centre, offsite backup and Disaster recovery, we also partner with Transparity (www.transparity.com) who are an Azure Expert Partner and also ISO27001 Certified.

AccountsIQ regularly evaluates the implemented security controls by conducting: 1) internal audits, 2) regular penetration testing, 3) external audits 4) regular reviews with its MSP and CISO.

AccountsIQ's approach to the storage of Personal Identifiable Information and the protections applied to this information is explained in detail within our Privacy Statement accessible here.

AccountsIQ is registered with the Information Commissioner's Office in the UK (Registration is ZA305592).

2. AIQ People & Process Security

Our people are core to the success of AccountsIQ since 2006 when we started commercially developing the product. Integrity, standards, and value fit are important criteria we use when selecting new team members.

As part of the hiring process, we always check references and have engaged a 3rd party company to carry out background checks on key hires prior to starting.

Each employee is required to sign a Non-disclosure agreement on their first day. This agreement strictly prohibits employees from disclosing any data of AccountsIQ or its clients to 3rd parties.

All employees are required to attend Security Awareness Training from when they start with the company on topics such as cybersecurity and Data Protection

matters including GDPR. Attendance and completion of this training is tracked and overseen by the internal security team.

All employees are in receipt of and are required to review, sign and adhere to our internal IT security policies including Acceptable Usage & Mobile Acceptable Usage Policies. Our engineers are required to review, accept and sign our Software Development Lifecycle security policies. Policies and signatures are managed using our internal ISO27001 compliance management system.

Our Incident Management Policy provides for the CEO to invoke a disciplinary process for each violation of security rules depending on the priority of the security incident/breach.

All AccountsIQ office user network Active Directory accounts are monitored constantly and audited by both our production MSP (Transparity) and corporate IT MSP (Spector Ltd).

Role Based Access Controls (RBAC) are in place incorporating segregation of duties so that production access where client data is hosted is on a strict need to have basis.

All internal user accounts that have not been logged in over 90days are disabled by default and all user accounts that have not been logged into in over 180days are deleted.

All user accounts will be verified by CTO first to confirm actions. The tools used are Rapid Fire and AD tidy.

3. Data Access Security

To restrict access to AIQ's Information assets including client data, a variety of IT and physical measures are in place.

a) Local AIQ Office IT Security Controls

In terms of internal office IT security, there are Network Access Controls in place as part of our Information Security Policy.

These are implemented by Spector and they manage and tracks all devices (PCs, laptops & mobile devices) that connect to our network. Quarterly security audits are carried out, the results of which are sent to AIQ's CTO for oversight. All

devices are hardened from a security perspective with the disks encrypted at the OS level. Our security policy disallows the use of portable media drives such as memory sticks for storing any client related data. All external access to our internal office network is over secure VPN connections only. Two factor security and mobile device enrolment policies are mandatory on all employee Office 365 accounts used internally. Office AD accounts are locked after 5 unsuccessful attempts and vpn accounts are locked after 3 unsuccessful attempts.

b) Client Data Physical Data Security Controls

The technical architecture supporting the AccountsIQ Cloud Accounting Platform is entrusted to Microsoft Azure for cloud hosting services and Transparity for managed services on top of the Azure platform.

AccountsIQ currently offers our clients 3 geographic Azure regions in which to host data, EU (Dublin), UK (London) and US (Virginia).

Microsoft Azure's world class data centres have ISO 27001 & SOC accreditation and use a layered security model controlling physical access to each site. Physical security defences include alarm systems, biometric systems for access, metal detectors and so on. The data centres are secured 24/7 with CCTV and only authorised employees with specific roles have access. Fire suppression systems and other measures to counteract the effects of natural disasters such as earthquakes or floods are also in place.

c) Network & System Architecture Controls

External client company users log on directly to our application web servers via the public internet by access URL over an encrypted SSL connection. Data in transit is encrypted over HTTPS with TLS 1.2 (RSA 2048 SHA256) between AIQ's environment and the client browser. The web servers are protected by firewalls to protect against intrusion. All data transmitted to/from the hosting site is encrypted, including any documents attached to accounts or transactions.

The application resides on servers within a DMZ behind a network firewall and there is a firewall separating the application and database layers. Client data is stored in Azure shared storage volumes controlled by separate dedicated database server (fault tolerant) clusters running Microsoft SQL Server. These database servers are further protected behind a firewall with only one port open to allow SQL queries generated by the web server to be passed through. No user access channels are open to these database servers.

AccountsIQ platform infrastructure and security events are monitored 24x7 by the Transpartity's Security Operation Center (SOC) team who work in tandem with AccountsIQ's security team. Microsoft Azure Cloud Defender protects the AccountsIQ platform and the underlying infrastructure from malware and associated cybersecurity threats.

Remote access to the production environment is secured via encrypted point-to-point VPN channels. VPN users are required to authenticate with a user account and password before being granted access to the network. VPN system is configured to log VPN connections. Network personnel review these logs on an ad hoc basis.

Regarding database storage architecture, each client entity organisation has its own database (i.e. their records are held in a separate unique database and not comingled with records from other companies in one large database). All client databases are encrypted at rest using SQL Server Transparent Data Encryption (TDE). Data is also encrypted at rest when stored within Microsoft's Azure storage and also all backups are encrypted.

