Azure Virtual Desktop (AVD) Infrastructure & Cloud Compliance Initiative with FWI

A Professional Readiness Experiential Program (PREP) Project Effort

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

Matthew Burd is a dedicated and highly motivated Cybersecurity student at Old Dominion University, currently pursuing a bachelor's degree in Cybersecurity, with a strong foundation built even before entering college. Through dual enrollment in high school, he earned a Cybersecurity Fundamentals certificate, gaining early hands-on experience with networking concepts, Python programming, and Linux systems, and C++, demonstrating both initiative and a clear commitment to the field from an early stage.

Since enrolling at ODU, he has significantly expanded his technical skill set, developing deeper expertise in Linux environments, network architecture, and core cybersecurity principles through both academic coursework and practical application. He has earned his CompTIA Network+ certification, validating his knowledge of networking infrastructure, troubleshooting, and security fundamentals, and is actively preparing to obtain the Security+ certification to further strengthen his qualifications.

With a proven ability to quickly learn and apply complex technical concepts, combined with a strong work ethic and passion for cybersecurity, he is well-positioned to contribute effectively in professional environments. His background reflects not only technical competence but also a proactive mindset and long-term commitment to growth in the cybersecurity field, and this continued to expand upon learning skills in Azure, Power Automate, and Intune with this Internship

Ian Burd is a student at Old Dominion University graduating with a bachelor’s degree in Cybersecurity. Before enrolling in Old Dominion, he dual enrolled in Cybersecurity classes through Central Virginia Community College with classes based around Networking, Cybersecurity Law, Cyber Attacks and. He is a Cybersecurity Intern at Fedwriters. He has some experience with Linux, SIEMS in Wazhuh, Firewalls, and Wireshark. He is CompTIA Network+ Certified which allowed him to prove his knowledge of networking and security concepts. He is currently pursuing CompTIA Security+ as well.

Through the internship, he expanded his skills in building virtual desktops and configuring devices and user settings with both security and usability in mind. He also worked with new tools such Power Automate to automate workflows and improved his troubleshooting skills while learning how they work. Furthermore, Ian developed baseline configurations aligned with organizational requirements, enabling efficient restoration of digital infrastructure in the event of an emergency. He learns quickly through hands-on experience and demonstrates a strong work ethic, along with a genuine desire to develop new skills.

Aniah Daniels is a student at George Mason University graduating with a bachelor's degree in Computer Science with a concentration in Cybersecurity. She is AWS Certified with practical skills in AWS, Microsoft Azure, Linux, Python, Java, and C, coupled with hands-on penetration testing experience leveraging tools such as Kali Linux, Virtualbox/VMware, Wireshark, and Metasploitable to identify vulnerabilities and test exploits. She is well-versed in federal cybersecurity compliance frameworks, including CMMC and NIST SP 800-171, with experience translating complex security standards into actionable, technical guides. Additionally, Aniah has cultivated a foundational understanding of artificial intelligence and its intersection with cybersecurity, having evaluated and refined large language model outputs to ensure accuracy, fairness, and quality.

William Hoang is a student at James Madison University, graduating with a bachelor's degree in Computer Information systems with a concentration in Information and Cybersecurity Management. He has practical skills in Microsoft Azure, cybersecurity operations, and cloud security, with experience using tools such as Microsoft Sentinel, Wireshark, Kali Linux, Nmap, and VirtualBox to monitor networks, analyze threats, and assess system security. He is proficient in Python, SQL, and HTML, with experience in database management and developing secure technical solutions. William also brings strong analytical, communication, and teamwork skills, with the ability to adapt quickly and collaborate effectively in fast-paced environments.

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

Steven Reece
IT Manager
FWI FedWriters, Inc.

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

Brian K. Ngac, PhD
FWI Corporate Partner Faculty Fellow
Assistant Dean, Centers of Excellence
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

Across four months, our team worked with Steven Reece, Project Mentor and IT Manager of FWI FedWriters, to design and implement a secure, scalable cloud infrastructure. For our use case, we focused on the design, configuration, and automation of a cost-effective cloud environment built on Microsoft Azure. Our efforts included deploying and managing Azure Virtual Desktop (AVD) infrastructure, provisioning and configuring virtual machines, establishing dynamic device and user groups to streamline VM management, and automating key workflows through Power Automate and Azure Runbooks. We also developed compliance documentation, configured Microsoft Intune/Entra security policies, and worked to ensure the environment aligned with current CMMC compliance standards.

