



TAX SHELTERED COMPENSATION, INC.

**SERVICE ORGANIZATION CONTROL (SOC2) REPORT
INFORMATION SECURITY, CONFIDENTIALITY AND
PROCESSING INTEGRITY
OF NON-PUBLIC CONFIDENTIAL INFORMATION**

**FOR THE PERIOD:
OCTOBER 1, 2010 – SEPTEMBER 30, 2011**



TABLE OF CONTENTS

CONTENTS	PAGE
INTRODUCTION	1
SECTION I	
INDEPENDENT SERVICE AUDITOR’S REPORT	2
SECTION II	
MANAGEMENT ASSERTION REGARDING CONTROLS PLACED IN OPERATION	6
• COMPANY OVERVIEW	7
• CONTROL PHILOSOPHY	8
• RISK ASSESSMENT	8
• RISK , SENSITIVITY, AND CRITICALITY	11
• ADMINISTRATIVE ACCESS CONTROL	14
• SECURITY OF FACILITIES	18
• ENCRYPTION	19
• MALICIOUS CODE	19
• ELECTRONIC AND PAPER-BASED MEDIA HANDLING	20
• LOGGING AND DATA COLLECTION	21
• SERVICE PROVIDER OVERSIGHT	21
• BUSINESS CONTINUITY CONSIDERATIONS	22
• OPERATIONS	22
• CONTINUING EVALUATION AND ADJUSTMENT	25



TABLE OF CONTENTS

SECTION III

CRITERIA IN TSP SECTION 100

26

SECTION IV

DESCRIPTION OF TESTS OF CONTROLS AND RESULTS THEREOF

40



INTRODUCTION

Tax Sheltered Compensation, Inc. (hereinafter “TSC”), believes that it and each of its customers (hereinafter “client”) is a repository of Non-Public Confidential Information (NPCCI) and that each respective party has an affirmative and continuing obligation to protect the security and confidentiality of the NPCCI it maintains as well as all NPCCI it may gain access to through its business relationships.

This document is intended to provide TSC’s clients and their independent accountants with information about its control structure specific to protecting NPCCI. This report has been prepared taking into consideration the guidance contained in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. The description is intended to provide clients with information about TSC, particularly system controls intended to meet the criteria for the security, confidentiality and processing integrity principles set forth in TSP section 100, *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

There are four sections to this document. The first section includes a copy of the report provided by the independent accounting firm of Baune Dosen & Co LLP. The second section provides a description of TSC’s controls placed in operation for the period of October 1, 2010 to September 30, 2011. The third section outlines the criteria in TSP section 100. The fourth section describes the controls in place including the service auditor’s tests of operating effectiveness and results of tests performed.



SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT

Board of Directors
Tax Sheltered Compensation, Inc.

Scope

We have examined the accompanying description of controls related to the information security and confidentiality of NPCI at Tax Sheltered Compensation, Inc. (TSC) for the period October 1, 2010 to September 30, 2011 and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, processing integrity, and confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period October 1, 2010 to September 30, 2011.



Service organization's responsibilities

TSC has provided the attached assertions titled “Management Assertions Regarding Controls Placed in Operation,” which is based on the criteria identified in management's assertion. TSC is responsible for (1) preparing the description and assertions; (2) the completeness, accuracy, and method of presentation of both the description and assertions; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in TSC's assertions and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2010 to September 30, 2011.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.



Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of management's description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in TSC's assertions and the applicable trust services criteria

- a. the description fairly presents the system that was designed and implemented throughout the period October 1, 2010 to September 30, 2011.
- b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2010 to September 30, 2011.
- c. the controls tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period October 1, 2010 to September 30, 2011.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of our tests are presented in the section III of this report titled "Description of Tests of Controls and Results Thereof."



Intended use

This report and the description of tests of controls and results thereof are intended solely for the information and use of TSC; its user organizations during some or all of the period October 1, 2010 to September 30, 2011; and prospective user entities, independent auditors and practitioners providing services to such user organizations, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

Baume Doren : Co LLP

January 13, 2012
Minneapolis, Minnesota



SECTION II – MANAGERMENTS ASSERTION REGARDING CONTROLS PLACED IN OPERATION

We have prepared the following description of TSC for the period of October 1, 2010 to September 30, 2011 based on the criteria for service organizations as outlined in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. The description is intended to provide clients with information about TSC, particularly system controls intended to meet the criteria for the security, confidentiality and processing integrity principles set for the in TSP section 100, *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids)* (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

- a. The description fairly presents TSC's system throughout the period October 1, 2010 to September 30, 2011, based on the following description as it relates to security, confidentiality and processing integrity criteria:
 - i. The description contains the following information:
 - (1) The types of services provided
 - (2) The components of the system used to provide the services, which are the following:
 - *Infrastructure*. The physical and hardware components of a system (facilities, equipment, and networks).
 - *Software*. The programs and operating software of a system (systems, applications, and utilities).
 - *People*. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
 - *Procedures*. The automated and manual procedures involved in the operation of a system.



- *Data.* The information used and supported by a system (transaction streams, files, databases, and tables).
- (3) The boundaries or aspects of the system covered by the description
 - (4) Relevant details of changes to the service organization's system during the period covered by the description
- ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- b. The controls stated in the description were suitably designed throughout the specified period to meet the applicable security, confidentiality and processing integrity criteria.
 - c. The controls stated in the description operated effectively throughout the specified period to meet the applicable security, confidentiality and processing integrity criteria.

MANAGEMENT DESCRIPTION

COMPANY OVERVIEW

Founded in 1966, TSC helps businesses provide successful retirement plans. TSC provides expert consulting, design and administration services for businesses throughout the United States.



