DEMO PROJECT

Digital Transformation of “Three Lines of Defense Model”

(Business Case: User’s IT Network Access Controls)

Business Requirements Document

Sateesh Babu

Dec 30,2021

Version 1.0

Disclaimer: Any data or opinions presented in this project presentation are solely those of the author and do not necessarily represent those of his organization or any other organizations. It’s a hypothetical problem. Solution is designed by the author to exhibit his skills and experience.

1 Document Purpose

1.1 Project Information

Project ID	**xyz2021**
Project Manager	***Sateesh***
Project Sponsor	**xyz IT team**
Business Lead	***Sateesh***

1.2 Revision History

Revision	*Date*	*Status*	*Contribution By*	*Summary of Changes*
1	***2021/12/30***	***Draft***	***Sateesh***	
2	***2021/12/30***	***Final***	**Sateesh**	

1.3 Document Approval List

Revision	*Date*	*Status*	*Reviewed By*	*Summary of Changes*
1	***2021/12/30***	***Approved***	**Sateesh**	

1.4 Document Distribution List

Revision	*Date*	*Status*	*Reviewed By*	*Summary of Changes*
1	***2021/12/30***	***Final***	**Sateesh**	

Contents

2 Introduction

2.1 Executive Summary

Digital transformation is the integration of digital technology into all areas of a business, fundamentally changing how you operate and deliver value to customers. It's also a cultural change that requires organizations to continually challenge the status quo, experiment, and get comfortable with failure.

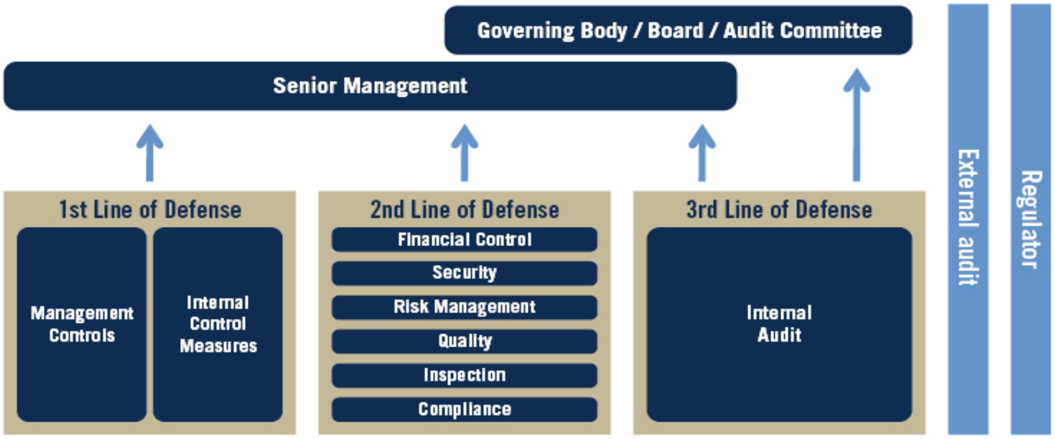
In the post COVID era, as most of workforce started connecting to the IT network remotely and IT Infrastructure managed by cloud service vendors, our enterprise has implemented "Three lines of Defense Model" control measures in reviewing user network access on timely manner.

Digitalizing these control measures will bring the following benefits:

1. It will improve efficiency, transparency, and coordination among the stakeholders of "Three lines of Defense Model"
2. It will break the data silos and saves cost as well as processing time.
3. It will help in quicker problem identification (including unauthorized access) and enables a secured environment.
4. Finally, it provides better experience and motivation to the workforce while connecting to the IT network remotely.

2.2 Three lines of Defense Model and Project stakeholders

The three lines of defense framework is a fundamental pillar of corporate governance structures and enterprise risk management. Its objective is to provide a right information at right time to the governing body and the senior management for their risk-based decisions. Also, provides assurance to regulators and external auditors.



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

2.2.1 Primary Stakeholders

Business stakeholders in the "Three lines of defense model" play a distinct role within the three lines of defense. But they use the same organizational data for different perspectives/or reporting. Inaccurate reporting will lead to wrong management decisions and conflicting assurance opinions.