Business Challenge

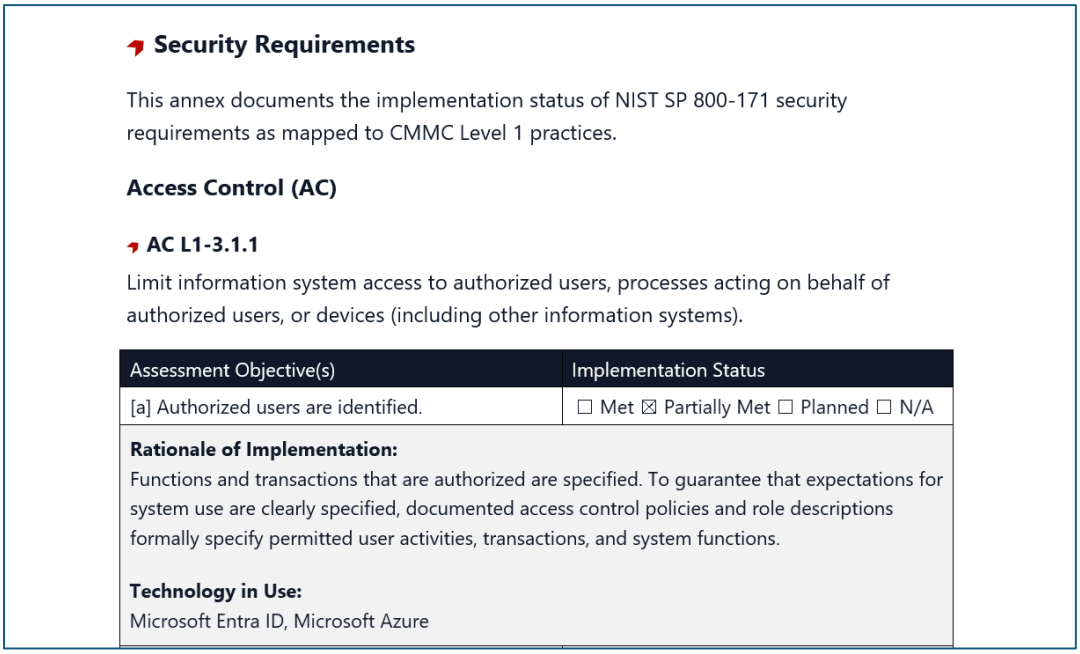
At FWI, our team needed to build a robust, secure cloud infrastructure to support remote workforce operations while adhering to CMMC L1 compliance standards. We also needed to establish role-based access control (RBAC) policies to ensure users and administrators had appropriate levels of access, protect Controlled Unclassified Information (CUI), standardize and simplify the user experience, monitor system activity and potential security threats, and automate routine IT processes. To demonstrate adherence, our team had to develop extensive compliance documentation throughout the project as evidence of our efforts.

Activities Done to Address the Business Challenge

To address our business challenge, our team completed the following main objectives:

- **Created an Infrastructure and Pre-Deployment Plan** outlining cloud resource requirements, hardware specifications, application access needs, and estimated monthly costs covering licensing and Azure services — scoped for a small-scale environment of 5-10 users and ≥ 3 virtual machines.
- **Mapped CMMC Controls to AVD** in Microsoft Excel by documenting CMMC Level 1 domains and their practical solution to our AVD environment, outlining how each compliance requirement would be implemented and enforced across the cloud based on the previously established infrastructure plan.
- **Created a Baseline Corporate Compliance Policy** that accurately reflected the settings, configurations, and requirements currently enabled, to allow for quick recovery in the event of emergency. This initiative also helped standardize systems across the organization and improve overall operational readiness.
- **Created a Dynamic Device Group and User Group** for VMs and VM users. All devices added to the FWI Host pool were added to the Dynamic Device group, with their respective users. This enabled devices to receive required configurations and updates automatically, improving efficiency, consistency, and administrative management.
- **Configured Remote FX Device Redirection** in the Local Group Policy editor to ensure users could leverage USB device redirection capabilities within their virtual desktop sessions.