To perform services, TSC receives information from plan sponsors, their CPA's and/or the financial company hired to invest the plan assets. TSC's clients include businesses and non-profit organizations that sponsor 401(k), Profit Sharing, Defined Benefit, Cash Balance, 403(b) and Money Purchase Pension plans for the benefit of its employees. The services offered to each client vary based upon a range of services offered to meet the specific needs of each client based on the type of plan design they have and the resources available to them.

CONTROL PHILOSOPHY

To assist in TSC's efforts to protect and secure the NPCI of it, its clients, and its client's customers, TSC has adopted an Information Security Plan to work in concert with TSC's information security and confidentiality methods and procedures. In addition, key operating methods and procedures are documented. This information is presented in Section II of this report and further describes TSC's controls placed in operation.

RISK ASSESSMENT

TSC management has placed into operation a risk assessment process designed to identify and mitigate risks that could affect the organization's ability to meet its contractual obligations. This process requires management to identify and mitigate risks, to implement appropriate measures to address those risks, and to monitor effectiveness of the controls. The risk assessment process focuses on analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. The risk assessment process is an ongoing process as business operations, workflow, or technologies change. TSC maintains policies and procedures and communicates them to employees when changes occur.

TSC has evaluated the extent and availability of insurance coverage and maintains insurance on a range of general areas of risk including, but not limited to:



- Automobile
- Business Travel
- Electronic Vandalism
- Employee Dishonesty
- Equipment
- Forgery or Alteration
- General Liability
- Special Business Income
- Structure Fire and Hazard Insurance
- Theft
- Umbrella
- Workers' Compensation

MONITORING

TSC management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, client conference calls and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Senior management evaluates the specific facts and circumstances related to suspected failures in internal control procedures. Management makes the decision for addressing control weaknesses based on whether the incident was isolated or requires a change in the company's procedures or personnel. Management accomplishes this through ongoing monitoring activities, separate evaluations, or combination of the two.



INFORMATION SYSTEMS

TSC's operations center is located in a multi-tenant facility in Edina, Minnesota. The network systems are fully managed and supported by TSC. Workstation and server operating systems include Microsoft technologies. TSC has a variety of control mechanisms established including router and firewall technology. TSC uses anti-virus and anti-spyware applications to protect systems from viruses and malicious code.

Logical access to TSC's systems, applications, and data is limited to properly authorized TSC employees. Auditing is implemented on systems, where possible, to track a variety of events, including but not limited to, security access violations and database access.

TSC maintains backups and are stored off-site at a secure storage facility. TSC hosts an online application for client access called Secured Plan Access.

COMMUNICATION SYSTEMS

TSC management is closely involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within the company. Management believes open communication channels help ensure exceptions are reported and acted on. For that reason, formal communication tools are in place, such as an organizational chart, employee handbooks, training classes, job descriptions, and a corporate intranet. Management's communication activities are made in written form, electronically, verbally and through the actions of management.

TSC's internal network is the central repository for company communications, as well as the primary tool used to disseminate information to employees. Individual departments are charged with designing and developing their procedures. Once a procedure is finalized, it is published to the internal network for distribution. Publishing to the corporate network is performed by information technology personnel who follow a process ensuring all changes are approved prior to release. Restrictive access controls are applied if the material being published is not intended for general viewing.



I. RISK, SENSITIVITY, AND CRITICALITY

To assist in TSC's efforts to protect and secure the NPCI of it, its clients, and its client's customers, TSC has adopted an Information Security Plan to work in concert with TSC's security methods and procedures. The plan generally outlines TSC safeguards to protect NPCI but it does not detail the precise methods, standards and procedures used by TSC. Doing so would provide a tool that external parties might use in an effort to breach TSC's security measures. Therefore precise details regarding TSC's security methods, standards and procedures are provided in a confidential document to the firm that audits TSC and issues reports regarding TSC's adherence to its control objective.

A. SECURITY AND CONFIDENTIALITY GOALS

The general procedures and safeguards that TSC has adopted to achieve its security and confidentiality goals include, but are not limited to:

1. Ensure the security and confidentiality of NPCI in TSC's possession.
2. Protect against any anticipated threats or hazards to the security, integrity or confidentiality of NPCI.
3. Protect against unauthorized access to or use of NPCI. The compromise of which could result in substantial harm to TSC, TSC's clients and other third parties.
4. Identify and assess risks that may threaten NPCI on a periodic basis.

B. IDENTIFIED SECURITY AND CONFIDENTIALITY RISKS

TSC recognizes that it is not possible to make a definitive list of all security and confidentiality risks to NPCI due to the rapidly changing and evolving technology landscape. However, TSC has recognized the following internal and external risks:



1. Unauthorized access to NPCI by an unauthorized individual;
2. Compromised computer system security as a result of system access by unauthorized personnel.
3. The physical or electronic interception or destruction of NPCI during transit;
4. Loss of NPCI and/or computer systems that contain NPCI due to a natural disaster;
5. Accidental or deliberate errors introduced into a computer system that contains NPCI;
6. Accidental or deliberate corruption of physical or electronic versions of NPCI;
7. Misuse of NPCI by TSC employees and/or representatives;
8. Requests for NPCI by unauthorized personnel;
9. Compromise of TSC's physical security that results in the unauthorized access of NPCI;
10. Unauthorized transfer of NPCI by or to a vendor.
11. Malware, viruses, download of executable via e-mail or other file transfers to employees.

C. CONFIDENTIALITY/SECURITY BREACH NOTIFICATION

In the event of a confidentiality/security breach, TSC will follow the procedures presented herein to provide notification to those clients whose NPCI is reasonably believed to have been compromised. Notification will occur without unreasonable delay, except when:



1. A law enforcement agency has determined that notification will impede a criminal investigation. In such instances, client notification will occur as soon as the law enforcement agency determines that such notifications will not compromise its investigation.
2. A reasonable delay is felt necessary in order to ascertain the scope of the breach and to restore the integrity of the compromised system.

