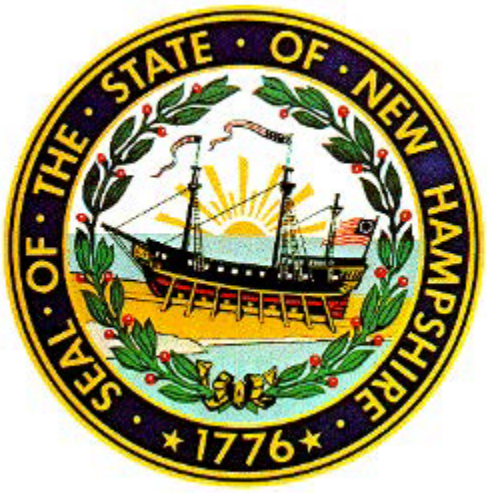
State of New Hampshire
Cyber Security Group




# Vendor Risk Assessment Report (VRAR)

Version 1.1

## Executive Summary

The State of NH requires that all systems connected to the State Network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

The State of NH has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 as the baseline for security requirements with NIST 800-53 as the source for identifying and implementing specific information technology security controls. This security baseline provides the State of New Hampshire basic requirements to protect citizen data and services. These basic requirements and controls are referenced or described in the State of NH Statewide Information Security Manual (SISM).

The following is a high-level view of specific security requirements that are needed to meet compliance. The control references (e.g., AC-2) refer to the specific NIST 800-53 control as listed in the SISM, which may be found at the following Link: New Hampshire Statewide Information Security Manual (nh.gov)

**Note**: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates, or agency specific requirements. If a Privacy Impact Assessment is required, it should be submitted as a separate document.

# Contents

# List of Tables

## VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate or Low security impact level, in accordance with the FIPS Publication 199 Security Categorization.

***Table 2-1. System Information***

| |
|---|
| VENDOR Name:<br>Solution/System Name:<br>Service Model: (e.g., IaaS, PaaS, SaaS)<br>FIPS PUB 199 System Security Level: (e.g., Moderate, Low)<br>Fully Operational as of: Enter the date the system became fully operational.<br>Number of Customers (State/Others): Enter # of customers / # of other customers<br>Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe.<br>System Functionality: Briefly describe the functionality of the system and service being provided. |

### Relationship to Other Vendors or CSPs

*If this system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 2-2 and 2-3 below.* ***Please note****, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.*

**IMPORTANT:** If there is a leveraged system, be sure to note below every capability that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

***Table 2-2. Leveraged Systems***

| # | Question | Yes | No | N/A | If Yes, please describe. |
|---|---|---|---|---|---|
| 1 | Is this system leveraging an underlying provider? | | | | *If "yes," identify the underlying system.* |

*List all* ***services*** *leveraged. The system from which the service is leveraged must be listed in Table 2-2 above.*

***Table 2-3. Leveraged Services***

| # | Service | Service Capability | System |
|---|---|---|---|
| 1 | *State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.* | *List the capability the service provides (e.g., load balancer, SIEM, database, audit logging).* | *Identify the system from which the service is being leveraged.* |

## Data Flow Diagrams

*Insert Vendor-validated data flow diagram(s) and provide a written description of the data flows. The diagram(s) must:*

- *clearly identify anywhere State data is to be processed, stored, or transmitted;*
- *clearly delineate how data comes into and out of the system boundary;*
- *clearly identify data flows for privileged, non-privileged and customer access; and*
- *depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.*

## Separation Measures [AC-4, SC-2, SC-7]

*Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.*

*The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.*

## System Interconnections

*A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.*

*The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 2-5 below.*

***Table 2-4. System Interconnections***

| # | Question | Yes | No | If Yes, please describe. |
|---|---|---|---|---|
| 1 | Does the system connect to the Internet? | | | |
| 2 | Does the system connect to a corporate or state infrastructure/network? | | | |
| 3 | Does the system connect to external systems? | | | *If "yes," complete Table 2-5 below.* |

*If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type "None" in the first row.*

***Table 2-5. Interconnection Security Agreements (ISAs)***

| # | External System Connection | Does an ISA Exist? | | Interconnection Description. If no ISA, please justify below. |
|---|---|---|---|---|
| | | Yes | No | |
| 1 | | | | |
| 2 | | | | |

# Capability Risk

## State Mandates

This section identifies State requirements applicable to all State approved systems. Requirements labeled **B+** (Baseline Plus) indicate handling of restricted, confidential, or federally regulated information which corresponds to Section Two of the SISM. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 3.2, *State Requirements,* below.

*Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.*

***Table 3-1. State Mandates***

| # | Compliance Topic | Fully Compliant? | |
|---|---|---|---|
| | | Yes | No |
| 1 | Data at Rest, Authentication: Are only FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules used where cryptography is required? | | |
| 2 | Transmission, Remote Access: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? | | |
| 3 | Can the VENDOR'S solution integrate with the State's IAM solution(s)? | | |
| 4 | Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application…e.g., firewalls intrusion detection/ prevention systems, end point protection etc.? [SC-7] [SI-3/SI-4] | | |
| 5 | Can the VENDOR consistently remediate High risk vulnerabilities within 30 days and Medium risk vulnerabilities within 60 days? [SI-2] | | |
| 6 | Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? | | |
| 7 | Does the VENDOR store, process or transmit **State data** only in the continental US and is that data backed up in only US locations? | | |
| 8 | Does the VENDOR have a process to securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 **and** will provide to the State a certificate of data destruction? [MP-6] | | |
| 9 | All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement? | | |

| | | | |
|---|---|---|---|
| **10**<br>**B+** | Does the vendor have a current 3rd party attestation certification **and** is it regularly renewed? The State desires an independent 3rd party attestation (e.g., FedRAMP, StateRAMP, SOC 2 Type 2, ISO 27001, or HITRUST) ***prior to*** contract award for systems containing **Restricted/Highly Restricted** data. ***Note:*** *SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments.* [CA-7, RA-3, SA-9] | | |
| **11**<br>**B+** | Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to **Federal and/or State Restricted/Highly Restricted** regulations and procedures for those systems that require it? [AC-2, PS-3] | | |

## State Requirements

This section identifies additional State requirements. All requirements in this section must be met; however, compensatory controls and non-applicability justifications will be considered as part of the Risk Assessment.

### Data at Rest and Authentication [SC-13]

*The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 Compliant is not sufficient. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.*

***Table 3-2a. Data at Rest & Authentication***

| | **Cryptographic Module Type** | **FIPS 140-2 Validated?** | | **NSA Approved?** | | **Describe Any Alternative Implementations (if applicable)** | **Describe Missing Elements or N/A Justification** |
|---|---|---|---|---|---|---|---|
| | | **Yes** | **No** | **Yes** | **No** | | |
| 1 | Data at Rest [SC-28] | | | | | | |
| 2 | Authentication [IA-5, IA-7] | | | | | | |

## Transport Layer Security [NIST SP 800-52, Revision 2]

*The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules relating to block ciphers, digital signatures and hash functions. Full FIPS mode is not required unless other regulatory requirements must be met. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.*

***Table 3-2b. Transport Encryption***

| | Cryptographic Module Type | FIPS 140-2 Validated? | | NSA Approved? | | Describe Any Alternative Implementations (if applicable) | Describe Missing Elements or N/A Justification |
|---|---|---|---|---|---|---|---|
| | | Yes | No | Yes | No | | |
| 1 | Transmission [SC-8 (1), SC-12, SC-12 (2, 3)] | | | | | | |
| 2 | Remote Access [AC-17 (2)] | | | | | | |

*The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate but must not remove the original rows.*

***Table 3-3. Transport Protocol***

| # | The Cryptographic Module Type | Protocol In Use? | | If "yes," please describe use for both internal and external communications |
|---|---|---|---|---|
| | | Yes | No | |
| 1 | SSL (Non-Compliant) | | | |
| 2 | TLS 1.0 (Non-Compliant) | | | |
| 3 | TLS 1.1 (Non-Compliant) | | | |
| 4 | TLS 1.2 (Compliant) | | | |
| 5 | TLS 1.3 (Compliant) | | | |

## Identification and Authentication, Authorization, and Access Control

*Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.*

***Table 3-4. Identification and Authentication, Authorization, and Access Control***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation? [IA-2, IA-4] | | | |
| 2 | Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2 (1), IA-2 (2)] | | | |
| 3 | Is role-based access used, managed, and monitored? [IA-4, IA-5] | | | |
| 4 | Does the system restrict non-authorized personnel's access to resources? [AC-6, AC-6 (1), AC-6 (2)] | | | |
| 5 | Does the system restrict non-privileged users from performing privileged function? [AC-6, AC-6 (1), AC-6 (2), AC-6 (10)] | | | |
| 6 | Does the system ensure secure separation of customer data? [SC-4] | | | |

