Module 04 Course Project – Performing an Audit

John Doe, Student

College

Author Note

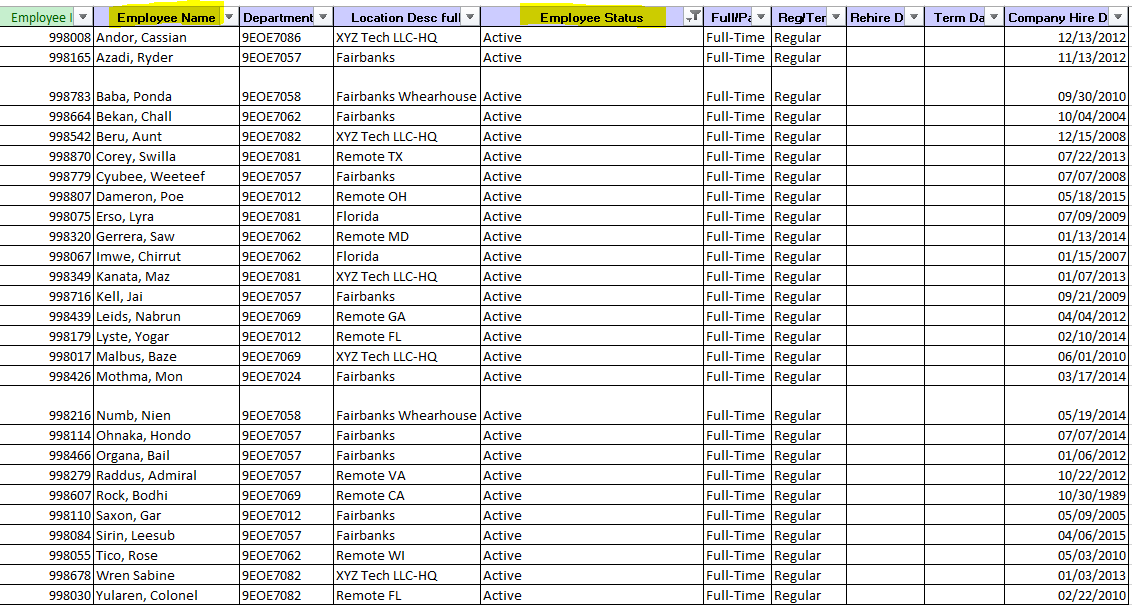
This assignment is being submitted on July 26, 2019, for Clifton Krahenbill’s CIS3240C Section 01 Security Controls.

# Auditing

Typically, the term audit can refer to the examination and evaluation of an organization’s financial statements (Tuovila, 2019). However, this is not the only method of auditing. ISO 19011 is another set of guidelines, resourceful for auditing management systems (American Society for Quality, 2019). Furthermore, ISO 19011 can involve process auditing, product auditing, or system auditing. XYZ Technology Services engages in frequent auditing procedures, to validate employees, who all have access to XYZ’s VPN network. The current auditing process requires a comparison of XYZ Technology Services Active Directory (AD) users and computers; to XYZ Technology Services HR employee census report. This document, reveals the inconsistent results, from the informational process comparison.

