NYLE

FedRAMP Gap Analysis Report

NYLE FedRAMP Readiness SaaS

Prepared for: **NYLE Technologies**
Report Contact: **Adrienne**
Version: **1.0.0**
Date: **February 10, 2026**

About This Report

The NYLE FedRAMP Gap Analysis Report is generated based on information and responses provided by representatives of the organization. The report leverages those inputs to perform an automated assessment against the FedRAMP High, Moderate, and Low baselines, derived from the NIST Special Publication 800-53 Revision 5 security control framework.

This assessment is designed to identify areas where the organization's current security and compliance practices may not align with applicable FedRAMP requirements, as well as areas that appear to meet those requirements based on the information provided.

The analysis is intended to provide insight and preparation support for organizations seeking to understand and improve their readiness for FedRAMP authorization. The findings and recommendations in this report are advisory in nature and should be used for internal readiness planning and program development.

Intended Audience

This report is intended for internal use by FedRAMP stakeholders within the organization, including security professionals, compliance officers, technical architects, product leaders, and executive sponsors, to support readiness planning and guide next steps toward achieving FedRAMP authorization.

Disclaimer

> *NYLE is not a Third-Party Assessment Organization (3PAO), and this report does not constitute an official FedRAMP assessment, certification, or authorization determination. The accuracy of the report depends on the completeness and correctness of the information provided by the organization, which NYLE does not independently verify. This report is intended for informational and readiness purposes only and does not guarantee FedRAMP Ready or Authorized status.*
> *This document and its contents do not constitute legal advice. Organizations should consult qualified counsel or accredited assessors when pursuing formal FedRAMP authorization. While NYLE endeavors to provide accurate and current information, no warranties, express or implied, are made regarding the completeness or fitness of this report, and NYLE assumes no liability for any decisions, actions, or outcomes resulting from its use.*

NYLE

Table of Contents

I. Assessment Summary

An assessment of NYLE FedRAMP Readiness SaaS was performed against the NIST Special Publication 800-53 Revision 5 security controls that form the basis of the FedRAMP High, Moderate, and Low security baselines. These baselines represent the graduated levels of security required for cloud systems based on the potential impact of a security incident on organizational operations, assets, and individuals.

FedRAMP defines three security impact levels and corresponding control sets:

- Low Impact: 156 security controls
- Moderate Impact: 323 security controls
- High Impact: 410 security controls

The NYLE FedRAMP Gap Analysis Report evaluates the organization's responses against these control baselines to determine where the system appears to meet FedRAMP requirements and where gaps may exist.

Controls that appear to be met, based on the information provided, are captured and reflected in this report. Controls that appear not to be met are also identified, along with recommendations for strengthening alignment with the corresponding FedRAMP requirements.

This report is intended to help organizations prepare for FedRAMP authorization by identifying areas requiring improvement and providing a structured foundation for pursuing FedRAMP Ready or FedRAMP In Process status.

II. Findings

The compliance status below summarizes the results of the FedRAMP gap analysis. These results indicate how many FedRAMP High, Moderate and Low requirements the organization appears to meet, and how many appear not to be met.

Based on the FedRAMP High, Moderate, and Low security controls identified as met, the organization's self-attested compliance status for each FedRAMP baseline is shown below.

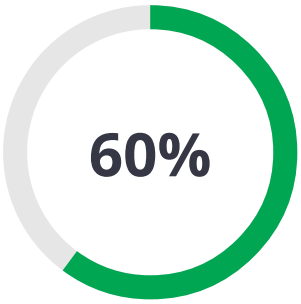
1. Security Controls

The following table summarizes the status of the evaluated system against 410 NIST SP 800-53 Revision 5 security controls used to categorize FedRAMP High, Moderate, and Low systems. A granular breakdown can be viewed in your organization's NYLE portal.

Controls Met:	**285**
Not Met:	**125**
Not Applicable:	**0**
TOTAL CONTROLS:	**410**

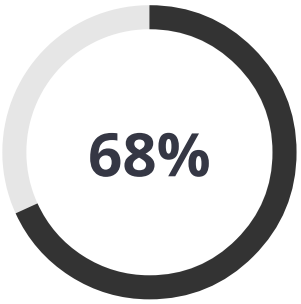
2. Tiered Compliance Readiness Score

Readiness assessment across different FedRAMP impact levels



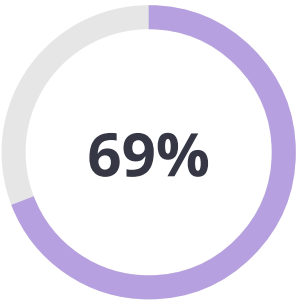
FedRAMP Low

95 met + 0 N/A /
156 total controls



FedRAMP Moderate

220 met + 0 N/A /
323 total controls



FedRAMP High

285 met + 0 N/A /
410 total controls

3. Recommendations

The following technical and operational recommendations address identified gaps to facilitate alignment with FedRAMP requirements.

SECURITY CONTROL ID(S): PE-02, PE-03, PE-05

IMPLEMENTATION STEPS:

Issue permanent access credentials for employees and temporary credentials or identifiers for visitors. Use card readers, locks, or guards to restrict movement from public areas (e.g. lobby, reception) to non-public areas (e.g. working spaces). Escort visitors in restricted spaces. Keep a visitor log (paper or digital) for check-in/check-out. Log employee badge activity automatically through the access control system. Revoke access immediately when someone leaves the organization and change keys or lock combinations if lost or after a security incident. Document your organization's physical security approach in a policy or procedures.

