| **BANK OF SOMEWHERE**  **INSTRUCTIONS:**  Complete this checklist as appropriate and make it a part of the review work papers. Complete only the areas that apply. To complete this checklist, record a "Yes" to indicate that you have acquired document(s) or have completed the task and record a "Not Applicable" (N/A) to highlight instances where the task or function does not apply to the Bank’s policy, procedures or practices. For every "N/A" recorded answer, utilize the **Comment** field to document that the task/function does not apply to the Bank’s remote audit operations.  **NOTE**: This checklist is intended to assist you with completing your Bank’s audits via remote vendors. It is not intended to be all-inclusive or to fit all situations or areas of responsibilities for banks of all asset sizes. | | | |
| --- | --- | --- | --- |
| **ACTION** | **COMPLETED** | **N/A** | **COMMENT** |
| **Examine the virtual environment** | | | |
| 1. Define the working environment criteria most likely to benefit from online auditing. |  |  |  |
| 1. Apply ISO Standard Elements to remote team global supply chain. |  |  |  |
| 1. Define what sectors are impacted: BSA Management, Deposit Operations, Loan Operations and Compliance oversight. |  |  |  |
| **Define the following types of online auditing** | | | |
| 1. Traditional site model (on-site). |  |  |  |
| 1. Hybrid site model (on-site and off-site). |  |  |  |
| 1. Online auditing model (off-site) |  |  |  |
| **Illustrate how online auditing is accomplished** | | | |
| 1. Collaborative programs – Synchronous communication (immediate exchange). |  |  |  |
| 1. Centralization programs – Asynchronous communication (intermediate exchange). |  |  |  |
| **Discuss the benefits for online auditing** | | | |
| 1. Record control and centralization. |  |  |  |
| 1. Reduce your email workload. |  |  |  |
| 1. Understand QMS communication issues associated with working online. |  |  |  |
| **Discuss the controls for online auditing** | | | |
| 1. Data security |  |  |  |
| 1. Access control |  |  |  |
| 1. Security awareness |  |  |  |
| 1. Communications security |  |  |  |
| 1. Asset management |  |  |  |
| 1. Data backups |  |  |  |
| 1. Disaster recovery |  |  |  |
| 1. Business continuity planning |  |  |  |
| **Discuss IT Risk Management** | | | |
| 1. How well can IT identify, assess, manage, accept, and remediate risks? |  |  |  |
| 1. How effective is the IT risk assessment process? |  |  |  |
| 1. Are there formal and documented IT governance processes for decisions regarding project approvals, capital allocations, and others? |  |  |  |
| 1. Does your organization take advantage of the insights provided by your existing GRC (governance, risk, and compliance) software, if any? |  |  |  |
| **Discuss Program Risk** | | | |
| 1. Does your organization address areas that pose significant risks to the execution of projects and programs, such as partnerships with third parties, data migration, and business change? |  |  |  |
| 1. How are program and project risks assessed? |  |  |  |
| 1. Are program protocols followed properly? |  |  |  |
| 1. When business objectives change, how is the program portfolio managed? |  |  |  |
| **Information Security** | | | |
| 1. Is your existing information security strategy comprehensive? |  |  |  |
| 1. Does it include adequate vulnerability assessment, awareness, monitoring, detection and reporting controls for remote activities? |  |  |  |
| 1. Are there mechanisms in place that appropriately address known issues and identified threats for remote activities? |  |  |  |
| **Business Continuity Management** | | | |
| 1. Is your business continuity plan holistic and include remote activities? |  |  |  |
| 1. Does it cover essential business continuity procedures such as business impact analysis, vendor assessment, change management, testing, and maintenance? |  |  |  |
| 1. How soon can remote functions resume should a disruption or disaster occur? |  |  |  |
| **Remote Activities Management** | | | |
| 1. Are the right remote activities strategies in place, including risk and vulnerability identification, configuration settings, intrusion detection and response, and management of stolen or lost devices? |  |  |  |
| 1. Would you know if an attack occurs?   If so, how will you respond? |  |  |  |
| **Electronic Access** | | | |
| 1. Are there existing policies stored electronically? |  |  |  |
| 1. Does electronic storage make sense for the institution? |  |  |  |
| 1. Has the institution assessed electronic storage implications? |  |  |  |
| 1. Do user authentication and access protocols exist? |  |  |  |
| 1. Are role-based access protocols and duties segregated? |  |  |  |
| 1. Do individuals know their roles, access permissions, and responsibilities? |  |  |  |
| 1. Where is sensitive data stored and what access is available? |  |  |  |
| 1. Are adequate controls in place to reduce vulnerabilities? |  |  |  |
| 1. Are end user procedures in place to ensure security and compliance? |  |  |  |