NIST 800-53 Rev. 5 Targeted Compliance Gap Analysis: February 10, 2026

Project: NIST 800-53 Rev. 5 Gap Analysis | **Entity**: Mathnasium | **Scope**: Educational Storefront Baseline | **Auditor**: K. Oriol | Date: February 2026 | **Status:** Final Report (Version 1.0) | **Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID

AC	**AC-02**	Account Management	Create, track, and disable user accounts (staff/manager IDs) and review them regularly for accuracy.	Applicable (Shared)	Partially Implemented	Examine: Access control policy (or Corporate employee handbook); Portal User Export (Active Accounts List); Local Personnel Roster (Check-in log); Account creation/termination records (to check for missing exit dates).
						
						Interview: Center Director (regarding local onboarding/offboarding notification procedures); Corporate IT Help Desk (to confirm how they receive termination notices).
						
						Test: Account Deactivation Process (Testing the timeframe between a staff member's last day and their account's actual disabling); Cross-referencing current active logins against the list of former employees.
							The organization lacks a formal, localized process for Account Lifecycle Management.
							
							Failure to Disable (AC-02.f[4]): Review of the Portal User Export identified three (3) administrative accounts for personnel no longer employed at the center. These accounts have remained active and accessible since August 2025.
							
							Alignment Gap (AC-02.l): Account management processes are not aligned with personnel termination processes. There is no trigger for the Center Director to notify the account manager (Corporate IT) when a staff member departs.
							
							Review Deficiency (AC-02.j): Accounts are not reviewed for compliance at a defined frequency (AC-02_ODP[10]), allowing 'Ghost Accounts' to persist indefinitely.
								`ARTIFACT AC-02-01: Portal User Export: Showing active 'Admin' status for [Redacted Names].`
								`ARTIFACT AC-02-02: Local Personnel Roster: Cross-referenced to confirm the aforementioned users separated from the center on 08/15/2025.`
								`REF-INT-AC02: Director Interview: Confirmation that no 'Exit Checklist' or 'Termination Ticket' was submitted to Corporate for the departed staff.`
									The organization fails to satisfy AC-02. The presence of 'Ghost Accounts'—active credentials belonging to former employees—represents a critical security vulnerability. Without a synchronized offboarding procedure, the organization cannot ensure that access is revoked 'immediately' upon termination. This violates the Principle of Least Privilege and provides an avenue for unauthorized access to student PII by former staff members, significantly increasing the risk of data theft or malicious system modification.	**R-01**

AC	**AC-03**	Access Enforcement	Use technical settings to ensure users only access data and functions allowed by their specific job role.	Applicable (Shared)	Partially Implemented	Examine: System configuration settings (Admin Mac/iPads); List of approved user privileges (Portal); Access control policy; System Design Documentation (to see how the network is supposed to be separated).
						
						Interview: Center Director (regarding who is supposed to have "Sudo" or "Admin" rights); Tutors (to see if they use the "Master Password" for restricted tasks).
						
						Test: Privilege Escalation Test (Attempting to perform an administrative task—like installing software—using the shared tutor credentials to see if the "Master Password" works); Session Lock Test (Verifying if the Admin Mac locks itself after inactivity).
							Access enforcement is fundamentally undermined by a failure in local session management and credential secrecy.
							
							Privilege Escalation: The primary staff account possesses full sudo privileges. Because this is a shared account, there is no technical barrier preventing a general user from making system-level changes.
							
							Credential Convergence: The administrative sudo password is identical to the public-facing Guest Wi-Fi password, allowing any visitor to potentially gain root access to local workstations.
							
							Session Exposure: Administrative tablets are configured with 'Auto-Lock' set to 'Never.' This allows persistent access to authenticated sessions, meaning any individual with physical proximity inherits the privileges of the logged-in user.
							
							Physical Bypass: Core network infrastructure is located in an unlocked closet (PE-03), allowing a physical bypass of logical access controls via manual hardware resets.
								`IMG-AC03-01: Unsecured MDF Closet (PE-03)`
								`SCRN-AC03-02: iPad #04 'Auto-Lock: Never' setting`
								`LOG-AC03-03: Terminal output of 'sudo -v' confirming successful privilege elevation using Guest Wi-Fi password.`
								`REF-IA-05: The 'Master Password' sticker provides the physical proof of shared credential usage.`
									The organization fails to satisfy AC-03. The current implementation of access enforcement is ineffective because it relies on a single shared authenticator for multiple users. By granting 'Admin' rights to a shared account, the center has removed the ability to enforce Least Privilege. This creates a critical vulnerability where any individual (including guests on the shared Wi-Fi) could potentially gain full control of the center's primary workstation and the PII stored within it, as there is no technical enforcement to prevent unauthorized system-level changes.	**R-02**

AC	**AC-07**	Unsuccessful Logon Attempts	Set a limit on incorrect password guesses before a user is locked out or delayed.	Applicable (Shared)	Partially Implemented	Examine: System configuration settings; System security plan;
						
						Interview: Organizational personnel with information security responsibilities;
						
						Test: Mechanisms implementing access control policy for unsuccessful logon attempts.
							The organization demonstrates inconsistent enforcement of logon protection across service layers:
							
							Application Layer (Inherited): Mathnasium Portal enforces a lockout threshold of five (5) failed attempts.
							
							Hardware Layer (Local): 100% of the iPad fleet (4/4 devices) lacks a passcode or biometric challenge. Devices transition from 'Sleep' to 'Active' with a single swipe, bypassing all unsuccessful logon protections.
							
							Governance: No Mobile Device Management (MDM) solution is deployed to enforce device-level authentication policies.
								`SCRN-AC-07-01: Mathnasium Portal Lockout Notification`
								`LOG-AC-07-02: iPad Security Audit Log (Site Walkthrough) confirming 'No Passcode' on 4/4 devices.`
								`REF-INT-DIR: Center Director confirmation of lack of MDM and local device policy.`
								`Artifact AC-07-03`
									The organization fails to satisfy AC-07 at the local hardware level. The absence of device passcodes renders the 'Unsuccessful Logon' control moot, as there is no authentication gate to fail. This creates a high risk of Physical Brute Force bypass; while the Portal is secure, the local device is an open 'trust-pipe.' If an iPad is stolen or accessed by an unauthorized visitor, they have immediate, unrestricted access to the cached credentials and student data stored within the hardware.	**R-03**

AC	**AC-18**	Wireless Access	Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access, ensuring all connections are authorized prior to use.	Applicable (Shared)	Partially Implemented	Examine: System configuration settings (Verizon CR1000A Admin Panel); System Security Plan (SSP); Wireless authorization records (or lack thereof).
						
						Interview: Center Director (Wireless management responsibilities); Corporate IT (to confirm standard wireless security policies).
						
						Test: Wireless access management capability; Verification of SSID isolation (testing if guest traffic is separated from admin traffic).
							The organization lacks a secure wireless architecture, resulting in a Bypassed Perimeter.
							
							Lack of SSID Isolation (AC-18a): Configuration requirements for wireless access are not established. Both staff and students utilize the same primary SSID, allowing student-owned devices to reside on the same network segment as the Admin Mac and CCTV DVR.
							
							Unauthorized Connection Persistence (AC-18b): Usage restrictions are not enforced; once a device connects via the 'Master Password,' it remains authorized indefinitely. There is no mechanism to re-authorize or 'kick' stale devices from the network.
							