SECURITY CONTROL ID(S): PE-01

IMPLEMENTATION STEPS:

Create a formal physical and environmental protection policy covering purpose, scope, roles, responsibilities, and how you protect facilities and infrastructure. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after physical security incidents or facility changes. FedRAMP Low and FedRAMP Moderate require overall policies to be reviewed and updated at least every 3 years, however the procedures within those policies shoud be reviewed and updated t least annually.

SECURITY CONTROL ID(S): PE-08, PE-08 (01)

IMPLEMENTATION STEPS:

Use a digital visitor management system such as Envoy, ProxyClick, or even a Google Form to record: Name, identification, company, person visited, purpose, date/time in & out. Align security personnel to review and verify the visitor's submitted information with the visitor upon arrival to implement daily real-time checks. Escalate any anomalies such as duplicate entries, unusual entry times, missing information, etc.

SECURITY CONTROL ID(S): PL-01

IMPLEMENTATION STEPS:

Create a formal planning policy covering purpose, scope, roles, responsibilities, and how security and privacy integrate into organizational planning. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or when organizational objectives change. FedRAMP Low and FedRAMP Moderate require overall policies to be reviewed and updated at least every 3 years, however the procedures within those policies shoud be reviewed and updated t least annually.

SECURITY CONTROL ID(S): PE-17

IMPLEMENTATION STEPS:

Determine and document alternate work sites allowed for use by employees. Employ defined controls at alternate work sites. Assess the effectiveness of controls at alternate sites. Provide a means for employees to communicate with information security and privacy personnel in case of incidents. This addresses remote work scenarios and ensures security controls extend beyond traditional office environments.

SECURITY CONTROL ID(S): PL-02, PL-08

IMPLEMENTATION STEPS:

Create security and privacy plans for each system documenting: components, how it operates, roles, information types, security categorization, threats, requirements, implemented controls, and risk decisions. Develop security and privacy architectures describing protection approaches and enterprise architecture integration. Get leadership approval before implementation. Review and update at least annually or when significant changes happen. Protect plans from unauthorized access.

SECURITY CONTROL ID(S): PL-10, PL-11

IMPLEMENTATION STEPS:

1) Choose your FedRAMP baseline (Low, Moderate, High). 2) Decide which controls are provided at the organizational or enterprise level (like centralized logging, patch management) vs. system-specific. 3) Determine which controls from the baseline may not be applicable to your system. 4) If you can't meet a control as written, document an alternative control that provides equivalent or greater protection. 5) Determine the "organization-defined" parameters in controls (e.g., "lock accounts after [3] failed logins within [15 minutes]"). You've reviewed all required security controls and established which will be met by your organization vs. system-specific. You don't have to have the controls implemented yet.

SECURITY CONTROL ID(S): PL-04, PL-04 (01), PS-06

IMPLEMENTATION STEPS:

Establish rules of behavior that outline how personnel are expected to use the system from a security, privacy, and appropriate use perspective. Outline restrictions such as no posting sensitive info online, no using work emails/passwords for external accounts, rules for social media use. Require all users to read and sign the rules of behavior as a formal access agreement before system access is granted. Retain acknowledgments for your records. Review the rules of behavior at least once per year (or sooner if policies or systems change). Make updates as required and require all users to re-sign any changes. Even if no changes, require annual re-signing to maintain access. Suspend access if a user has not signed or re-signed within a specific timeframe that your organization defines. FedRAMP Moderate and Low only require rules of behavior to be reviewed and updated at least every 3 years, but they still must be acknowledged annually.

SECURITY CONTROL ID(S): PS-02, PS-09

IMPLEMENTATION STEPS:

All system roles have an associated risk designation, with security and privacy criteria defined for each risk level. For example, all roles undergo standard security and privacy training, but Moderate-risk roles also have role-based training and High-risk roles are required to implement MFA for privileged access. Risk levels are reviewed at least annually for FedRAMP High, at least every 3 years for FedRAMP Moderate and FedRAMP Low. Criteria for each type of role is defined based on the risk level. Assign risk designations to all organizational positions and establish screening criteria for individuals filling those positions. Incorporate security and privacy roles and responsibilities into organizational position descriptions.

SECURITY CONTROL ID(S): PS-03, PS-03 (03)

IMPLEMENTATION STEPS:

Perform background checks on all personnel with access to the FedRAMP system. For FedRAMP High systems, perform I-9 identity proofing to ensure all personnel are U.S. Persons. Screen individuals prior to authorizing system access. If security clearances are required, ensure personnel are re-screened in alignment with federal clearance re-screening requirements. Rescreen according to defined conditions and frequencies where rescreening is indicated. Verify individuals accessing systems processing information requiring special protection have valid access authorizations demonstrated by assigned official government duties and satisfy additional personnel screening criteria.

SECURITY CONTROL ID(S): PS-08

IMPLEMENTATION STEPS:

Establish a formal sanctions process for security and privacy policy violations. Define what violations look like and what sanctions may be applied. Set up notifications so security leads are informed within 24 hours when sanctions are initiated, including who's being sanctioned and why. Document this in your policies and coordinate with HR. FedRAMP Low does not have a 24 hours notification period requirement.

SECURITY CONTROL ID(S): PS-07

IMPLEMENTATION STEPS:

For all contractor and vendor personnel who have access to your system, include contract language that requires immediate notification of terminations and notification within 24 hours of transfers or role changes, for all personnel with system access. Establish a standardized process for vendors to submit changes via a standardized process. When notified, immediately disable credentials and revoke badges for terminated personnel. Review and adjust access levels for transferred personnel.