Line of Defense	Responsibility/Description in	Business Stakeholders/Users	Primary Contact Email id	RACI Chart
1st Line: IT Operational Management	Responsibility to own and manage risks associated with day-to-day operational activities of the “IT network access and security”. Other accountabilities assumed by the first line include design, operation, and implementation of controls.	IT Security and networking team	abc@xyz.com	Accountable, Consulted, Informed
2nd Line: Risk Control and Compliance	Specialize in the oversight of risk management and compliance. It does this by providing compliance and oversight in the form of frameworks, policies, tools, and techniques to support risk and compliance management.	Risk & Compliance committee; Cybersecurity team	qwer@xyz.com	Accountable, Informed
3rd Line: Risk Assurance	Ensure whether the first- and second-line functions are operating effectively. It is charged with the duty of reporting to the board and audit committee, in addition to providing assurance to regulators and external auditors that the control culture across the organization is effective in its design and operation.	Assurance team/auditors	yoyoyyoy@xyz.com	Accountable, Informed

Note: IT Security and networking team are the project sponsor and act as a point of contact for all network systems processes.

2.2.2 Secondary Stakeholders

Data Owners/Stewards/Custodians, Domain Experts, Project team and Enterprise Data Governance are the secondary stakeholders, who play an important role in the delivering the project.

Description/Context	Secondary Stakeholders	Primary Contact Email id	RACI
HR datasets	HR reporting team	hrrep@xyz.com	Responsible, Consulted
Active Directory (network) datasets	Vendor (Cloud Service Provider)	vendor@vendy.com	Responsible, Consulted
Work order/ RFI approvals	Procurement team	proc@xyz.com	Informed
Solution & Data architecture review	Enterprise Architect team	ea@xyz.com	Consulted
Project delivery team	Third party IT vendor	vend@ibxy.com	Responsible
Enterprise Data Governance	Data Governance Committee	edg@xyz.com	Informed

2.3 Problem Statement

As stakeholders of the three lines of defense mechanism of “Users’ IT network access review”, we don’t have an integrated data and analytics platform or capabilities that focused on driving results for risk-based decisions and assurance reporting. Digitalization would help us to set risk control mechanism with strong corporate governance for better decision making and assurance reporting in monitoring “User Network Access” of xyz enterprise.

2.4 Business Needs

Summarized the business needs as below:

- Need access to accurate and organized data analysis of “Users’ IT network access”. This gives the ability to spot risk trends/alerts and make effective decisions in monitoring organization’s IT resources.
- Centralized integrated data platform (digital asset) should have capabilities to collect, store, process, analyze, and visualize high volumes of a wide variety of data, drive value in many ways by considering standard enterprise data taxonomies, data integrity checks and data security measures.
- The integrated data and analytical platform should be flexible, scalable, cost economical and the freedom to design and deploy standard as well as custom controls that fit business context at any given time.