							Absence of Implementation Guidance: No documentation exists for tutors or parents regarding the 'Acceptable Use' of the center's Wi-Fi, nor are there security settings to prevent peer-to-peer communication between connected devices.
								`ARTIFACT AC-18-01: Screenshot of Verizon CR1000A 'Connected Devices' list showing student/personal devices on the primary subnet.`
								`ARTIFACT AC-18-02: Visual confirmation: 'Guest Wi-Fi' feature is disabled in the router management console.`
								`REF-IA-05: The 'Master Password' (sticker) serves as the sole 'Authorization' mechanism, which fails to restrict access to authorized personnel only.`
									The center fails to satisfy AC-18. By failing to establish separate connection requirements for visitors versus staff (AC-18a), the organization has effectively neutralized its internal network boundaries. This 'Flat Wireless' environment allows any student device to potentially scan or attack critical infrastructure (CCTV, Admin Mac). Without prior individual authorization (AC-18b) or usage restrictions, the center cannot detect or prevent unauthorized data exfiltration over the wireless medium, creating a high-impact risk to the Confidentiality of student PII.	**R-04**

AT	**AT-02**	Literacy Training and Awareness	Provide role-based security training to personnel with assigned security roles and responsibilities.	Applicable (Shared)	Partially Implemented	Examine: Security and privacy literacy training materials; Training records; System security plan.
						
						Interview: Organizational personnel comprising the general system user community (Tutors); Organizational personnel with responsibilities for literacy training (Director).
						
						Test: Mechanisms managing information security and privacy literacy training
							While basic security training is mandated via the Mathnasium Training Hub (Inherited), there is a total absence of Role-Based or Location-Specific security awareness (Local). Assessment identified three primary training voids:
							
							Social Engineering: Staff exhibit an 'Implicit Trust' posture toward visitors, with no training on tailgating or unauthorized access to the MDF closet (PE-03).
							
							Technical Risks: Personnel are unaware of the security implications of a 'Flat Network' (SC-07) or the risks of utilizing a shared 'Master Password' (IA-05) for both Wi-Fi and System Admin.
							
							Phishing/DNS: There is no training regarding specialized digital threats like DNS Spoofing (SC-21) or credential harvesting.
								`ARTIFACT AT-02-01: Training Hub Completion Report (showing 100% completion of generic modules only).`
								`REF-INT-AT02: Interview Summary with Lead Tutors confirming zero training on phishing or local network security protocols.`
								`OBS-AT-02: Observed behavior of staff allowing unescorted visitor access near the core network gateway (PE-03).`
									The organization fails to satisfy AT-02(b) and AT-02(d). The current 'one-size-fits-all' training model ignores the specific operational vulnerabilities of a storefront center. Because the curriculum is not updated with 'Lessons Learned' from local physical security gaps, the staff—the center's 'Human Firewall'—cannot effectively recognize or report the specific threats identified in this audit (e.g., unauthorized router access or session persistence on iPads).	**R-05**

Project: NIST 800-53 Rev. 5 Gap Analysis | **Entity**: Mathnasium | **Scope**: Educational Storefront Baseline | **Auditor**: K. Oriol | Date: February 2026 | **Status:** Final Report (Version 1.0) | **Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID

AT	**AT-03**	Role-based Training	Provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the system.	Applicable (Shared)	Partially Implemented	Examine: Security training curriculum; Training records/certificates; Job descriptions with security roles.
						
						Interview: Center Director (Training oversight); Tutors (to verify training content received).
						
						Test: Training monitoring system; Process for tracking training completion before granting system access.
							The organization lacks a specialized Role-Based Training program. While staff receive general 'Onboarding' instructions, the program fails to address specific security responsibilities.
							
							Generic Curriculum (AT-03a): There is no distinction between training for a Tutor (Low Risk) and the Center Director (High Risk). Specific training for managing the network gateway or handling sensitive student PII is non-existent.
							
							Lack of Monitoring (AT-03b): No formal system exists to track when security training was last completed or when 'Refresher' training is due.
							
							Access Before Training: Interviews reveal that new staff are often given the 'Master Password' (IA-05) on day one, prior to completing any formal security awareness or role-specific training.
								`REF-INT-AT03: Tutor interview confirmed: 'I was shown how to use the iPads, but I never had a specific class on data privacy or security.'`
								`ARTIFACT AT-03-01: Employee Training Log (Review): Confirmed the log only tracks 'Math Instruction' hours, with no entries for 'Security/Privacy' training.`
								`NEGATIVE ARTIFACT: Absence of role-specific training modules for the Center Director regarding MDF closet security or incident reporting.`
									The center fails to satisfy AT-03. Security training is currently 'Ad-Hoc' rather than 'Role-Based.' Without targeted instruction, personnel in high-privilege positions (like those with access to the Admin Mac) remain unaware of the specific threats and compliance requirements related to their access. This lack of documented monitoring creates a significant liability; if a data breach occurs due to staff error, the organization cannot prove that the individual was appropriately trained to prevent such an event, violating the principle of Administrative Accountability.	**R-06**

AU	**AU-06**	Audit Record Review, Analysis, and Reporting	Review and analyze information system audit records for indications of unusual activity.	Applicable (Shared)	Partially Implemented	Examine: Reports of audit findings (or lack thereof); Procedures addressing audit review, analysis, and reporting; System security plan.
						
						Interview: Center Director (Personnel with audit review and reporting responsibilities).
						
						Test: Portal user activity reports; Automated notification triggers (if any).
							Audit record review is strictly reactive, occurring only during post-incident troubleshooting. Assessment identified the following gaps:
							
							Lack of Defined Roles: No personnel are assigned the responsibility for periodic log review (AU-06_ODP[03]).
							
							Neglected Local Logs: Technical audit of the CR1000A Gateway and CCTV DVR confirmed that local system logs are generated but never reviewed for Indicators of Compromise (IoCs) or unauthorized access attempts.
							
							Absence of Reporting: Because no analysis occurs (AU-06a), no audit findings are reported to management (AU-06b), resulting in a failure of the 'Detective' control layer.
								`ARTIFACT AU-06-01: CR1000A Router 'System Logging' menu screenshot (showing unreviewed logs).`
								`ARTIFACT AU-06-02: Blank 'Log Review Sheet' (confirming no historical record of review).`
								`REF-INT-DIR: Director interview confirming logs are only accessed for technical support, not security monitoring.`
									The organization fails to meet AU-06. By maintaining a purely reactive posture, the center essentially operates with a 'Security Blind Spot.' The existing logs—which could detect unauthorized physical entry to the MDF (PE-03) or brute-force attempts on the 'Master Password' (IA-05)—remain unanalyzed. This failure transforms a 'Detective Control' into a 'Forensic-Only' tool, meaning the organization cannot detect an ongoing breach until after data exfiltration has occurred.	**R-07**

CA	**CA-07**	Continuous Monitoring	Establish a continuous monitoring strategy and implement a program to monitor the security state of the system.	Applicable (Shared)	Partially Implemented	Examine: System Security Plan (SSP); Organizational continuous monitoring strategy; System monitoring records (Portal logs/CCTV history); Status reports.
						
						Interview: Center Director (Local monitoring responsibilities); Corporate IT (via documentation/policy).
						
						Test: Mechanisms implementing continuous monitoring (e.g., automated alerts in the Portal or CCTV "Motion Detection" notifications).
							The organization's monitoring strategy is bifurcated and incomplete. While Corporate IT maintains centralized application monitoring, there is a total absence of localized Continuous Monitoring for center-level assets. Key deficiencies include:
							
							Undefined Metrics (CA-07a): No local metrics exist to track the 'Security State' of the facility (e.g., CCTV uptime, network closet lock integrity, or Wi-Fi performance baselines).
							
							Frequency Failures (CA-07b): There is no defined schedule for local security health checks.
							
