**SOC2 Annual/Initial Audit Checklist V1.02**



|  |  |
| --- | --- |
| **System Name:** |  |
| **Business Owner:** |  |
| **Tech. Reviewer:** |  |
| **Review Date:** |  |



|  |  |  |  |
| --- | --- | --- | --- |
| **Annual Review Items** | **Reviewed?** | | **Comments / Exceptions** |
| **Yes** | **No** |
| Date on cover page of report |  |  |  |
| Look for AICPA certification emblem – usually located on cover page |  |  |  |
| Date on Bridge letter |  |  |  |
| Subcontractor list and tasks assigned |  |  |  |
| List of Data Centers – review to ensure there are no foreign DCs |  |  |  |
| Testing performed and results – look for exceptions that are usually in **bold** |  |  |  |
| High-level system diagram of servers – if applicable |  |  |  |
| Independent Evaluator – review the scope and subsequent results to ensure that the independent review conducted is consistent with applicable American Institute of Certified Public Accountants (AICPA) Standards (i.e., AT Section 801) for Reviewing Service Provider Controls. |  |  |  |
| User Complimentary Controls - review to ensure that any requisite internal State of Illinois (SOI) controls have been identified and implemented, that interoperate with and compliment the Service Provider's controls thereby providing effective controls to meet or exceed overall business and system control objectives. |  |  |  |
| Sub-Provider Controls - In the event the primary Service Provider utilizes one or more sub-providers, the Business Owner/Technical Reviewer should acquire SOC2 Reports from each of these sub-providers and conduct a review of their controls as well. |  |  |  |
| Contractual Controls – review to ensure that all applicable contractual, statutory and regulatory controls have been met. (Note: This may require interviews with the Service Provider/Sub-Provider.) |  |  |  |
| **Initial Review Items** | | | |
| ***The following are items that may be contained in the SOC Report or you may have to ask the Service Provider (vendor) for additional information:*** | | | |
| Code Migration Process - Review the SOC Report, if not directly included in the SOC Report, interview the Service Provider and determine whether the development, testing, and production environments have been distinctively defined. |  |  |  |
| Access to Production Code and Data - Review the SOC Report, if not directly included in the SOC Report, interview vendor and determine whether controls are in place to prevent programmers from normal access to production code and data. |  |  |  |
| Access to Production Program Libraries – 1. Identify what is needed to gain access to Production program libraries. (Who has access to the Production libraries)  2. Identify what security monitoring exists on production program libraries. |  |  |  |
| Emergency Change Procedures - Review the SOC Report, if not directly included in the SOC Report, inquire about emergency program changes and verify procedures and controls have been established. |  |  |  |
| Quality Assurance - Review the SOC Report, if not directly included in the SOC Report, determine whether quality checks are performed on modified software to ensure standards are followed, and documentation and testing are complete before moving the changes into production. |  |  |  |
| Business Continuity Plan (BCP) - Verify that the BCP is current and that it covers both the Service Provider(s) and the Business Owner's responsibilities in order to preserve data integrity, security, and sustain the operability of business processes in the event of partial or complete system failure. |  |  |  |
| Disaster Recovery (DR) plan – Verify that internally, a DR plan has been created that identifies both Service Provider and Business Owner and the DR Category, RTO Stage, and Disaster Recovery Justification have been provided.  Additionally, determine if the Service Provider (vendor) is responsible for disaster recovery. If yes, ensure the disaster recovery location has been identified and determine if disaster recovery tests are completed annually. |  |  |  |
| Vulnerability Scan - If applicable (web based applications) verify that the system/application has had vulnerability testing/preproduction scans performed by the Technical Safeguards Unit or a state approved 3rd party. Vulnerability Scans should be conducted whenever code changes are implemented and, at a minimum, annually thereafter. |  |  |  |

|  |  |
| --- | --- |
| **Comments:** |  |
| SOC2 Report to be reviewed annually by Business Owner | |
|  |  |
| **Approval** |  |

**Business Owner Date**