Applied Cybersecurity, Compliance Documentation, and IT Automation in a Microsoft 365.

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Cynthia Korankye is a student at George Mason University graduating with a bachelor's degree in information technology with a concentration in Cybersecurity. Her academic focus includes cybersecurity, information security and compliance. During this project, she supported security control analysis, policy documentation, system compliance mapping, and the development of an automated IT ticketing system within a Microsoft 365 environment. This work included documenting compliance requirements related to Federal Contract Information (FCI) and implementing secure operational processes.

Aaron Leinberger is a student at Virginia Tech graduating with a bachelor's degree in Cybersecurity Management and Analytics. During this project, he contributed to policy documentation, creation and enforcement of policy restrictions focusing on conditional access policies and media restrictions, as well as working on the development of an automated IT ticketing system. He worked to help FWI create a CMMC level 1 compliance report that focused on securing FCI and cleaning up their environment.

Matthew Ryan is a student at Virginia Tech graduating with a bachelor's degree in Cybersecurity Management and Analytics. During this project he worked mainly on the CMMC level one System Security Plan. Mainly Focusing on Access Control, Media Protection and Physical Protection. He also, created a daily scan through Intune to ensure defender regular scans devices for malicious files and potential threats. Additionally, He contributed to the development of an automated IT ticketing system to streamline issues tracking and response. Overall, this project provided hands-on experience applying security controls and automation to support CMMC Level 1 compliance.

Sabiya Shoukat is a student at George Mason University graduating with a Bachelor of Science in Information Technology with a concentration in Cloud Computing. Her academic focus includes cloud computing, Microsoft 365 services, IT automation, and secure system design. During this project, she contributed to Microsoft 365 based automation workflows, SharePoint and Power Automate solutions, and compliance documentation. Her work included documenting Microsoft 365 services, system boundaries, users, devices, data flows, and Federal Contract Information (FCI) handling, supporting System Security Plan evidence, and developing an automated IT ticketing system to improve operational tracking and accountability.

----- ***Industry Participant / Mentor*** -----

Steven Reece
IT Manager
FedWriters, Inc. (FWI)

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

FWI served as the industry partner for this PREP project and provided real-world guidance on cybersecurity practices and compliance expectations. The mentor worked closely with the student team to explain how security controls are applied in a Microsoft 365 cloud environment. This guidance helped ensure the project deliverables aligned with organizational needs, operational processes and practical security standards.

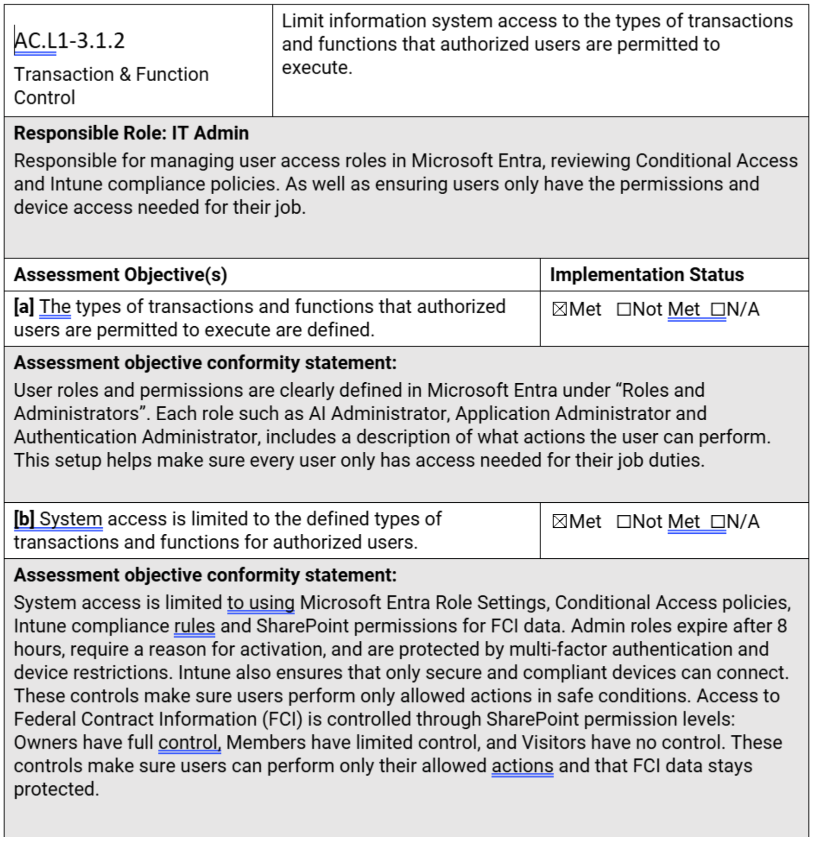
Business Challenge

FWI needed assistance documenting and organizing cybersecurity controls for its Microsoft 365 environment to support compliance and audit readiness. The organization required clear documentation showing how Federal Contract Information (FCI) is stored, processed and protected across Microsoft 365 applications and Monday.com. In addition, FWI needed help defining system boundaries, identifying users and devices, documenting access control and authentication practices and improving internal IT request tracking and accountability.