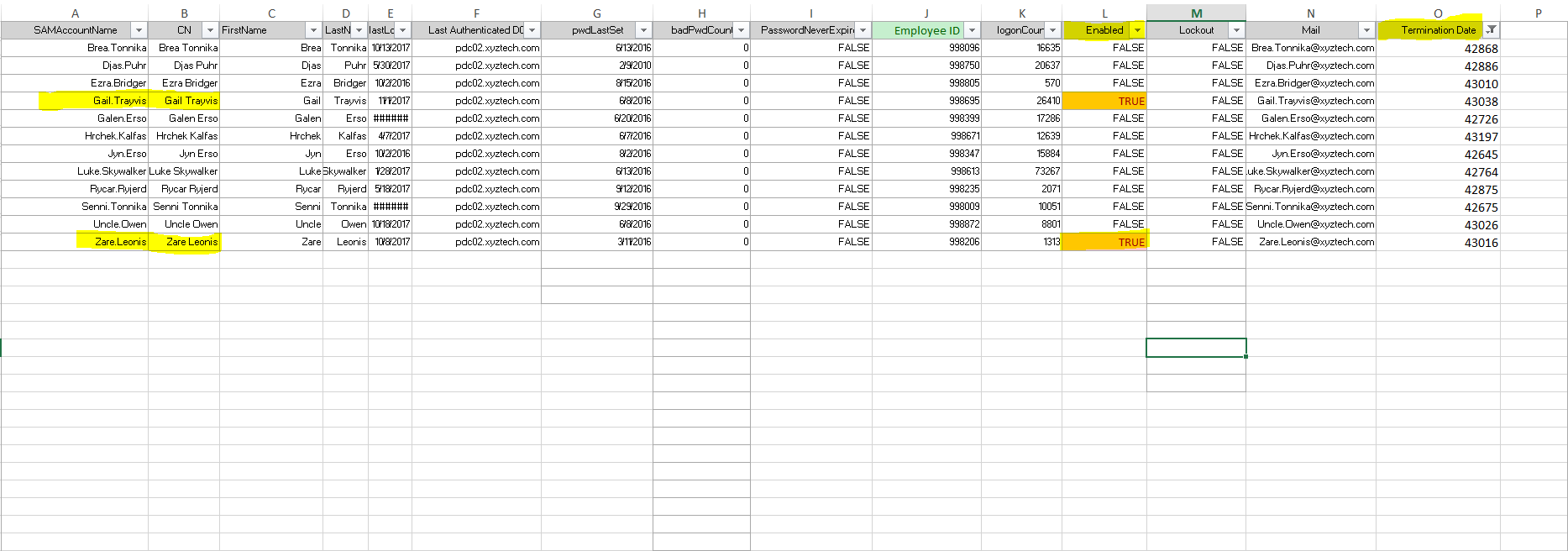
# HR Sheet (Employee Census Report)

This image displays the active employees within XYZ Technology Services.



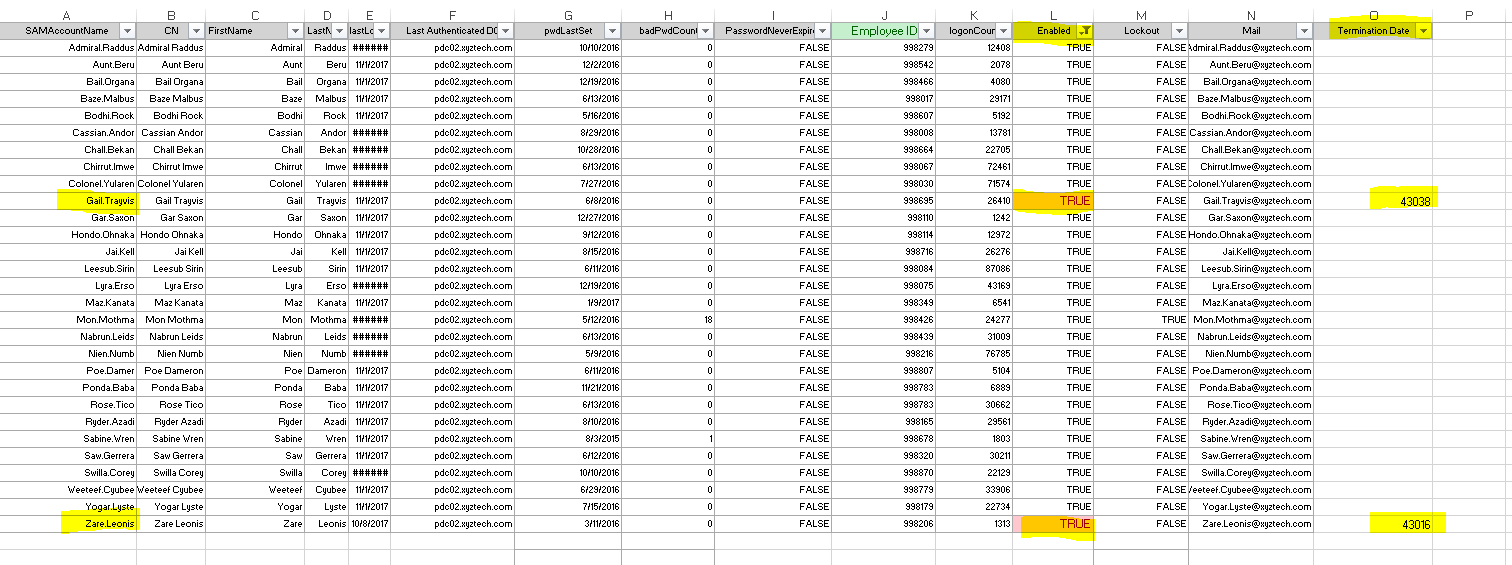
# AD List (Terminated Employees)