							Correlation Gap (CA-07e): Local security events (such as the MDF closet being left open or the router being rebooted) are not correlated or analyzed against the broader security posture.
								`ARTIFACT CA-07-01: Corporate Monitoring Policy (demonstrates lack of local requirements).`
								`NEGATIVE EVIDENCE: Absence of a 'Daily/Weekly Security Checklist' or 'System Health Log' at the center level.`
								`OBS-CA-07: Verified 'Silent Failure' of CCTV DVR monitor (Screen was off/unresponsive during walkthrough, yet no one had noticed or reported the downtime).`
									The organization fails to satisfy CA-07. The center relies on a 'Passive' rather than 'Continuous' monitoring model. This creates a high risk of Silent Control Failure; for example, if the CCTV system or the network gateway fails, the organization may remain unaware of the outage for days. Without real-time security status reporting (CA-07g) for local physical and network infrastructure, the organization cannot provide a comprehensive 'Security State' assessment to stakeholders, leaving the center vulnerable to unmonitored breaches.	**R-08**

CM	**CM-02**	Baseline Configuration	Develop, document, and maintain under configuration control, a current baseline configuration of the information system.	Applicable (Shared)	Partially Implemented	Examine: System component inventory; system configuration settings and associated documentation; configuration management policy (Corporate).
						
						Interview: Center Director (Responsibility for device setup); Tutors (To verify if setup is consistent across devices).
						
						Test: Organizational processes for managing baseline configurations (Comparing settings on two different iPads to see if they match).
							The organization lacks a Standard Operating Environment (SOE) for local hardware. Assessment identified the following gaps:
							
							No Gold Image: iPads and Chromebooks are manually configured at the time of purchase rather than deployed via a Master Image or MDM profile.
							
							Version Divergence: Technical testing of the iPad fleet (4 units) identified multiple disparate Operating System versions and varying application suites.
							
							Absence of Control (CM-02a): There is no 'Master Configuration' document defining the minimum-security settings (e.g., encryption, firewall, or privacy settings) required before a device is deployed for student use.
								`ARTIFACT CM-02-01: Comparison Table of iPad OS Versions (showing 2 devices on iPad iOS 16.x and 2 on 17.x).`
								`ARTIFACT CM-02-02: Screenshot of inconsistent app libraries across student devices.`
								`REF-INT-CM02: Director interview confirming that devices are set up 'by hand' using a personal Apple ID rather than an organizational management account.`
									The organization fails to satisfy CM-02. The absence of a documented baseline maintained under Configuration Control results in significant Configuration Drift. Without a 'Gold Image,' there is no guarantee that every device used to access student PII meets the center's security requirements. This ad-hoc deployment method increases the attack surface, as 'ghost' settings or unpatched vulnerabilities on one non-standardized device could compromise the integrity of the entire local network.	**R-09**

CM	**CM-06**	Configuration Settings	Establish and document configuration settings for information technology products.	Applicable (Shared)	Not Implemented	Examine: Verizon CR1000A Configuration settings; System design documentation; Common secure configuration checklists (e.g., CIS Benchmarks for iOS/macOS); Asset inventory.
						
						Interview: Center Director (regarding the setup process for "new" refurbished hardware); Corporate IT (to verify if a standard "Gold Image" or MDM profile is required).
						
						Test: Vulnerability verification (Testing if UPnP is actually responsive); Verification of "factory default" credential access; Manual check of iPad "Restrictions" settings to see if non-essential services are blocked.
							System configuration settings are maintained at factory-default levels, with no evidence of Security Hardening.
							
							Permissive Gateway Settings: The CR1000A Router is configured with UPnP Enabled and Remote Administration accessible via a factory-default 'Sticker Password.'
							
							Lack of Least Functionality: Local workstations and tablets retain non-essential services, guest accounts, and unverified third-party applications.
							
							Refurbished Hardware Risks: Second-hand assets are deployed without a sanitization protocol, evidenced by residual configuration data and active sessions from previous administrative owners.
								`ARTIFACT CM-06-01: Router Config Screenshot: UPnP 'Enabled' status and WAN ICMP Echo active.`
								`ARTIFACT CM-06-02: iPad Audit Log: Documenting remnants of a third-party Apple ID and consumer-grade apps on a 'refurbished' unit.`
								`ARTIFACT CM-06-03: Photo of factory-default login credentials affixed to the network gateway (PE-03).`
									The organization fails to satisfy CM-06. By utilizing 'Refurbished' hardware without a formal Hardening Baseline (such as CIS Benchmarks or NIST STIGs), the center operates with an unverified security posture. The presence of 'Residual Data Persistence' and active non-essential services (like UPnP) significantly expands the Logical Attack Surface, providing multiple unmonitored vectors for unauthorized system exploitation and data exfiltration.	**R-10**