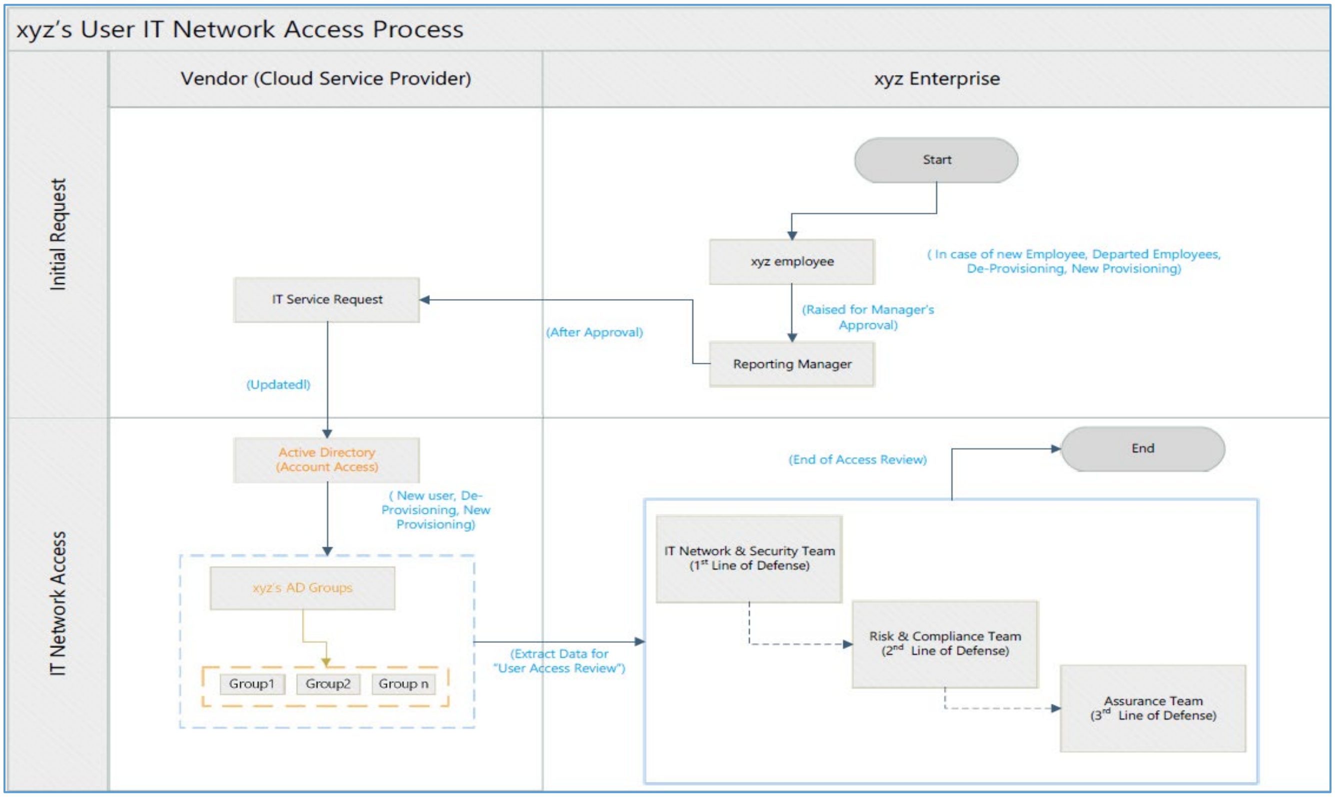
3 Current State

3.1 High Level Current State Business Process

Current state business process to review the IT user access in xyz enterprise as follows:

Process	Application Access flow
Step 1: Initiation from Employee or reporting Managers	a. Employee must submit the request form if he/she needs access to an application or an application group within the IT network. The request should get approved the reporting manager to get processed by the vendor – cloud service provider. b. In case of new employee or departed or terminated employees or transfers or modification, the reporting manager must submit the request form on his/her behalf.

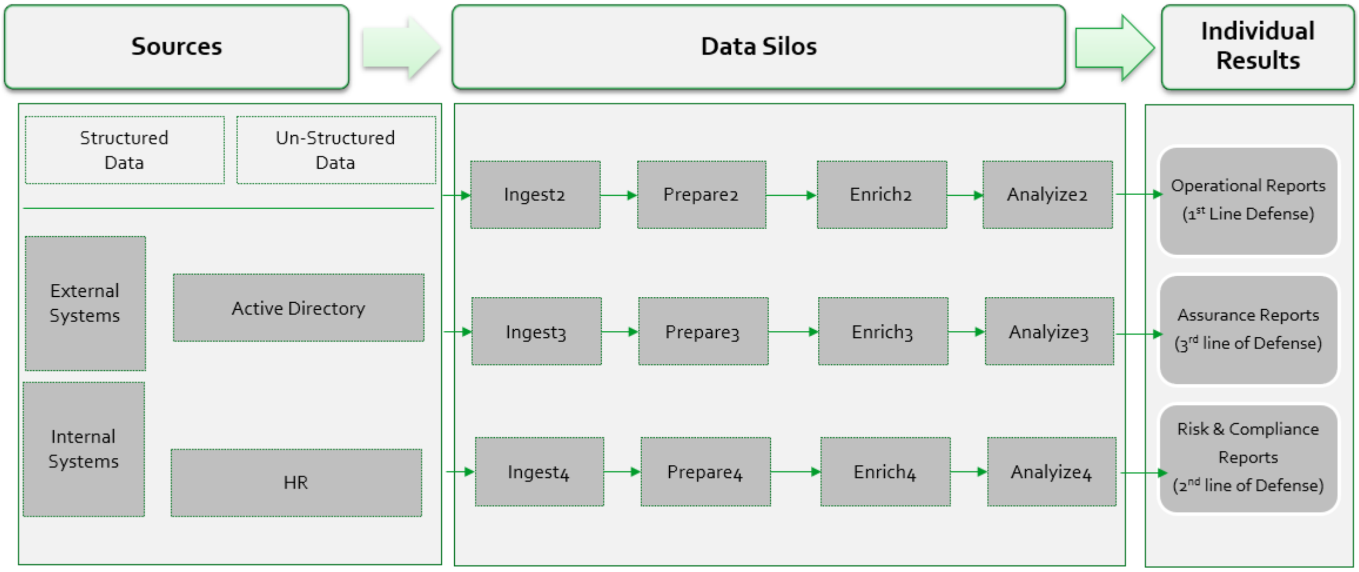
Step 2: Vendor’s IT security team will update the active directory.	Active Directory (AD) authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers, and installing or updating software. It is used to configure accessibility of users and groups to services and resources. Vendor’s IT security team is managing this service at the behest of xyz enterprise. They grant or de-provisioning AD groups to a particular xyz user based on the service ticket request. Also, Vendor uses the same active directory to manage the networks of other clients. The tag’s like “xyz” in Department attribute and in the group attribute, will be helpful to identify the xyz specific groups and users.
Step 3: xyz Three lines of Defense model stakeholders gets the data for the user access review	The following stakeholders of xyz Three lines of Defense model, get the data from the vendor to complete the user access review: 1. IT Network & Security team (primary data owner and point of contact for all xyz network related information) – need the data for their daily monitoring and decision making. 2. Risk & Compliance team – Need data for their monthly reviews 3. Assurance team – Need data for their adhoc reviews