TSC may determine the language to be used in the notification, which may be distributed in either a written, hard copy notice or by e-mail, in reference to the specifics of the security breach committed. If sufficient contact information is not available for a hard copy or e-mail notice, a telephone call may be used to provide prompt notification to clients.

D. INFORMATION SECURITY TEAM

Certain members of management will meet on an as-needed basis, but not less than once each year, to conduct a review of current security procedures and policies. This will be done to help determine if security adjustments and/or additional employee training are required. The team has the authority to respond to a security breach and is responsible for:

1. Assessing TSC's risks associated with NPCI;
2. Preparing cost comparisons for varying confidentiality or security approaches appropriate to TSC's environment;
3. Creating standards that guide managers and employees in implementing TSC's security and confidentiality methods and procedures;
4. Making certain employees in the various work units, departments and divisions in TSC abide by procedures and policies;



5. Maintaining comprehensive lists outlining:

- a) All NPCI repositories at TSC
- b) TSC hardware assets
- c) TSC software assets
- d) TSC network connections; and
- e) TSC telephone and facsimile connections.

In the event that exceptions and situations are not specifically outlined in its security policies and procedures, the CEO of the Company will make the final decisions.

The Information Security Team relies on its in-house legal counsel to provide for the identification of and consistency with applicable laws, regulations, commitments and contracts. The Information Security Team relies on its Network System Administrator to recommend technological changes to the system.

II. ADMINISTRATIVE ACCESS CONTROL

Administrative access controls have been established to restrict access to all TSC systems and system resources that house NPCI. Access to TSC systems that house NPCI is provided only to those employees who need access to such system(s) to complete their assigned work. This section outlines various administrative controls including, but not limited to, access rights administration and authentication protocols as they pertain to computer networks, operating systems, applications, via local and remote access. To help minimize the risk of unauthorized access, the following precautions have been instituted:

1. System Administrators who have controlling access to TSC's computer systems are appointed by the Information Security Team.
2. The access rights of each employee are configured at the proper level pertaining to the employee's position in the company.



3. All preconfigured “guest accounts” incorporated into hardware and software are disabled.
4. Mechanisms are in place to lock out users when there are repeated failed attempts to gain access.
5. All employees are made aware of the serious consequences that may result from security breaches and their individual responsibilities to help prevent incidences.

System Administrators are provided full system access to perform essential system administration functions critical to the continued operation of TSC including, but not limited to: i) establishing User ID's; ii) maintaining authorization levels for all accounts; iii) terminating an employee's session; iv) correcting problems; v) removing users who no longer need access vi) and other broadly-defined system privileges. The number of System Administrators accounts is to be kept to the absolute minimum number necessary for TSC to have appropriate and satisfactory System Administrator coverage at all times. It specifically restricts the granting of System Administrator rights to only those employees whose job duties require them.

A. AUTHENTICATION PROCEDURES

Authentication involves the verification of a user's identity prior to providing access to computer resources. It is based on the user entering a unique username and password into the computer system to gain access to the system.

Upon request from a TSC manager to grant initial system access, a System Administrator will assign the employee to an existing access class. The employee is then given a registered and unique “User Name” that identifies the employee in the computer system and a password. The password must conform to established criteria to ensure the password is considered secure. The user has the option to periodically change his or her password throughout their term of employment.



To mitigate Authentication related risks, TSC has adopted the following requirements:

1. Employee passwords are required to be a minimum of seven characters.
2. The password authentication system is protected by an encryption algorithm when a privileged user logs into the network remotely.
3. Lockout mechanisms are currently in place to lockout access to the User ID after five failed attempts.
4. All messages regarding failed log-ins are non-descriptive in nature.
5. If a server or workstation session is inactive for longer than fifteen minutes, a screen blanking mechanism is activated. Prior to resuming activity, the System Administrator or workstation user must re-authenticate before any action can take place.

B. NETWORK SECURITY

The Network System Administrator, one additional System Administrator and a third party contractor are authorized to add, remove, or replace network components. They are also charged with making certain all network and client devices, including their respective software, are appropriately maintained and managed.

To adequately secure access to TSC's systems and NPCI, a variety of control mechanisms have been established including router and firewall technology. The network controls that distinguish security domains include access control software permissions, firewalls, remote access servers, and Virtual Private Networks (VPNs). To help identify and administer all of these access control points, a network diagram is continually updated to reflect any and all changes in the system's topology.



Information regarding the firewall is deemed sensitive and is included in TSC's firewall standards. Those standards establish the rules for traffic coming into and going out of the TSC computer network and designate how the firewall will be managed. Areas covered by TSC's firewall standards include, but are not limited to:

1. Firewall topology and architecture;
2. Types of firewalls being utilized;
3. Monitoring firewall traffic when/if applicable;
4. Permissible traffic;
5. Firewall updating;
6. Protocols and applications permitted based upon port filtering.

All administrative access to the DNS Hosts, routers, and switches are limited to only System Administrators. Remote administration must be done using encrypted communication and password authentication. To further secure any transmissions through the firewall, it has been configured to accept Network Address Translation and Virtual Private Network gateways.

Additional measures adopted by TSC to control access to the system software within the various network clients and servers or via stand-alone systems include:

1. Restricted access to sensitive or critical system resources.
2. Restricting user and program access to sensitive system resources including files, programs, or processes.
3. Update operating systems with security patches and using appropriate change control mechanisms



C. REMOTE ACCESS

System Administrators and the pre-authorized staff are the only employees eligible to access TSC's network remotely. TSC uses Virtual Private Network (VPN) as the method of accessing TSC's network remotely. All remote users are to adhere to TSC's Remote Access Policy. The activity of remote sessions are logged and reviewed as management determines necessary.

