| **Security Dimension** | **MyCollab v1** | **OneDrive** |
| --- | --- | --- |
| **Compliance** | Compliant with firm's Entitlement Standard; uses RMS | No firm-standard compliance noted; multiple security gaps identified |
| **Access Control** | Governed by manager + owner approvals; permissions via PERMIT | Non-owner sharing; admins retain control post-departure |
| **Risk Mitigation** | Lifecycle automation, recipient-based access control, structured creation | Lacks automation; risks from manual disassociation and persistent access |
| **Encryption** | HTTPS encryption; AWS-hosted with cloud security practices | HTTPS assumed (standard in Microsoft); no cloud infra details mentioned |
| **Audit & Logging** | Uses BigQuery for security audits; CloudWatch for future versions | Activity reporting assumed; detailed audit control not mentioned |
| **Documented Security Gaps** | None in current documentation | **10 known high-risk gaps** including: orphaned ODs, quota issues, geo-location risk |

| **Feature Area** | **MyCollab v1** | **OneDrive** |
| --- | --- | --- |
| **Centralized Collaboration Management** | Yes – Unified storefront for Teams, SharePoint, and others | No – Each user manages their own space |
| **File Sharing Controls** | Requires approvals from manager and owner for access | Non-owner members can share without approval |
| **Lifecycle Management** | Automated workflows for joiners and leavers, reducing risk of orphaned spaces | Manual; orphaned OneDrives not disassociated automatically |
| **Integration** | Deep integration with Teams, SharePoint, PERMIT, InventoryCentral, and others | Native Microsoft 365 integration; no mention of additional systems |
| **UI & Compatibility** | Mobile-friendly; integrates with Teams Tabs on desktop and mobile | Mobile-friendly; integrated with Office apps |
| **Additional Features** | Webhook support, API access control, recipient ID-based access | Standard Microsoft features; site admins have persistent control |

| **Feature/Entitlement Control Name** | **MyCollab v1** | **OneDrive** |
| --- | --- | --- |
| **Role-Based Access (e.g., Project Admin, Viewer)** | Likely includes roles like Project Admin and Viewer, managed on-premises with custom configurations. | Not explicitly role-based; uses permission levels like "Can View" and "Can Edit" for granular control. |
| **Add Member** | Managed via API with team name in URL; requires manual or API-driven addition with potential manager approval. | API supports adding members with "regManRecipientID" and "webhookURL"; team name passed in URL, with native client options. |
| **Remove Member** | API or manual removal possible; access revocation recommended after 7 days per Entitlement Standard (AC-6.101). | API removes members; automatic removal if access exceeds 7 days, aligning with Firmwide Entitlement Standard. |
| **Create Team** | API creates teams with "regManRecipientID," "regManDescription," and "newTeamRequest"; requires owner approval. | API creates teams with similar payload structure; native client allows creation with owner oversight. |
| **Delete Team** | Not explicitly detailed; likely manual or API-driven with owner approval. | Not natively supported via API; requires manual deletion or admin action. |
| **Granular Access to SharePoint Sites** | Supports granular access via API to Teams-connected SharePoint sites, managed on-premises. | Provides granular access with security groups (e.g., "Read," "Write") to SharePoint sites, cloud-managed. |
| **Leavers and Transfers** | API handles leavers and transfers; ensures access removal per AC-6.101 Removal of Leavers process. | API automates leavers and transfers; removes access after 7 days with Firmwide Standard compliance. |
| **Reconciliation of Membership** | Requires regular reconciliation and reporting to Inventory Central via API or manual checks. | Automated reconciliation via API, reporting to Inventory Central, with ongoing monitoring. |
| **Security Group Access Type (Read, Write, Edit)** | Custom security groups likely defined on-premises; types not specified but inferred as Read/Write. | Explicitly supports "Read," "Write," "Edit" via security groups, managed in Microsoft 365. |
| **Hide Team from GAL** | Supports "hideTeamFromGAL" boolean in API payload for privacy. | No equivalent feature; visibility managed via sharing settings. |
| **Privilege Manager Approval** | Requires Privilege Manager approval for team creation; bypass triggers a risk ticket. | No specific Privilege Manager role; approvals handled by owners or admins. |
| **Ownership Validation** | Teams owned by virtual owners (human owners in practice); validated via API. | Ownership tied to creators; validated through native client or API. |

