Forvis Mazars' Security Overview

forvis mazars

Contents

Revision History

Approver's Name & Title	Approver's Signature	Date/Time
Andrew Thayil, Chief Information Security Officer	Andrew Thayil Digitally signed by Andrew Thayil Date: 2024.07.18 15:10:33 -04'00'	July 2024

Effective Date	Version Number	Author(s)	Description
5/15/2023	2.0	MyForvisMazars Product Team	Combined LBKD & LDHG Security Review
	3.0	MyForvisMazars Product Team	Updated for Engage Specifications

1.0 Introduction

1.1 What Is Engage?

Engage is an online application hosted by Forvis Mazars, LLP. With Engage, Forvis Mazars hosts client data, provides engagement management, and enables client collaboration through the entire client life cycle.

Engage allows clients to easily upload documentation, oversee their engagement, provide updates, and collaborate with other client users and staff from Forvis Mazars.

Forvis Mazars recognizes that with the increased efficiency and communication of online applications, there are advanced security concerns and risk. This document describes the controls implemented by Forvis Mazars specific to Engage for the purpose of clients to determine if Engage is suitable for their business.

1.2 Engagement Creation

A new engagement can only be created by internal professionals at Forvis Mazars who are responsible for the administration and management of Engage. Professionals from Forvis Mazars are responsible for adding an external admin to each client's engagement.

1.3 Client Authentication & Access

Upon creation of the engagement, professionals from Forvis Mazars will add an external admin. This account will be responsible for adding additional external admin. If they decide to have additional external admin, it is the client's responsibility to ensure the permissions are managed properly. The external admin is responsible for managing all external client access.

As the external admin adds to or edits the external client list, each individual user is systematically added to or removed from specific permission groups based on the selections made by the external admin. When new users are added to the external user list, system-generated invitations are sent requesting registration. Upon successful registration, the user will be granted access to the engagement. When individual users are removed from all external client lists, all permissions to the engagement are systematically removed.

More information about setting up external users can be found on the Engage Help Center page.

Each engagement is created by internal professionals from Forvis Mazars for a specific client purpose only accessible to the client users assigned to that engagement. Professionals from Forvis Mazars are assigned to an engagement by an authorized professional from Forvis Mazars, while client users are assigned by the external admin.

2.0 Security Design

2.1 Confidentiality

Confidentiality ensures that client data is only accessible by authorized entities. Forvis Mazars provides confidentiality in the following ways:

2.1.1 Least Privilege & Role-Based Security

The principle of least privilege is widely accepted as a best practice, and as such, Forvis Mazars has implemented role-based security within Engage. With this security model, the client has the ability to assign specific access permissions to their staff. Forvis Mazars recommends all clients make use of this security feature.

The following roles are available within Engage:

- Infrastructure Team – Internal IT users from Forvis Mazars responsible for the hardware and operating system of the application. This team is responsible for system stability and maintenance and does not have access to the Engage application or data.
- System Administrator – Internal IT users from Forvis Mazars responsible for the Engage application and underlying databases. These users are responsible for patching and maintaining the stability of the application.
- Users of Forvis Mazars – Internal users from Forvis Mazars responsible for managing client engagements and the client's access. A user of Forvis Mazars creates the external client admin and assigns staff from Forvis Mazars as users of Forvis Mazars.
- External Admin – Used by the client to assign client users from client staff. In addition, this account can set access permissions for the accounts they create.
- Client Users – Client staff assigned to the engagement, with member-level access. This account(s) is maintained by the external admin. Client users with member-level permissions are granted access: member-level to the engagement to allow access to upload files, and assignments along with the management of the status of requests.

  Member-level external client users cannot add or remove external permissions.

2.1.2 Access Controls in Engage

Access controls have been implemented within the Engage application. Each engagement is restricted and only accessible by the accounts assigned specifically listed on that engagement. This prevents an account from one engagement being used to gain access to other engagements.

2.1.3 Network Segmentation

Network segmentation creates a collection of isolated networks within a larger network. Each network then becomes its own separate broadcast domain. This segmentation severely hinders a would-be attacker since each one is essentially a standalone network, with no ability to access another network. Virtual local area networks (VLANs) provide this capability and are used to segregate Engage systems from their respective databases.

2.1.4 Separate Authentication Mechanisms

Separate user management and authentication systems are used for users of Forvis Mazars and client users. This design ensures that users of Forvis Mazars cannot create "client accounts" and clients cannot create "Forvis Mazars accounts," which prevents attempts to circumvent security controls and gain unauthorized access to data.

This segregation also allows each client to implement role-based security for their users that matches their own internally designated roles.

2.1.5 Encryption

Data is encrypted both "at rest" and "in motion" with Engage. This is accomplished using encrypted databases and HTTPS/TLS 1.2, respectively.

