Modern Workplace Services Implementation – Regina Open Door Society

Client: Regina Open Door Society
Users: 268 active users
Devices: 127 active endpoints
Total Effort: 260 Professional Services Hours (+ 24 for appendix A)
Estimated Duration: 4-6 weeks

Below costs are estimates based on the amount of work needed for the project tasks. These tasks themselves are not amendable, and the dollars associated with those tasks make up a total project cost that would remain complete and intact. The breakdown is for educational purposes only and would not be amended in the case of project acceptance.

Estimated Professional Services Summary

Phase	Hours
Discovery and Planning	$660.00
Conditional Access & Authentication	$990.00
Intune Device Management	$2,310.00
Application Management & Deployment	$1,650.00
Pilot Deployment & Testing	$1,650.00
Migration to the Modern Workplace	$24,750.00
Security Bundle and Hardening	$2,640.00
Documentation & Closeout	$7,260.00
Server Licensing	$2,446.80
Total	$44,356.80

Potential additional costs:
If RODS Finance does not move to Sage 50 Cloud, there will be additional expenses incurred:

- Anticipated expense, Azure set up for Sage Cloud Accounting *if needed* $4,950.00
  (Additional Azure costs of $550.00 per month would come from the operating budget)

Summary of total estimated costs:

Modern Workplace & Server licensing	**$44,356.80**
Azure Setup (if needed)	**$ 4,950.00**
	$49,306.80
Tax:	**$ 5,423.75**
Total	**$54,730.55**

Executive Summary

Moving from an on-premise server environment to a modern workplace platform strengthens security by replacing locally managed infrastructure with enterprise-grade, cloud-based protection. On-prem servers require constant patching, monitoring, backup validation, and hardware maintenance, and a single missed update or failed backup can expose the organization to ransomware, data loss, or extended downtime. Modern workplace solutions provide built-in security features such as multi-factor authentication, conditional access policies,

advanced threat detection, automated patching, encrypted data storage, and geographically redundant backups. These protections are continuously updated to address emerging threats, reducing reliance on manual processes and lowering the risk of human error. By centralizing identity, device management, and data protection under a secure cloud framework, organizations significantly improve their security posture while ensuring resilience, compliance, and business continuity.
Hardware server projects should be completed every 5 years, the Modern Workplace project would allow for one move, and no further server hardware replacement projects in the future.

Platform: Microsoft 365 / Intune / Entra ID

1. Project Objectives

- Establish a cloud-first identity and device management infrastructure using Entra ID and Intune
- Implement modern workplace security controls aligned with Zero Trust principles
- Enable seamless user productivity through cloud-connected devices and applications
- Establish baseline security posture with conditional access and device^ compliance
- Reduce IT administrative overhead through automated management and policy deployment
- Provide centralized documentation and support for ongoing management

2. Scope of Services

Phase 0: Discovery and Planning

Activities

- **Object (User and Group) Review**
    - Review current user list, ensure accuracy
    - Review current group list and determine migration status
    - Ensure all users have attributes set, including:
        - User Principal Name (username) and primary email address
        - Direct Manager
        - Department
        - Job Title
        - Phone Number
        - Legal First and Last Name
        - Display Name
    - Create plan for migrating any synchronized users or groups to cloud-only status
- **Network Services Review**
    - Review current network services running within the networks
    - Determine network architecture (Site-to-Site VPN, VLANs, etc.)
    - Document changes that are needed as part of the project
- Application Review
    - Review current line of business applications running within the environment
    - Document migration path and plan
    - Confirm actions with the customer

Phase 1: Conditional Access & Authentication Security

Activities

- **Multi-Factor Authentication (MFA) Setup**:

    - Configure Microsoft Authenticator app deployment strategy
    - Enable MFA for all users (phased rollout plan)
    - Configure MFA enforcement policies
    - Set up passwordless sign-in (Windows Hello for Business)
    - Setup SMTP2GO for legacy email sending (e.g., Scan to Email)
    - Communication with end-users regarding authentication requirements
    - Procurement of Security Keys (FIDO2 devices) for users without mobile devices
- **Conditional Access Policy Implementation**:
    - Define access policies based on:
        - User and group membership
        - Device compliance status
        - Location and network conditions
    - Implement baseline policies:
        - Require MFA for all users accessing cloud apps
        - Require compliant device access
        - Block legacy authentication
        - Require strong password policies
    - Create policies for admin access (stricter requirements)
    - Configure policies for mobile device access
- **Session & Sign-In Risk Management**:
    - Configure sign-in frequency policies
    - Implement token lifetime policies
    - Set up browser session policies (persistent or require re-auth)