III. PHYSICAL SECURITY

A. SECURITY OF FACILITIES

TSC maintains locked, access controlled office space.

A risk assessment has been performed relative to various external physical risks such as: fire, water, smoke, theft, destruction (accidental or by design), static electricity, dust and power surges. To mitigate these and other physical risks, TSC has adopted various standards and procedures.

Key elements of TSC's facilities security include, but are not limited to:

1. Access to TSC's office space is limited to three entrances. They are the employee entrances and the visitor entrance.
2. The employee entrances are each locked 24 hours a day with a code required for entrance.
3. The visitor entrance is locked during non-business hours. A receptionist monitors access during business hours.



4. The building is equipped with a variety of motion, fire, smoke, heat and glass break detectors. During non-business hours, an offsite security firm monitors the building security systems. Fire extinguishers with contents matched to the area of deployment have been placed throughout the building. They are inspected, serviced, and recharged by a licensed fire safety company.

B. INFORMATION TECHNOLOGY DEPARTMENT SECURITY

The Information Technology (IT) department houses TSC's physical network controls and the backups to the entire system.

The IT department has one access point and is kept locked unless authorized personnel are in this office. A fireproof cabinet is used to hold installation and system back up media. System backups are created outside of business hours Monday through Friday (excluding days when the office is closed for holidays or company events). Each Friday backup is retained for one month. End of month backups are retained for an undetermined length of time, never less than 8 years. Access to this area is controlled solely by the Network Systems Administrator and is granted only to those individuals who require the access to conduct business.

IV. ENCRYPTION

TSC uses encryption protocols a) when communications must be secured; b) for authentication processes; c) for the transmission of sensitive information; d) to secure applications and remote access communications.

V. MALICIOUS CODE

TSC defines malicious code as any program that acts in unexpected and potentially damaging ways. Since malicious code is highly dynamic, has many mobile connection possibilities, and does not specifically have to be targeted at TSC, it maintains a high-risk potential. To reduce risk and protect TSC systems from malicious code TSC has established the following procedures including, but not limited to:



1. Use of anti-virus and anti-spyware products, which use both signature and heuristic methods of detection and identification, on clients and servers;
2. Training system users not to open unexpected messages or executable files.
3. Training system users on what to do if they see an on screen alert that a virus has been detected.
4. Use of e-mail filters helps prevent the receipt of executable files.

VI. ELECTRONIC AND PAPER-BASED MEDIA HANDLING

NPCI is frequently contained on media such as paper documents, reports, back-up tapes, optical storage, test data, and system documentation. To maintain the security of NPCI requires that the media be secured. TSC considers all media to be equally sensitive and therefore, protects it all with equal diligence. Media handling and security is addressed in the following manner:

A. HANDLING AND STORAGE

All short-term storage of original media and media being worked on is kept on site at TSC until it is returned to the client, archived or destroyed. All NPCI in long-term storage is packed, labeled, and arranged in a specific manner to reduce the risk of loss and destruction.

B. DISPOSAL

1. PAPER BASED NPCI: To preclude the accidental inclusion of NPCI information in the regular trash, TSC employees are prohibited from discarding any paper, which contain NPCI, into regular trash bins. NPCI paper-based media must be placed into locked and secured destruction bins that are emptied as they fill. Once a sufficient amount of paper-based media has accrued, a designated employee will make certain it is delivered to a designated media-disposal company. The media will then be destroyed in such a manner that it cannot be reasonably compromised or re-claimed.



2. ELECTRONIC-BASED NPCI: Since residual data frequently remains on electronic media even after erasure, all electronic-based media has specific disposal requirements. When possible, electronic media (i.e., CD's, disks, etc.) is destroyed. If not destroyed, the electronic media is overwritten by the System Administrator.

C. TRANSIT

TSC is not responsible for the security of any physically transported NPCI a client transports to TSC until the NPCI is received by TSC. The receipt of the NPCI is logged. If the NPCI is damaged in transit, or missing, when compared to TSC's expectation, the applicable client is contacted.

VII. LOGGING AND DATA COLLECTION

TSC takes steps to ensure sufficient data is collected to identify security incidents. TSC logs the following data:

1. Operating System Access.
2. Remote Access.

VIII. SERVICE PROVIDER OVERSIGHT

TSC rarely contracts for services outside of the company requiring access to NPCI. However, should it be necessary to enter into an agreement with an outside services provider, that provider will be required to demonstrate: a) implement appropriate security controls to comply with TSC's Information Security Plan; or b) provide TSC a copy of the provider's Information Security Plan with proof of audit.



IX. BUSINESS CONTINUITY CONSIDERATIONS

Events that could trigger the implementation of TSC's Business Continuity Plan would likely have significant security considerations. Therefore, TSC's Business Continuity Plan addresses the risk mitigation that would be necessary to protect TSC and the client in the event the continuity plan must be implemented. Risk mitigation procedures have been established to cover a variety of contingencies including, but not limited to the following:

1. TSC's office must be evacuated.
2. There is an equipment malfunction regarding computers or security systems.
3. Data or original media is corrupted, destroyed, and/or lost.

X. OPERATIONS

TSC employees prepare plan documents, amendments, summary plan descriptions, annual valuations, discrimination testing, 5500s, 5558s on a complete, accurate and timely basis so that execution can occur in a timely manner.

In addition, TSC prepares a newsletter that is emailed quarterly to all clients. The purpose of the newsletter is to keep clients abreast of changes in retirement plan legislation and to provide informative data as it relates to client's day-to-day administrative plan duties.

