

Security Summit Self- Assessment Guide for External Users



Table of Contents

Table of Contents	2
Introduction	3
FAQs	4
Appendix A – Self-Assessment template	9
Introduction tab	9
Test Cases tab.....	10
Test Cases tab cont.	11
Test Cases tab cont.	12
Document Marking	13
Appendix B – Sample Narratives for Critical Controls.....	14
Background:	14
Purpose:	14
Organization:.....	14
<i>Audit Narrative [Addressing Year 4 critical controls AU-2(3), AU-3(1) & AU-4]</i>	14
<i>Vulnerability Scanning [Addressing Year 4 Critical Control RA-5(1)(2)(5)]</i>	15
<i>Allocation of Resources (System Acquisition) [Addressing Year 4 critical control SA-2]</i>	16
<i>System Communications [Addressing Year 4 Critical Control SC-8 (1), SC-12, SC- 28]</i>	16
<i>System Integrity [Addressing Year 4 Critical Control SI-5]</i>	17
Appendix C – Tax Ecosystem Selected Security Controls.....	19
Appendix D – SDT Instructions	23
Appendix E – Glossary	24
Appendix F – References.....	29

Introduction

This guide was created by the Strategic Threat Assessment and Response (STAR) Working Group to assist tax industry members in completing a self-assessment of their organization. The self-assessment provides an organization with a tool for determining their level of risk management on the Tax Ecosystem Selected Security Controls (see Appendix B). This is intended to facilitate the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which was adopted by the STAR Working Group as a common framework for managing the risk to taxpayer data.

The next section provides frequently asked questions (FAQs) about the STAR Working Group, its approach to CSF and the self-assessment process.

FAQs

What is the Vision of the STAR Work Group?

Provide technical leadership to the Security Summit and secure the tax ecosystem's information assets and systems through people, processes and technology.

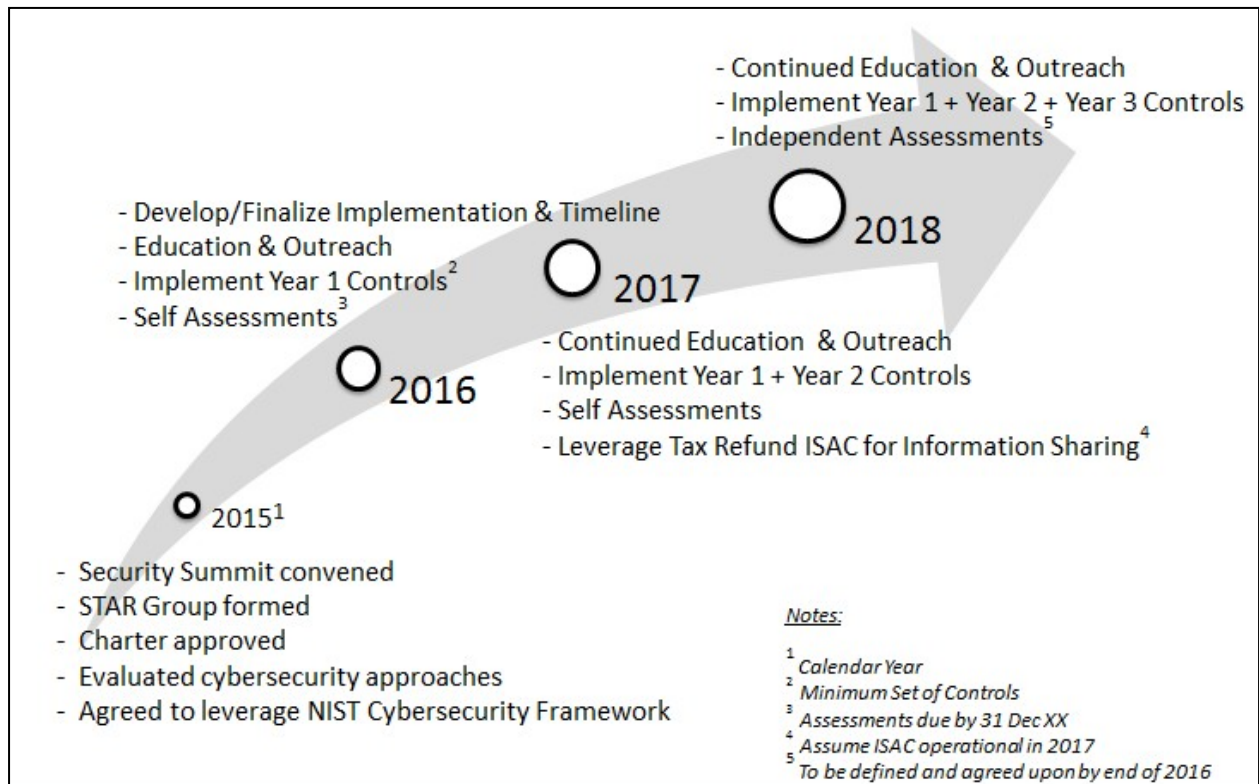
What is the Mission of the STAR Work Group?