Activities Done to Address the Business Challenge

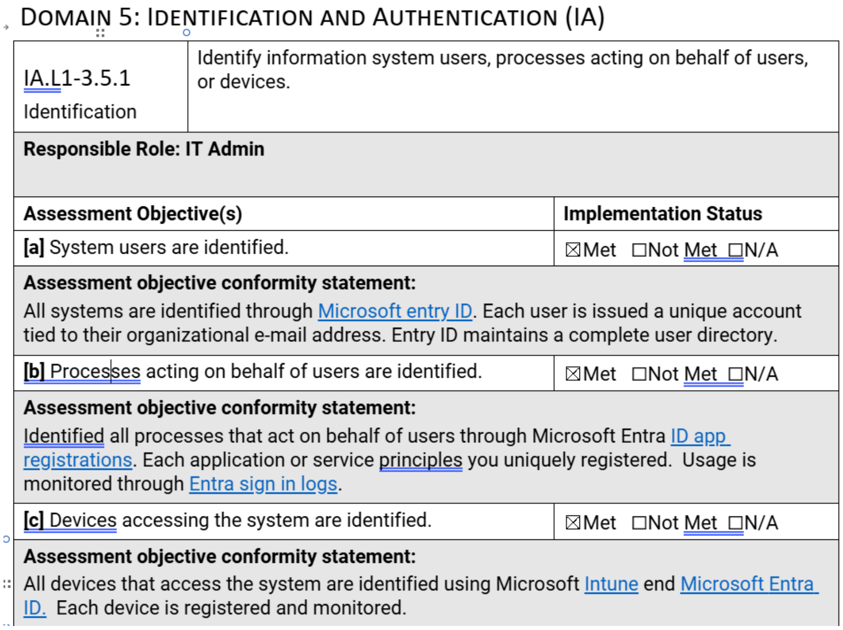
The student team completed the following activities:

- **Documented Transaction and Function Control (AC L1-3.1.2)** by reviewing how the system limits information system access to only the transactions and functions authorized users are permitted to perform. The screenshot provided demonstrates how access controls are enforced to restrict user actions and protect Federal Contract Information (FCI).



AC.L1-3.1.2 Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
Responsible Role: IT Admin Responsible for managing user access roles in Microsoft Entra, reviewing Conditional Access and Intune compliance policies. As well as ensuring users only have the permissions and device access needed for their job.	
Assessment Objective(s)	**Implementation Status**
[a] The types of transactions and functions that authorized users are permitted to execute are defined.	☒Met ☐Not Met ☐N/A
Assessment objective conformity statement: User roles and permissions are clearly defined in Microsoft Entra under "Roles and Administrators". Each role such as AI Administrator, Application Administrator and Authentication Administrator, includes a description of what actions the user can perform. This setup helps make sure every user only has access needed for their job duties.	
[b] System access is limited to the defined types of transactions and functions for authorized users.	☒Met ☐Not Met ☐N/A
Assessment objective conformity statement: System access is limited to using Microsoft Entra Role Settings, Conditional Access policies, Intune compliance rules and SharePoint permissions for FCI data. Admin roles expire after 8 hours, require a reason for activation, and are protected by multi-factor authentication and device restrictions. Intune also ensures that only secure and compliant devices can connect. These controls make sure users perform only allowed actions in safe conditions. Access to Federal Contract Information (FCI) is controlled through SharePoint permission levels: Owners have full control, Members have limited control, and Visitors have no control. These controls make sure users can perform only their allowed actions and that FCI data stays protected.	