| **Control Name** | **MyCollab v1** | **OneDrive** |
| --- | --- | --- |
| **AC-3.103 Privilege configuration registration** | Managed on-premises; requires manual specification of entitlements and reporting to a central inventory. | Cloud-based; entitlements automatically registered and reported via Microsoft 365 inventory systems. |
| **IA-4.4 User accounts owner and operator** | Requires active HCM identity; managed manually by Technical Owner on-premises. | Automated HCM integration with active identity checks via Azure AD. |
| **AC-3.105 Entitlement approval workflow definition and implementation** | Business Sponsors and Technical Owners define workflows manually; implemented via API with approval. | Workflows defined by admins; implemented automatically via Microsoft 365 role systems. |
| **MP-7.100 Removable media privileges must be accepted by divisional PMDs** | Not applicable on-premises; manual risk acceptance if removable media used. | Not directly applicable; cloud storage negates removable media needs, managed by admins. |
| **AC-24.100 Entitlement messages to allow informed decisions** | Meaningful descriptions provided via API; managed by Technical and Business Owners. | Automated entitlement descriptions in sharing settings, managed by Microsoft 365. |
| **AC-5.103 Detect Toxic Combination of Access** | Segregation rules defined manually; detected via on-premises SoD tools. | Automated detection of toxic combinations via Microsoft 365 security groups. |
| **AC-5 Separation of Duties** | Privileges mapped manually; toxic access prevented by Business Sponsors. | Automated privilege mapping and prevention via Azure AD policies. |
| **AC-3 Access Enforcement** | Entitlement grants require documented approval; fulfilled manually or via API. | Grants enforced post-approval; automated via API and native client. |
| **AC-3.106 Prevent Self-approval** | Self-approval prevented via manual checks by Entitlement Administrators. | Prevented automatically by Microsoft 365 approval workflows. |
| **AC-3.102 Auto-fulfilment of entitlements** | Auto-fulfillment enabled post-approval via API for supported systems. | Fully automated fulfillment via Microsoft 365 for supported applications. |
| **MP-2.100 Removable media privileges restrictions** | Restrictions on secondary admin accounts managed manually on-premises. | Not applicable; cloud-based, no secondary admin accounts needed. |
| **AC-6.5.100 Elevated access minimum amount of time required to perform activity** | Enhanced entitlements limited to 180 days manually by Administrators. | Automated time limits (180 days) enforced by Microsoft 365 policies. |
| **AU-3.102 Grant of authorization audit trail** | Audit trail recorded manually by Solution Owner via API. | Automated audit trail logged by Microsoft 365 for all authorizations. |
| **AC-24.1 Transmit Access Authorization Information** | Weekly reporting to central inventory managed by Technical Owner. | Daily automated reporting to Microsoft 365 inventory. |
| **IA-4.4.100 Improper Login Detection** | Logins matched to GS identity quarterly by Technical Owner. | Automated login matching and detection via Azure AD daily. |
| **AC-24.1.100 AMP feed completeness** | Quarterly validation by Technical Owner and Entitlement Approver. | Automated monthly validation by Microsoft 365 systems. |
| **AC-6.7 Review of user privileges** | Privileged access reviewed quarterly by Privilege Manager. | Automated quarterly review via Microsoft 365 admin tools. |
| **AC-6.7.100 Privileged Access recertification** | Quarterly recertification within 35 days by Privilege Manager. | Automated recertification within 35 days by Microsoft 365. |
| **PS-5 Personnel Transfer** | Entitlements reviewed within 45 days manually by Privilege Manager. | Automated review within 45 days via Microsoft 365 HR integration. |
| **PS-5.100 Sensitive user transfers** | Sensitive transfers flagged manually; rules recertified annually. | Automated flagging and annual recertification by Azure AD. |
| **AC-6.101 Removal of leavers' access** | Flagged and revoked manually within 90 days by Solution Owner. | Automated flagging and revocation within 90 days by Microsoft 365. |
| **AC-3.104 Remove Entitlements Flagged for Removal** | Removed within 15-90 days manually by Entitlement Administrator. | Automated removal within 15-90 days by Microsoft 365. |
| **AC-3.8 Enhanced entitlement revocation** | Enhanced entitlements revoked at expiration manually. | Automated revocation at expiration by Microsoft 365. |