xyz’s User IT Network Access Process
Vendor (Cloud Service Provider)
xyz Enterprise
Initial Request
IT Network Access
Start
xyz employee
(In case of new Employee, Departed Employees, De-Provisioning, New Provisioning)
(Raised for Manager’s Approval)
Reporting Manager
(After Approval)
IT Service Request
(Updatedl)
Active Directory (Account Access)
(New user, De-Provisioning, New Provisioning)
xyz’s AD Groups
Group1
Group2
Group n
(Extract Data for "User Access Review")
IT Network & Security Team (1st Line of Defense)
Risk & Compliance Team (2nd Line of Defense)
Assurance Team (3rd Line of Defense)
(End of Access Review)
End

3.2 High Level Current State Analysis and Architecture

The following picture depicts the current state of the data silos.



Current State analysis as follows:

1. Due to data silos, the data collected by one team is not fully accessible to the other teams. It has created barriers to information sharing and collaboration across the key stakeholders.
2. Generic transformation and business rules are designed and interpreted differently by team that led to inconsistencies in their results. There is no single source of truth (SSOT). This has impact on the decision-making process in managing and monitoring xyz's "user IT network access".
3. Outdated HR data is used for "user IT network access" review.
4. No data governance principles and no standardization checks are implemented to manage Active Directory data.
5. As a result, there is a lag in deactivating the network access of departed/terminated employees.
6. Currently, there is no clean revoke of user's AD group assignments in case of rehired or transfers.
7. Dormant users' access is still not revoked after 90 days.
8. No automation is implemented to save cost and reduce processing time.
9. Unable to update the Vendor Active Directory when managers forgot to approve or submit the IT service requests of his/her reportees.