For applicable clients, quarterly participant statements are prepared by TSC. When requested by the client, TSC will calculate the employer contribution allocation pursuant to the terms of the plan document. If an employer contribution is required (safe harbor or top heavy), TSC will calculate the allocation and advise the client accordingly.

TSC maintains policies and procedures to ensure employees prepare complete and accurate information for clients on a timely basis. They consist of the following:



1. Prior to the last day of the plan year, TSC sends a Year End Request Package (YERP) to each client requesting the information necessary for TSC to perform the services outlined in our service agreement with the client. The YERP provides specific instructions for clients to provide the necessary information and outlines testing deadlines applicable to each client.
2. If a client has not provided TSC with the information needed to complete the Average Deferral Percentage (ADP) testing within one month of the correction deadline, a follow-up email is sent reminding the client to forward the information. If the information has not been received two weeks before the correction deadline, a follow up phone call is made requesting the information
3. Once the ADP test has been completed, prior to the correction deadline for failed ADP tests an email is sent to the client advising them of the test results or a hard copy of the test results is included with the valuation reports mailed to the client.
4. In the event that late deposits of employee contributions are indicated, TSC will calculate lost earnings pursuant to the corrective measure chosen by the client. If the client chooses the VFCP process, all forms and instructions are prepared and forwarded to the client.
5. When the valuation has been completed, TSC will forward a hard copy of the reports to the client with clear instructions on the action items that the client must complete. Also included in the correspondence is an explanation for any compliance issues identified during the valuation process.
6. When the Form 5500 has been completed, TSC will send an email to the client with their instructions to electronically sign the Form 5500. Once TSC has received the confirmation email that the client has electronically signed the Form 5500, the administrator will electronically submit the form(s) to the EFAST2 system and confirm that the form(s) have been accepted without errors by the EFAST2 system.
7. All documentation for loans and distributions processed through TSC is retained in the TSC client files.



8. Contributions and loan repayments recorded in the plan's investment statements are reconciled to the information provided to TSC in the YERP.

TSC employees are required to communicate on a timely basis by performing the following:

1. Each TSC employee must respond to a client phone or e-mail inquiry directed to them within 24 hours.
2. All TSC employees that will be out of the office for a full business day are required to have an out-of-office message and voicemail message advising callers that they are out of the office and to contact another member of the team for immediate assistance.
3. If a plan is identified as falling out of compliance for any reason, clear communication regarding corrective action is provided to the client.

TSC employees track the status of each client's job to be completed by performing the following:

1. TSC maintains a database of current clients that tracks key dates for necessary workflow. Internally this database is referred to as Work-in-Process (WIP) reporting. Updating of the WIP database is performed by each TSC Retirement Plan Administrator for their assigned block of clients on at least a monthly basis. Monitoring of key WIP dates is performed by each TSC Retirement Plan Administrator and by each respective team manager/supervisor on at least a monthly basis. A third review of key WIP dates is performed by the VP of Operations on a periodic basis.
2. TSC requires each applicable client to provide by a specified date the information necessary to ensure TSC can timely complete the average ADP test. TSC maintains a separate tracking list for each client subject to the ADP test. Internally this tracking list is referred to as ADP Test Report. Updating of the ADP Test Report is performed by each TSC Retirement Plan Administrator for their assigned block of clients. Monitoring of ADP Test Report is performed by each TSC Retirement Plan Administrator and by each respective team manager/supervisor.



3. Client requests for Plan Document changes are input into the TSC database and monitored by our legal department to ensure timely completion.
4. For those clients that did not provide information prior to the testing deadline, additional follow up requests are sent prior to the un-extended and extended due dates for the Form 5500 filing.

XI. CONTINUING EVALUATION AND ADJUSTMENT

The Information Security Plan and any policies it references is subject to periodic review and adjustment. The most frequent of these reviews will occur within the TSC Information Technology department, where constantly changing technology and risks mandate that standards and procedures evolve to be effective. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the Information Security Team which will assign specific responsibility for TSC information technologies implementation and administration as appropriate. The Information Security Team will review the standards set forth in the Plan and all associated policies, recommending updates and revisions to reflect changes in technology, the sensitivity of NPCI and internal/external threats to information security.



SECTION III – CRITERIA IN TSP SECTION 100

Security Principle and Criteria

The system is protected against unauthorized access (both physical and logical).

- 1.0 The entity defines and documents its policies for the security of its system.
- 1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.
- 1.2 The entity's security policies include, but may not be limited to, the following matters:
 - a. Identifying and documenting the security requirements of authorized users.
 - b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.
 - c. Assessing risks on a periodic basis.
 - d. Preventing unauthorized access.
 - e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.
 - f. Assigning responsibility and accountability for system security.
 - g. Assigning responsibility and accountability for system changes and maintenance.
 - h. Testing, evaluating, and authorizing system components before implementation.
 - i. Addressing how complaints and requests relating to security issues are resolved.
 - j. Identifying and mitigating security breaches and other incidents.
 - k. Providing for training and other resources to support its system security policies.
 - l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.



- m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
 - n. Providing for sharing information with third parties.
-
- 1.3 Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.
 - 2.0 The entity communicates its defined system security policies to responsible parties and authorized users.
 - 2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.
 - 2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.
 - 2.3 Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.
 - 2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.
 - 2.5 Changes that may affect system security are communicated to management and users who will be affected.
 - 3.0 The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.



- 3.1 Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.
- 3.2 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:
 - a. Logical access security measures to restrict access to information resources not deemed to be public.
 - b. Identification and authentication of users.
 - c. Registration and authorization of new users.
 - d. The process to make changes and updates to user profiles.
 - e. Distribution of output restricted to authorized users.
 - f. Restriction of access to offline storage, backup data, systems, and media.
 - g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).
- 3.3 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.
- 3.4 Procedures exist to protect against unauthorized access to system resources.
- 3.5 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.
- 3.6 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.
- 3.7 Procedures exist to identify, report and act upon system security breaches and other incidents.
- 3.8 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.