- **Developed an IT Ticket System** using Power Automate, featuring a 5-question intake Microsoft Form, a structured SharePoint list capturing all responses, attachments, submission timestamps, completion timestamps, user details, and manager information. Automated email notifications were set up to alert users upon successful ticket submission and upon ticket completion, with a status column tracking each ticket through its lifecycle.
- **Configured a Local Administrator Policy Group** for VMs and VM Users. This consisted of the IT Interns User Group, and required authentication through Entra ID. Users who were properly authenticated were given local admin privileges; those that were not had standard user privileges.
- **Authored a System Security Plan (SSP)** encompassing key compliance documentation sections, including, but not limited to: System Details, FCI Data Flows, System Inventory, System Environment, System Requirements, CMMC L1 control implementations, and supporting appendices (as relevant to our cloud environment).



Security Requirements

This annex documents the implementation status of NIST SP 800-171 security requirements as mapped to CMMC Level 1 practices.

Access Control (AC)

AC L1-3.1.1

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Assessment Objective(s)	Implementation Status
[a] Authorized users are identified.	☐ Met ☒ Partially Met ☐ Planned ☐ N/A

Rationale of Implementation:
Functions and transactions that are authorized are specified. To guarantee that expectations for system use are clearly specified, documented access control policies and role descriptions formally specify permitted user activities, transactions, and system functions.

Technology in Use:
Microsoft Entra ID, Microsoft Azure

Figure 1: Example of Domain Control Rationale for AC-L1-3.1.1

- **Researched and Created a VPN Solution** by evaluating secure remote access options and implementing a reliable connectivity method that enabled users to securely access internal resources, while also improving remote productivity and maintaining network security.
- **Deployed a Virtual Machine Golden Image** with modified registry keys to enforce the auto-installation of O365 applications (e.g., Microsoft Teams, Outlook, Word, Excel, etc.), third-party applications (e.g., Adobe, Chrome), as well as a uniform desktop background to ensure a consistent and production-ready user environment across the cloud. This allowed for the deployment of several session hosts with the same base, significantly reducing time spent configuring each VM individually.
- **Configured a Monitoring Solution Using a Log Analytics Workspace** to allow logs to be captured and monitored from specified VMs.