Project: NIST 800-53 Rev. 5 Gap Analysis | **Entity**: Mathnasium | **Scope**: Educational Storefront Baseline | **Auditor**: K. Oriol | Date: February 2026 | **Status:** Final Report (Version 1.0) | **Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID
CP	**CP-02**	Contingency Plan	Develop a contingency plan for the information system that addresses recovery objectives and restoration of business functions.	Applicable (Local)	Not Implemented	Examine (800-53A): Contingency plan; procedures addressing contingency planning; business impact analysis; system security plan; other relevant records. Interview: Personnel with contingency planning responsibilities (Director); Personnel with responsibilities for essential center functions. Test: Mechanisms implementing the contingency plan (e.g., checking if there is a physical "Emergency Binder" with student rosters).	The organization utilizes a decentralized, paper-based fallback system for emergency student data. Assessment identified: Availability: Paper binders containing student emergency contacts are maintained in a filing cabinet for use during system outages. Lack of Procedure: No written Contingency Plan (CP-02) exists to define the 'Trigger' for manual operations or the 'Synchronization' process to ensure paper records are kept up-to-date with the digital Portal. Training Gap: Staff are not verbally or formally instructed on the location or use of these binders as part of a disaster recovery strategy."	ARTIFACT CP-02-01: Photo of the student binders/filing cabinet (Note: ensure no names are visible). REF-INT-CP02: Director interview confirming that while binders exist, no formal 'Offline Mode' training has been conducted for tutors.	While 'Manual Media' (Paper Binders) exists to provide data availability, the organization fails CP-02 due to the absence of a documented plan. Relying on paper without a synchronization procedure leads to Data Staleness—where the emergency contact in the binder may be months out of date compared to the Portal. Furthermore, without a written plan, the center cannot guarantee a consistent Recovery Time Objective (RTO) for safety-critical information during a crisis.	**R-11**
IA	**IA-02**	Identification and Authenticati on (Organizational Users)	Ensure the system uniquely identifies and authenticates users (or processes acting on behalf of users).	Applicable (Shared)	Partially Implemented	Examine: System security plan; List of system accounts; System configuration settings and associated documentation. Interview: Organizational personnel with system operations responsibilities (Center Director); Tutors (System users). Test: Mechanisms supporting and/or implementing identification and authentication capabilities (e.g., attempting to access the router or iPad).	The organization maintains a bifurcated identity posture. While the Mathnasium Portal (Inherited) requires unique credentials, the local infrastructure is managed via Shared Authenticators. Key findings include: Lack of Unique IDs: The network gateway (CR1000A) and CCTV DVR do not support individual user accounts; all management actions are performed under a single 'Admin' profile. Shared Credentials: Technical testing and observation confirmed that the 'Master Password' (shared with the Guest Wi-Fi) is the sole authenticator used by all staff to access the Admin Mac and local network hardware. Process Bypass: There is no mechanism to link specific configuration changes or system access events to an individual human actor.	ARTIFACT IA-02-01: Photo of the 'Master Password' (PE-03) used across multiple systems. SCRN-IA-02-02: Router management interface showing the absence of individual user management features. REF-INT-IA02: Staff interviews confirming that no tutor has a unique local login for center workstations or tablets.	The organization fails to satisfy IA-02. The use of shared credentials for local system administration creates a total failure of Non-Repudiation. Because actions cannot be associated with a specific individual (IA-02[02]), the organization cannot maintain an audit trail that holds personnel accountable for unauthorized changes or data access. This 'Identity Masking' effectively nullifies the effectiveness of any local audit logs (AU-06), as every logged action is attributed to the same generic 'Admin' account.	**R-12**
IA	**IA-05**	Authenticato r Management	Manage information system authenticators (passwords, tokens, or biometrics) to maintain security.	Applicable (Shared)	Partially Implemented	Examine: System configuration settings (Router/CCTV admin panels); Identification and authentication policy; System security plan. Interview: Center Director (Authenticator management responsibilities); Tutors (To verify password change triggers). Test: Mechanisms implementing authenticator management (Attempted to set a 4-character password on the router to test complexity enforcement).	Assessment of IA-02 reveals a significant breakdown in lifecycle management. While the organization satisfies the initial distribution of authenticators, it fails to define a time period for refreshment (IA-05_ODP[01]). Furthermore, Substantive Testing of local system configuration settings confirms that mechanisms for enforcing complexity (IA-05c) and reuse (IA-05_ODP[02]) are disabled. This results in the use of 'forever' passwords, which significantly increases the risk of credential replay attacks and unauthorized persistence within the network.	ARTIFACT IA-05-01: Router Admin Screenshot showing 'Password Complexity: None.' ARTIFACT IA-05-02: Technical Test Log: Successfully set a 4-character, all-lowercase password on local hardware, confirming lack of enforcement. REF-IMG-PE-ROUTER: Photographic evidence of the 'Sticker Password' on the network gateway. REF-INT-DIR: Director confirmation that no password rotation has occurred since center opening.	The organization fails to satisfy IA-05. The reliance on static, shared, and low-entropy authenticators nullifies the effectiveness of the 'Identification' control (IA-02). This creates a critical vulnerability to Credential Replay and Brute Force attacks. By using a 'Sticker Password' and a converged 'Master Password,' the organization has created a Single Point of Failure: the compromise of the Wi-Fi password (intended for guests) grants an attacker full administrative 'root' access to the center's primary data-processing workstation.	**R-13**
IR	**IR-06**	Incident Reporting	Report security incident	Applicable (Shared)	Partially Implemented	Examine: Incident response policy (Corporate); Incident reporting records; Incident response plan (if any). Interview: Center Director; Tutors (to see if they know who to call for a "suspected" hack vs. a technical glitch). Test: Organizational processes for incident reporting (Simulated a question to a tutor: "What do you do if you think the router was tampered with?").	The organization maintains a Functional-Only reporting posture that fails to distinguish between technical glitches and security incidents. Key findings include: Convergence of Support: Staff utilize a single 'Help Desk' channel for all issues; no specialized pathway exists for reporting Suspected Security Anomalies (IR-06a). Lack of Thresholds: There is no defined reporting window (IR-06_ODP[01]) or 'Trigger' for alerting management to potential breaches, such as an unauthorized individual accessing the MDF closet (PE-03). Infrastructure Blind Spot: Because all functions (Admin, Student, Guest) run on a single Wi-Fi network with no isolation, staff are unable to differentiate between normal network congestion and a targeted attack, leading to zero reporting of network irregularities.	ARTIFACT IR-06-01: Corporate IT Support History (Analysis confirms 100% of tickets are for 'Functional Repairs' with 0% for 'Security Anomalies'). ARTIFACT IR-06-02: Staff 'Quick-Reference' Guide (Verified to list only 'Tech Support' contact info; no 'Security/Incident' hotline identified). REF-INT-IR06: Tutor Simulation: Staff confirmed they would 'restart the router' if it appeared tampered with, rather than preserving evidence or reporting a security event.	The organization fails to satisfy IR-06. The absence of a formalized Incident Reporting Culture creates an unacceptable Dwell Time for malicious actors. By treating security anomalies as simple 'technical support' issues, the center misses the opportunity for early detection and containment. Furthermore, the lack of local reporting authorities (IR-06_ODP[02]) ensures that physical breaches—like the 'Sticker Password' (IA-05) being compromised—remain undocumented and unmitigated.	**R-14**
MA	**MA-02**	Controlled Maintenance	Schedule, perform, document, and review records of maintenance and repair on system components.	Applicable (Local)	Not Implemented	Examine: Maintenance policy; maintenance records/logs; equipment repair receipts; system security plan. Interview: Personnel with maintenance responsibilities (Director); Personnel with security/privacy responsibilities. Test: Maintenance record-keeping system (Ask to see the log of the last time an iPad screen was replaced).	The organization maintains a Zero-Verification maintenance posture. Assessment identified the following critical gaps: Uncontrolled Access: The absence of a front-desk receptionist or access control gate allows third-party technicians to enter the facility and access the MDF closet (PE-03) without identity verification or authorization. Lack of Documentation (MA-02a): No Maintenance Log exists to record who touched what equipment, when, or why. There is no historical record of repairs or hardware modifications. Sanitization Failure (MA-02d): Devices (iPads/Chromebooks) are sent for external repair with active sessions and cached student PII, as no 'Sanitization-before-Service' protocol exists.	OBS-MA-02: Direct observation of 'Tailgating' potential; verified that visitors can walk directly to the network closet without being challenged for credentials. REF-INT-DIR: Director confirmation that no maintenance records are kept and no ID check is performed for 'ISP' or 'Repair' personnel. NEGATIVE EVIDENCE: Review of the facility entrance log (Sign-in sheet) confirmed zero entries for technical maintenance in the last 12 months, despite ongoing hardware use.	The organization fails to satisfy MA-02. The current 'Open-Door' maintenance model results in a total failure of Chain of Custody. Without verifying the identity of maintenance personnel or documenting their actions, the center is vulnerable to Malicious Hardware Insertion (e.g., keyloggers or rogue access points). Furthermore, the failure to sanitize devices before they leave the premises (MA-02d) constitutes a high-risk data spill, as unvetted third parties gain physical and logical access to hardware containing student PII.	**R-15**

Project: NIST 800-53 Rev. 5 Gap Analysis	**Entity**: Mathnasium | **Scope**: Educational Storefront Baseline	**Auditor**: K. Oriol | Date: February 2026	**Status:** Final Report (Version 1.0)	**Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID

MP	**MP-06**	Media Sanitization	Control and restrict the use of portable storage devices on information systems.	Applicable (Local)	Not Implemented	Examine: System media protection policy (or lack thereof); records retention and disposition procedures; hardware disposal receipts.
						
						Interview: Center Director; Organizational personnel with information security/privacy responsibilities.
						
						Test: Organizational processes for media sanitization (Checked a "retired" iPad in storage to see if PII was still accessible).
							The organization maintains a Passive Abandonment posture toward decommissioning. Assessment identified the following critical gaps:
							
							Data Persistence: 'Retired' iPads and Chromebooks are stored in an unsecured utility closet (PE-03) without being wiped. Technical testing on one 'retired' unit confirmed that user profiles and cached application data remained accessible.
							
							Lack of Technique (MP-06a): No formal sanitization techniques (Clear, Purge, or Destroy) have been defined or implemented. The organization relies on 'storage by neglect' rather than 'destruction by policy.'
							
							Physical Media Exposure: Hard-copy student records (PII) are disposed of in standard, un-shredded recycling bins, representing a failure to sanitize physical media before it leaves organizational control.
								`OBS-MP-06-01: Visual confirmation of 'Retired Hardware Pile' in the unsecured MDF closet.`
								`ARTIFACT MP-06-02: Photo of standard (non-shredding) recycling bin containing un-shredded student progress reports.`
								`REF-INT-MP06: Director statement: 'When they stop working, we just put them in the back; we don't have a way to wipe them if they won't turn on.'`
									The organization fails to satisfy MP-06. The accumulation of 'brick' devices creates a high-impact Data Spill risk. Without a verified sanitization protocol, these assets remain 'In-Scope' for audit and liability because they still contain student PII. The current method of abandoning hardware in an unlocked closet (PE-03) allows for the potential theft of media that has not been properly 'Cleared' or 'Purged' (NIST 800-88 standards), which could lead to a significant privacy breach if the devices are ever recovered or improperly recycled.	**R-16**

PE	**PE-03**	Physical Access Control	Control physical access to the facility by verifying individual authorization before granting access.	Applicable (Local)	Not Implemented	Examine: System entry and exit points (Front/Back doors); physical access control devices (Locks/Keys); inventory records of physical access control devices (if any).
						
