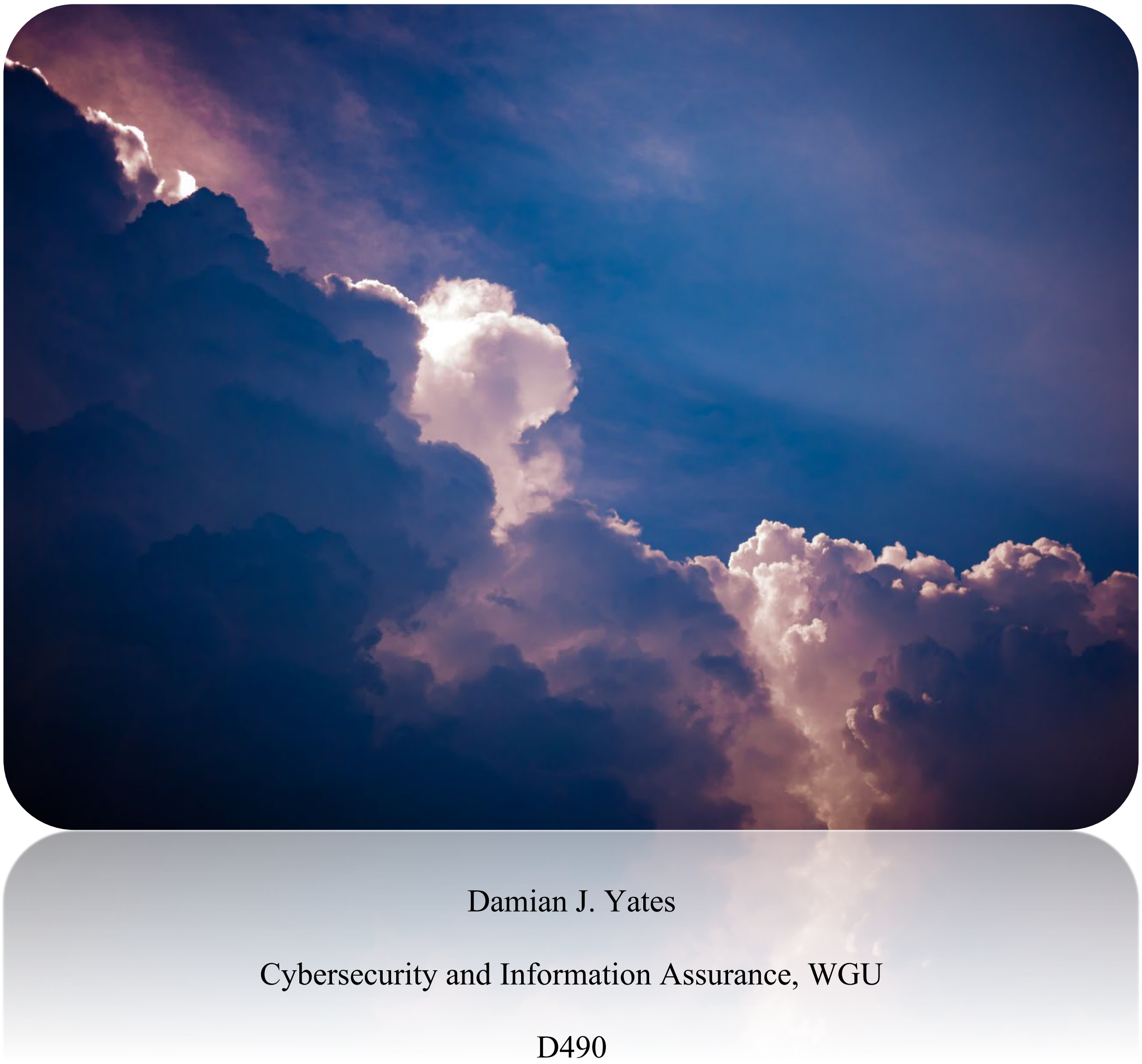
# DDN1 TASK 2: Project Proposal



Damian J. Yates

Cybersecurity and Information Assurance, WGU

D490

July 14, 2025

# Project Proposal

## Introduction

Nonprofit organizations rely heavily on digital tools to communicate, collaborate, and serve their communities. However, without dedicated technical staff or structured IT policies, many nonprofits face challenges securing sensitive data and managing user access effectively. This proposal outlines a plan to transition a small nonprofit organization from its current Google Workspace (G Suite) environment to Microsoft 365 Business Premium. The goal is to improve data security, streamline access control, and reduce the risks associated with misconfigured cloud settings and unmanaged devices. The migration will establish a foundation for secure collaboration, regulatory compliance, and sustainable IT practices tailored to the organization's needs and resources.

## Security Problem Under Investigation

A small nonprofit organization uses Google Workspace (formerly G Suite) for communication, document sharing, and operational needs. However, this environment lacks essential security and identity management features, putting the organization at risk of data breaches, unauthorized access, and regulatory noncompliance. The core security issue stems from the absence of centralized control over user access, device security, and data sharing policies. Staff members often use personal devices to access sensitive documents, and file sharing is frequently conducted using publicly accessible links without expiration or audit trails.

Multi-factor authentication (MFA) is not enforced, and there are no standardized policies for managing user roles or removing access when employees or volunteers leave the organization.

This problem is particularly critical given the nature of the data handled by the nonprofit, including personally identifiable information (PII) of clients, volunteers, and donors. The organization operates without dedicated IT personnel, and administrative staff typically make technological decisions informally. This lack of governance has created an environment where sensitive data is vulnerable to accidental exposure or malicious access. As the organization grows and expands its digital presence, the risks associated with unmanaged cloud usage continue to increase.

