

**TABLE OF CONTENTS**

CONTENTS

[INTRODUCTION 3](#_Toc500790035)

[BACKGROUND 4](#_Toc500790036)

[OBJECTIVE 4](#_Toc500790037)

[AUDIT APPROACH 5](#_Toc500790038)

[AUDIT BUDGET AND TIMEFRAMES 5](#_Toc500790039)

[RISK, CONTROLS, AND EVIDENCE – Refer to Appendix A 6](#_Toc500790040)

# INTRODUCTION

Dear ITACS Audit Committee,

MBT&P is an external auditing company that audits credit unions for the soundness of IT governance and policy implementation. We have a focus on financial institutions and have been in business since 1990. We understand the technical, procedural, and regulatory issues faced by financial institutions in safeguarding private information.

We are pleased to present our audit of the ITACS Social Security Number Policy. Our audit includes an analysis of key risks, audit strategy, and suggested control objectives. Through an initial assessment we found the following risks that could adversely affect ITACS business objectives if not properly mitigated:

* PII policy content is outdated and doesn’t reflect the current protocol
* Access to PII information is provided to individuals without knowledge of policy and its requirements which could lead to policy violation
* Employees with access to PII information lack policy awareness
* Controls have not been evaluated to ensure the risk of unauthorized access/distribution of PII information is appropriately mitigated
* Deviations from policy are not appropriately validated and present unnecessary risk to the organization
* Devices are not properly configured to maintain the security of data
* Unencrypted PII are distributed externally which could result in unauthorized access

We look forward to further discussion with the Committee and believe this audit engagement aligns with your Strategic Objective of providing a safe and secure environment for your members and employees. If there are any questions or concerns prior to the next scheduled Audit Committee meeting, please do not hesitate to reach out to MBT&P.

# BACKGROUND

As part of its day-to-day business operations, the ITACS Credit Union (ITACS) maintains, stores, processes, and exchanges sensitive information related to its members and employees. ITACS has drafted a Social Security Number Policy to set a principle of action on how the ITACS user community should handle information that contains social security numbers (SSN). ITACS has commissioned Internal Audit to audit the ITACS Social Security Number Policy to determine whether the security controls and practices outlined in the policy are effective and consistent in promoting the proper handling of SSN to protect member and employee SSN from unauthorized access, disclosure and destruction

# OBJECTIVE

Our audit objective is to determine that the internal controls associated with the ITACS Social Security Number Policy provides reasonable assurance regarding the effectiveness and efficiency of operations, compliance with applicable laws and regulations, and safeguarding of ITACS assets.

1. Perform a comprehensive analysis of the Social Security Policy
2. Analyze the control environment to ensure compliance with the Social Security Policy.
3. SCOPE

The scope of the review will include an assessment of ITACS Social Security Number Policy as it is related to governance (oversight, training, risk assessment, handling, etc.), and user acceptance.

1. Governance - Are structures and processes outlined in the policy designed to ensure accountability, transparency, and stability when handling SSN?
2. Risk Assessment - Is the risk of the mishandling of SSN properly identified and are proper controls implemented to bring risk to an acceptable level? “Right things done right”
3. Compliance - Is there assurance that the policy promotes proper handling of SSN in accordance with appropriate laws and regulations?
4. Identify internal control and regulatory deficiencies that could affect the Credit Union.
5. Training and awareness of employees in the handling and processing of PII and data privacy

# AUDIT APPROACH

For a comprehensive audit of the ITACS Social Security Number Policy, Internal Audit has selected to use the COBIT 5 principles. COBIT 5 ensures that a policy framework meets stakeholders’ needs, covers the end-to-end process, and establishes the additional documentation required to ensure that governance and management goals and activities are achieved. According to COBIT 5, the core components of a policy framework are:

* Appointment of individuals who have the authority to approve policies and their associated responsibilities
* Determination of the consequences for failing to comply with given policies
* Definition of a process for handling exceptions to policies
* Definition of a method for measuring and monitoring compliance with policies
* Definition of the scope of the policy and the group of stakeholders that must follow the policy

# 

# AUDIT BUDGET AND TIMEFRAMES

MBT&P IT Auditing Services is proposing that it will take 260 hours to complete the engagement.

**Audit Period:** January – December 2017

**Start Date:** January 15th, 2018

**Planning:** January 8 – 13

* Internal Control Questionnaire to Management
* Finalize budget and staff

**Fieldwork:** January 15 – Feb 2nd

* Risk and Control Evaluation
* Finalize Work Program

**Reporting:** February 5 – 16

* Issues identified and discussed with Management
* Recommendations given to Management
* Draft Management Actions / Response

**Final Report:** February 23

* Issue Final report with Management Response

# RISK, CONTROLS, AND EVIDENCE – Refer to Appendix A