

***MBLP***

**Auditing Solutions**

Audit Proposal

For

Pennsylvania State Credit Union

December 11, 2017

Dear PSCU Committee Members,

We at MBLP are pleased to have the opportunity to present our proposal to provide professional external auditing services to Pennsylvania State Credit Union. We are confident that MBLP is the right fit for PSCU’s needs with regards to auditing services.

Our Firm has experienced constant growth and success as we continue to meet and exceed our client’s expectations. Our overall goal is to provide a responsive and advanced service of the highest quality to our clients. We add value to our audits through specialized resources and technical proficiency. MBLP’s expertise in IT auditing and accounting coupled with our broad access to resources allows us to resolve any challenges that may be encountered during the audit. Our engagement team is highly trained and knowledgeable with regards to the Acceptable Memory Drive Usage policy and regulations. We understand that PSCU is committed to ensuring that the usage of electronic devices and the storage of all informational assets comply with all relevant regulations. To address your concerns and objectives our audit plan will:

* Determine the effectiveness of the current memory drive usage policy and its supporting controls
* Identify if the current policy and controls reduce risk to the organization and identify any policy failure
* Determine how well the corporate culture and guidance from leadership assist in the successful implementation of the policy.
* Inspection all registered devices every 90 days

We look forward to discussing your audit plan expectation in detail to ensure that MBLP effectively meets all of your expectations during the engagement. We commit to you that MBLP will include management in all facets of the engagement to ensure the highest quality of service.

If you have any questions regarding our audit plan proposal please contact me at 215.204.2222.

Yours Truly,

Michelangelo Collura- CSO

**Audit Objectives**

Our audit review will determine the efficacy of the current memory drive usage policy and its supporting controls. Success is defined as how much the policy and controls mitigate risk to PSCU from risks the audit will identify with policy failure. Our audit plan will identify what works well, isolate the risks, and bridge the gaps to eliminate the identified risk. Finally, the audit will determine how well the corporate culture and guidance from leadership assist in successful implementation of the policy.

**Audit Strategy**

The audit will begin by identifying the business objectives overall. We will then proceed to identifying and quantifying the greatest risks to the firm and its objectives from an ineffective memory drive usage policy. With this knowledge as a basis, analysis would shift to the controls currently in place to safeguard company data and PII. Analysis would seek to identify levels of compliance across the firm, from tellers up to executive leadership. The robustness of governance, and its ability to emphasize the value of compliance, will also be assessed. This will be achieved through a combination of policy review and interviews with staff.

**Audit Scope**

The audit shall involve assessment of bank staff at all levels and locations. This assessment will focus on staff compliance with your memory drive usage policy, and not on supporting policies. Policy will be assessed with company documentation of the policy, and any policies deemed relevant to understanding and measuring this documentation, as determined in policy #0874 (see control table).

**Audit Schedule**

The audit will require four months to complete, barring any interruptions due to interference from management.

* January 2018
* Initial communications to upper management and staff
* Interview executive leadership, including CFO John Smith and CIO Jane Doe.
* Concurrently, review memory drive usage policy documentation and cross-reference with interview results.
* February & March 2018
* Begin interviewing staff at headquarters and branch locations. The month will begin with interviews at HQ then proceed to the geographically most distant branches first and work back to HQ. Branches will be assessed through observation and direct interviews with managers and tellers.
* February & March 2018 (continued)
* Audit testing frame where we can test the controls and see if risks are mitigated
* Schedule interviews with staff as needed and obtain additional evidence
* Weekly touch points with staff to inform them on the status of the audit
* April 2018
* Gather any remaining evidence if needed, and finalize testing
* Compile work papers for audit findings
* Write up audit results
* Communicate audit results to LOB (line of business)

**Control & Risk Assessment Tables**

(See Appendix A and B)

Violation of any one of the controls related to the memory drive usage policy poses a significant risk to the organization.

* The Control and risk assessment table identifies the controls that we will review to determine sufficiency.
* For each control that was identified we have also included what evidence would show you that the control is effective and how the evidence would be collected.

**Audit Team**

|  |  |  |
| --- | --- | --- |
| **Name** | **Position** | **Experience/Recognitions** |
| **Michelangelo Collura** | Chief Security Officer | MBA, CISA, CISSP |
| **Brandan Mackowsky** | Audit Program Director | CISA, CISSP |
| **Lezlie Jiles** | Audit Account Manager | CISA, CISSP |
| **Patrick DeStefano** | Audit/Investigations Team Lead | CISA, CISSP |
| **Bob Smith** | Auditor/Audit Analyst | CISA |
| **Janet Riley** | Auditor/Audit Analyst | CISA |
| **Alex Jacobs** | Auditor/Audit Analyst | CISA |

**Appendix A**

**Appendix B**