SECURITY CONTROL ID(S): RA-01

IMPLEMENTATION STEPS:

Create a formal risk assessment policy covering purpose, scope, roles, responsibilities, and how you'll identify and manage risks. Establish a risk management program defining how risks are identified, analyzed, prioritized, and addressed. Assign someone to own and maintain this policy. Review and update at least annually or when the threat landscape changes significantly. FedRAMP Low and FedRAMP Moderate require overall policies to be reviewed and updated at least every 3 years, however the procedures within those policies shoud be reviewed and updated t least annually.

SECURITY CONTROL ID(S): PS-01

IMPLEMENTATION STEPS:

Create a formal personnel security policy covering purpose, scope, roles, responsibilities, and screening/vetting procedures. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after insider incidents or changes to background check requirements. FedRAMP Low and FedRAMP Moderate require overall policies to be reviewed and updated at least every 3 years, however the procedures within those policies shoud be reviewed and updated t least annually.

SECURITY CONTROL ID(S): RA-03 (01), SR-05, SR-06, SR-08

IMPLEMENTATION STEPS:

Establish a supply chain risk assessment framework that identifies critical suppliers and the systems or services they provide. Assess and document risks such as outages, data loss, vendor lock-in, or malicious code, and review supplier compliance reports (e.g., SOC 2, FedRAMP, ISO 27001) to verify their controls. Monitor vendor advisories and status pages to maintain visibility into emerging risks. Conduct these assessments at least annually and whenever major changes occur. Require agreements with suppliers that obligate them to notify your organization of supply chain compromises and share assessment or audit results. Contracts should include key security terms such as breach notification, secure development practices, data handling requirements, prohibition of counterfeit components, and right to audit where appropriate.

SECURITY CONTROL ID(S): RA-05 (02)

IMPLEMENTATION STEPS:

Configure your scanning tool to automatically update vulnerability definitions before each scan, ideally within 24 hours. Enable automatic updates from the vendor's threat feed and schedule scans to run after updates complete. Maintain logs showing when updates occurred.

SECURITY CONTROL ID(S): RA-03

IMPLEMENTATION STEPS:

Conduct risk assessments including: identifying threats and vulnerabilities, determining likelihood and magnitude of harm from unauthorized access/use/disclosure/disruption/modification/destruction, and determining likelihood and impact of adverse effects on individuals from processing PII. Integrate risk assessment results with organization and mission/business process perspectives. Document results in security and privacy plans or risk assessment reports. Review results at defined frequencies. Disseminate results to designated personnel. Update risk assessments at defined frequencies or when significant changes to the system, environment, or other conditions may impact security or privacy state.

SECURITY CONTROL ID(S): PS-04, PS-04 (02), PS-05

IMPLEMENTATION STEPS:

Upon termination, disable system access and revoke credentials immediately (within hours, not days). Use automated mechanisms to notify appropriate personnel of termination actions and to disable access to system resources. Conduct exit interviews covering security topics and retrieve all security-related organizational property. When individuals are reassigned or transferred, review and confirm ongoing operational need for current access authorizations. Initiate transfer or reassignment actions within defined timeframes following the formal action. Modify access as needed to correspond with changes in operational need. Integrate these processes with your HR system for automatic triggering.

SECURITY CONTROL ID(S): RA-05

IMPLEMENTATION STEPS:

Document remediation timelines: 30 days for Critical/High, 90 days for Moderate, 180 days for Low. Use a ticketing system to track vulnerabilities from identification through remediation. Prioritize based on severity, exploitability, system criticality, and exposure. Document remediation activities including compensating controls for vulnerabilities that can't be immediately patched.

SECURITY CONTROL ID(S): RA-05 (11)

IMPLEMENTATION STEPS:

Share scan results and remediation status internally with IT, security, development, and executives. Create a public security page or notification system where customers can learn about vulnerabilities affecting your services. Set up a responsible disclosure program or bug bounty. Define procedures for publicly disclosing customer-impacting vulnerabilities.

SECURITY CONTROL ID(S): RA-05 (04)

IMPLEMENTATION STEPS:

Do web searches, use vulnerability scanners, or cloud security center tools to see what outsiders can find about your system. Look for things like open ports, passwords, system documents, etc. posted online that reveal too much about your systems. Notify your IT or security leads if sensitive info is found, and remove the information. Reconfigure the system to hide or minimize exposed details.

SECURITY CONTROL ID(S): SA-02

IMPLEMENTATION STEPS:

Include security and privacy requirements when planning new initiatives or systems. During budget planning, allocate specific funding for security and privacy (tools, personnel, training, assessments, etc.) as separate line items rather than hiding them in general IT costs. This ensures security gets proper funding and visibility.

SECURITY CONTROL ID(S): SA-04 (05), SA-11, SA-11 (01)

IMPLEMENTATION STEPS:

Implement secure code development standards such as OWASP secure coding practices or NIST 800-218 Secure Software Development Framework. Integrate common SAST tools such as GitHub CodeQL, AWS CodeGuru Reviewer, Google Cloud Build, or SonarCloud to ensure secure coding practices are implemented. Your organization has secure coding practices implemented by developers. Systems appropriately limit functions, ports, protocols, and services. Developers perform ongoing testing during initial development and during any changes or modifications, including static code analysis to check for and remediate any vulnerabilities or weaknesses in code. Require developers to deliver systems with defined security configurations implemented and use as default for reinstallation or upgrade. Require developers at all post-design stages to develop and implement assessment plans, perform testing/evaluation at defined frequencies and depth, produce evidence of execution and results, implement verifiable flaw remediation process, and correct flaws identified during testing. Employ static code analysis tools to identify common flaws and document results.