Deliverables

- MFA deployed and enforced for all users
- Conditional Access policies active and operational
- Passwordless authentication configured (if applicable)
- Sign-in security baselines established
- Legacy authentication disabled

Phase 2: Intune Device Management Setup

Activities

- **Intune Tenant Configuration**:
    - Configure Intune settings and tenant customization
- **Device Enrollment Setup**:
    - Configure Autopilot for new Windows device provisioning
    - Configure MDM scope for existing Windows 10/11 enrollment
    - Configure macOS enrollment
    - Configure iOS/iPadOS enrollment
    - Configure Android enrollment
    - Test enrollment process with pilot group
- **Device Configuration & Compliance**:
    - Create and deploy device configuration profiles and security policies
    - Create device compliance policies:
        - Windows device compliance rules
        - macOS compliance rules

        - Mobile device compliance rules
    - Configure remediation for non-compliant devices
- **Security Baseline Deployment**:
    - Deploy endpoint security baseline
    - Configure Microsoft Defender settings
    - Deploy Microsoft Defender for Endpoint
    - Configure endpoint detection and response

Deliverables

- Intune environment fully configured
- Enrollment methods tested and operational
- Device configuration profiles deployed to pilot users
- Compliance policies active
- Security baselines applied
- Pilot devices successfully managed

Phase 3: Application Management & Deployment

Activities

- **Microsoft 365 Applications**:
    - Configure Intune to install modern Microsoft 365 apps
    - Configure update channels and policies
    - Configure Microsoft Office settings policies
- **Application Publishing & Deployment**:
    - Configure managed application policies
    - Deploy line of business applications via Intune
    - Set up application assignment based on user/device groups
    - Configure app protection policies (Mobile Application Management)
- **Cloud Printing Setup** (if applicable):
    - Configure Azure Universal Print
    - Determine approximate license usage
    - Deploy print drivers via Intune
    - Configure scan-to-email functionality
    - Test printing from managed devices
- **Current On-Premises Applications** (if applicable)
    - Review current application usage
    - Create plan with client to migrate to a modern SaaS platform (if applicable)
    - Current line of business applications used: (if applicable)
        - Sage 50 Accounting to Quickbooks Online (or see below)
        - BrightSign VM to be hosted locally on a windows 11 PC, on an isolated network, setup as hyperV and backed up to cloud.

Phase 4: Pilot Deployment & Testing

Activities

- **Pilot User Group Selection**:
    - Select 5 pilot users representing different departments
    - Communicate pilot timeline to participants
    - Establish feedback mechanisms
- **Device Enrollment & Configuration**:

    - Enroll pilot devices in Intune
    - Deploy configurations and policies to pilot devices
    - Validate device compliance status
    - Test conditional access enforcement
- **User Testing & Validation**:
    - Verify MFA enrollment and functionality
    - Test single sign-on for applications
    - Validate device access to network resources
    - Test VPN connectivity (if applicable)
    - Verify application availability and functionality
    - Validate mobile device access policies
- **Issue Identification & Resolution**:
    - Collect pilot user feedback
    - Identify and document issues
    - Troubleshoot configuration problems
    - Adjust policies based on feedback
    - Resolve application compatibility issues
- **Performance & Security Validation**:
    - Monitor device performance impact
    - Validate security policy enforcement
    - Review compliance reports
    - Verify conditional access decisions

Deliverables

- Pilot devices successfully enrolled and managed
- All policies and configurations validated
- User feedback collected and addressed
- Pilot test report with findings
- Ready-to-deploy configuration baselines

Phase 5: Full Rollout & User Training

(1 hour per device, 5 mins per user)