- 3.9 Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.
- 3.10 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- 3.11 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.
- 3.12 Procedures exist to maintain system components, including configurations consistent with the defined system security policies.
- 3.13 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.
- 3.14 Procedures exist to provide that emergency changes are documented and authorized timely.
- 4.0 The entity monitors the system and takes action to maintain compliance with its defined system security policies.
- 4.1 The entity's system is periodically reviewed and compared with the defined system security policies.
- 4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.
- 4.3 Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.



Processing Integrity Principle and Criteria

System processing is complete, accurate, timely, and authorized.

- 1.0 Policies: The entity defines and documents its policies for the processing integrity of its system.
- 1.1 The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.
- 1.2 The entity's system processing integrity and related security policies include, but may not be limited to, the following matters:
 - a. Identifying and documenting the system processing integrity and related security requirements of authorized users
 - b. Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements
 - c. Assessing risks on a periodic basis
 - d. Preventing unauthorized access
 - e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access
 - f. Assigning responsibility and accountability for system processing integrity and related security
 - g. Assigning responsibility and accountability for system changes and maintenance
 - h. Testing, evaluating, and authorizing system components before implementation
 - i. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved
 - j. Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents
 - k. Providing for training and other resources to support its system processing integrity and related system security policies



- l. Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies
 - m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
- 1.3 Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.
- 2.0 The entity communicates its documented system processing integrity policies to responsible parties and authorized users.
- 2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.
- 2.2 The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.
- 2.3 Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.
- 2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.
- 2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.
- 3.0 The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.



- 3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.
- 3.2 The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies.
- 3.3 The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.
- 3.4 The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.
- 3.5 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.
- 3.6 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:
 - a. Logical access security measures to access information not deemed to be public
 - b. Identification and authentication of authorized users
 - c. Registration and authorization of new users
 - d. The process to make changes and updates to user profiles
 - e. Distribution of output restricted to authorized users
 - f. Restriction of access to offline storage, backup data, systems, and media
 - g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
- 3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.
- 3.8 Procedures exist to protect against unauthorized access to system resources.



- 3.9 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.
- 3.10 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.
- 3.11 Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.
- 3.12 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary
- 3.13 Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.
- 3.14 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.
- 3.15 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.
- 3.16 Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.
- 3.17 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.
- 3.18 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).
- 3.19 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.



- 3.20 Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.
- 3.21 Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.
- 4.0 The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.
- 4.1 System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.
- 4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.
- 4.3 Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

Confidentiality Principle and Criteria

Information designated as confidential is protected by the system as committed or agreed.

- 1.0 The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.
- 1.1 The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.



- 1.2 The entity's policies related to the system's protection of confidential information and security include, but are not limited to, the following matters:
 - a. Identifying and documenting the confidentiality and related security requirements of authorized users
 - b. Classifying data based on its criticality and sensitivity that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements
 - c. Assessing risk on a periodic basis
 - d. Preventing unauthorized access
 - e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access
 - f. Assigning responsibility and accountability for confidentiality and related security
 - g. Assigning responsibility and accountability for system changes and maintenance
 - h. Testing, evaluating, and authorizing system components before implementation
 - i. Addressing how complaints and requests relating to confidentiality and related security issues are resolved
 - j. Handling confidentiality and related security breaches and other incidents
 - k. Providing for training and other resources to support its system confidentiality and related security policies
 - l. Providing for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies
 - m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
 - n. Sharing information with third parties
- 1.3 Responsibility and accountability for developing and maintaining the entity's system confidentiality and related security policies, and changes and updates to those policies, are assigned.



- 2.0 The entity communicates its defined policies related to the system's protection of confidential information to responsible parties and authorized users.
- 2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.
- 2.2 The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:
 - a. How information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information.
 - b. How access to confidential information is authorized and how such authorization is rescinded.
 - c. How confidential information is used.
 - d. How confidential information is shared.
 - e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.
 - f. Practices to comply with applicable laws and regulations addressing confidentiality.
- 2.3 Responsibility and accountability for the entity's system confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.
- 2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.
- 2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.



- 3.0 The entity placed in operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.
- 3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system confidentiality commitments and (2) assess the risks associated with the identified threats.
- 3.2 The system procedures related to confidentiality of inputs are consistent with the documented confidentiality policies.
- 3.3 The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.
- 3.4 The system procedures related to confidentiality of outputs are consistent with the documented confidentiality policies.
- 3.5 The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.
- 3.6 Does not apply to this organization.
- 3.7 Does not apply to this organization.
- 3.8 Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters:
 - a. Logical access security measures to restrict access to information resources not deemed to be public
 - b. Identification and authentication of all users.
 - c. Registration and authorization of new users.
 - d. The process to make changes and updates to user profiles.
 - e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.



- f. Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.
 - g. Distribution of output containing confidential information restricted to authorized users.
 - h. Restriction of access to offline storage, backup data, systems, and media.
 - i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).
- 3.9 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.
- 3.10 Procedures exist to protect against unauthorized access to system resources.
- 3.11 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.
- 3.12 Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.
- 3.13 Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.
- 3.14 Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.
- 3.15 Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.
- 3.16 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined confidentiality and related security policies.



- 3.17 Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.
- 3.18 Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.
- 3.19 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.
- 3.20 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).
- 3.21 Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.
- 4.0 The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.
- 4.1 The entity's system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.
- 4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.
- 4.3 Environmental, regulatory, and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.