The proposed solution is a structured migration to Microsoft 365 Business Premium, a platform that offers built-in identity management, advanced security controls, endpoint protection, and compliance tools specifically tailored for nonprofit organizations. According to Microsoft's white paper "Secure your nonprofit with Microsoft 365 Business Premium", this solution enables nonprofits to enforce MFA, manage user access through Azure Active Directory, and gain visibility into threats through Defender for Office 365 (Microsoft, n.d.). Industry guidance from the Center for Internet Security Controls v8.1 also highlights the need for access control (Control 6) and secure configuration management (Control 4), both of which are lacking in the nonprofit's current environment (CIS Controls v8.1 update overview, 2025). Additionally, the Verizon Data Breach Investigations Report emphasizes that over 70% of security incidents in small organizations involve misconfiguration or credential misuse, risks directly present in this case (Verizon, 2023).

The root causes of the problem can be traced to several factors. First, the organization lacks an internal IT team or advisor to guide technology planning and risk assessment. Second, G Suite's baseline offerings do not provide enterprise-grade security features, such as conditional access, device compliance policies, or email threat protection. Third, there is no consistent onboarding or offboarding process for users, resulting in orphaned accounts with access to sensitive information. Fourth, staff are unaware of safe data handling practices, contributing to poor file-sharing habits. Lastly, the nonprofit does not maintain regular backups or logging capabilities, which impedes incident response and compliance readiness.

Addressing these root causes by migrating to Microsoft 365 will position the organization to operate more securely, meet emerging compliance requirements, and confidently support future growth.

## Project Stakeholders

The success of this migration project depends on the collaboration of internal and external stakeholders who each play a role in planning, execution, and long-term adoption. Internally, the Executive Director serves as the primary decision-maker and project sponsor. Their support is critical for allocating resources, approving timelines, and communicating the project's value to the broader organization. The Executive Director's key need is confidence that the new system will protect sensitive data while remaining easy to use for staff.

Program Managers and administrative staff represent daily users of the platform. Their involvement is essential during the training and testing phases, as they provide feedback on usability and report any operational disruptions. These individuals require a smooth transition, minimal downtime, and clarity on how the new tools support their workflows. Since they manage case files, schedules, and communications, they are directly affected by access controls and email security configurations.