Activities

- **Phased Rollout Planning**:
    - Create detailed rollout schedule by department/location
    - Migration of users from synchronized accounts to Cloud-only accounts
    - Establish help desk support procedures
    - Define escalation procedures for issues
    - Prepare rollback procedures if needed
    - Migration of users to cloud-only accounts
- **Device Migration at Scale**:
    - Migrate and enroll 127 devices in Intune and Entra ID (phased approach)
    - Deploy configurations and policies to all users
    - Monitor enrollment success rates
    - Address enrollment issues promptly
- **User Training & Communication**:
    - Conduct training sessions for all users:

        - MFA setup and usage
        - Modern device features
        - Application access
        - Troubleshooting common issues
        - Password management best practices
    - Distribute training materials and quick-reference guides
    - Create FAQ documentation for common questions
    - Establish ongoing support channels
- **Help Desk Enablement**:
    - Train IT staff on Modern Workplace support procedures
    - Document common issues and resolutions
    - Provide access to support tools and resources
    - Establish escalation procedures
- **Monitoring & Optimization**:
    - Monitor device compliance and enrollment metrics
    - Track conditional access alerts and blocks
    - Monitor device security posture
    - Optimize policies based on real-world usage
    - Address performance and usability issues

Deliverables

- All devices successfully enrolled and deployed
- Users trained and productive on Modern Workplace
- Help desk trained and ready to support
- Monitoring dashboards established
- Documentation completed

Phase 6: Security Bundle and Environment Hardening

Activities

- **Microsoft 365 Environment Hardening**:
    - Email Hardening
        - Implement email quarantine policies
        - Adjust email screening policies for security protection
        - easyDMARC and easySPF for Email Authentication management
    - Secure Score Review and Action
        - Review all secure score recommendations
        - Action recommendations that are available
        - Communication regarding changes and impact with the client
- **Verify and implement MicroAge Security Bundle**:
    - Huntress Managed Detection and Response
    - SaaS Alerts for ITDR
    - AvePoint Elements for Cloud-to-Cloud Backup
    - Microsoft Defender for Endpoint

Deliverables

- Advanced security policies deployed
- Privileged access properly managed
- Monitoring and alerting operational

- Threat detection and response procedures established

Phase 7: Decommission on-premises environment

Activities

- **Migrate network services to MicroAge network appliance** (if applicable)
  - Transfer DHCP service to Meraki equipment
  - Transfer DNS service to Meraki equipment
  - Establish Site-to-Site VPN links between sites (if applicable)
  - Ensure security baselines are applied to security appliances
- **Decommission virtual servers**
  - Confirmation between the customer and project team
  - Safely shutdown any virtual servers running within the environment
  - Disable automatic startup of the virtual servers
  - Take final disk image backup of the virtual servers to external or cloud storage
- **Decommission physical servers**
  - Confirmation between the customer and project team
  - Safely shutdown the physical servers running within the environment
  - Disable automatic startup
  - Disconnect any cabling (networking, power, etc.)
- **Disposal and recycle**
  - Receive “Transfer of Title” sign-off
  - Physically remove server from the environment
  - Remove any data storage media (hard drives, SSDs, etc.)
  - Securely wipe any data stored on the storage media
  - Send storage media for secure data destruction (if applicable)
  - Place all hardware for sustainable recycling

Phase 8: Documentation & Project Closeout

Activities

- **Comprehensive Documentation**:
  - Document Entra ID configuration and structure
  - Document Intune device policies and baselines
  - Document conditional access policies
  - Document application deployment procedures
  - Create runbooks for common IT tasks
  - Document troubleshooting procedures
  - Create user guides and FAQs
- **Knowledge Transfer**:
  - Conduct knowledge transfer sessions with IT team
  - Review configuration, policies, and procedures
  - Demonstrate monitoring and reporting tools
  - Provide access to configuration management tools
  - Document any custom configurations or scripts
- **Ongoing Support & Maintenance**:
  - Establish support SLA with client
  - Define procedures for policy updates and changes

    - Plan quarterly reviews of modern workplace health
    - Identify future optimization opportunities
- **Project Closeout**:
    - Final review with stakeholders
    - Collect feedback on implementation
    - Document lessons learned
    - Close project in project management system

Deliverables

- Complete and current technical documentation
- User and IT staff guides
- Configuration and policy documentation
- Knowledge transfer completed
- Project formally closed