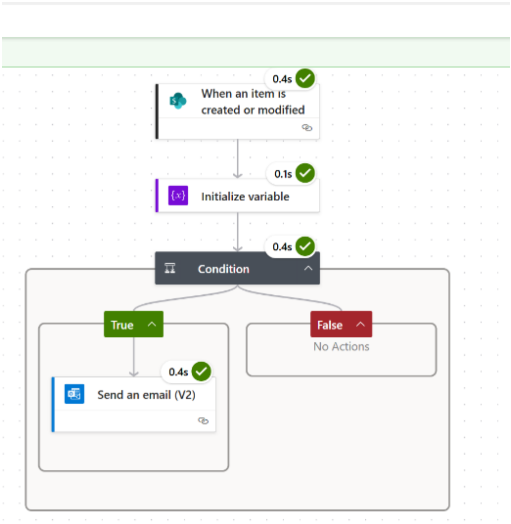
- **Documented Identification controls (IA L1-3.5.1)** by reviewing how information system users and processes acting on behalf of users or devices are uniquely identified. The identification screenshot shows how user identities are established and verified to support secure system access.



Domain 5: Identification and Authentication (IA)

IA.L1-3.5.1 Identification	Identify information system users, processes acting on behalf of users, or devices.
Responsible Role: IT Admin	
Assessment Objective(s)	**Implementation Status**
[a] System users are identified.	☒Met ☐Not Met ☐N/A
Assessment objective conformity statement: All systems are identified through Microsoft entry ID. Each user is issued a unique account tied to their organizational e-mail address. Entry ID maintains a complete user directory.	
[b] Processes acting on behalf of users are identified.	☒Met ☐Not Met ☐N/A
Assessment objective conformity statement: Identified all processes that act on behalf of users through Microsoft Entra ID app registrations. Each application or service principles you uniquely registered. Usage is monitored through Entra sign in logs.	
[c] Devices accessing the system are identified.	☒Met ☐Not Met ☐N/A
Assessment objective conformity statement: All devices that access the system are identified using Microsoft Intune end Microsoft Entra ID. Each device is registered and monitored.	

- **Designed and implemented an automated IT Ticketing System** using Microsoft Forms, SharePoint Lists, and Power Automate to support internal IT request tracking and accountability.
- **Configured automated email notifications** for the IT Ticketing System. Screenshots include confirmation emails sent to users when a ticket is successfully submitted and notification emails sent to IT staff when a new ticket is assigned, including ticket ID, category, description, and assigned personnel.
- **Developed the IT Ticket Submission Power Automate flow**, which includes actions such as when a new response is submitted, get response details, create a SharePoint list item, apply conditions, process uploaded screenshots, attach files, and send confirmation emails. The submission flow screenshot demonstrates how tickets are automatically created and documented.
- **Developed the IT Ticket Completion Power Automate flow** to track ticket resolution. This flow triggers when a ticket is updated, checks ticket status, and sends a completion email to the requester. The screenshot shows how ticket completion is automated and communicated.



- **Documented ticket lifecycle tracking within the CMMC Readiness system**, including Ticket GUID, ticket description, submission date and time, status, requester, assigned staff, completion comments, and file attachments. The screenshot provided shows how supporting evidence uploaded by users is stored and displayed in SharePoint.
- **Verified secure storage of ticket attachments**, ensuring uploaded screenshots appear correctly in the ticket record and support audit readiness and compliance documentation.

Results & The Positive Impact

As a result of this project, FWI received:

- Clear and organized security policy documentation aligned with compliance requirements.
- Improved documentation of how FCI is stored and processed within Microsoft 365 applications and Monday.com.
- Better visibility into system users, administrators, devices and access controls.
- Structured explanations of system boundaries, network topology and data flow.
- A fully functional automated IT ticketing system that improves issue tracking, documentation, and response accountability.
- Improved operational visibility through ticket attachments and status tracking stored in SharePoint.
- Increased readiness for audits, assessments and future compliance efforts.

These outcomes strengthened FWI's security documentation, operational processes, and overall compliance posture.

Conclusion

This PREP project allowed the student team to apply classroom knowledge to a real-world cybersecurity and compliance challenge. By translating technical configurations into clear documentation and building an automated IT ticketing solution, the team helped FWI improve both its security governance and daily operational practices. The collaboration highlighted the value of experiential learning while providing meaningful support to an organization managing sensitive information in a cloud environment.

PREP Student Reflection

Participating in this PREP project provided hands-on experience with real-world cybersecurity documentation, cloud security practices, and workflow automation. Working directly with an industry mentor helped connect academic concepts to practical implementation. The project strengthened skills in technical writing, system analysis, automation, teamwork and problem-solving. It also emphasized the importance of clear documentation and secure operational processes in protecting Federal Contract Information and supporting compliance in modern organizations.