# 1. Introduction

The purpose of this document to describe what Circit is, how it works at a high-level and the technical details for its implementation.

## Current Challenges

Banks have to process tens of thousands of paper request letters from auditors for the same customers every year. This is costly, time-inefficient and error prone for the following reasons:

- **No Visibility** - Tracking is not end-to-end and is done on internal spreadsheets, leading to disputes with the auditor. The customer is often delayed with the signing of their year-end accounts.
- **Slow Issue Resolution** – Errors from either party is a time drain with follow up phone calls, a duplication of work and a poor customer experience.
- **Data Security Risk** – Customer information is delivered by paper to unauthenticated individuals, in an unsecured environment and with limited audit trail.

## The Solution: Circit's Auditor Query Management Platform

Circit is a platform for managing auditor query requests in a fully digital, highly secure system. Circit brings all **auditors**, **banks** and **solicitors** onto one platform which delivers significant value to each party and greatly benefits their mutual SME **customer**.

A typical process involves three parties, which are:

- The **auditor** requesting information
- The bank's **customer** whose authorisation is required
- The **bank** responding to the request

## Diagram. Audit Query Process Overview

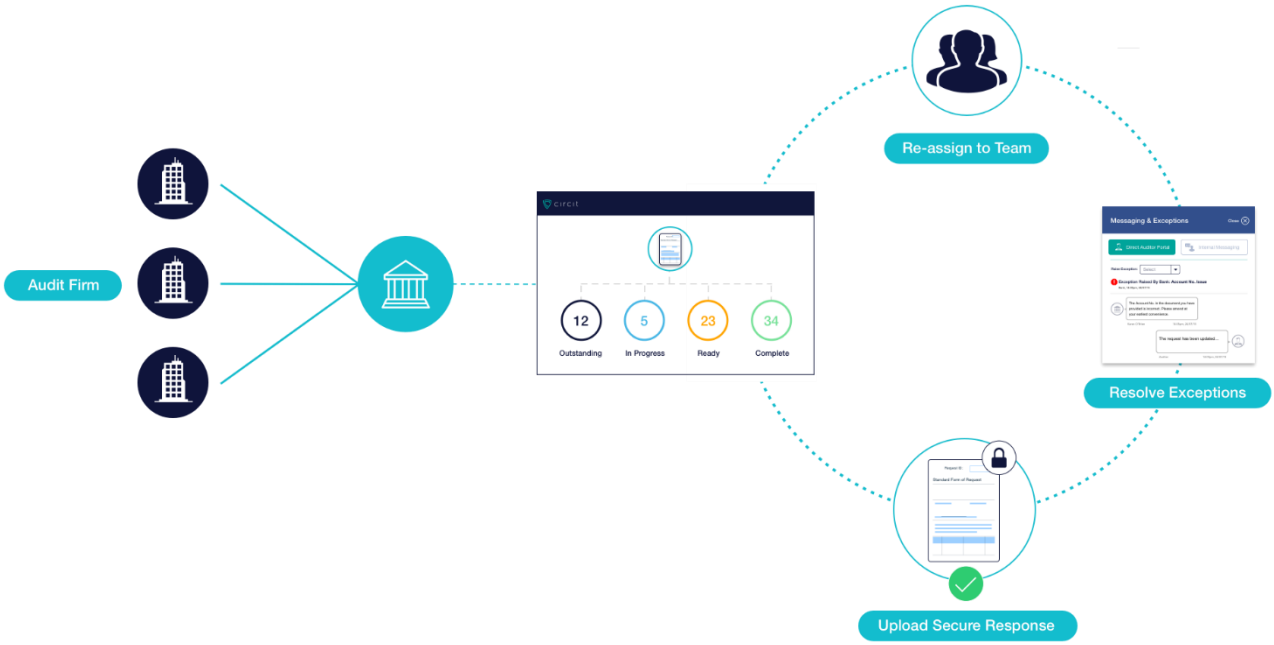
# 2. Circit for Banks

## How it works

Once authenticated and logged in, bank staff can perform the following:

- Track all incoming and outgoing requests from one place
- Re-assign to other bank staff members and resolve internal queries with team messaging
- Securely upload response documents directly to the auditor who made the request
- Raise exceptions externally directly with an auditor and instantly resolve an issue through in-app messaging

## Diagram. How the bank uses Circit




# A Single, Secure Solution

## Bank Benefits

- Validated auditor for secure communication
- Automatic segregation of future dated requests
- Eliminate follow up phone calls
- Designed for maximum workflow efficiencies
- Internal performance reporting
- No software installation
- Customer experience improved

# 3. Technical Setup

## Hosted

Circit is a cloud-based application hosted using Microsoft Azure. It is a SaaS based product, there is no software to install and updates are handled by Circit.

## Access & Authentication

Users access the application by visiting the following URL in their web browser:

**https://app.circit.io**

In order sign in for the first time, a user must do the following:

1. Click authentication link in their e-mail which is sent by Circit during setup.
2. Enter a valid e-mail
3. Enter a Password
4. Enter a 2 factor one-time passcode if configured by the bank

After these steps users are authenticated through Circit's Identity Provider module (IDP). This module is developed by Escher group and is a secure and powerful authentication solution. It is built around open standards including SAML that will facilitate single sign on in future versions.

## Data Backup & Storage

Application data is stored in two locations: a SQL Server database for relational data and Azure storage accounts for binary document files. The database server is SQL Server 2016 Enterprise Edition hosted within an Azure Virtual Machine. Data is stored on Azure disks configured for high performance and reliability.

A full backup of the system is taken every night with transaction log backups taken every fifteen minutes. The database backups are themselves stored in a separate Azure storage account, configured with geo-redundancy so that data is replicated in two geographically distinct datacentres. Database restores are tested regularly on a hot staging environment that mirrors the production configuration.

Azure storage containers are an ideal solution for storing the document files created and stored by the Circit application. Multiple versions of a file can be tracked and redundancy is built-in. Access and permissions can be granted on a granular level using shared access signatures. The live files are stored within an Azure container with geo-redundant storage. A daily snapshot is also taken of the document files in Azure and backed up to another Azure storage account.

All Circit application data is configured so that the data is stored within the EU, in Microsoft's Northern Europe (Ireland) and Western Europe (The Netherlands) locations. This applies to live databases, the document files and all backups.

## Browser Compatibility

The following browsers are supported:

- Google Chrome
- Firefox
- Internet Explorer (Version 10 or above)

# 4. Security Features

## ISO 27001 Certification

Circit's offices and software development processes and operations have been certified to the ISO 27001:2013 control standard.

## Encryption

To ensure the confidentiality and integrity of data, all content is encrypted in transit and at rest. Multiple layers of encryption are used to support customers' needs for reliability, security and control over their sensitive content.

Microsoft SQL Server 2016 Enterprise Edition is used as a database in order to take advantage of Transparent Data Encryption (TDE). This ensures that all databases and backups are always encrypted with 256-bit AES encryption.

Files stored within Azure Storage account containers are also encrypted using 256-bit AES, using keys stored within Azure Key Vault.

Both TDE and Azure Key Vault make use of Hardware Security Modules (HSM's) to safeguard cryptographic keys. These prevent tampering of the keys, restrict access to authorised applications only and prevent exporting of the original key, as well as providing audit history on key access.

All data in transit is protected using TLS. The Circit application can only be accessed over HTTPS. Circit's Extended Validation certificate is used to verify the identity of the application.

## Audit Trail

Documents created by the Circit application include a comprehensive and immutable audit trail between all parties that includes a timestamp, IP address and end-user information.

These records include a cryptographic hash of any PDF document which can determine whether or not it has been modified or tampered with. Circit's extended validation certificate is used to verify the application's identity is correct.

## Physical Data Infrastructure

Services provided by Circit are hosted on Microsoft Azure in state-of-the-art SAS70 Type II, SSAE 16 facilities with ISO 27001 certification. Physical access is strictly controlled by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication no fewer than three times to access data centre floors. Circit uses multiple data centres with reliable power sources and backup systems with 99.9% SLAs and redundancy. Physical servers are located in Dublin, Ireland and failover servers are located in the Netherlands.