SECURITY CONTROL ID(S): SA-03, SA-08

IMPLEMENTATION STEPS:

Build security and privacy into your development lifecycle from the start. Define security and privacy roles throughout development (architects, testers, etc.) and assign people to fill them. Apply security engineering principles like least privilege, defense in depth, and secure defaults during design and development. Integrate risk management into all lifecycle phases.

SECURITY CONTROL ID(S): SA-04 (09), SA-09 (02)

IMPLEMENTATION STEPS:

During system design, require developers to list the specific functions, ports, protocols, and services the system will use and document these in system design docs or system requirements.

SECURITY CONTROL ID(S): SA-01

IMPLEMENTATION STEPS:

Create a formal system and services acquisition policy covering purpose, scope, roles, responsibilities, and how you'll handle third-party acquisitions securely. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after supply chain incidents. FedRAMP Low and FedRAMP Moderate require overall policies to be reviewed and updated at least every 3 years, however the procedures within those policies shoud be reviewed and updated t least annually.

SECURITY CONTROL ID(S): SA-04, SA-09 (01)

IMPLEMENTATION STEPS:

Include security and privacy requirements in vendor contracts covering functional requirements, required controls, documentation, acceptance criteria, and responsibility allocation. Before acquiring or outsourcing security services, conduct a risk assessment and get approval from designated leadership. Require vendors to comply with your security requirements and monitor their compliance.

SECURITY CONTROL ID(S): RA-05 (05)

IMPLEMENTATION STEPS:

Use RBAC to restrict scanning to specific privileged roles or service accounts. Document which roles/accounts can initiate scans. Ensure non-privileged users can't run scans. Log all scan activities including who initiated them and regularly review scanning privileges.

SECURITY CONTROL ID(S): SA-05

IMPLEMENTATION STEPS:

Security documentation (system architecture, security roles/responsibilities, incident response playbooks, vulnerability management processes, etc. are distributed to personnel with system access. The documents are securely stored with role-based access control applied so only system owners, admins, and privileged users can view/edit documentation. Owners are assigned for each asset, in alignment with their system roles.

SECURITY CONTROL ID(S): SA-09

IMPLEMENTATION STEPS:

Build your proposed FedRAMP system on a FedRAMP-authorized cloud services platform. Verify each provider's FedRMAP authorization package. If you use any 3rd party services that will also handle federal data, confirm that they are also FedRAMP authorized in alignment with your system categorization. Document your security posture in a System Security Plan (SSP) and continuously monitor your compliance.

SECURITY CONTROL ID(S): SA-09 (05)

IMPLEMENTATION STEPS:

Restrict the location of information processing, information/data, and system services to defined locations based on requirements or conditions. This is typically met by leveraging U.S.-only geographic regions for your cloud services environment. Document the restriction and verify that all system components, data storage, and processing occur only within approved U.S. locations. Ensure vendor contracts specify geographic restrictions.

SECURITY CONTROL ID(S): SA-11 (02), SA-15

IMPLEMENTATION STEPS:

Develop and implement secure development practices based on industry standards such as NIST Secure Software Development Framework (SSDF), OWASP Software Assurance Maturity Model (SAMM), or OWASP Secure Coding Practices & ASVS. Require developers to perform threat modeling and vulnerability analysis early in the system development lifecycle to ensure design and implementation changes don't include security and privacy gaps. Document the specific tools and configurations that are standard for use in the development process. Review the policy or procedure at least annually to ensure it still meets security and privacy requirements.

SECURITY CONTROL ID(S): SA-16

IMPLEMENTATION STEPS:

Develop role-based guides or training that explain how to securely configure and use your platform's security and privacy features (such as authentication, encryption, logging, etc). Tailor content for both internal and external users. Offer training in easy-to-consume formats: online modules, micro-trainings, recorded walkthroughs, or short workshops. Include this as part of onboarding for developers and refresher training when new features or controls are introduced. Update training content whenever system security or privacy features change, or when new risks are identified. Incorporate lessons from incidents, audits, or vulnerability findings. For internal users, record who completed the training and retain records according to your compliance requirements.

SECURITY CONTROL ID(S): SA-17

IMPLEMENTATION STEPS:

When using external developers, require them to provide design specs and security/privacy architectures that align with your organizational standards. Documentation should clearly describe security functionality, control allocation, and how everything works together. Review and approve their documentation before proceeding with development.

SECURITY CONTROL ID(S): SA-22

IMPLEMENTATION STEPS:

Replace system components when support is no longer available from the developer, vendor, or manufacturer. Alternatively, provide options for continued support such as in-house support or support from external providers. Document end-of-life timelines for all system components. Plan for replacements before vendor support expires. For components that must remain in use after vendor support ends, implement compensating controls and document alternative support arrangements including who will provide support and how security patches will be addressed.

SECURITY CONTROL ID(S): SC-01

IMPLEMENTATION STEPS:

Create a formal system and communications protection policy covering purpose, scope, roles, responsibilities, and network security requirements. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after network security incidents.

SECURITY CONTROL ID(S): SA-21

IMPLEMENTATION STEPS:

Establish a personnel security process that also covers 3rd party/subcontractor developers. Internal developers are screened through your personnel security processes. If you use external developers (3rd parties or subcontractors) they are also screened before being granted access, and their access is limited using role-based access controls. Require developers to have appropriate access authorizations determined by assigned official government duties and satisfy additional personnel screening criteria.

SECURITY CONTROL ID(S): SC-05

IMPLEMENTATION STEPS:

Implement features such as web application firewalls (WAFs), cloud load balancers, and similar services that implement network security controls and absorb network traffic in the event of an attack. Protect against or limit the effects of defined types of denial-of-service events. Employ defined controls to achieve the denial-of-service objective.