SECTION IV – DESCRIPTION OF TESTS OF CONTROLS AND RESULTS THEREOF

The following section provides a matrix which individually lists the controls provided by TSC as described throughout this report which combined assure the control objective is met. Each control listed on the left side of the matrix is designed to provide reasonable assurance that the stated control objective is met. The right side of the matrix describes tests of operating effectiveness and the results of those tests. The description of control is prepared by TSC. The tests of operating effectiveness and test results are prepared by Baune Dosen & Co LLP. The tests apply only to the stated control policies and procedures. They may not address all aspects of the processing activities included in the description.

Management has developed reasonable controls to ensure they meet the criteria in TSP section 100 applicable to the principles of security, confidentiality and processing integrity.

	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
a	Documented security and confidentiality policies and procedures are in place to guide personnel in security administration. The policies are periodically reviewed and approved by the Information Security Team.	Inspected the security and confidentiality policies and procedures to determine that documented policies and procedures were in place, reviewed and approved by the Information Security Team and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
b	A unique user ID is assigned to all new employees along with a password.	Observed process of creating a new employee user ID and password and conducted corroborative inquiry of management.	No relevant exceptions noted.
c	Passwords must be seven or more characters in length.	Inquired of the System Administrator regarding the use of passwords and existence of password policies. Observed system password settings.	No relevant exceptions noted.
d	A screen blanking mechanism is activated if the user is inactive for longer than fifteen minutes. The user is forced to re-authenticate to resume activity.	Inspected the group policy network parameters and conducted corroborative inquiry of management.	No relevant exceptions noted.
e	TSC has a Sonicwall firewall to protect applications and data.	Observed the existence of firewall protection and inspected system configuration. Conducted corroborative inquiry of management.	No relevant exceptions noted.
f	Virus protection is installed on both servers and workstations. Virus signature updates are systematically pushed down to all workstations as updates are identified.	Observed the existence of anti-virus software on both servers and workstations and the settings that configure automatic virus updates and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
g	If a virus has been detected a message will appear on a user's computer.	Inspected virus detection system configurations for the existence of detection reporting and conducted corroborative inquiry of management.	No relevant exceptions noted.
h	Access to the TSC network and applications require that a user authenticate by entering in their network user ID and a confidential password.	Observed system logon scripts and corroborative inquiries of the System Administrator and management.	No relevant exceptions noted.
i	After five invalid access attempts, the user ID is locked for duration of 30 minutes.	Inspected the global access controls and system options and verified proper set up and conducted corroborative inquiry of management.	No relevant exceptions noted.
j	Remote Access to TSC's network must be added to an employee's user profile by a System Administrator.	Observed the system functions require the proper access within an employee's user profile and conducted corroborative inquiry of the system administrator and management.	No relevant exceptions noted.
k	All prefigured "guest accounts" incorporated into hardware and software are disabled to prevent unauthorized access.	Inspected settings on the network and a sample of computers to determine guest accounts were disabled and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
l	All remote contact with the TSC network is encrypted via a VPN connection.	Inspected system settings and read operational documentation to determine existence of encryption and conducted corroborative inquiry of management.	No relevant exceptions noted.
m	Company issued cell phones with company email access can be remotely wiped clean immediately upon knowledge of the cell phone being lost or stolen.	Inspected settings to determine existence of remote wipe clean of email access and conducted corroborative inquiry of management.	No relevant exceptions noted.
n	Authorization levels for all accounts are maintained by the System Administrator.	Observed that authorization levels are maintained by the system administrator and conducted corroborative inquiry of the system administrator and management.	No relevant exceptions noted.
o	The side entrance of the office is locked with a keypad combination that only employees can use to enter. This entrance is always locked.	Observed side entrances with locked down keypad access and conducted corroborative inquiry of management.	No relevant exceptions noted.
p	During business hours, 8:00 a.m. to 5:00 p.m., Monday to Friday, a receptionist is situated in the lobby and monitors access to the office.	Observed presence of Lobby Receptionist and conducted corroborative inquiry of the receptionist and management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
q	The network equipment is located in a controlled room segregated from main office traffic. The room is secured by a key lock when the Network Administrator's office is not in use.	Observed the location of the network equipment was segregated from regular office traffic. Observed that the room was secured by a keypad access door. Inquired of management regarding personnel with keys to the network room.	No relevant exceptions noted.
r	File servers are configured in freestanding rack mounted cabinets in the server room.	Observed the existence of servers configured in freestanding rack mounted cabinets in the server room and conducted corroborative inquiry of management.	No relevant exceptions noted.
s	A fireproof cabinet is used to hold computer media.	Observed that the storage cabinet used for computer media is fire rated and conducted corroborative inquiry of management.	No relevant exceptions noted.
t	UPS units are installed to protect the file servers and telecommunications equipment from power surges.	Observed the existence of UPS systems in the server room and that server's were connected and conducted corroborative inquiry of management.	No relevant exceptions noted.
u	Environmental controls are used to protect the network equipment.	Observed thermostat controlled environment and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
v	The Network Systems Administrator solely controls access to the IT area and is granted only to those individuals who require the access to conduct business.	Observed locked access to the IT area and conducted corroborative inquiry of management.	No relevant exceptions noted.
w	System users are trained to not open unexpected messages or executable files.	Inquired of a sample of system users.	No relevant exceptions noted.
x	Policy is established that all laptops taken outside of the office and left unattended in a vehicle be locked in the trunk and always maintained out-of-sight. If kept in a hotel room, they are appropriately secured. Laptop cable locks are used whenever possible.	Inquired of all laptop users regarding the use of laptops when taken outside the office and the existence of laptop policies. Inspected the existence of employee signed laptop policies acknowledgements.	No relevant exceptions noted.