4 Future State

4.1 High Level Future State Business Process

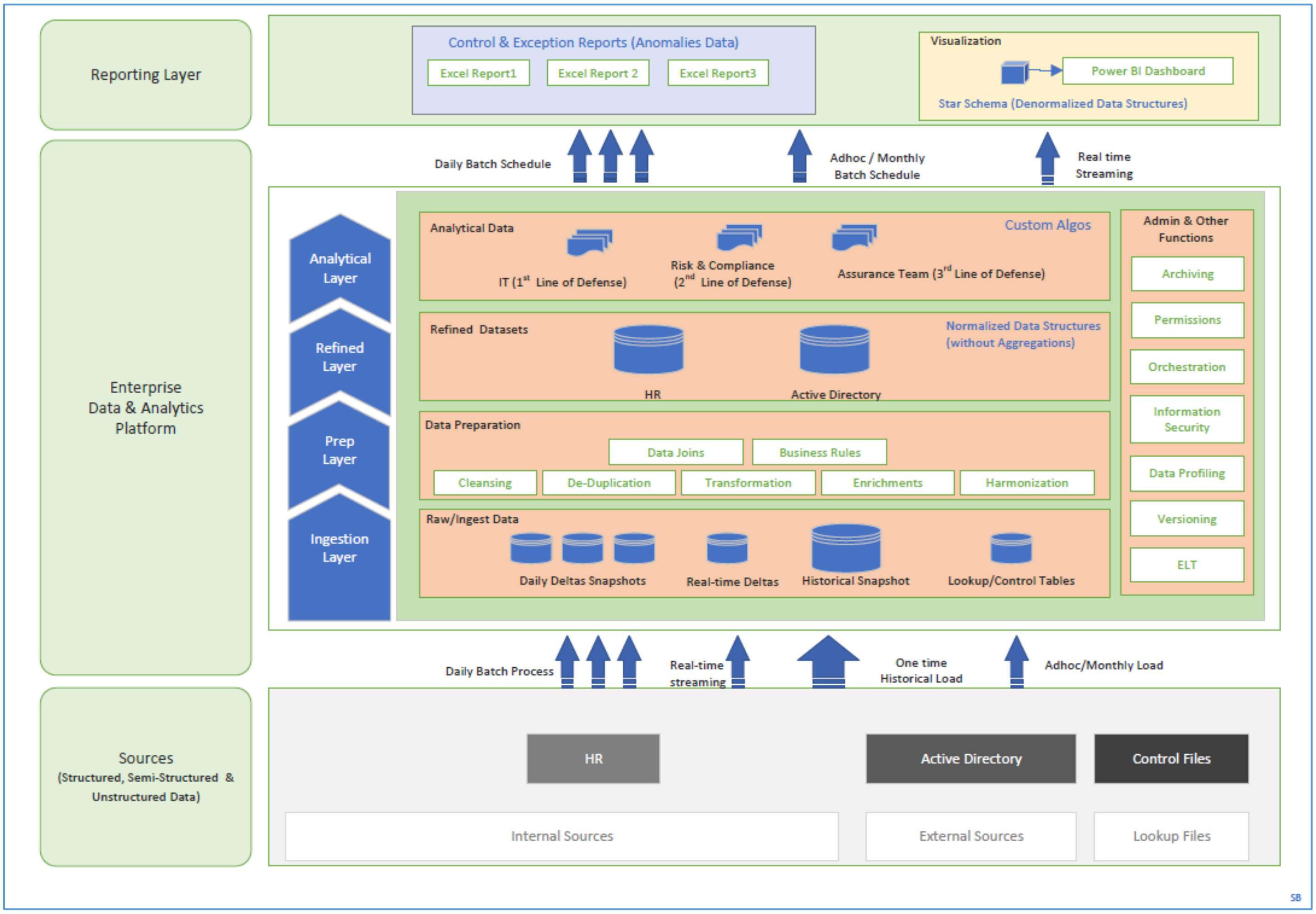
There are no changes required in the current business processes. But the following recommendations will be helpful to enhance data quality in active directory.

1. "Three lines of Defense" stakeholders should use single source of truth (SSOT), share and collaborate in review "user IT network access".
2. 90 days policy (clean revoke user access and assignments if account is not active more than 90 days) should be implemented strictly.

3. Daily cross validation with HR data will be helpful in removing the access of unauthorized users and terminated employees.
4. AD master date should be reviewed more frequently.

4.2 High Level Future State Analysis and Architecture

The below depicts the future architecture by leveraging enterprise data lake and analytics services.



5 Gap Analysis

The stakeholders of three lines of defense model should

1. Coordinate and use single source of truth (SSOT) by avoiding data inconsistencies.
2. Leverage enterprise data lake in sourcing and curating the active directory data and break data silos. Thereby, it would help in saving cost and data processing time.
3. Run control/exceptions reports more frequently and should have independent objectives to foster an efficient environment.