Externally, a contracted IT consultant will oversee the technical implementation, including data migration, security configuration, and training. Their role includes aligning the migration with best practices and minimizing disruption to ongoing operations. This stakeholder must understand the organization’s goals and technical constraints to tailor the solution accordingly.

Finally, donors and community partners, while not directly involved in the migration, are indirect stakeholders. The organization’s ability to protect constituent data and operate securely enhances trust and credibility with these partners. A successful and secure implementation contributes to broader organizational sustainability and reputation.

## Data Supporting Decision-Making

The decision to transition from Google Workspace to Microsoft 365 Business Premium is supported by internal observations, user behavior analysis, and industry best practices. Although the organization lacks a formal IT audit history, several internal indicators reveal a growing security and operational gap. Logs from the Google Admin Console show repeated instances of publicly shared documents with no expiration settings. In one instance, a sensitive client intake form remained accessible to anyone with the link for over six months before it was discovered and removed. This type of misconfiguration highlights the risks associated with the current system’s lack of oversight and alerts.

Email security is another area of concern. The organization has experienced multiple phishing attempts that bypassed Google’s standard spam filters. One phishing attempt included a spoofed domain posing as a partner agency and was not flagged by existing email protections. Since Google Workspace's basic plan does not include advanced threat detection, the organization relies on user awareness, which varies widely among staff.

In discussions with administrative staff and volunteers, it became clear that there is no consistent process for adding or removing users, especially for departing interns or short-term volunteers. This has led to multiple inactive accounts remaining enabled and unmonitored in the system — a clear violation of access control best practices. Informal access logs and shared spreadsheet tracking methods further support the need for centralized identity and role management.

These issues align with findings in industry research. For example, Microsoft's nonprofit cybersecurity guide emphasizes the importance of conditional access, account lifecycle management, and MFA enforcement — all of which are absent in the current environment (Microsoft, n.d.). Additionally, guidance from the NIST Cybersecurity Framework and the CIS Controls (particularly Controls 4, 5, and 6) points to centralized log management, secure account provisioning, and consistent device protection (CIS Controls v8.1 update overview, 2025).

These internal observations and external benchmarks form the foundation for a structured migration and modernization effort to protect the organization's mission and digital assets.

# Project Requirements and Implementation Plan

## Solution Requirements

To effectively address the identified security challenges, the migration to Microsoft 365 Business Premium must fulfill several key technical and operational requirements. First, multi-factor authentication (MFA) will be enforced for all users to protect against credential theft. Azure Active Directory (Azure AD) will be configured to centralize identity management, with user roles defined by job function. Conditional access policies will be implemented to restrict access based on location, device compliance, and risk level. Endpoint security will be established using Microsoft Defender for Business, ensuring that only secure devices can access organizational data. Microsoft Purview Information Protection will also apply sensitivity labels to files containing personally identifiable information (PII), helping prevent unintentional sharing or data loss.

Operational requirements include straightforward onboarding and offboarding procedures to ensure that accounts are created and removed promptly and securely. Email security will be enhanced through Defender for Office 365, providing phishing detection, safe links, and attachment scanning. Mobile device management (MDM) will be implemented using Intune, allowing the organization to manage and wipe data from lost or stolen devices. Staff will be trained on using these new tools effectively, and access to administrative functions will be limited to designated personnel.

## Methodology and Design Principles

The solution will be designed and implemented in alignment with the NIST Cybersecurity Framework and the Center for Internet Security (CIS) Controls. These frameworks emphasize the principles of least privilege, defense in depth, secure configuration, and continuous monitoring. The implementation will also follow Microsoft's Cloud Adoption Framework for Nonprofits, ensuring best practices for governance, compliance, and scalability (Microsoft, n.d.). The project will prioritize simplicity and sustainability, using automation to reduce the burden on non-technical staff.