						Interview: Center Director (Physical access responsibilities); Building Management (to see if they control the MDF closet).
						
						Test: Mechanisms supporting and/or implementing physical access control (Attempted to access the MDF closet during business hours without an escort).
							The facility lacks a defined Physical Security Perimeter for critical infrastructure. Assessment identified the following critical vulnerabilities:
							
							Unrestricted Ingress: The Main Distribution Frame (MDF) closet—housing the CR1000A Gateway, CCTV DVR, and retired hardware—is unlocked and located in a common area accessible to students, parents, and visitors.
							
							Lack of Monitoring (PE-03d): There is no 'Line-of-Sight' or receptionist at the front entrance to challenge unauthorized visitors. This allows for unescorted access to the MDF closet (verified during walkthrough).
							
							Inventory Failure: No record exists of who possesses keys to the facility (PE-03_ODP[07]), and no policy exists for rotating locks or combinations (PE-03_ODP[09]) upon staff turnover.
								`ARTIFACT PE-03-01: Photo of the unsecured MDF closet showing exposed network cabling and hardware.`
								`LOG-PE-03-02: Assessment Walkthrough Log: Confirmed successful unescorted access to the MDF closet for 10+ minutes without staff intervention.`
								`REF-INT-DIR: Director confirmation that no key inventory is maintained and no 'Visitor Management' protocol is in place.`
									The organization fails to satisfy PE-03. The current 'Open-Access' model creates a total loss of Physical Accountability. By failing to secure the MDF closet, the organization permits an attacker to perform a 'Physical Bypass' of all logical controls—such as resetting the router to factory defaults (recovering the 'Sticker Password') or disabling the CCTV DVR to erase evidence of a crime. This represents a critical failure in protecting the Availability and Integrity of the center's information systems.	**R-17**

PE	**PE-06**	Monitoring Physical Access	Monitor physical access to the facility to detect and respond to physical security incidents.	Applicable (Local)	Not Implemented	Examine: CCTV footage/records; physical access monitoring records; System Security Plan.
						
						Interview: Center Director (Monitoring responsibilities); Tutors (to see if they are aware of who monitors the cameras).
						
						Test: Mechanisms supporting and/or implementing the review of physical access logs (Asked the Director to demonstrate how they pull footage from a specific date/time).
							The organization maintains a Passive Surveillance posture. Although a multi-camera CCTV system is operational, it fails as a 'Detective' control due to the following gaps:
							
							Lack of Proactive Review: Interviews confirm that CCTV footage is never reviewed systematically. The frequency for review (PE-06_ODP[01]) is undefined, occurring only after a known theft or incident is reported.
							
							Fragile Monitoring Infrastructure: The CCTV DVR—the very system responsible for detecting tampering—is housed within the unsecured MDF closet (PE-03), allowing an intruder to disable the monitoring system before an alert can be generated.
							
							Absence of Coordination (PE-06c): There is no link between the surveillance system and an Incident Response (IR) plan. Suspicious activities (e.g., a visitor loitering by the MDF) are not treated as 'Security Events' for analysis or reporting.
								`ARTIFACT PE-06-01: CCTV Management Console Screenshot showing active recording but zero 'Review/Audit' logs for the past 90 days.`
								`REF-INT-PE06: Director statement: 'We only pull the tapes if something is missing.'`
								`OBS-PE-06: Verified camera placement provides 'Line-of-Sight' to the MDF closet, yet unauthorized access during the walkthrough was not flagged or reviewed.`
									The organization fails to satisfy PE-06. The absence of a regular review cadence (PE-06b) transforms the surveillance system from a Detective Control into a Forensic-Only tool. This creates a 'Security Lag'—where a physical breach of the network or a theft of student PII could go unnoticed for the duration of the 30-day retention cycle. Without active monitoring and a defined escalation path (PE-06c), the CCTV system provides a false sense of security while failing to mitigate the risk of ongoing, stealthy physical tampering.	**R-18**

PL	**PL-02**	System Security and Privacy Plans	Develop, document, and maintain a system security plan (SSP).	Applicable (Shared)	Partially Implemented	Examine: Corporate Security Plan; Local inventory records; System Architecture diagrams (if any).
						
						Interview: Center Director (to confirm if they have a local copy of any security blueprint); Corporate IT (to confirm the scope of the Corporate SSP).
						
						Test: Organizational processes for plan updates (Checked if the recent addition of new Chromebooks was reflected in any security documentation).
							The organization lacks a defined Security Authorization Boundary for local operations. Assessment identified the following critical governance gaps:
							
							Undefined Scope (PL-02a): While an SSP exists for the Corporate Portal, there is no localized SSP to account for the center's specific hardware (iPads, Chromebooks, Router).
							
							Operational Environment (PL-02a.09): No Network Topology or Data Flow Diagrams exist. The 'NYC Center' exists as an unmapped extension of the corporate network.
							
							Information Mapping (PL-02a.05): The types of information processed locally (e.g., student PII cached on tablets) are not documented, preventing the establishment of an accurate privacy baseline.
								`ARTIFACT PL-02-01: Mathnasium Corporate Security Plan (Scope Section) confirming local storefront hardware is excluded from the corporate boundary.`
								`ARTIFACT PL-02-02: Local Asset Inventory (Drafted by Auditor) representing the 'Unmapped' components currently missing from governance.`
								`REF-INT-PL02: Director statement confirming the absence of a 'Security Blueprint' or 'Boundary Definition' for the NYC location.`
								`NEGATIVE EVIDENCE: Visual inspection confirms zero documentation regarding local LAN topology or data flow.`
									The organization fails to satisfy PL-02. By operating without a localized SSP, the center exists in a Governance Vacuum. Without an established Authorization Boundary, the organization cannot perform valid privacy risk assessments or coordinate security requirements (PL-02_ODP[01]). This lack of formalization ensures that local hardware stays 'Out of Scope' for security updates and oversight, directly contributing to the Configuration Drift (CM-02) and Sanitization Failures (MP-06) identified throughout this assessment.	**R-19**

PS	**PS-02**	Position Risk Designation	Assign risk designations to all organizational positions, establish screening criteria, and review/update designations periodically.	Applicable (Shared)	Partially Implemented	Examine: Personnel security policy; Local job descriptions; Background check records; Employee handbook.
						Interview: Center Director (Personnel responsibilities); Corporate IT (to confirm corporate-level screening standards).
						Test: Process for assigning risk levels to new hires; Process for identifying high-risk vs. low-risk roles.
							The organization lacks a formal Position Risk Designation framework. All personnel—from part-time tutors to the Center Director—are treated as a single 'User' category.
							
							Lack of Risk Mapping (PS-02a): There is no documentation identifying which roles have access to sensitive PII versus those with only general operational access.
							
							Universal Privilege: Because a 'Master Password' (IA-05) and shared accounts (IA-02) are utilized, there is no technical or administrative distinction between high-risk and low-risk positions.
							
							Screening Disparity: While some staff undergo basic background checks, the depth of screening is not correlated to the level of system access they are granted.
								`REF-INT-DIR: Director confirmation that no formal 'Risk Tiers' exist for center staff.`
								`ARTIFACT PS-02-01: Employee Handbook: Review confirms that job descriptions do not include 'Security Responsibility' or 'Risk Designations.'`
								`REF-IA-05: The use of the 'Master Password' by all staff levels proves that no role-based risk management is being enforced.`
									The organization fails to satisfy PS-02. By failing to designate positions as High, Moderate, or Low Risk, the center cannot implement the Principle of Least Privilege. This creates a 'Flat Access' environment where a temporary employee has the same level of authority as management. This lack of role-based screening and access control significantly increases the Insider Threat risk, as there is no specialized oversight for individuals who have access to the center's most sensitive data assets.	**R-20**

Project: NIST 800-53 Rev. 5 Gap Analysis | **Entity**: Mathnasium | **Scope**: Educational Storefront Baseline | **Auditor**: K. Oriol | Date: February 2026 | **Status:** Final Report (Version 1.0) | **Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID

PS	**PS-04**	Personnel Termination	Notify the appropriate personnel when an individual is terminated or transferred.	Applicable (Shared)	Partially Implemented	Examine: Records of personnel termination actions; List of system accounts (Portal Export); Personnel security policy.
						