6 Requirements

6.1 Business Requirements

The following are the business requirements of the business stakeholders to digitalize three lines of defense checks:

#BR	Business Requirement	Description	Business Stakeholder/Owner
1	Daily Operational Review of network access of XYZ's users.	To provide operational visual dashboard so that IT security team can review the user's network access and can make decisions in controlling user's network access in their day-to-day activities. And also, should able to manage the master date, especially for attributes – department and groups	IT Security operations team (1st line of defense)
2	Monthly validation of active Network access of XYZ's users by their managers	To generate excel files at end of each month for each manager in XYZ so that they can review and validate their reportee's network access.	Risk & Compliance team (2nd line of defense)
4	Adhoc review of active Network access of XYZ's terminated users.	To generate excel file with list of terminated users having network access to XYZ entities/groups, for assurance/audit team on adhoc basis.	Assurance team (3rd line of defense)

6.2 Data Requirements

Please consider the below source datasets:

1. HR daily snapshot
2. AD daily snapshot

7 High Level Solution Definition

7.1 Strategic Solution

As describe in the section 4 - Future State Architecture, the following

Layers	Solution Description	Data Toolsets

Ingestion Layer	• Establish connection with source systems (HR, AD, Control excel files) and schedule data extractions either through EOD batch feeds or adhoc feed.	**Azure ecosystem**: Azure Data Factory or Azure Databricks **Salesforce/AWS ecosystem**: Mulesoft
Storage & Preparation Layer	• Storage the raw (as-is) datasets and refined normalized datasets in format accessible to query & analytical processing. • Apply all standardization, cleansing, de-duplication, and enrichments. • Optimize for low cost, scalability, high performance, and security. • Ensure that the data management activities are performed based on enterprise data governance framework and enterprise architecture principles.	**Azure ecosystem**: Azure Data Lake or Azure Delta Lake **Salesforce/AWS ecosystem**: Amazon S3
Analytical Layer	• Should empower every analyst across your organization to quickly build complex custom analytics by using SQL and Python. • Easy to store and able to share outcomes to key stakeholders of three lines of defense model.	**Azure ecosystem**: Azure Synapse or Azure Databricks **Salesforce/AWS ecosystem**: Amazon Athena
Reporting Layer	• Should provide provision to build denormalized data structures and rich custom visuals using Power BI or Tableau. • Also, able to present the data in different formats – excel, csv, txt.	**Azure ecosystem**: Power BI, Power App, MS-Excel/CSV **Salesforce/AWS ecosystem**: Tableau, MS-Excel/CSV, Amazon Quick Sight

7.2 Tactical Solution

If the building the ecosystem takes more time, the below short-term steps should be taken to achieve the project objective and to gain customer confidence. This will also help to understand the nitty-gritty of the data issues and code can be reusable.

Layers	**Solution Description**	**Data Toolsets**
Ingestion Layer	• Source systems datasets (HR, AD) and Control excel files are placed in SFTP drive. • Design the data extraction pipelines using Python.	Python Analytical workbook; Google Colab (for demo)

Storage & Preparation Layer	• Storage the raw (as-is) datasets and refined normalized datasets in secured network drive. • Apply all standardization, cleansing, de-duplication, and enrichments. • Ensure that the data management activities are performed based on enterprise data governance framework and enterprise architecture principles.	Python Analytical workbook; Save to local drive Google Colab (for demo); Save to Github (for demo)
Analytical Layer	• Can build and deploy build complex custom analytics by using Python. • Easy to store to secured network drive and able to share outcomes to key stakeholders of three lines of defense model.	Python Analytical workbook; Google Colab (for demo)
Reporting Layer	• Should provide provision to build denormalized data structures and rich custom visuals using Power BI or Tableau. • Also, able to present the data in different formats – excel, csv, txt.	Power BI, MS-Excel/CSV

8 Project Scope Statement

8.1 Project Objective

Project objective is to digitalize the “User’s IT Network Access Controls” by leveraging the enterprise data lake and analytics. Thereby, it would help key stakeholders of “Three Lines of Defense Model” to set risk control mechanism with strong corporate governance for better decision making and assurance reporting in monitoring “User Network Access” of xyz enterprise.

8.2 Project Scope

- All users in vendor’s active directory who are tagged to xyz departments and xyz groups. Both active and inactive users.
- Digitalize the “User’s IT Network Access Controls” by leveraging the enterprise data lake and analytics
- Train stakeholders of “Three Lines of Defense Model” on the analytics outcomes and exceptions handling.
- Design operational visual dashboard in Power BI.
- Reviewing IT network access of rehired FTEs (employee) is part of the scope

8.3 Project Out-Of-Scope

- Entities/users/user groups within the active directory of cloud service provider (vendor), which don’t belong to XYZ, are not in scope.
- Does not cover security at the database, operating system, network, client stations level, etc.
- Active directory’s segregation of duties is not in scope. Unable to identify conflict responsibilities.