Improve the tax ecosystem's security posture by adopting a security framework and methodology to assess threats and develop strategic responses.

What are the Roles & Responsibilities of the STAR Working Group?

- *Adopt and refine an IT security-related framework that improves the security capabilities for each partner in the tax system, regardless of such things as size, level of technology, business model and whether they are government or private sector.*
- *Develop an assessment methodology to help organizations in identifying, addressing and resolving their own security risks in an orderly, cost-effective and consistent manner.*
- *Act as the clearinghouse for the other Security Summit working groups and participants by reviewing, identifying, coordinating and communicating IT and security-related best practices through people, processes and technology.*

I'm new to the Security Summit, what is the three-year implementation of the NIST CSF?



Why is the tax ecosystem implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)?

In March 2015 the IRS, tax industry and state revenue offices kicked off a Security Summit to discuss common challenges (e.g. refund fraud related to identity theft) and explore ways to collectively leverage resources to address current and future threats to the tax ecosystem. The STAR Work Group was charged with providing technical leadership to the Security Summit and recommend activities to secure the tax ecosystem's information and information systems through people, processes and technology. To reduce cybersecurity risk across the ecosystem, participants agreed to align with the IRS and the states using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to promote the protection of information technology (IT) infrastructure.

What is the intent behind implementing security controls?

The goal is to reduce cybersecurity risk and identify theft related to refund fraud across the tax ecosystem. In a large, complex ecosystem criminals typically attack and exploit security gaps. Effectively implementing security controls should reduce cybersecurity risk and identify areas for organizations to improve their individual security posture.

How was the implementation process developed?

Through a series of collaborative engagements with Security Summit participants, an incremental, three-year approach to reach the target baseline security posture was adopted. Incremental implementation of the security controls addresses the diverse attributes of the ecosystem (public, private, large, small) as well as acknowledges each organization's individual cybersecurity maturity level.

What is the scope of the work for implementing controls?

The scope of the implementation of the NIST CSF is to protect taxpayer's PII in transit and at rest on computers and networks controlled by the implementing entity from unauthorized disclosure. It is intended for the organization's employees, vendors, contractors or any subcontractors who provide services to the organization. Taxpayer and Preparer's access is currently addressed by the Security Summit –Authentication requirements.

What are the Year 1, 2 and 3 security controls?

Collectively they represent the NIST security controls selected for the Tax Ecosystem. To The controls were spread out over three years to accommodate an incremental implementation. The security controls are listed at the end of this document in "APPENDIX B: Tax Ecosystem Security Controls"

Why are some NIST security controls not included in the required security controls?

Security controls with limited impact to overall cyber hygiene or limited impact in reducing identity theft and refund fraud were not included. While some security controls are considered a best practice, unless required by law, implementation should be considered based on an organizations individual risk tolerance.

Is there an expectation for uniform implementation of security controls?

No. Each organization has a unique information technology environment. Multiple factors contribute to determining what risk(s) may be present within an environment and what might be required to demonstrate full compliance with a NIST security control. Factors that need to be taken into consideration include, but are not limited to: hosting environment; application architecture; organizational size and structure; 3rd party service providers; usage of commercial and/or open-source technology.

Is the expectation for uniform completion of security control test cases?