SECURITY CONTROL ID(S): SC-04, SI-04 (04), SI-04 (11), SI-04 (18)

IMPLEMENTATION STEPS:

Deploy network monitoring tools (IDS/IPS, SIEM) at external boundaries and strategic internal locations. Monitor both inbound and outbound traffic continuously. Establish baselines for normal traffic and alert on anomalies like unusual volumes or suspicious destinations. Use DLP tools to identify sensitive data in transit.

SECURITY CONTROL ID(S): RA-05 (08)

IMPLEMENTATION STEPS:

Make sure all system, application, and security logs flow into a central service such as a SIEM. Set a time period for reviewing historic logs (e.g., 30 days, 90 days, 1 year), based on your regulatory or business requirements, and ensure logs are retained for at least this period. Establish a process that when a new vulnerability is identified, your logs are queried for indicators of exploitation. Set up alerting rules that automatically check logs for common exploit patterns when a new CVE or vulnerability alert is received. Record whether the vulnerability was exploited, what evidence was found, and what response steps were taken.

SECURITY CONTROL ID(S): SC-07, SC-07 (18)

IMPLEMENTATION STEPS:

Implement managed interfaces such as web or application gateways, routers, firewalls, security scanners, virtualization systems, or encrypted tunnels. Establish subnetworks (demilitarized zones or DMZs) that are physically or logically separated from internal networks. Monitor and control communications at external and key internal managed interfaces. If these boundary protections failed, they fail-closed, preventing external data or connections from entering your internal networks. Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

SECURITY CONTROL ID(S): SC-07 (08)

IMPLEMENTATION STEPS:

Route internal communications traffic destined for external networks through authenticated proxy servers at managed interfaces. Configure proxy servers to require authentication before allowing traffic to pass through. Use the proxy to monitor and log all outbound communications for security analysis. This provides centralized control and visibility into what internal systems are communicating with external networks. Maintain access controls on proxy servers to ensure only authorized traffic passes through.

SECURITY CONTROL ID(S): SC-07 (04), SC-07 (05)

IMPLEMENTATION STEPS:

Use software-defined networking (SDN) within cloud-based virtual private clouds (VPCs) to centrally manage and enforce network traffic flow policies, and to maintain a centralized inventory of network traffic flow rules and exceptions across environments (e.g., firewall rules, ACLs, and security group allow rules). Configure these controls using a default-deny-all posture, and create explicit allow rules only for network traffic required for business operations. For any unique or temporary exceptions, document the business justification, responsible owner, review schedule, and expiration date. Review each exception at least every 180 days (FedRAMP Moderate) or 90 days (FedRAMP High), and also whenever significant environment changes warrant a review, then remove exceptions that are no longer necessary. Use ticketing or workflow tools to track approvals and periodic reviews, and regularly audit firewall/ACL/security group rule sets to identify and remove unnecessary allow rules and outdated exceptions.

SECURITY CONTROL ID(S): SC-07 (10)

IMPLEMENTATION STEPS:

Tools such as Amazon GuardDuty, AWS WAF, Azure DDoS, Microsoft Defender for Cloud, Google Cloud Armor, Google Cloud DLP, cloud-based network firewalls, CrowdStrike Falcon, or Palo Alto Prisma Cloud are common solutions. Implement protections at internal endpoints, external boundaries, and managed interfaces to prevent data exfiltration. These protections might include things like firewalls, load balancers, or data loss prevention tools. Conduct exfiltration tests at defined frequencies to verify effectiveness. Prevent exfiltration of information.

SECURITY CONTROL ID(S): SC-07 (20), SC-07 (21)

IMPLEMENTATION STEPS:

Provide the capability to dynamically isolate system components from other components when needed. Employ boundary protection mechanisms to isolate system components supporting specific missions or business functions. This allows you to contain security incidents, perform maintenance, or protect critical functions without affecting the entire system. Implement network segmentation, VLANs, security zones, or micro-segmentation that can be adjusted dynamically. Document which components support critical missions and ensure they can be isolated quickly when necessary.

SECURITY CONTROL ID(S): SC-12

IMPLEMENTATION STEPS:

Develop a key management policy that documents how your organization will generate, distribute, store, use, and retire cryptographic keys. Require the use of approved tools to generate and manage keys using trusted, approved cryptographic libraries or hardware like cloud KMS and HSMs. Make sure only authorized personnel or systems can access the keys.

SECURITY CONTROL ID(S): SC-07 (12), SI-04, SI-04 (23)

IMPLEMENTATION STEPS:

Implement host-based boundary protection mechanisms at defined system components (servers, workstations, endpoints). Implement host-based monitoring mechanisms at defined system components. Use endpoint detection and response (EDR) tools, host-based intrusion detection systems (HIDS), or host-based firewalls to detect attacks, unauthorized access, or suspicious activity. Configure these tools to report findings to appropriate security personnel automatically.

SECURITY CONTROL ID(S): SC-23, IA-03

IMPLEMENTATION STEPS:

Implement mobile device management to allow only approved or managed devices to connect to your corporate network. Enforce device compliance checks to maintain device security posture. Protect the authenticity of communication sessions using modern authentication protocols such as TLS 1.2+, 802.1X, and HTTPS. Use secure tokens with short lifetimes and automatic refresh, like OAuth 2.0 and OIDC, to prevent session hijacking and MITM attacks.

SECURITY CONTROL ID(S): SC-18

IMPLEMENTATION STEPS:

Establish a Mobile Code Policy that states which types of downloadable or executable code are approved, restricted, or prohibited in your environment (ex. allowing trusted JavaScript and HTML5, but prohibiting unsigned Java applets, VBScript, or code from untrusted and unknown sources). Configure browsers, servers, and email systems to block or restrict unapproved code types. Use secure code review and CI/CD controls to ensure only vetted and signed code is deployed. Only allow mobile code that's digitally signed by your organization or a trusted vendor certificate authority. Use security monitoring tools or SIEM systems to detect suspicious or unauthorized code execution. Generate alerts when unknown or unapproved code types are run within the environment.