## Rollout Plan and Project Management Strategy

**The project will follow a phased rollout approach:**

- **Phase 1 – Planning and Assessment (Week 1–2):**
  Gather requirements, assess current data and account inventory, and define user roles and access policies.
- **Phase 2 – Pilot Migration (Week 3–4):**
  Select a small group of users (e.g., administrative staff) to test the migration process and ensure email, file sharing, and Teams functionality.
- **Phase 3 – Full Migration and Configuration (Week 5–6):**
  Migrate all user data (email, calendar, and Drive files), enforce security policies, configure Intune, and deploy Defender.
- **Phase 4 – Training and Support (Week 7):**
  Deliver role-based training sessions and provide documentation and hands-on support.
- **Phase 5 – Post-Implementation Review (Week 8):**
  Validate security controls, collect user feedback, and adjust policies based on operational needs.

The project will use a hybrid project management methodology, combining elements of Waterfall for planning and documentation with Agile-style check-ins during each rollout phase. Regular milestone reviews and stakeholder updates will be incorporated to maintain transparency and alignment.

## Implementation Risks and Impact

Several risks have been identified:

- **User Disruption Risk**: Staff may experience temporary confusion or downtime during the migration. This will be mitigated through pre-migration training and a pilot phase to uncover potential issues.
- **Data Loss Risk**: Improper migration of files or email could lead to data loss. Mitigation includes performing backups prior to migration and validating transfer logs.
- **Adoption Risk**: Non-technical users may resist adopting new tools. This risk will be addressed through user-friendly documentation and one-on-one support.
- **Configuration Errors**: Misconfigurations during setup may introduce new vulnerabilities. To prevent this, implementation will follow Microsoft best practices and use secure baselines validated by checklists and external documentation.

Each risk has been assigned a likelihood and impact rating, with mitigation plans to ensure the project's overall success without disrupting the nonprofit’s mission.

## Training Strategy

A comprehensive training strategy is essential to ensure a smooth transition and successful adoption of Microsoft 365 by all nonprofit organization members. Given that the organization has limited technical experience among its staff, the training program will be designed to be accessible, role-specific, and focused on practical day-to-day usage.

## Audience

The training will be targeted at three primary groups:

1. **Administrative and Program Staff** – Daily email, file storage, and collaboration tool users.

2. **Executive Leadership** – Oversight of users requiring visibility into communication and security reporting.

3. **IT Consultant or Technical Advisor** – Responsible for managing administrative controls, access policies, and compliance settings.

## Delivery Method

Training will be delivered through live virtual sessions and self-paced resources. Live sessions will be hosted via Microsoft Teams and recorded for on-demand access. Step-by-step job aids, video tutorials, and printable quick reference guides will be developed for everyday tasks such as accessing email, sharing documents securely, and using multi-factor authentication.

## Training Content

The training curriculum will cover:

- Introduction to Microsoft 365 tools (Outlook, Teams, OneDrive, SharePoint)
- How to securely access files and emails using MFA
- Best practices for document sharing and collaboration
- Recognizing and reporting phishing or suspicious emails
- Use of Microsoft Defender security notifications
- Role-specific administrative features (for leadership or designated staff)

## Duration

The training will be structured as follows:

- **Initial Onboarding Training:** One 60-minute live session for each user group
- **Follow-up Office Hours:** Two 30-minute optional Q&A sessions during the first week post-migration
- **Ongoing Access:** Self-paced materials available indefinitely through the organization’s shared Teams space

This multi-touch approach ensures staff learn the system and retain the information through practice and reference. The goal is to build confidence and establish Microsoft 365 as a trusted platform for daily operations.

## Required Resources

Successful execution of the Microsoft 365 migration project will require a combination of software licenses, professional services, hardware (if applicable), and time from key personnel. The following outlines the resources needed across each project phase, associated cost estimates, and sourcing references.

### Software and Licensing

The organization will utilize Microsoft 365 Business Premium licenses, which are specifically discounted for eligible nonprofit organizations.