						Interview: Center Director (Account management responsibilities); Corporate IT (to confirm the defined termination notification window).
						
						Test: Organizational processes for personnel termination (Verified the "lag time" between a staff member's last day and their account deactivation).
							The organization lacks a synchronized Offboarding Workflow, resulting in significant 'Access Latency' after staff departures. Assessment identified:
							
							Dormant Account Persistence: Cross-referencing the Portal User Export against the local personnel roster identified three (3) 'Ghost Accounts' for employees terminated over six months ago.
							
							Lack of Notification (PS-04a): There is no formal trigger or 'Notification Window' (PS-04_ODP[01]) requiring the Director to alert Corporate IT of a termination.
							
							Shared Credential Exposure: Because the center utilizes a 'Master Password' (IA-05) for Wi-Fi and system administration, every terminated employee retains full administrative access to the local network until a manual, center-wide password reset occurs—which has not been performed in over 12 months.
								`ARTIFACT PS-04-01: Access/Personnel Cross-Reference Matrix (highlighting 3 active IDs for non-active staff).`
								`ARTIFACT PS-04-02: IT Log Review: Confirmed no deactivation requests were submitted for the last three departed employees.`
								`REF-INT-DIR: Director confirmation that no 'Security Exit Interview' (PS-04c) or credential rotation policy is in place.`
									The organization fails to satisfy PS-04. The existence of a Communication Silo between local management and Corporate IT nullifies the effectiveness of personnel security. By allowing dormant accounts to persist, the center creates a permanent Backdoor for unauthorized data exfiltration. Most critically, the failure to rotate the 'Master Password' upon staff turnover means that any former employee within range of the center's Wi-Fi signal maintains full 'Root' access to the center's workstations, representing a high-impact risk to the Confidentiality and Integrity of student PII.	**R-21**

RA	**RA-02**	Security Catego	Categorize information and the system according to an inventory of information types and potential impact.	Applicable (Shared)	Partially Implemented	Examine: Information inventory; System Security Plan (SSP); Privacy Impact Analysis (PIA).
						
						Interview: "Center Director (to see if they know which data is ""Sensitive""); Corporate Compliance."
						
						Test: Process for labeling data (e.g., checking if digital folders are marked ""Confidential"").
							The organization has not performed a formal Security Categorization.
							
							Lack of Inventory (RA-02a): There is no master list of information types (e.g., Student Health Records, Financial PII, or Proprietary Curriculum) processed by local hardware.
							
							Impact Undefined: The center has not determined the 'Impact Level' (Low, Moderate, High) for a loss of Confidentiality, Integrity, or Availability for its local systems.
							
							Universal Data Treatment: All data is treated with the same level of security, meaning safety-critical student emergency info is given no more protection than a math worksheet.
								`REF-INT-RA02: Director confirmation: 'We don't really rank the data; it's all just on the iPads.'`
								`NEGATIVE ARTIFACT: Review of the local file system on the Admin Mac confirmed no use of 'Confidential' or 'Restricted' metadata/tags for PII folders.`
								`REF-PL-02: Absence of a localized SSP confirms that no categorization has been officially documented.`
									The center fails to satisfy RA-02. Without categorizing information, the organization cannot apply Proportionate Protections. This leads to a 'security mismatch' where high-value PII is protected by the same weak controls (the 'Sticker Password') as non-sensitive data. This failure to identify 'High-Impact' data assets makes it impossible to prioritize security spending or incident response efforts, leaving the center's most sensitive information vulnerable to under-protection.	**R-22**

RA	**RA-03**	Risk Assessment	Conduct an assessment of risk, including the likelihood and magnitude of harm.	Applicable (Local)	Implemented	Examine: Risk Assessment Report (Your Gap Analysis); Risk Assessment Policy (if any); System Security Plan.
						
						Interview: Center Director (Regarding previous risk identification methods); Yourself (as the Assessor).
						
						Test: Organizational processes for risk assessment (The execution of this current audit).
							The organization satisfies RA-03 through the execution of a comprehensive 2026 Gap Analysis. This assessment identifies specific threats to local infrastructure and the likelihood of adverse effects (RA-03a.03) regarding the processing of student PII. By documenting these results in a formal Risk Assessment Report (RA-03c), the center has established a baseline for risk management decisions. To maintain compliance, the center must now institutionalize the frequency (RA-03_ODP[03/05]) to ensure these results are reviewed and updated annually.	`Artifact RA-03-01: Completed Gap Analysis Spreadsheet (The document we are working on).`
								
								`Artifact RA-03-02: Risk Assessment Executive Summary (Your final report for the class/center).`
								
								`Artifact RA-03-03: Email/Meeting Invite: Proof of dissemination of these findings to the Center Director (satisfying RA-03e).`
									While the current assessment successfully fulfills the requirement to identify vulnerabilities, the center previously operated in an 'Assessment Vacuum' without a defined Risk Management Strategy. The findings of this report must be integrated into the System Security Plan (PL-02) to ensure that risk-based decisions are documented and disseminated to the appropriate authorities (RA-03_ODP[04]). The primary risk now is 'Forensic Decay'—where this report is treated as a one-time event rather than a recurring Continuous Monitoring (CA-07) component.	**N/A**

RA	**RA-05**	Vulnerability Monitoring and Scanning	Scan for vulnerabilities in the information system and hosted applications.	Applicable (Shared)	Partially Implemented	Examine: System vulnerability scanning results; Records of vulnerability remediation; Security advisory subscription records (e.g., CISA, Apple, Verizon).
						
						Interview: Center Director (to determine if they receive alerts about iPad/Router bugs); Corporate IT (to confirm if they scan the local network remotely).
						
						Test: Mechanisms for updating device firmware; Verification of "Auto-Update" settings on endpoint devices (iPads/Mac).
							The organization maintains a Reactive vulnerability posture. Assessment identified that there is no proactive process for identifying flaws in local hardware:
							
							Lack of Scanning (RA-05a): No local or remote vulnerability scans are performed on the center's network. The 'Refurbished' iPads and the Verizon Router are not checked for known exploits or 'Out-of-Date' firmware.
							
							Undefined Frequency: The center has not defined how often devices should be checked for vulnerabilities. Updates are handled 'Ad-Hoc' when a device stops working or an app requires a version jump to function.
							
							Absence of Advisories: The Center Director does not subscribe to security alerts or advisories for the hardware in use, meaning the center is unaware of 'Zero-Day' threats until they are potentially exploited.
								`ARTIFACT RA-05-01: Visual Inspection: Confirmed that one 'retired' iPad was running an iOS version three cycles behind the current release, containing several unpatched CVEs.`
								`REF-INT-RA05: Director interview: 'We don't use any scanning software. If the iPad tells us it needs an update, we usually hit "later" if we are busy with students.'`
								`ARTIFACT RA-05-02: Verizon Router Logs: Confirmed no 'Security Scan' or 'Intrusion Detection' reports have been generated or reviewed.`
									The center fails to satisfy RA-02. The absence of a Vulnerability Management Program leaves the center's network exposed to 'Low-Hanging Fruit' exploits. By relying on manual, ad-hoc updates rather than automated scanning and monitoring, the center significantly increases the likelihood of a System Compromise. This is especially critical for the 'Refurbished' hardware, which may have a shorter security support lifecycle. Without a scanning capability, the organization remains 'Blind' to technical vulnerabilities that could be used to bypass the shared 'Sticker Password' (IA-05).	**R-23**

SA	**SA-09**	External System Services	Identify and manage external information system services and providers.	Applicable (Local)	Not Implemented	Examine: Acquisition documentation; Service Level Agreements (SLAs); ISP contracts; Equipment repair receipts; System Security Plan.
						