y	It is Company policy that sensitive client data is not stored on the c: drive of a company issued laptop when it is taken outside of the office. Only the network system administrator may have such data for the purpose of project work and development.	Inquired of the Vice President of Operations and the System Administrator regarding the use of sensitive data and existence of sensitive data policies.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
z	Paper-based information received from clients is retained in the client hard-copy folders. All hard-copy information is electronically scanned into our system timely after the valuation has been completed. After being scanned, the hard-copies are kept in secure locked bins until shredded on site by a company contracted to perform this service.	Inquired of four of the five Team Leads regarding the process of scanning and depositing hard copies into shred bins upon completion of valuations.	No relevant exceptions noted.
aa	Electronic-based information received from clients is retained in the client electronic folders.	Observed the process of receiving client information and retention of the information in electronic folders and conducted corroborative inquiry of management.	No relevant exceptions noted.
bb	Remote system access is logged.	Observed the access log and conducted corroborative inquiry of management.	No relevant exceptions noted.
cc	A Business Continuity Plan is in place to ensure the availability of services should a disastrous event interrupt service. The plan contains procedures for the recovery of the operating system and critical business applications.	Inspected the Business Continuity Plan for evidence of procedures for the recovery of operating systems and critical business applications and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
dd	System back ups are maintained for a minimum of four weeks.	Inspected back-up documentation covering a recent four-week period and conducted corroborative inquiry of management.	No relevant exceptions noted.
ee	Media is properly labeled.	Observed copies of the backup media and noted that they were all labeled and stored and conducted corroborative inquiry of management.	No relevant exceptions noted.
ff	A copy of a full back-up is sent to off-site storage on a weekly basis.	Observed process for sending back-up media to off-site storage facility and conducted corroborative inquiry of management.	No relevant exceptions noted.
gg	The Business Continuity Plan is documented and updated to reflect the changing environment. The plan is updated as changes occur.	Inspected the Business Continuity Plan and observed that it was last modified in the current year for the changing environment and conducted corroborative inquiry of management.	No relevant exceptions noted.
hh	Back-up data is restored on a monthly basis to ensure that back-ups are running correctly.	Observed most recent month's back-up data being restored and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
ii	Documented processing integrity and related security policies and procedures are established and policies are periodically reviewed and approved by the Information Security Team.	Inspected the processing integrity and related security policies and procedures to determine that documented policies and procedures were in place, reviewed and approved by the Information Security Team and conducted corroborative inquiry of management.	No relevant exceptions noted.
jj	Prior to the last day of the plan year, TSC sends a Year End Request Package (YERP) to each client requesting the information necessary to perform the services outlined in the service agreement with the client.	Inspected documentation supporting the performance of this verification procedure and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
kk	If a client has not provided the information needed to complete the Average Deferral Percentage (ADP) testing within one month of the correction deadline, a follow-up email is sent to the client to forward the information. If the information has not been received two weeks before the correction deadline, a follow up phone call is made requesting the information.	Obtained and inspected a selection of client files to determine if follow-up communications are made as it relates to the Average Deferral Percentage (ADP) testing deadline and conducted corroborative inquiry of management.	No relevant exceptions noted.
ll	If a plan is identified as falling out of compliance for any reason, clear communication regarding corrective action is provided to the client.	Obtained and inspected a selection of client files to determine follow-up communications are made as it relates to corrective actions and conducted corroborative inquiry of management.	No relevant exceptions noted.
mm	For those clients that did not provide information prior to the testing deadline, additional follow up requests are sent prior to the un-extended and extended due dates for the Form 5500 filing.	Obtained and inspected a selection of clients that did not provide information prior to the testing deadline to determine if additional follow up requests were sent to the clients prior to the un-extended and extended due dates and conducted corroborative inquiry of management.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
nn	A manual tracking checklist is prepared each year for each client to monitor the preparation and review of each item prepared. The reviewer initials and dates the checklist when steps are completed.	Obtained and inspected a selection of tracking checklists as prepared by each Team Lead to determine if the checklists were completed and reviewed and conducted corroborative inquiry of management.	No relevant exceptions noted.
oo	Each Retirement Plan Administrator updates the work-in-process database for their assigned block of clients on at least a monthly basis.	Obtained and inspected a selection of work-in-process listings by Team Lead to determine if the work-in-process database is updated at least on a monthly basis and conducted corroborative inquiry of management.	No relevant exceptions noted.
pp	Each Retirement Plan Administrator and respective team managers/supervisors monitor key dates on at least a monthly basis.	Inquired of all Team Leads regarding the monitoring of key dates.	No relevant exceptions noted.
qq	The Vice President of Operations reviews key dates on a periodic basis.	Inquired of Vice President of Operations regarding the review of key dates on a periodic basis. Inspected the Valuation Completion Worksheet by Team prepared by the Vice President of Operations.	No relevant exceptions noted.



	DESCRIPTION OF CONTROLS	TESTS OF OPERATING EFFECTIVENESS	TEST RESULTS
rr	Contributions and loan repayments recorded in the plan's investment statements are reconciled to the information in the YERP.	Obtained and inspected a selection of reconciliations to determine existence of control and conducted corroborative inquiry of management.	No relevant exceptions noted.
ss	All employees must respond to a client phone or email inquiry directed to them within 24 hours.	Inquired of a selection of employees regarding the response time to client inquiries.	No relevant exceptions noted.
tt	All employees that will be out of the office for a full business day are required to have an out-of-office message and voicemail message advising callers that they are out of the office and to contact another member of the team for immediate assistance.	Inquired of and sampled a selection of employees regarding steps taken when out of the office by sending an email and calling the voicemails of individuals out of the office when testing was performed.	Finding: One of four employees tested did not have their out of office auto email reply on or their voicemail message set accordingly.
uu	Client requests for plan document changes are input into the TSC database and monitored by the legal department to ensure timely completion.	Obtained a listing of plan document changes for the year and for a selection of changes observed changes are input into the TSC database and conducted corroborative inquiry of management.	No relevant exceptions noted.