In addition to the above, an independent security penetration company (Edgescan) is retained to carry out ongoing vulnerability testing using their automated solution and they annually complete an independent security assessment of the public facing networks and AccountsIQ software application. This involves testing the main AccountsIQ software application itself to establish any weaknesses in the application or technologies utilised. This area of testing is designed to replicate the position of an externally located malicious threat, with the intention of compromising the applications in scope, as well as to replicate the position of a user with legitimate access seeking to escalate their assigned level of access or otherwise abuse their position of trust, to gain access to restricted information.

d) Front-end User Access Controls

In terms of front-end data access to the application itself, AccountsIQ system users can only be created from within the Practice Admin layer, which is essentially a portal that practice users with appropriate permissions to create users can add or edit new users. Upon creating a new user record, an email invite is sent to the designated client company user enabling them to set up their own username and password. Note that no passwords are ever created automatically or sent in clear text to any user. The password the user enters is checked for strength, and only strong passwords are accepted, users are notified as to what constitutes a strong password. Note that if a user persistently enters an incorrect password for their user account 10 times or more, their account will be locked out. An email indicating that this has happened is sent to the Practice

Administrator email account. This person then can unlock the account using the user access controls.

AccountsIQ also has Two Factor Authentication included as an additional user access control feature which we strongly advise our clients to implement across their users. We have incorporated very strong user access control and user profile settings into AccountsIQ. Access to every feature in the system as well as every report and dashboard object can be turned on or off at admin level simply by checking a box for each element at a user profile level. If you would like a user to have access to a report screen only (where they cannot post or view or other parts of this system) this is very easy to set up. Likewise, if your client has a staff member who should only have access to a specific function(s) this can be set by the admin user (who has authority to make amendments to User Profiles). For example, User Profiles can be set so that specific users cannot edit or see bank details.

e) Technical Support Staff Access Controls

In accordance with the AccountsIQ's Information Security Policy, support personnel access privileges are assigned to individuals based on the concept of "least privileged", which assigns each user the minimum set of rights and only provides additional access to data if required by job function e.g., the requirement for a support technician to review client data in response to a support ticket. This is assigned and tracked via management oversight. All notable modifications are logged (including the user who made the changes) and regularly reviewed.

Second level technical support staff with a requirement to access production backend servers for support purposes do so using a secure Azure Bastion VPN and a dedicated Microsoft Active Directory account that is monitored via the MSP's (Transparity) Security Operations Centre. Additional layers of security and provided with two factor authentication in combination with geo-location white-listing for all AD logins.

As part of AccountsIQ's Security policy in connection with people leaving the organisation, their VPN, AD, and system accounts are disabled immediately once they leave the organisation.

As noted above, all development and support staff are required to sign a separate NDA and ongoing training which specifically covers the confidentiality of 3rd party data they are handling as part of their role.

4. Software Development Security Methodology

In terms of the management of software development, our Application Development Security Policy is adopted to ensure that security is designed and embedded into all phases of the development lifecycle. We have validated our security measures against the Top 10 vulnerabilities of web applications as set down by The Open Web Application Security Project (OWASP), who are a leading non-profit foundation to improve the security of web applications such as AccountsIQ.

We incorporate secure design, threat modelling, secure coding, security testing, and best practices surrounding privacy throughout all application development phases and in the management of these phases. The primary phases include:

- Developer Training
- Requirements gathering
- Design
- Implementation
- Testing
- Deployment and Release
- Maintenance and Incident Response

All changes go through a formal Change Control Process in accordance with Information Security Policy.

5. Information Backup

Each night a “full” scheduled SQL Server backup is taken and every 30 mins a transaction log backup is taken. This enables us to restore a database to an up-to-date version in the event of a failure. Each night the backed-up data from the Azure storage and other operating system and relevant files are then replicated to another geo-location in the Azure network for offsite storage. We retain a 30-day set of backups for restoration purposes.

The offsite backup service compresses and encrypts the data prior to the data leaving the server, then transfers it though a secure network connection to the offsite facility where it is stored on disk and then restored to another SQL instance, where it is also encrypted “at rest”.

Note that the same access controls apply to backed up data as to any live production data on the platform. The Transparity Managed Services team carries out monthly backup restore tests and this activity is audited by ticket.

AccountsIQ is unique amongst other Cloud Accounting providers in that we do not seek to obstruct or make difficult the export of data if the client wishes to export it for backup purposes or if they decide to move off AccountsIQ. The following end user export capabilities are available:

- **Data Exporter' function**. This screen enables the user to do a straightforward export to csv of all main database tables including Customer & Supplier Master record, GL Accounts, Transactions etc.
- **'Excel Add-In'**. This is a downloadable add-in that can be installed on a client Excel installation. It is designed to facilitate reporting but could also be used to export all the main datasets from the system into Excel and refreshed when required.
- **'SQL Database Extract'**. This feature, recently released enables a user to request an extracted copy of data from their database. Again, this is used for preparing bespoke reports, but it could be used for downloading key datasets for backup purposes should the client request it.