SECURITY CONTROL ID(S): SC-20, SC-21, SC-22

IMPLEMENTATION STEPS:

Implement DNS servers that provide additional data origin authentication and integrity verification along with authoritative name resolution data. Enable DNSSEC to provide cryptographic signatures that verify DNS responses haven't been tampered with. Services that support DNSSEC include: Google Cloud DNS, AWS Route 53, Azure DNS, and Cloudflare DNS. Note that DNSSEC is not supported in private hosted DNS zones. Request and perform data origin authentication and integrity verification on name/address resolution responses from authoritative sources. Ensure your DNS infrastructure is fault-tolerant by implementing internal and external role separation across multiple servers.

SECURITY CONTROL ID(S): SC-24

IMPLEMENTATION STEPS:

Ensure your system fails closed: If IdP is unavailable, deny logins and log attempted login activities. If data integrity checks fail, reject the data object and revert to a prior known-good version. If a failure occurs in your system, the system defaults to deny, refuse, or block access to maintain system security. The state of the system is preserved so that you can still recover and operate after the failure, and failure details are logged. Fail to a defined known system state for defined failures while preserving defined system state information in failure.

SECURITY CONTROL ID(S): SI-01

IMPLEMENTATION STEPS:

Create a formal system and information integrity policy covering purpose, scope, roles, responsibilities, and integrity protection requirements. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after integrity-related incidents.

SECURITY CONTROL ID(S): SC-12 (01)

IMPLEMENTATION STEPS:

Require the use of a key management system (KMS) such as AWS KMS, Azure Key vault, or Google KMS, to manage keys, backup and recovery. Enable key escrow to keep an encrypted backup copy of keys in a secure location so they can be restored if needed. Link keys to organizational accounts, so admins can recover them if a user leaves or forgets a passphrase. Have documented steps for how to retrieve a lost key, who is allowed to do it, and how you'll log and approve recovery.

SECURITY CONTROL ID(S): SC-39, SI-16

IMPLEMENTATION STEPS:

Utilize major cloud service providers like AWS, Azure, and GCP to inherit process isolation and separate execution domains by default. As a best practice, use hardened OS images. Configure IAM roles and permissions so workloads and processes only get the access they need. Ensure that your OSes and runtimes are patched regularly. Implement separate execution environments for development, testing, and production workloads to enforce logical isolation.

SECURITY CONTROL ID(S): SI-02 (02), RA-05 (03)

IMPLEMENTATION STEPS:

Deploy automated vulnerability scanning tools (Nessus, Qualys, Rapid7, AWS Inspector, Defender for Cloud) and scan all components at least monthly. Cover all networks, systems, applications, databases, and containers. Schedule regular monthly scans plus ad-hoc scans when new vulnerabilities are announced. Generate reports that prioritize remediation based on risk.

SECURITY CONTROL ID(S): SI-02, SI-02 (03)

IMPLEMENTATION STEPS:

Implement a patch management solution that does automatic security scans and automatic updates if possible. When security-relevant patches, service packs, or signature updates are released, incorporate them into the configuration management process within 30 days. Test updates in a staging environment before pushing to production. Identify, test, integrate, and track updates to resolution. Measure the time between flaw identification and remediation and establish benchmarks for taking corrective actions. Prioritize remediation based on risk tolerance, regulatory thresholds, and criticality of the flaw, but address all security updates promptly.

SECURITY CONTROL ID(S): SI-03

IMPLEMENTATION STEPS:

Install auto-updating antivirus/anti-malware (e.g., Microsoft Defender for Endpoint, CrowdStrike, SentinelOne) on all laptops, servers, and mobile devices used to access or manage the system. Ensure agents are configured for real-time scanning and weekly full scans. Enable anti-malware scanning at email servers, web gateways, and firewalls. Configure these to scan downloads, attachments, and web traffic in real time. Integrate antivirus/anti-malware alerts with a central logging or SIEM system (e.g., Splunk, Azure Sentinel, AWS Security Hub). Ensure security staff get near real-time notifications of blocked or quarantined threats.

SECURITY CONTROL ID(S): SC-15

IMPLEMENTATION STEPS:

Configure collaborative devices to block/prevent remote access. Establish a policy that requires all physical corporate collaborative devices to be used in-person, within the organization's network and physical boundaries.

SECURITY CONTROL ID(S): SI-04 (01), SI-04 (02), SI-04 (16)

IMPLEMENTATION STEPS:

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system. Employ automated tools to support near real-time analysis of events. Correlate information from monitoring tools employed throughout the system. This is commonly addressed by using tools like AWS Security Hub, Microsoft Defender for Cloud, or Google Security Command Center and integrating those systems with SIEMs like Splunk, Chronicle, or Microsoft Sentinel.

SECURITY CONTROL ID(S): SI-04 (10), AC-04 (04)

IMPLEMENTATION STEPS:

Deploy SSL/TLS inspection at network boundaries to decrypt, inspect, and re-encrypt traffic. Block unknown encrypted protocols or require traffic through inspection points. Define which encrypted traffic must be inspected versus exempted for compliance reasons. For traffic that can't be inspected, use alternative controls like endpoint detection or connection metadata logging.