- **Implemented the following additional Power Automate Algorithm(s):**

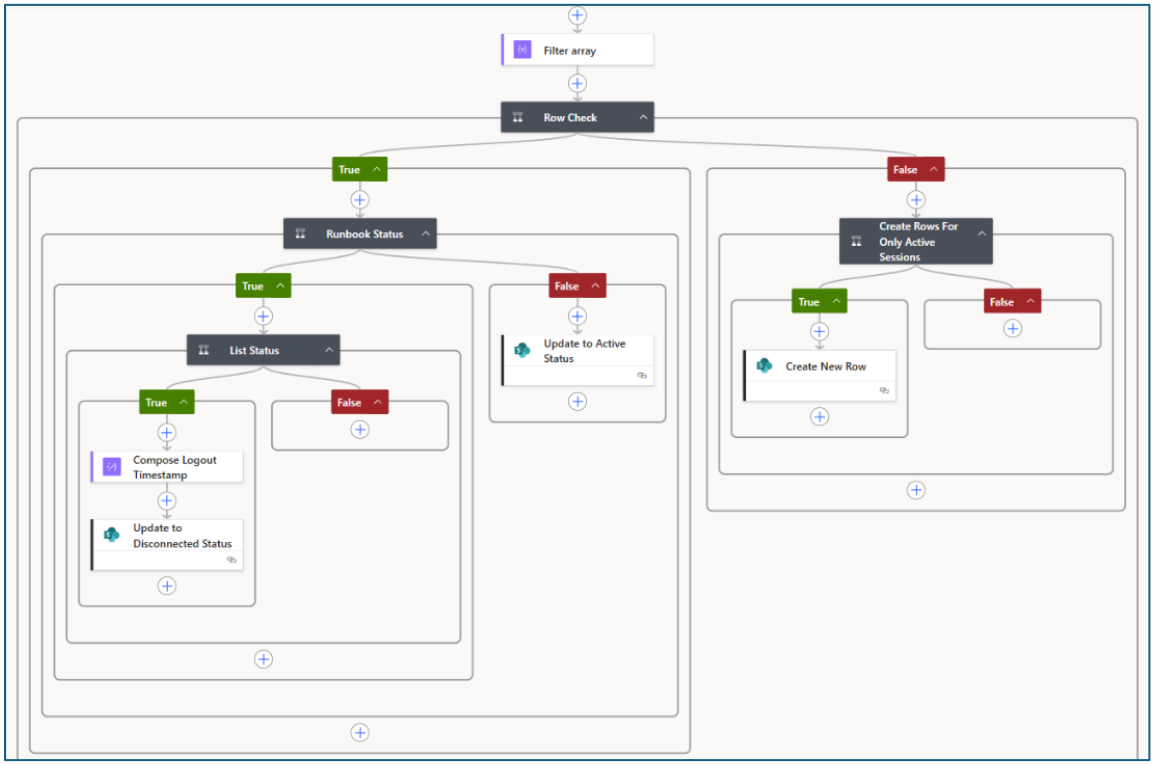


Figure 2: Example of Login History/Session Host Tracking Algorithm

  - **An Automated Login History Algorithm** using an Azure Runbook PowerShell Script to capture and export VM user login history to a structured SharePoint list, enabling consistent and automated record-keeping of authentication activity across the virtual environment.
  - **An Automated Secret/Certificate Expiration Monitoring Algorithm** using an Azure Runbook PowerShell Script to pull secret and certificate expiration dates across Enterprise Applications and Application Registrations; this data was populated into a structured SharePoint list and triggered automated notifications for any secrets or certificates expiring within 60 days.
  - **An Automated Auto-Disabler** Created a Power Automate access review workflow to automatically identify and disable accounts that have not signed in within a set inactivity period. The automation was scoped to a test group first, using a shorter time threshold for testing before applying the full 30-day inactivity rule.
  - **An Automated Subscription Tracking Algorithm** to include a Power Automate flow, a list through SharePoint, and a Microsoft form for people to complete; this data would populate in the SharePoint list and update consistently with all necessary information, making it easier to keep track of company subscriptions.
  - **An Automated Sign-In Frequency Tracker** to monitor Entra user sign-in activity, triggering automated alerts to the user's manager when no sign-in activity is

detected within three days or more, ensuring proactive oversight of account engagement across the organization.

- **Configured Session Rules and RDP Properties** for our host pool within the AVD environment to optimize user sessions by enforcing timeout policies, reconnection settings, and remote desktop performance configurations, improving stability, security, and overall user experience.

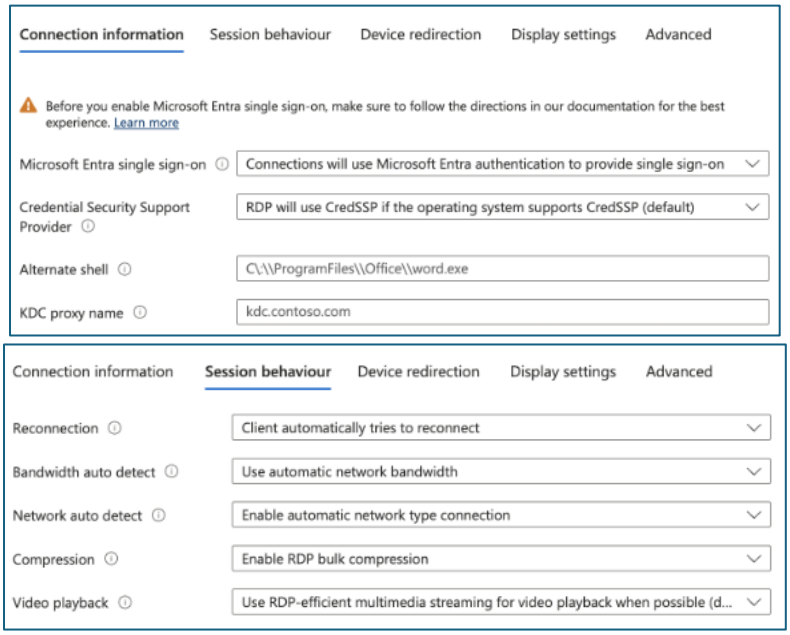


Figure 3: RDP Properties Connection Config

- **Configured Local Folder Structure via OneDrive Shortcuts** using a PowerShell Script that searched through the IT Interns User Group; this data would output SharePoint sites, IDs, and user emails. Any sites each user was a member of were shared to their respective OneDrive accounts.
- **Implemented Auto-Scale Execution for Virtual Machines** within the AVD environment to automatically start or shut down virtual machines based on user demand; when demand increased, auto-scale increased capacity by scaling horizontally. When demand dropped, auto-scale deallocated VMs to save and reduce costs.