No. Each organization has a unique information technology environment. Organizational size, complexity and a host of other considerations dictate how tests are implemented. The companion assessment template allows for organizations to articulate how test cases have been

satisfied.

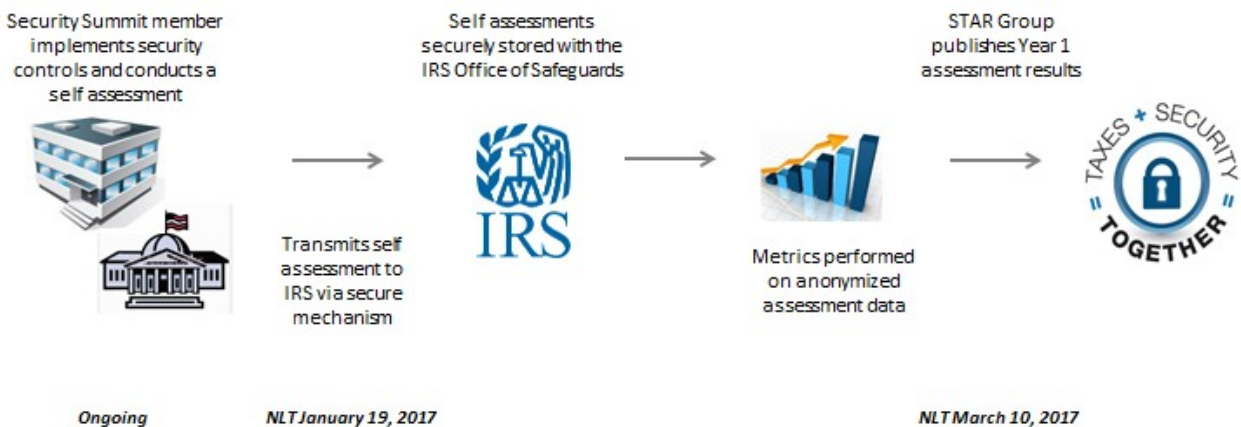
What if an organization plans on implementing a security control, but has not yet fully implemented and assessed for effectiveness?

The organization should complete the Self-Assessment template and document when the security control will be fully implemented. Note, organizations may implement compensating controls when implementation guidance or a control conflicts within its environment.

What if an organization chooses not to implement a security control?

The organization should complete the Self-Assessment template and document how they arrived at that decision. For example, the organization may have a compensating measure and should describe.

I'm new to the Security Summit, what is the security control implementation and assessment process?



Why was an assessment template created?

To consistently assess security control implementation and capture meaningful metrics, a security control assessment with over 500 test cases template was developed. In addition to identifying trends measuring progress over time, this assessment template could be leveraged to facilitate independent, or third-party, assessments at a later date.

How will the Self-Assessment data be protected?

Security Summit participants should provide the assessments via Secure Data Transmission (SDT), via encrypted email, or in person. The IRS will store these submissions consistent with IRS Office of Safeguard's Publication 1075, Protecting Federal Taxpayer Information (FTI) through Network Defense-in-Depth.

How do I use the self-assessment template?

The self-assessment template is a password protected excel document. See Appendix A for a description of the template and how to use it.

Appendix A – Self-Assessment template

Introduction tab

- Describes the intent of the self-assessment process
- Table of contents listing for each worksheet