- **Licensing:**
  - 10 users x Microsoft 365 Business Premium
  - Cost: $0–$5 per user/month (depending on eligibility through Microsoft Nonprofit Program) (Microsoft, 2025)
  - Source: Microsoft Nonprofit Portal

- **Microsoft Intune & Defender for Business:**
  - Included in Business Premium
  - Enables endpoint protection and mobile device management

- **Microsoft Azure AD Premium P1**
  - Cost: $1–$3 per user/month (Nonprofit discounted rate) (Microsoft, 2025)
  - Source: Microsoft Licensing Guide

## Personnel and Services

- **IT Consultant (Part-Time Contractor):**
    - Estimated 40 hours over 8 weeks
    - Responsibilities: Migration planning, configuration, testing, and staff support
    - Rate: $125/hour
    - Estimated Cost: $5,000

- **Internal Staff Time:**
    - Executive and administrative staff will participate in planning, training, and user testing.
    - Estimated: 1–3 hours per week per staff member for 4–6 weeks
    - Cost impact: Operational downtime, no direct expense

## Hardware (If needed)

- **Secure Endpoint Devices (Optional):**
    - If staff use outdated personal devices, consider allocating funding for secure alternatives.
    - Example: Microsoft Surface Go or similar laptops – $500–$800 each
    - Quantity: 2–3 replacements (based on staff inventory audit)
    - Estimated Total: $2,000

## Training and Documentation

- **Training Materials:**
    - Developed internally with consultant support
    - No direct cost if the consultant's hours include training
    - Printing or optional job aids may incur $50–$100 if physical materials are required

## Total Estimated Budget

| **Resource** | **Estimated Cost** |
|---|---|
| Microsoft 365 Licenses | $0–$600/year |
| Azure AD Premium (optional) | $120–$360/year |
| IT Consultant | $5,000 |
| Replacement Devices (optional) | $2,000 |
| Training Materials | $100 |
| **Total (Estimated Range):** | **$5,220–$8,060** |

This budget ensures the project is secure and sustainable while remaining financially achievable for a nonprofit organization.

## Deliverables and Timeline

This project will produce key deliverables for migrating, configuring, and adopting Microsoft 365 Business Premium. Each deliverable aligns with the organization's goal of enhancing security, centralizing management, and enabling sustainable IT practices. The timeline reflects an 8-week implementation period, broken down into clearly defined milestones.

## Final Project Deliverables

- **Microsoft 365 Environment Deployed**
    - Ten users fully migrated from G Suite to Microsoft 365
    - Email, calendar, and file data transferred
- **Azure Active Directory Configured**
    - User roles assigned, groups established, MFA enforced
- **Microsoft Defender for Business Activated**
    - Endpoint protections configured and tested
- **Intune Mobile Device Management Deployed**
    - Device enrollment and compliance policies in place
- **Data Protection Policies Implemented**
    - Sensitivity labels and data loss prevention policies applied
- **User Training Completed**
    - Live sessions, recordings, and job aids delivered
- **Post-Migration Report**
    - Summary of changes, audit of user access, and configuration checklist

## Timeline and Milestones

| **Milestone** | **Duration** | **Start Date** | **End Date** | **Resources Assigned** |
|---|---|---|---|---|
| Project Planning & Requirements | 1 week | Week 1 | Week 1 | Executive Director, IT Consultant |
| Pilot Group Migration & Testing | 1 week | Week 2 | Week 2 | IT Consultant, 2–3 Pilot Users |
| Full User Migration | 2 weeks | Week 3 | Week 4 | IT Consultant, All Staff |
| Security & Policy Configuration | 1 week | Week 5 | Week 5 | IT Consultant |
| Intune Setup & Device Enrollment | 1 week | Week 6 | Week 6 | IT Consultant, Staff (for device testing) |
| Staff Training & Documentation | 1 week | Week 7 | Week 7 | IT Consultant, Executive Assistant |
| Post-Migration Review & Optimization | 1 week | Week 8 | Week 8 | IT Consultant, Executive Director |

*Note: All weeks are consecutive and allow for slight overlap to accommodate minor delays without significantly impacting completion.*

This phased schedule ensures a manageable pace for the organization while building in time for staff engagement, testing, and adjustment.