This image displays employee terminations, containing inaccurate data. Terminated employees should not have active AD accounts. However, it appears that two termination accounts (Gail Trayvis and Zare Leonis) are still active.



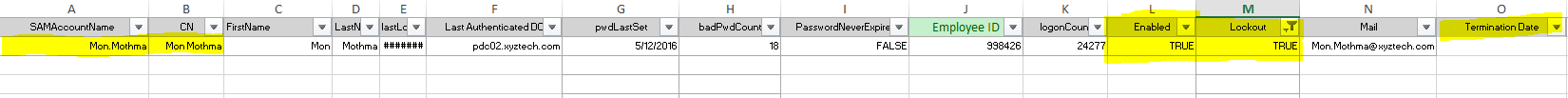
# AD List (Active Accounts)

This image displays all AD active accounts, including the two termination accounts causing numerical discrepancies.



# AD List (Unique exception found)

One active AD account appears to be on lockout! Active Directory contains lockout policies to prevent intruders from performing password attacks (Bertram, 2018). Furthermore, an employee who forgot their password could also experience a lockout.



# Auditing Checklist

Periodic Employee / VPN access audit

|  |  |
| --- | --- |
| **Auditor Information** | |
| Date Audit Completed: | November 1, 2017 |
| Audit Conducted By: | Nicholas Blackshire |
| Detail any exceptions found, and remediation processes | |
| There are two active employee termination accounts, which should be disabled immediately. Another exception is the one Active Directory account that is currently on lockout. This account belongs to Mon Mothma, who is an active employee. Administrators can remove the lockout on this account or investigate the authenticity of this event, to remediate the issue. | |

|  |  |  |
| --- | --- | --- |
| **Control Monitoring** | | |
| CC5.5-4 | Periodically, the IT Security Analyst compares the current employee listing from the payroll system to active employees in the XYZ Technology Active Directory system to ensure that any existing employees have system access disabled within 24 hours of termination. | |
| CC5.6-6 | Periodically, the IT Security Analyst compares the current employee listing from the payroll to employees with VPN access. | |
| Number of Enabled Active Directory Accounts: | | 29 |
| Number of Active Employees Based on Employee Census Report: | | 27 |
| Difference of Enabled Accounts from Employee Census: | | 2 |
| In the space below, detail what is known by the data why these two numbers do not match, and include details of the Employee Names or Active Directory Account Names: | | |
| The results from the VLOOKUP formula reveal that two termination employee accounts are still active. Thus, allowing them to access Active Directory. Gail Trayvis and Zare Leonis are the names of these employees, who no longer work for XYZ Technology Services. These are the two Active Directory accounts causing inconsistencies. | | |

References

American Society for Quality. (2019). ISO 19011. Retrieved from <https://asq.org/quality-resources/iso-19011>

Bertram, A. (2018). How to resolve Active Directory account lockouts with PowerShell. Retrieved from <https://www.business.com/articles/powershell-active-directory-lockouts/>

Tuovila, A. (2019). Audit. Retrieved from <https://www.investopedia.com/terms/a/audit.asp>