SECURITY CONTROL ID(S): SI-04 (14)

IMPLEMENTATION STEPS:

Implement a wireless intrusion detection system or scanning tool to detect all access points and investigate any unknown results. Examples of WIDS include: Cisco Meraki Air Marshal, Aruba (HPE) RFProtect, Fortinet FortiWLC/FortiAP, Microsoft Defender for Endpoint (with Wi-Fi threat detection), Snort + wireless plugins, or Kismet. Your organization has authorized access points configured for network access, and regularly scans for unauthorized wireless access points to make sure your organization's systems and devices aren't connected to them. Employ a wireless intrusion detection system to identify rogue wireless devices and detect attack attempts and potential compromises or breaches.

SECURITY CONTROL ID(S): SI-04 (19)

IMPLEMENTATION STEPS:

Implement additional monitoring of individuals who have been identified by defined sources as posing an increased level of risk. This could include individuals flagged by HR, security investigations, behavioral indicators, or threat intelligence. Corporate systems commonly notify users that activity may be monitored - this is an indicator that such capabilities are likely in place. Document the criteria for increased monitoring, approval processes, and privacy considerations.

SECURITY CONTROL ID(S): SI-04 (05), SI-04 (12), SI-05 (01), SI-07 (02)

IMPLEMENTATION STEPS:

Deploy security monitoring tools (SIEM, IDS/IPS, EDR) that automatically detect and alert on security events and anomalies. Define indicators of compromise that trigger alerts like failed logins, malware detection, or unauthorized access. Configure automated alerting via email, SMS, ticketing, or SOC dashboard. Test alerting regularly and tune thresholds to minimize false positives.

SECURITY CONTROL ID(S): SI-06

IMPLEMENTATION STEPS:

Integrate system health and performance monitoring that produces failure or error alerts. Your system produces notifications and alerts when operations fail during various system states such as startup, restart, shut down, and abort. Notification should include electronic alerts to system admin, light indicators, or console messages. Verify correct operation of defined security and privacy functions at defined system transitional states, upon command by user with appropriate privilege, or at defined frequencies. Alert defined personnel to failed security and privacy verification tests. Take defined alternative actions when anomalies are discovered (shut down system, restart system, etc.).

SECURITY CONTROL ID(S): SI-07

IMPLEMENTATION STEPS:

Implement configuration managers, system, data, and event audit logging to detect system configuration changes, file, and system changes. Verify the integrity of deployed software and images using cryptographic hashes or checksums. Configure security alerts to your monitoring or SIEM platform when unauthorized changes are detected. Establish automatic responses such as reverting to a known-good state or restarting the affected system or service. Con

SECURITY CONTROL ID(S): SI-08, SI-08 (02)

IMPLEMENTATION STEPS:

Implement email servers (like Microsoft 365 and Google Workspace), WAFs, secure proxies, gateways, endpoint security software, and firewalls that filter ingress and egress traffic for spam, with auto-updates configured to keep the system up to date with signatures and patches. Firewalls, email systems, corporate devices, and other system entry and exit interfaces have spam filtering implemented with automatic updates enabled to prevent systems filters from being outdated. Employ spam protection mechanisms at system entry and exit points. Automatically update spam protection mechanisms at defined frequencies.

SECURITY CONTROL ID(S): SI-05

IMPLEMENTATION STEPS:

Subscribe to security alerts from US-CERT, CISA, and other relevant organizations. Use automated mechanisms to receive and disseminate alerts to security teams and technical staff. Establish documented procedures and timelines for implementing directives. Track implementation and report compliance status when required.

SECURITY CONTROL ID(S): SI-11

IMPLEMENTATION STEPS:

Implement a standard for error-handling that enforces safe user-facing responses, secure logging with redaction of sensitive data when it is not needed, and routing detailed errors to logs not to UI. Apply least privilege IAM roles so only approved staff can view or query detailed logs. Control error message content by showing generic user-facing messages, e.g., “Something went wrong. Please try again.” Make sure that details like stack traces, usernames/passwords, internal paths, or sensitive IDs, are not exposed to end-users.

SECURITY CONTROL ID(S): SI-10

IMPLEMENTATION STEPS:

Ensure input validation is performed on your applications using tools like web security scanners that test input fields for security vulnerabilities to XSS and injection attacks. Incorporate WAFs, reCAPTCHA, and other input validation features. Perform input validation on your system to verify that inputs match your secure input definitions for format and content. This prevents input injection and cross-site scripting attacks. Check validity of defined information inputs to the system.

SECURITY CONTROL ID(S): SI-07 (01)

IMPLEMENTATION STEPS:

This can be done by implementing things like hash checks, package scanning to check cryptographic signatures, and running comparisons of new versions of software against an approved software bill of materials (SBOM). Having a configuration manager installed supports implementation of this control family. Your system performs integrity checks during various system states such as startup, restart, shut down, and abort. Integrity checks are also performed during security-relevant events, for example when new software, firmware, or hardware is installed or when a new exploit or vulnerability is identified. Perform an integrity check of defined software, firmware, and information at startup, at defined transitional states or security-relevant events, or at defined frequencies.

SECURITY CONTROL ID(S): SR-02, SR-02 (01), SR-03

IMPLEMENTATION STEPS:

Develop a supply chain risk management (SCRM) plan that aligns to NIST 800-161 rev1 cybersecurity requirements. Include details on how you select, approve, and monitor 3rd party vendors. Designate specific roles and responsibilities for managing supply chain risks. Subscribe to vendor/CSP security advisories and industry alerts to help you track vulnerabilities in key dependencies. If a vendor or supply chain issue impacts your service, notify your customers clearly and quickly; leverage your incident response plan to facilitate external communications.