## Evaluation and Testing

A thorough evaluation and testing plan is critical to ensure the Microsoft 365 migration achieves its security and operational goals. This section outlines how the implementation will be assessed through structured test plans, defined success criteria, contextual test cases, and a straightforward method for analyzing results.

### Formative and Summative Test Plans

**Formative testing** will take place during implementation to catch issues early and make iterative improvements. This includes:

- Verifying successful migration of pilot user mailboxes and files
- Testing multi-factor authentication (MFA) enrollment and access scenarios
- Validating endpoint compliance with Microsoft Defender policies
- Checking basic access and usability in Teams, Outlook, and OneDrive

**Summative testing** will occur after the full rollout and will include:

- Review of audit logs to confirm no unauthorized access occurred
- Testing of file sharing restrictions and data loss prevention (DLP) labels
- Simulated phishing email to test Defender for Office 365 capabilities
- User feedback surveys on accessibility, usability, and confidence with the new system

### Acceptance Criteria and Key Performance Indicators (KPIs)

The following criteria must be met for the project to be considered successfully implemented:

- 100% of staff accounts enrolled in MFA
- Successful migration of all email and files with no data loss
- At least 80% of staff pass the post-training quiz and confirm successful login to all assigned apps
- All file sharing set to internal-only by default, with no public links allowed
- Microsoft Secure Score baseline of 75% or higher

These KPIs align with both formative and summative testing stages and serve as benchmarks for technical success and user readiness.

## Justification for Test Cases and Scenarios

Each test case is designed around the nonprofit's actual working environment and common risks. For example:

- **MFA testing** reflects the need to protect user credentials from phishing attacks, which have already occurred in the current G Suite environment.

- **File sharing tests** are justified by known incidents of public exposure of sensitive documents.

- **Endpoint compliance testing** ensures that staff devices meet minimum security requirements, crucial for protecting constituent data.

- **User satisfaction and functionality testing** ensure that productivity is maintained despite the technical upgrade.

These scenarios validate both the security controls and the practicality of the solution for non-technical users.

## Analyzing Results

Testing results will be collected and reviewed by the IT consultant in collaboration with the Executive Director. Logs from Microsoft 365 Security Center, Intune, and Azure AD will be exported for review. Survey results from end-users will be analyzed to identify common concerns and support needs.

A final report will be compiled by summarizing:

- Any failed test cases and the remediation steps taken
- Final configuration status
- User readiness indicators
- Recommendations for continuous improvement

This analysis will guide both future technology planning and support efforts, ensuring the system remains effective and secure over time.

## Conclusion

This proposal outlines a practical and security-focused approach to modernizing the digital infrastructure of a nonprofit organization through migration to Microsoft 365 Business Premium. By addressing key vulnerabilities in the current environment, such as a lack of centralized identity management, insecure file sharing practices, and limited endpoint protection, this project ensures that the organization can operate more safely and efficiently. The proposed solution is grounded in industry standards, tailored for non-technical users, and designed to scale with the organization's future growth. Through careful planning, stakeholder engagement, and user-focused training, this initiative will not only strengthen the nonprofit’s cybersecurity posture but also empower its staff to serve the community with confidence in a secure digital environment.

## References

*CIS Controls v8.1 update overview*. (2025). Retrieved from Center for Internet Security: https://www.cisecurity.org/controls/v8-1

Microsoft. (2025, May 15). *Changes to Microsoft nonprofit Business Premium grant*. Retrieved from Microsoft: https://techimpact.org/news/changes-microsofts-business-premium-grant-announced

Microsoft. (n.d.). *Microsoft 365 Nonprofit Solutions*. Retrieved from Microsoft: https://www.microsoft.com/en-us/nonprofits/microsoft-365

Microsoft. (n.d.). *Nonprofit security program & AccountGuard*. Retrieved from Microsoft: https://www.microsoft.com/en-us/nonprofits/data-security

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. Retrieved from Verizon: https://www.verizon.com/business/resources/reports/dbir/