**Memo to Document Management’s Review of Periodic Controls That Did Not Operate During the Period**

|  |  |
| --- | --- |
| Name of Service Organization:  |  |
| Period Covered by the Report: |  |
| Name of Individual Preparing this Memo: |  |
| Date that this Memo was Prepared: |  |

**Background:**

According to the AICPA, controls should generally only be included in a Type 2 SOC report and tested by the service auditor if they occurred during the period being examined. When a Type 2 SOC report covers a period less than 12 months, there is a risk that certain periodic controls will not be performed during the period.

Company X elected to use a period of X months for its SOC report and as a result, certain periodic controls were not performed during the period. The Company determined that these controls were necessary in order to address certain Trust Services Criteria (SOC 2) / control objectives (SOC 1). From a business perspective, it was not considered practical to move the full performance of these controls into the audit period. Therefore, Company X took steps to update / revisit / refresh these controls during the audit period in order to appropriately address the related Trust Services Criteria (SOC 2) / control objectives (SOC 1). The purpose of this memo is to document the procedures that the Company took to update the controls during the period so that they can be leveraged and included in the current SOC report.

**Update Procedures:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Description of Control** | **When is the Control Normally Scheduled to be Performed?** | **Describe the Update Procedures Performed** | **Date that Update Procedures Were Performed** |
| A risk assessment is performed on an annual basis. | March | The CISO reviewed the most recent risk assessment prepared in March 2020, updated it and provided it to the Compliance Committee and Executive Management. The updates were primarily focused on new and emerging cyber security risks, risks related to COVID-19 and changes that have occurred in the Company’s operations, vendors and service offerings since March 2020. As part of the updated risk assessment, the CISO identified certain new controls that will be considered for implementation: security awareness training for the Company’s remote workforce and MFA for accessing all system components. | August 2020 |
| Control self-assessments are performed on an annual basis. | March 2020 | The Compliance Manager reviewed the most recent control self-assessment prepared in March 2020, performed update testing and provided it to the Compliance Committee and Executive Management. The update testing was primarily focused on high risk areas such as logical access, change management and network security. One or more key controls from each of these domains was selected and tested as part of the update procedures and the results were communicated to control owners. | August 2020 |
| The business continuity / disaster recovery plan is tested on an annual basis. | March 2020 | The Company conducted a Tabletop Exercise / Structured Walk-Through Test of the BC/DR plan in August 2020. This test was less in scope than the full testing that occurs in March each year, but still touched on the key components of the BC/DR plan. It included all critical personnel that are involved in the plan and consisted of a discussion and evaluation of scenarios that would cause the BC/DR plan to be activated. Each team provided responses to the scenarios and walked through the procedures their team will follow during an event. | August 2020 |