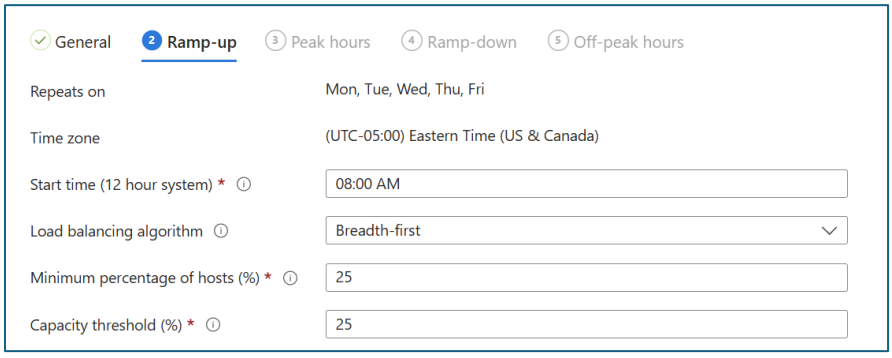


Figure 4: Autoscaling Ramp-Up Config

- **Configured Automated Microsoft Defender Vulnerability Notifications** to automatically alert administrators of newly detected high/critical vulnerabilities and security risks, enabling faster remediation, improved system security, and proactive threat management across the environment.
- **Configured a Default Homepage for all VMs**, including Adobe, Outlook, Teams, Excel, Word, Chrome to improve the professionality of Virtual Machines, keeping all the necessary software accessible and organized while increasing the ease of use.
- **Created a Group of Admins to Be Added Locally to All VMs**; our team created a centralized group of administrators that were automatically added to the local Administrators group on all VMs, ensuring consistent privileged access across systems. It simplified management by allowing our team to control admin permissions from one group instead of configuring each VM individually.

Results & The Positive Impact

Overall, the projects we collaborated on collectively and individually contributed to improving FedWriters's security posture while also enhancing the usability of its cloud infrastructure in key areas. Furthermore, the implementation of these additional improvements supports long term scalability and stronger security resilience. From a compliance standpoint, our documentation and control mapping efforts positioned FWI with a stronger foundation for meeting federal cybersecurity requirements, establishing reusable frameworks the organization can build upon as its compliance needs evolve.

The automation workflows we designed also significantly reduced the burden of manual IT oversight, giving the IT team greater visibility into the environment while freeing up time that would otherwise be spent on repetitive administrative tasks.

Conclusion

Over the course of this Internship, our team successfully designed and implemented a secure, scalable cloud infrastructure tailored to the operational and compliance needs of FedWriters. By leveraging Microsoft Azure and associated services, we built a fully functional Azure Virtual Desktop environment that supports remote workforce capabilities while aligning with CMMC Level 1 requirements. Through a combination of technical implementation, automation, and documentation, we addressed key business challenges including secure access control, system monitoring, standardized configurations, and operational efficiency. Our use of dynamic groups, automated workflows, and baseline configurations not only strengthened security but also streamlined administrative processes and improved consistency across the environment.

The development of compliance documentation, including the SSP, control mappings, and technical solutions, were directly aligned with regulatory expectations. This integration of compliance and engineering highlights the importance of building security into every layer of

system design rather than treating it as an afterthought. Beyond the technical outcomes, this project provided valuable hands-on experience in cloud infrastructure, cybersecurity operations, and team collaboration within a real-world business context. It reinforced our ability to translate complex requirements into practical solutions while maintaining a focus on security, usability, and scalability.

PREP Student Reflection

This internship with FedWriters gave all of us invaluable practical experience in developing and deploying real-world cloud architecture while striking a balance between security and usability needs. We improved our technical proficiency with Microsoft Azure, Azure Virtual Desktop, Power Automate, Entra, and Intune, and learned more about the practical applications of compliance frameworks like CMMC. Learning how automation can greatly increase productivity and decrease human error, especially via routines like inactivity tracking, ticketing systems, and monitoring solutions—was one of the most important lessons learned.

We developed our troubleshooting and problem-solving abilities in addition to our technical skills, especially when configurations didn't work as intended and needed to be tested and reworked again. Working in a team atmosphere also helped us improve our communication and teamwork skills because we had to coordinate tasks, communicate information, and align our ideas with both technological limitations and business goals. This event reinforced the importance of planning, documentation, and adaptability in cybersecurity and IT projects.

Through this experience, this internship helped all of us close the gap between academic and real-world use, increasing our confidence in our ability to support professional IT settings and cloud infrastructure. It also made our interest in cloud security and automation clear, and we intend to keep improving these skills in the future.