- The source datasets don’t cover processing of Manager’s requests to the vendor.
- Current IT infrastructure as well as business processes do not support real-time analytics. To achieve that all IT system should be well integrated on real-time basis and should provide their real-time/near-time feeds to enterprise data lake.
- AD's daily EOD snapshot doesn't have historical versions and their metadata changes, like who approved, who created etc. Hence, the analytical reports don’t include any of these metadata attributes.

8.4 Project Dependencies

- Availability of key stakeholders to participate in necessary business processes and technical reviews.
- Establishing the data ingestion connection or SFTP connection to vendor system after adhering to their security checks as well as internal security checks.

8.5 Project Assumptions

- Ensure all necessary and appropriate stakeholders are available to participate in necessary business processes and technical reviews.
- Assume that the work email in active directory could be possible match with HR Email id of each FTEs
- Unmatched emails or users with no emails in active directory are treated as contractor or mismatch
- Within the unmatched email list, if the user’s email id has suffix as xyz.com than they will be considered as “FTEs mismatch”
- All datasets are available on every day between 10pm to 12pm after completion of the dependent jobs in the respective source systems.
- Vendor and xyz’s security teams will implement a clean revoke in scenarios like - Termination, Transfers or any other events that are linked to role change.
- Assume that data owners/stewards/custodians will provide complete and validated daily datasets in tandem to the business processes.
- Project virtual servers or environments are configured as expected.
- The project scope will not change once the stakeholders sign off on the BRD.
- The system of the project is compatible, functions properly and stable for the project to take place smoothly.
- Project will be completed in expected timelines and within the budget allocated.

8.6 Project Constraints

- As AD don’t have metadata information on the version history in its dataset, it’s not feasible to provide version changes of each user account.
- No primary key for AD user/ group assignments, there will be some challenges in maintaining the delta extractions.
- Vendor’s Active Directory does not delineate between xyz FTEs and contractors.
- HR datasets don’t have information on the contractors. HR system is only for the FTEs
- Data quality issues (like email mismatches, user id mismatches, no standard master data etc) in the vendor AD, might be a constraint in designing and maintaining the dashboard visuals.

8.7 Project Risks

- No control over staff priorities in unexpected events like COVID-19 pandemic.
- Vendor’s statement of work (SOW) might be delayed in getting approved by procurement team due to post COVID-19 changes in the business processes.

8.8 Project Cost Estimates, Team and Timelines

Strategic Solution	• $25k for Design, Build, Test and Deploy (One time) • $10k per annum (for Maintenance support) • Project timelines are approx. 6-8 months • Automation of continuous analytics and process digitalization • **Project team:** Integration/ETL specialist, Data Engineer, Data Architect, Business Analyst, Power BI Developer, QA and Project Manager.
Tactical Solution	• $15k for Design, Build, Test and Deploy (One time) • $5k per month (for Maintenance support) • Project timelines are approx. 2-3 months • Resources are required to run data pipelines manually. Prone to errors. • **Project team:** Data Engineer, Data Architect, Business Analyst, Power BI Developer.

9 Appendices

9.1 List of Acronyms

Acronyms	Meaning
ETL	Extract Transform and Load
DW	Data warehouse
DB	Database
API	Application Programming Interface
AD	Active Directory

9.2 Glossary of Terms

Data wrangling (ELT), sometimes referred to as data munging, is the process of transforming and mapping data from one "raw" data form into another format with the intent of making it more appropriate and valuable for a variety of downstream purposes such as analytics. A data wrangler is a person who performs these transformation operations.

Extract-Transform-Load (ETL) is different from data wrangling. Here, we extract source data and apply the required transformations and then, load the refined data to target system.

9.3 Related Documents

Link(s)
Three lines of Defense Model: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf
Three lines of Defense Model to Cloud Operations Segment: https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defense
Digital Transformation: https://www.i-scoop.eu/digital-transformation/
COVID-19 impact on business strategy :https://www.ibm.com/thought-leadership/institute-business-value/report/covid-19-future-business