SECURITY CONTROL ID(S): SI-07 (07)

IMPLEMENTATION STEPS:

Add procedures to your incident response plan for handling unauthorized changes to security configurations, controls, or critical files. Define what counts as unauthorized changes. Set up detection tools and alerts. Include steps for investigating, containing, and recovering from unauthorized changes when detected.

SECURITY CONTROL ID(S): SR-09, SR-09 (01)

IMPLEMENTATION STEPS:

Implement anti-tampering tools and techniques such as code signing, checksums and hashes, or immutable images. Perform integrity checks to detect system changes that are not authorized or that drift from the standard. Enforce strong IAM and use logging and monitoring to detect tampering. Use features like AWS Config, Azure Policy, or GCP Config Controller to prevent or detect configuration drift. Implement a tamper protection program. Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

SECURITY CONTROL ID(S): SR-11, SR-11 (01)

IMPLEMENTATION STEPS:

Establish an anti-counterfeit policy, procedures, or training that all product and security personnel are required to review or complete. Include requirements to only procure hardware, software, and firmware from authorized, trusted vendors. Prohibit the use of unverified or pirated software; require verification of authenticity before any system components are installed. Educate personnel on how to recognize signs of counterfeit components (e.g., tampered packaging, unsigned software, unofficial downloads). Include guidance on how to report suspected counterfeit hardware, software or firmware.

SECURITY CONTROL ID(S): SR-10, SR-11 (02)

IMPLEMENTATION STEPS:

Inspect systems or components at defined frequency or when there are indications of tampering to detect physical tampering. Develop and implement anti-counterfeit policies and procedures that include means to detect and prevent counterfeit components from entering the system. Report counterfeit components to the source of the counterfeit and appropriate external organizations. Maintain configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service. Implementing binary authorization (verifying digital signatures) is one way to address counterfeit component detection. Train personnel to detect counterfeit components.

SECURITY CONTROL ID(S): SR-01

IMPLEMENTATION STEPS:

Create a formal supply chain risk management policy covering purpose, scope, roles, responsibilities, and how you'll manage supply chain security. Assign someone to own and maintain this policy. Review and update the policy and procedures at least annually or after supply chain incidents.

SECURITY CONTROL ID(S): SI-12

IMPLEMENTATION STEPS:

Establish a data management policy or procedures. Define the types of data you manage (e.g. customer data, system logs, audit records, etc). Document how long each data type must be kept to satisfy legal, regulatory, or contractual requirements. Ensure that any system-generated reports or logs are also stored, archived, and deleted per policy. Keep a record of data retention policies and who is responsible for enforcing them. Review data retention measures at least annually or when laws/policies change.

SECURITY CONTROL ID(S): SI-04 (22)

IMPLEMENTATION STEPS:

Establish and enforce requirements for approved network services. Maintain a list of all devices, ports, services, etc that are appropriately authorized, and consider anything not on the list unauthorized. Run regular network scans (e.g., Nmap, Nessus, OpenVAS) to identify open ports and running services. Enable intrusion detection/prevention systems (IDS/IPS) or firewall logs to find unexpected services. Log any detections and configure firewalls, IDS/IPS, and/or SIEMs to send alerts to IT/security staff when unauthorized network services are detected.

SECURITY CONTROL ID(S): SR-12

IMPLEMENTATION STEPS:

Develop a data deletion policy or procedures. Outline approved ways to dispose of data and components. Require disposal any time sensitive data or components are no longer needed, and when components are formally retired. Make sure anyone handling data or components knows the approved methods.

III. Inherited Controls

The following security controls are generally inherited from the Infrastructure as a Service (IaaS) cloud service provider, and therefore are met by default.

Control ID(s)	FedRAMP High	FedRAMP Moderate	FedRAMP Low
PE-13	✅	✅	✅
PE-13 (01)	✅	✅	
PE-13 (02)	✅	✅	

Control ID(s)	FedRAMP High	FedRAMP Moderate	FedRAMP Low
PE-14 (02)	✅		
PE-15 (01)	✅		
PE-16	✅	✅	✅
PE-03 (01)	✅		
PE-06	✅	✅	
PE-06 (01)	✅	✅	
PE-06 (04)	✅		
PE-10	✅	✅	
PE-12	✅	✅	✅
PE-14	✅	✅	✅
PE-15 (01)	✅	✅	✅
MA-03 (02)	✅	✅	
MA-02	✅	✅	✅
MA-02 (02)	✅		
MA-04 (03)	✅		
MA-03	✅	✅	
MA-03 (01)	✅	✅	
MA-04	✅	✅	✅
MA-05	✅	✅	✅

Control ID(s)	FedRAMP High	FedRAMP Moderate	FedRAMP Low
MA-05 (01)	✅	✅	
MA-03 (03)	✅	✅	✅
PE-18	✅		
PE-09	✅	✅	✅
PE-11	✅	✅	✅
PE-11 (01)	✅		

IV. Next Steps

The Recommendations section of this report is based on the specific FedRAMP security controls your organization does not currently meet, based on your self-attested responses. A detailed view of met and not met security controls across all three FedRAMP baselines can be downloaded from your organization's NYLE portal. To advance toward FedRAMP authorization, reference the FedRAMP security baseline you are targeting Low, Moderate, or High and implement all corresponding recommendations outlined in the Recommendations section.

Use this report to:

- Benchmark and track your organization's ongoing FedRAMP readiness progress.
- Communicate your current compliance status internally or with potential agency partners to obtain sponsorship for an Authority to Operate (ATO).
- Leverage NYLE as a living roadmap to achieve FedRAMP Ready or FedRAMP In Process status.

Continue updating your self-attested responses in NYLE as your security posture matures. Each update will refresh your results and provide an up-to-date view of your organization's FedRAMP readiness.

END OF REPORT