6. Business Continuity

AccountsIQ has implemented a comprehensive business continuity strategy, conducted a business impact analysis, identified critical business processes and their dependencies (human and technological), and created plans to addressing the identified RTOs and RPOs.

In each Microsoft Azure region (US, EU, and UK), the client environments are set up using High Availability (HA) architecture within the region, and DR environments are created in a separate, paired Data Center in the same region.

a) Disaster Recovery Plan

Using Azure Site Recovery (ASR), all production VMs running AccountsIQ are fully backed up on a nightly basis and replicated offsite to another Azure region. For example, the UK South Azure region's VMs are replicated to the UK West region. This ensures that restoration of servers from recently taken images can be carried out in the event of a full disaster within a given one of the Azure regions. In addition, all customer SQL databases are stored in Microsoft Azure

data storage with geo-replication offsite for disaster recovery purposes and can be copied back to an alternative production environment if it required a rebuild in the event of a disaster.

b) Resilience Arrangements (Hosting)

Depending on the level of disaster experienced there are several resilience controls in place:

- Our current platform is fault tolerant with no single point of failure on the application or database layer with multiple web application VMs serving requests and a SQL Server active/passive database cluster. In the event of a major failure on one of the database nodes, the other node can take over immediately.
- Microsoft SQL Server backs up the database transaction logs every hour. These contain a full log of all database changes so they can be rolled back/forward to reconstruct at any stage from the nightly full backup.
- All AccountsIQ databases are backed up each night to another Azure region, ensuring that there will always be up-to-date versions to restore in the event of a disaster to the primary data centre.
- Test backups and database restores are carried out quarterly by Transparity.
- Contingency and business recovery is reviewed with Transparity on a quarterly basis and during bi-weekly governance review meetings.

In terms of physical business continuity in the Data Centre, these measures are of relevance:

- Redundant UPS and Generator backups for all systems.
- Redundant Tier I network connectivity to upstream Internet Service Provider(s) with connections ranging from 1 to 10 gigabits each.
- Redundant load balancers that provide high-speed, reliable web content delivery by using customizable health and resource tracking.
- Redundant switching and routing core providing full edge-to-server redundancy in the unlikely event of a core router or switch failure.
- 1-hour hardware SLA for replacement of critical components.
- Multi-zoned, dry pipe, water-based fire suppression systems.
- Monitors to sample air and provide alarms prior to pressurisation.
- Dual alarm activation necessary for water pressurisation, water discharge specific to alarm location.

7. Security Incident Management

Information security is of paramount importance and AccountsIQ has a robust set of security controls in place to prevent any unauthorised access to data.

24x7 SOC monitoring is in place by an Azure Expert Certified MSP (Transparity Ltd), with detailed Incident Response playbooks, procedures, and best practices.

If in any case all implemented security measures fail, there is a data breach policy in place that is described in our Information Security Incident Policy & Plan.

The policy and plan consist of the actions in relation to the classification of reported incidents, containment, eradication and formally issued communication both internally, with partners and clients affected.

Our partners and clients will be notified immediately when we suspect a data breach, even when we do not know the source or impact yet.

Further notifications on the cause and resolution will be sent thereafter. The appropriate authorities such as the Data Protection Office (DPO) and the Information Commissioner's Office (ICO) will be notified within the required timeframes for reporting a data breach.

8. Other

a) Support & Maintenance Arrangements

Please see current attached SaaS agreement that details our support arrangements.

In terms of normal systems maintenance, on average there is 30 mins scheduled downtime per month per host site which allow for standard Windows updates to be made to our servers (OS, Database updates). We issue service patches on a regular basis to fix bugs, release small feature enhancements and these do not involve system downtime.

For large product upgrades we schedule these to be deployed out of hours. Our methodologies for deploying upgrades do not require any system downtime

normally. If there is a requirement for system downtime, we schedule a maintenance window and provide user notifications.

Note that AccountsIQ provides a system status portal to notify users of any system incidents or upcoming platform maintenance.

Accessible off the login page, the status.accountsiq.com portal is hosted on a different host site to our existing sites so it will not go down if any of our sites do. The status page runs monitors which execute automatic logins into the system every few minutes across all sites. If the logins are successful, they will report an active status, if they are not, they will report a failure and an incident will be automatically created on this portal.

It is a useful way for us to also communicate to our users during any incidents as we can publish updates there.

Users can choose to subscribe to the status page and be notified of any incidents and upcoming maintenance windows by email or SMS.

b) Code Escrow Arrangements/Access in the event of Accounts IQ ceasing trading

We have an escrow arrangement with NCC Group (UK based) that was put in place with selected key customers as beneficiary of the agreement. This means that these customers have access to the source code of AccountsIQ in the unlikely event of AccountsIQ ceasing trading. NCC Group provide for additional beneficiaries to be added to the escrow agreement. If your organisation wishes to be added to this agreement it could be arranged and would involve a separate annual charge.

c) Standard terms of business

Please see current attached SaaS agreement that details this.

d) Contact Details

If you have any questions in relation to this document, please contact Gavin McGahey (CTO) gmcgahey@accountsiq.com