3. Modern Workplace Architecture & Components

Identity Management

- **Cloud-Only Model:** Users managed exclusively in Entra ID

Device Management

- **Windows Devices:** Entra ID joined and Intune-managed
- **Mobile Devices:** iOS/Android enrolled for Mobile Application Management

Security Layers

- Entra ID with MFA for authentication
- Conditional Access policies for access control
- Intune for device compliance and configuration
- Microsoft Defender for endpoint security

Applications & Services

- Microsoft 365 cloud applications (Teams, SharePoint, OneDrive, etc.)
- Microsoft 365 Apps for productivity
- Line of business applications via Intune

Network Services

- Migrated from server environment to MicroAge-managed networking infrastructure

4. Licensing Requirements

Base Licensing *(per user)*

- 317x Microsoft 365 Business Premium
    - Would utilize the Non-Profit pricing from Microsoft
    - ~$8.00/month/license on the Non-Profit pricing (Annual Paid Monthly term)
    - ~$9.00/month/license on the Non-Profit pricing (Monthly term)
    - Includes Intune, Entra ID, Microsoft Defender, Conditional Access
    - This number to be confirmed during Phase 0 of the Discovery and Planning Phase

5. Assumptions

- Client has appropriate Microsoft 365 licensing or will procure as recommended
- Client has Windows Server Active Directory environment (2012 R2 or later)
- Client has Windows 10/11 devices capable of Intune management

- Stakeholders are available for workshops, testing, and training
- Client will coordinate user scheduling for device enrollment
- 1-2 business days notice required for on-site work scheduling
- Maintains current backup and disaster recovery procedures

6. Out of Scope

- On-premises Active Directory migration or upgrade
- Major infrastructure upgrades or network modifications
- Custom application development or modifications
- Third-party identity provider integration (non-Microsoft solutions)
- Advanced threat protection for on-premises servers
- Insider Risk Management implementation (can be scoped separately)
- eDiscovery and compliance holds (can be scoped separately)
- Advanced DLP policies beyond standard configurations
- Incident response and forensics services
- Hardware procurement (unless specified in scope)

7. Project Phases & Timeline

Phase	Duration	Key Milestones
Discovery and Planning	2 days	Critical systems documented, plan in place for migration
Conditional Access & MFA	3 days	MFA enforced, access policies active
Intune Setup	4 days	Enrollment methods configured, pilot devices managed
App Management	4 days	Applications deployed, policies enforced
Pilot Deployment	1 week	Pilot validation complete, issues resolved
Migration to the Modern Workplace	2-3 weeks	All devices enrolled, users trained
Security Bundle and Hardening	4 days	Advanced policies deployed and operational
Closeout	2 days	Documentation complete, knowledge transfer finished

8. Estimated Professional Services Summary

Phase	Hours
Discovery and Planning	$660.00
Conditional Access & Authentication	$990.00
Intune Device Management	$2,310.00
Application Management & Deployment	$1,650.00
Pilot Deployment & Testing	$1,650.00
Migration to the Modern Workplace	$24,750.00
Security Bundle and Hardening	$2,640.00
Documentation & Closeout	$7,260.00
Total	$41,910.00

9. Success Criteria

- 100% of users provisioned in Entra ID

- MFA enforced for all users with >95% adoption
- 100% of managed Windows devices successfully enrolled in Intune
- All devices compliant with security policies
- Conditional Access policies active with zero critical bypass events
- Applications accessible via single sign-on
- Pilot and full rollout completed on schedule
- Zero critical security vulnerabilities introduced
- User training completed with positive feedback (>80% satisfaction)
- Help desk trained and supporting Modern Workplace independently
- Comprehensive documentation completed and accessible

10. Future Considerations

Post-implementation opportunities for continued optimization:

- Implementation of Privilege Identity Management (PIM) for admin access
- Advanced risk-based conditional access using Identity Protection
- Enhanced DLP policies for sensitive data protection
- Advanced insider risk management
- Zero Trust network implementation with adaptive access
- Quarterly security reviews and policy optimization
- Annual Modern Workplace health assessments
- Device and application refresh planning
- Integration with advanced SIEM and SOC solutions