						Interview: Center Director (Responsibility for selecting local vendors); Franchise Owner (Acquisition responsibilities).
						
						Test: Organizational processes for monitoring external provider compliance (Requested the "Security Annex" for the current ISP contract).
							Assessment of SA-09 reveals a significant breakdown in third-party risk management. Examine of local service contracts for the ISP and hardware repair shops confirms a lack of defined security and privacy requirements (SA-09a). The center lacks formal Service Level Agreements (SLAs) or contracts that include 'Right to Audit' or data protection clauses. This results in a 'Blind Trust' model where external providers have physical and logical access to system components without any organizational oversight (SA-09b) or ongoing monitoring (SA-09c) of their compliance posture. New asset procurement (MacBook) lacked a formal security review of the vendor's data protection capabilities.	`Artifact SA-09-01: ISP Monthly Statement/Contract: Note the absence of a "Data Processing Addendum" or "Security Annex."`
								
								`Artifact SA-09-02: Repair Shop Receipt: A copy of a receipt from a local repair shop that lacks any language regarding the sanitization or protection of data on the device.`
								
								`Artifact SA-09-03: Interview Record: Director statement confirming that vendor selection is based on price/convenience rather than a security assessment.`
									The center currently operates with an undocumented Supply Chain Risk. By utilizing unvetted third-party service providers for critical infrastructure (ISP) and endpoint maintenance (uBreakiFix) without formal contractual safeguards (SA-09_ODP[01]), the organization is exposed to unchecked external vulnerabilities. This 'Vendor Management Gap' means the center cannot ensure the integrity or confidentiality of the system when it is under the control of external parties, directly violating the requirements for External System Services oversight.	**R-24**

SC	**SC-01**	Policy and Procedures	Develop and disseminate a system and communications protection policy.	Applicable (Shared)	Partially Implemented	Examine: Corporate Network Standards; System Security Plan (SSP); Local Wi-Fi configuration notes (if any); Center Administrative Manual.
						
						Interview: Center Director (Responsibility for local Wi-Fi management); Corporate IT (to verify the dissemination of network policies).
							While the organization utilizes high-level network standards inherited from Corporate, it fails to satisfy SC-01a.[03] regarding the development of local procedures. Interviews confirm that the management of local communications protection—such as Wi-Fi credential lifecycle and router hardening—is performed ad-hoc. There is no defined frequency for review (SC-01_ODP[07]), and responsibilities (SC-01a.01(a)[04]) for maintaining the security of the local network perimeter are not formally assigned to center-level personnel.	`Artifact SC-01-01: Corporate "Franchise Technology Standards" Document: Shows the broad requirements but lacks center-specific configuration steps.`
								
								`Artifact SC-01-02: Negative Evidence: A review of the center's "Manager's Handbook" confirms the absence of a section dedicated to System and Communications Protection Procedures.`
								
								`Artifact SC-01-03: Interview Record: Director statement confirming that there is no "Official" (SC-01b) tasked with reviewing local network security posture.`
									The center suffers from a Procedural Void in its communications protection framework. Although a policy (SC-01a.[01]) exists at the enterprise level, the lack of localized standard operating procedures (SOPs) results in inconsistent security enforcement at the 'Last Mile.' Without documented procedures for boundary protection and wireless management, the organization cannot ensure a repeatable or verifiable security state, leading to 'Configuration Drift' and unmanaged risks in the local network environment.	**R-25**

Project: NIST 800-53 Rev. 5 Gap Analysis	**Entity**: Mathnasium | **Scope**: Educational Storefront Baseline	**Auditor**: K. Oriol | Date: February 2026	**Status:** Final Report (Version 1.0)	**Linked Artifacts:** [Risk Register Ref: RR-2026-01]

Control Family	Control ID	Control Name	Control Statement	Applicability	Implementation	Assessment Objects	Observations	Evidence	Gap Description / Findings	Risk ID
SC	**SC-07**	Boundary Protection	Limit unnecessary internal and external communications (Firewalls).	Applicable (Local)	Partially Implemented	Examine: System configuration settings (Router Admin Panel); Network topology diagram (or lack thereof); System Security Plan. Interview: Center Director (Responsibility for Wi-Fi access); Tutors (to see if they use the same password as students). Test: Mechanisms implementing boundary protection (Performed a "Network Scan" while connected to the Wi-Fi to see if other devices were visible).	Physical examination and technical testing of the local network infrastructure reveal a high-risk Flat Network Topology. While a managed interface exists at the perimeter (External Router), the organization fails to satisfy SC-07b, as there is no logical or physical separation between publicly accessible Wi-Fi and internal system components. Substantive Testing confirms that a device connected to the primary Wi-Fi can successfully communicate with the CCTV DVR and Staff iPads, bypassing the requirement for internal boundary protection (SC-07a.[04]). The administrative interface for the primary gateway (cr1000a) is secured using the factory-default 'Admin Password' printed on the chassis sticker. The device is located in an unlocked MDF/Server closet (PE-03), making the credentials physically accessible to any visitor or unauthorized person who enters the storage area.	`Artifact SC-07-01: Network Scan Log: A screenshot or list showing that a "Guest" device can see the IP addresses of the CCTV DVR and the Router Admin page.` `Artifact SC-07-02: Router Configuration Screenshot: Showing that only one SSID (Wi-Fi Name) is active for the entire center, with no "Guest Isolation" or "VLAN" settings enabled.` `Artifact SC-07-03: Observation Record: Confirmation that no physical firewalls or managed switches exist between the Tutoring floor and the MDF closet.` `Execution of the arp -a utility on the local workstation (192.168.1.56) identified 12+ active hosts on the 192.168.1.0/24 subnet. The presence of personal mobile devices (iPhone/iPad) alongside administrative workstations and network printers on a single broadcast domain confirms a Flat Network Topology. No evidence of logical isolation or VLAN tagging was observed.`  `REF-IMG-PE-ROUTER`	The center lacks Network Segmentation, creating a significant risk of Lateral Movement. Without the implementation of Virtual Local Area Networks (VLANs) or distinct subnetworks, the organization cannot enforce the Principle of Least Privilege at the network layer. This deficiency allows unvetted guest devices to sit on the same broadcast domain as systems processing Student PII and security infrastructure (CCTV), directly violating the SC-07 requirement for internal boundary protection and subnetwork separation. The center fails to meet SC-7(21) (Isolation of System Components). By allowing personal devices and administrative assets to reside on the same subnet, the center lacks a Managed Interface to control internal communications, facilitating potential lateral movement and packet sniffing by unauthorized or compromised devices. This violates SC-7(5) (Deny by Default) and SC-07(a). Boundary protection is rendered ineffective when the management credentials are: 1) Non-unique/Default, and 2) Physically exposed to unauthorized users. This allows an attacker to bypass all logical boundaries by logging into the router and disabling security features or rerouting traffic.	**R-26**

SC	**SC-21**	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Design the system with layers of protection and isolation.	Applicable (Local)	Not Implemented	Examine: Router configuration settings; System Security Plan; ISP service documentation.
						
						Interview: Center Director (Regarding local network setup); ISP Technical Support (to verify DNS defaults).
						