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 7 | Does the system ensure secure separation of customer processing environments? [SC-2] | | | *The capability description is not required here, but must be included in Section 2.3, Separation Measures.* |
| 8 | Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2] | | | *The capability description is not required here, but must be included in Section 2.3, Separation Measures.* |
| 9 | Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17] | | | |
| 10 | How will the State's password policy be enforced? State requires minimum 14-character complex passwords (Upper, Lower, Special Character & Numerical) [IA-5] | | | |

## Audit, Alerting, Malware, and Incident Response

*Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.*

***Table 3-5. Audit, Alerting, Malware, and Incident Response***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3] | | | |
| 2 | Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-4, AU-9] | | | |
| 3 | Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-4 (5), SI-7, SI-7 (7)] | | | |
| 4 | Does the VENDOR log and monitor access to the system? [SI-4] | | | |

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 5 | Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8] | | | |
| 6 | Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11] | | | *If the system contains no custom software development, do not answer Y or N. Instead, state "NO CUSTOM CODE" here.* |
| 7 | Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4, IR-4 (1), IR-6] | | | |
| 8 | Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least six (6) years to meet regulatory and organizational information retention requirements? [AU-11] *Note: This question has been modified for compliance with NH DHHS regulatory security incident reporting requirements.* | | | |
| 9 | Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NH DHHS' requirement for security incident/breach reporting is immediately upon suspect or incident confirmation. [IR-6] *Note: This question has been modified for compliance with NH DHHS regulatory security incident reporting requirements.* | | | |
| 10 | If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection? | | | *If the system does not support this feature, do not answer Y or N. Instead, state "Not Applicable" here.* |

## Contingency Planning and Disaster Recovery

*Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.*

***Table 3-6. Contingency Planning and Disaster Recovery***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-9, CP-10] | | | |
| 2 | Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with Statewide Information Security Manual? [CP-2, CP-4] | | | |
| 3 | Does the system have alternate storage and processing facilities? [CP-6, CP-7] | | | |
| 4 | Does the system have or use alternate telecommunications providers? [CP-8] | | | |
| 5 | Does the system have backup power generation or other redundancy? [PE-11] | | | |
| 6 | Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8] | | | |

## Configuration and Risk Management

*Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.*

***Table 3-7. Configuration and Risk Management***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2] | | | |
| 2 | Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8] | | | |

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 3 | Does the VENDOR have a Configuration Management Plan? [CM-9] | | | |
| 4 | Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4, CM-4 (2)] | | | |
| 5 | Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2, CM-2 (2), CM-6, CM-8] | | | |
| 6 | Does the VENDOR prevent unauthorized changes to the system? [CM-5] | | | |
| 7 | Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6, CM-7] | | | *If "yes," describe if the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or "most restrictive consistent with operational requirements."* |
| 8 | Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6] | | | |

*For the following questions, Vendors may use Table 3-18 "Continuous Monitoring Capabilities – Additional Details" to enter the capability descriptions, supporting evidence, and missing elements.*

| | | | | |
|---|---|---|---|---|
| 9 | Does the VENDOR perform **authenticated** operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5 (5)] | | | *Describe how the Vendor validated that vulnerability scans were fully authenticated.* |

| | | | | |
|---|---|---|---|---|
| 10 | Does the VENDOR demonstrate the capability to remediate High risk vulnerabilities within 30 days and Moderate risk vulnerabilities within 60 days? [RA-5, SI-2] | | | *Describe how the Vendor validated that the VENDOR remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 60 days.* |
| 11 | When a high-risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5] | | | |
| 12 | Does the VENDOR have a Supply Chain Risk Management (SCRM) plan and processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems? | | | *Describe the Vendor's SCRM plan and processes.* |

## Data Center Security

*Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.*

***Table 3-8. Data Center Security***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8] | | | |
| 2 | Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8] | | | |
| 3 | Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6, PE-6 (1)] | | | |

## Policies, Procedures, and Training

*The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 5 families listed in Table 3-9 below.*

