Narrative Information	
Date/Time:	November 13, 2025
Topic:	Systems Interfaces and Batch Jobs
Attendees:	Stakeholder name: Virgilie Fannon (Senior Director, Interfaces and Integrations) Audit Team

Narrative for System Interfaces and Batch Jobs

I. Systems Interfaces Configuration

The organization has two main data interfaces that receive daily batch files from third-party vendors named Merkle and Ruffalo Cody. The Oracle Batch Job Scheduler collects files and vendor data from an FTP server and gets it prepared for processing within the database. The technical team manages these configurations of the interfaces and makes sure that all of the batch jobs are being properly scheduled. When the files are received, they get routed through an FTP service and then loaded into the system internally so that the data can be captured. The configuration process is very dependent on third party vendors to deliver the correct batch job files. The technical team is then responsible for ensuring that the jobs run successfully and that the interfaces remain properly connected.

II. Systems Interfaces Monitoring

The team actively monitors all interfaces and Oracle-scheduled batch jobs that support the data flow. When jobs run as expected, no notifications are generated; however, any failures trigger an automated email to the designated resource group. Upon receiving an alert, a team member reviews the associated error report to identify the root cause of the failure. Files are transferred securely via FTP before being processed into the database. Based on the identified issue, the team either performs the necessary corrections and reprocesses the job the same day or allows it to run during the next scheduled cycle.

III. Systems Interfaces Access

The system interfaces provide the necessary access to support daily operations, including receiving batch files from Merkle and Ruffalo Cody and processing phone marathon data used for alumni and donor contributions. Interface files are retrieved by the Oracle Batch Job Scheduler into the FTP environment and subsequently transferred into the internal database to support routine data exchange and business workflows.

Access to system interface files is provided to users supporting interface operations; however access is not provisioned based on defined roles or job responsibilities. Users are assigned uniform access privileges, including modify-level access, regardless of business need, indicating that access controls are not designed in accordance with the principle of least privilege.

In addition, interface file transfers rely on unencrypted FTP, and encryption controls are not applied once data is transferred into internal systems. As a result, while access supports operational requirements, the design of access controls does not adequately restrict modification capabilities or protect sensitive alumni and donor data.

IV. Systems Interfaces Encryption

The current system design has no encryption during the vendor file transfer process, which can expose sensitive and important data to attackers. Also, once the file reaches the internal system, it is still not encrypted and has no additional security controls placed to protect that data. Without encryption at rest or in transit, the organization lacks the basic safeguard to protect its organization and meet industry standards.