						Test: Mechanisms implementing data origin authentication (Used a "DNSSEC Resolver Test" tool on a center iPad to see if validation was active).
							Technical testing of the center's local network confirms that the recursive DNS resolver (the local router) does not support or enforce DNSSEC validation (SC-21[02]). Examine of the router configuration settings shows a reliance on standard ISP DNS protocols, which lack data origin authentication and integrity verification (SC-21[04]). This leaves the local system vulnerable to DNS cache poisoning attacks, which could lead to the unauthorized redirection of traffic to malicious domains. Technical validation using delv returned a no crypto support and No trusted keys were loaded error. This confirms the local network environment lacks the necessary Trust Anchors to perform DNSSEC validation.	`Artifact SC-21-01: DNSSEC Test Result: A screenshot from a tool like dnssec-analyzer.verisignlabs.com or a local command line showing "Insecure" or "Validation: No." [delv @192.168.x.1 google.com ;; none:29: no crypto support delv: No trusted keys were loaded]`
								
								`Artifact SC-21-02: Router Admin Screenshot: Showing DNS settings set to "Automatic from ISP" with no option or configuration for DNSSEC or encrypted DNS.`
								
								`Artifact SC-21-03: Interview Record: Confirmation from the Director that the router was installed with "out-of-the-box" settings with no security-specific DNS configuration.`
									The center lacks DNS Security Extensions (DNSSEC) at the local boundary. By failing to request and verify authenticated name/address resolution responses, the organization is exposed to DNS Spoofing and Man-in-the-Middle (MitM) attacks. In the absence of 'DNS over HTTPS' (DoH) or DNSSEC-aware resolvers, the system cannot guarantee that requests to the Mathnasium Portal are directed to the legitimate authoritative source, creating a risk of credential harvesting and data exfiltration. The local recursive resolver (Gateway) fails to provide the cryptographic authentication required by SC-21. This constitutes a failure in Data Origin Authentication and Integriy Verification for DNS traffic.	**R-27**

SI	**SI-02**	Flaw Remediation	Identify, report, and correct system flaws in a timely manner (Patch Management).	Applicable (Local)	Not Implemented	Examine: System configuration settings (Software version info); List of recent security flaw remediation actions (or lack thereof).
						
						Interview: Center Director (Responsibility for updates); Tutors (To see if they are allowed/instructed to click 'Update').
						
						Test: Organizational process for installing software updates (Checked 5 devices for pending updates).
							Technical testing of the center's hardware fleet reveals a systemic failure in Flaw Remediation (SI-02). Substantive testing of iPads and Chromebooks identified multiple devices running outdated operating systems with pending security notifications. Most critically, the center utilizes Legacy Hardware that has reached 'End of Life' status, meaning these devices can no longer satisfy SI-02a.[03] as firmware and software flaws cannot be corrected. This results in a persistent, unmitigable risk to the local network and the student data accessed via these endpoints. The presence of End-of-Life (EoL) hardware creates an unmitigable vulnerability, as these devices no longer receive security-relevant updates, rendering the control 'Not Implemented' for a significant portion of the endpoint fleet causing a technical debt.	`Artifact SI-02-01: Device Status Log: A table listing 5 devices, their current OS version, and the "Latest Available" version (showing the lag).`
								
								`Artifact SI-02-02: Photo of 'Legacy' Device: A screenshot of an older iPad showing 'Your software is up to date' but showing an OS version from 3 years ago (proving it can no longer receive updates).`
								
								`Artifact SI-02-03: Interview Record: Director statement confirming there is no schedule or tool (like MDM) used to push updates to devices.`
									The organization lacks a Vulnerability Management Program. By relying on manual, user-driven patching, the center suffers from significant Patch Latency. The inclusion of legacy assets that no longer receive security-relevant updates (SI-02c) creates a 'Permanent Vulnerability' state. Without a defined remediation time period (SI-02_ODP) or a process for decommissioning obsolete hardware, the center is vulnerable to exploits targeting known vulnerabilities (CVEs) that have long since been patched by manufacturers but remain active on center devices.	**R-28**

SI	**SI-04**	System Monitoring	Monitor the information system to detect attacks and indicators of intrusions.	Applicable (Shared)	Partially Implemented	Examine: System security plan; system monitoring strategy/procedures; records of monitoring activities; audit logs; intrusion detection/prevention system (IDS/IPS) configurations.
						
						Interview: Organizational personnel with system monitoring responsibilities; personnel with information security responsibilities.
						
						Test: Mechanisms supporting and/or implementing system monitoring; automated tools for detecting indicators of compromise (IoC).
							The center lacks a Continuous Monitoring capability to detect unauthorized digital activity.
							
							Lack of Intrusion Detection (SI-04a): The organization does not employ tools to monitor the network for 'Attacks or Indicators of Intrusions.' The Verizon CR1000A Gateway is operating without active firewall alerts or Intrusion Detection System (IDS) rules configured.
							
							Inbound/Outbound Monitoring (SI-04b): There is no monitoring of 'Outbound Communications' to detect if a compromised iPad is 'calling home' to a malicious server (Command and Control).
							
							Unauthorized Secret Monitoring: No alerts are configured for 'Unauthorized Wireless Access' or 'Multiple Failed Login Attempts,' allowing an attacker to perform brute-force attacks on the shared 'Master Password' (IA-05) without detection."
								`ARTIFACT SI-04-01: Verizon Router Admin Panel Review: Confirmed 'Security Logs' are enabled but 'Proactive Alerting' and 'Traffic Inspection' are disabled.`
								`REF-INT-SI04: Director statement: 'We don't get notifications if someone tries to hack the Wi-Fi. We wouldn't know unless the internet went down.'`
								`ARTIFACT SI-04-02: Endpoint Check: Confirmed that neither the Admin Mac nor the iPads have 'Endpoint Detection and Response' (EDR) software installed to monitor for malicious system behavior.`
									The organization fails to satisfy SI-04. The current posture is 'Blind' to active threats. Without System Monitoring, a data breach could persist for months without detection, as there are no 'Tripwires' to alert management to unauthorized access. This deficiency significantly increases the risk of a Lateral Movement attack, where an intruder compromises a student's personal device on the shared Wi-Fi and then moves undetected to the Admin Mac to exfiltrate student PII. The absence of monitoring nullifies the effectiveness of any other digital controls in place.	**R-29**

SR	**SR-12**	Component Disposal	Use tools to verify that hardware/software is genuine and not counterfeit.	Applicable (Local)	Not Implemented	Examine: Disposal records for system components; Media disposal policy; hardware inventory list (to check for "Retired" status).
						
						Interview: Center Director (Responsibility for discarding old tablets/laptops).
						
						Test: Organizational techniques and methods for system component disposal (Asked to see the "Wipe" log for the legacy iPads mentioned in SI-02).
							Examine of the center's disposal records confirms a total absence of a formal decommissioning process for Information System components. The organization fails to satisfy SR-12, as there are no documented techniques or methods (SR-12_ODP[02]) for the destruction or sanitization of retired assets. Physical inspection of the facility identified legacy iPads and Chromebooks in an unsecured storage area, containing potential Student PII and cached credentials, with no Certificates of Destruction or sanitization logs to verify data removal. Physical accumulation of retired assets in the MDF closet (PE-03) creates a concentrated target for data theft.	`Artifact SR-12-01: Photo of "Retired" Hardware Pile: Showing iPads sitting in a dusty corner of the utility closet.`
								
								`Artifact SR-12-02: Interview Record: Director confirmation: "We usually just throw the old Chromebooks in the recycle bin once they stop turning on."`
								
								`Artifact SR-12-03: Negative Evidence: A review of the center's financial records showing no line items for "Secure Data Destruction" services.`
									The center lacks a Hardware Life-Cycle Management Policy. This failure in Supply Chain Risk Management allows for 'Data Spillage' during the disposal phase. Without a verified sanitization protocol, retired hardware remains a liability, as malicious actors could recover sensitive organizational data or PII from discarded media. The current ad-hoc disposal method violates regulatory requirements for data privacy and fails to ensure the finality of data destruction.	**R-30**