***To answer "yes" to a policy**, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each "-1" are fully addressed.*

***To answer "yes" to a procedure**, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.*

*VENDORs must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 3-10 below.*

***Table 3-9. Policies and Procedures***

| # | Family | Policy | | Procedure | | Title Version and Date |
|---|---|---|---|---|---|---|
| | | Yes | No | Yes | No | |
| 1 | Access Control [AC-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 2 | Awareness & Training [AT-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 3 | Audit & Accountability [AU-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 4 | Security Assessment & Authorization [CA-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 5 | Configuration Management [CM-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 6 | Contingency Planning [CP-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 7 | Identification & Authentication [IA-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 8 | Incident Response [IR-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 9 | Maintenance [MA-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |

| # | Family | Policy | | Procedure | | Title Version and Date |
|---|---|---|---|---|---|---|
| | | Yes | No | Yes | No | |
| 10 | Media Protection [MP-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 11 | Physical & Environmental Protection [PE-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 12 | Personnel Security [PS-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 13 | Risk Assessment [RA-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 14 | System & Services Acquisition [SA-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 15 | System & Communications Protection [SC-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 16 | System & Information Integrity [SI-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 17 | Planning [PL-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |
| 18 | Supply Chain Risk Management [SR-1] | | | | | Policy:<br>•<br>Procedure(s):<br>• |

*For any family with a policy or procedure gap, please describe the gap below.*

***Table 3-10. Missing Policy and Procedure Elements***

| Missing Policy and Procedure Elements |
|---|
| • |

*The Vendor must answer the questions below.*

***Table 3-11. Security Awareness Training***

| Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|
| Does the VENDOR train personnel on security awareness and role-based security responsibilities? [AT-2] | | | |

## Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis.

### Staffing Levels

*In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty.* ***Note****: It is not necessary to include specific names of individuals, but rather their roles/titles.*

***Table 3-12. Staffing Levels***

| Staffing Levels |
|---|
| |

### Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State decision, especially for larger systems.

*The Vendor must answer the questions below.*

***Table 3-13. Change Management***

| # | Question | Yes | No | If "no", please describe how this is accomplished. |
|---|---|---|---|---|
| 1 | Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)? | | | |
| 2 | Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment? | | | |

### Vendor Dependencies and Agreements

*The Vendor must answer the questions below.*

***Table 3-14. Vendor Dependencies and Agreements***

| # | Question | Yes | No | *Instructions* |
|---|---|---|---|---|
| 1 | Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support? | | | *If "yes," please complete Table 3-15. Vendor Dependencies below.* |
| 2 | Within the system, are all products still actively supported by their respective vendors? | | | *If any are not supported, answer, "No."* |

| # | Question | Yes | No | *Instructions* |
|---|---|---|---|---|
| 3 | Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering? | | | *If "yes," please complete Table 3-16. Formal Agreements Details below.* |

*If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.*

***Table 3-15. Vendor Dependency Details***

| | | | Still Supported? | |
|---|---|---|---|---|
| **#** | **Product and Vendor Name** | **Nature of Dependency** | **Yes** | **No** |
| 1 | | | | |
| 2 | | | | |

*If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.*

***Table 3-16. Formal Agreements Details***

| # | Organization Name | Nature of Agreement |
|---|---|---|
| 1 | | |
| 2 | | |

## Continuous Monitoring Capabilities

*In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.*

***Table 3-17. Continuous Monitoring Capabilities***

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 1 | Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period? | | | |
| 2 | Does the VENDOR have the ability to scan all hosts in the inventory? | | | |
| 3 | Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML files? | | | |

| # | Question | Yes | No | Describe capability, supporting evidence, and any missing elements |
|---|---|---|---|---|
| 4 | Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items? | | | |

*In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."*

***Table 3-18. Continuous Monitoring Capabilities – Additional Details***

| Continuous Monitoring Capabilities – Additional Details |
|---|
| Can the vendor provide a current 3rd party attestation certification ***annually*** when required? ***Note:*** *SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments*. [CA-7, RA-3, SA-9] |

## Status of System Security Plan (SSP)

*In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.*

***Table 3-19. Maturity of the System Security Plan***

| Maturity of the System Security Plan |
|---|
| |

*In the table below, state the number of controls identified as "Not applicable" in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.*

***Table 3-20. Controls Designated "Not Applicable"***

| <x> Controls are Designated "Not Applicable" |
|---|
| |

*In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.*

***Table 3-21. Controls with an Alternative Implementation***

| <x> Controls have an Alternative Implementation |
|---|
| |

**Organization's Security Representative or designee**

_____

PLEASE PRINT NAME

_____ _____

SIGNATURE Date