All communication and data encryption are compliant with the FIPS 140-2 standards.

2.1.6 Content Retention

Data is stored in Engage throughout the entire client life cycle for which the engagement was created. At the completion of the engagement, data is available to be rolled forward to future engagements or downloaded but otherwise cannot be modified.

2.0 Security Design

The AICPA sets the retention guidelines followed by Forvis Mazars.

All unfiled data and task documents stored on Engage are purged 24 months after engagement completion.

2.2 Integrity

Integrity refers to the trustworthiness of information. This means that data has not been changed inappropriately, either accidentally or intentionally. Forvis Mazars provides integrity through:

2.2.1 Audit Trails

Engage is configured to generate detailed audit logs. These logs record actions such as who accessed data, when they accessed the data, what pages were visited, and what they did within Engage with the data they accessed.

These logs are retained within a discrete database, are set to read only, and are accessible only by a System Administrator.

2.2.2 Document Control

To modify a document, it must be downloaded from the engagement, edited locally, and then uploaded back to the engagement. No documents can be edited directly in the application. Users of Forvis Mazars are notified daily when new documents have been added to their engagements. Multiple documents can be downloaded if they are all on the same page or section.

2.3 Availability

Availability refers to the ability to access and use data resources when needed and to protect against unplanned failures in service. Forvis Mazars provides availability by:

2.3.1 Segregated Environments

Engage uses a development environment for creating new code and changes to the Engage system. These changes are then moved to a Quality Assurance instance where they are thoroughly assessed and reviewed. Once all testing has been performed and the new or changed code is approved, it is moved into the production instance during a maintenance cycle.

This process ensures that unstable or malicious code does not go into production. This is a standard best practice of a systems development life cycle (SDLC).

2.3.2 Redundant Systems

Forvis Mazars uses best-in-class systems and network devices as part of the Engage infrastructure. This includes redundant internet connections, routers, firewalls, and servers. Forvis Mazars has removed all single points of failure through a layered approach, helping ensure peak availability and security for the Engage platform.

2.3.3 Load Balancers

Forvis Mazars uses enterprise-class load balancers to help ensure that high volumes of traffic do not limit service or reduce functionality.

2.3.4 Backups

All Engage servers and databases are backed up using Forvis Mazars' enterprise backup tool. Backups are performed hourly. These backups are replicated off engagement to a secure location.

3.0 Security Operations

3.1 Security Operations

While not necessarily specific to Engage, many security controls within Forvis Mazars contribute to the overall security of the Engage system.

3.2 Physical Security

Forvis Mazars uses best-in-class data centers to house systems. These facilities provide protection from all but the most severe natural disasters.

Each facility is staffed around the clock and provides physical access restrictions through a dead-man room, electronic access controls, and remote monitoring via cameras. In addition, each data center includes the environmental controls necessary for a continuous computing environment (redundant power, HVAC, fire suppression, etc.).

3.3 Personnel & Processes

Forvis Mazars not only uses best-in-class systems but enterprise-class personnel. With dedicated and trained IT personnel, Forvis Mazars enables stable and secure system operations through the use of best practice processes such as change control, patch management, SDLC, and other techniques.

3.4 Additional Security Controls

Dedicated IT Security – Forvis Mazars has a dedicated IT security team responsible for overseeing and ensuring the confidentiality, integrity, and availability of systems and data at Forvis Mazars.

- Information Security Program – Forvis Mazars has a formalized Information Security Program that consists of formalized policies and procedures, incident response, and IT continuity and recovery plans.
- Penetration Testing – Forvis Mazars performs routine vulnerability assessments against internal and external systems. In addition, Forvis Mazars has penetration testing performed annually.
- Application Testing – Engage has undergone an independent application test by an industry-recognized application testing company.
- Intrusion Detection – Forvis Mazars uses an enterprise-class intrusion detection system with 24/7 monitoring and alerting services.
- Antivirus Protection – Forvis Mazars uses enterprise-class antivirus software at both the operating system and application level to protect against malicious software.

3.5 MyForvisMazars

MyForvisMazars is the central launch point for all client interactions with Forvis Mazars.

MyForvisMazars provides identity provider function using Microsoft Business to Consumer mechanisms. This enforces multifactor authentication (MFA) to be chosen for each user of the system. The Microsoft B2C Identity Provider is designed to enable businesses to manage and secure customer identities effectively. It serves as a centralized platform that allows customers to authenticate themselves across various applications and services. By implementing this tool, businesses can enhance security while providing a seamless user experience. Microsoft B2C I also supports and enforces MFA. MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing their accounts. This significantly reduces the risk of unauthorized access and helps safeguard sensitive customer data. Microsoft B2C is able to support multifactor authentication by text message, email, or authenticator.

With client collaboration, we can support client-side SSO and federation.