A	B	C	D	E										
<p style="text-align: center;">Official Use Only</p> <p>This document belongs to the Internal Revenue Service. It may not be released without the express permission of IRS. Refer requests and inquiries for the document to: Michael Anthony, IRS IT Cybersecurity, 1111 Constitution Ave NW, Washington, DC 20224, 202.317.3028</p>														
<p>Introduction: This excel document is intended to provide the test cases to be used by members of the Tax Ecosystem. These test cases are for self-assessment of the implementation of the Tax Ecosystem Selected Security Controls. The test cases were derived from the security controls but are not implementation guidance. Each organization should review the Tax Ecosystem Selected Security Controls to determine how to implement them in their environment.</p>														
<table border="1"><thead><tr><th data-bbox="65 831 533 889">Section</th><th data-bbox="533 831 1858 889">Description</th></tr></thead><tbody><tr><td data-bbox="65 889 533 927">Self-Assessment Cases</td><td data-bbox="533 889 1858 927">The set of test cases for self-assessment</td></tr><tr><td data-bbox="65 927 533 964">Control Status def</td><td data-bbox="533 927 1858 964">Definitions of the options provided for the status of the control implementation for each test case</td></tr><tr><td data-bbox="65 964 533 1002">References</td><td data-bbox="533 964 1858 1002">Attachments of any relevant references are located in this tab</td></tr><tr><td data-bbox="65 1002 533 1073">Control Scoring</td><td data-bbox="533 1002 1858 1073">Worksheet to show how the test cases bear out for each control</td></tr></tbody></table>					Section	Description	Self-Assessment Cases	The set of test cases for self-assessment	Control Status def	Definitions of the options provided for the status of the control implementation for each test case	References	Attachments of any relevant references are located in this tab	Control Scoring	Worksheet to show how the test cases bear out for each control
Section	Description													
Self-Assessment Cases	The set of test cases for self-assessment													
Control Status def	Definitions of the options provided for the status of the control implementation for each test case													
References	Attachments of any relevant references are located in this tab													
Control Scoring	Worksheet to show how the test cases bear out for each control													

Test Cases tab

- NIST Control Name
- IRS Test ID or NIST control enhancement number
- Year (yr) Priority
- Case Number
- NIST Control Number
- Score
- Consolidated Assessment Cases

Official Use Only						
This document belongs to the Internal Revenue Service. It may not be released without the express permission of IRS. Refer requests and inquiries for the document to: Michael Anthony, IRS IT Cybersecurity, 1111 Constitution Ave NW, Washington, DC 20224, 202.317.3028						
NIST Control Name	IRS Test ID or NIST Moderate Control Enhancement Number	Yr Priority	Case Number	NIST Control Number	Score	Consolidated Assessment Cases <i>Derived from IRS Office of Safeguards Guidance or 800-53 Control Description where no IRS guidance is provided</i>
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.1	AC-1	.	1. An access control policy is documented and addresses: a. purpose
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.10	AC-1	.	3. The policy and procedures are disseminated to designated organization officials; reviewed and updated: b. Every 1 year for the procedures.
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.2	AC-1	.	1. An access control policy is documented and addresses: (b) scope
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.3	AC-1	.	1. An access control policy is documented and addresses: (c) roles and responsibilities
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.4	AC-1	.	1. An access control policy is documented and addresses: (d) management commitment
ACCESS CONTROL POLICY AND PROCEDURES	MOT-63	y1	AC-1.5	AC-1	.	1. An access control policy is documented and addresses: (e) coordination among organization entities

Test Cases tab cont.

- Additional Guidance
 - Notes to provide context and/or definitions
- Status
- Supporting Rationale
- Additional Notes
 - You may need to re-enter the password to update these columns with your results. The rest of the template is locked down to ensure no modifications can change the consistency.

H	I	J	K
Additional Guidance <i>(e.g., NIST Supplemental Guidance, Publication 1075 Requirements) when applicable.</i>	Status	Supporting Rationale <i>Note: This box must be completed if the Status is anything other than "Implemented"</i>	Additional Notes

Test Cases tab cont.

- Status drop-down list
 - Implemented
 - In Progress – Administrative
 - In Progress – Configuration
 - In Progress – Installation/Upgrade
 - Not Implemented – Compensating Control
 - Not Implemented – Partial Compensating Control
 - Not Implemented – Risk Nominal
 - Not Implemented – Risk Moderate
 - Not Implemented – Risk Accepted
 - Not Implemented – Planned
 - Not Implemented – Unplanned
 - Not Applicable

Control	Status	Note:
	<ul style="list-style-type: none"> Implemented In Progress - Administrative In Progress - Configuration In Progress - Installation/Upgrade Not Implemented - Compensating Control Not Implemented - Partial Compensating Control Not Implemented - Risk Nominal Not Implemented - Risk Moderate 	
	<ul style="list-style-type: none"> Not Implemented - Compensating Control Not Implemented - Partial Compensating Control Not Implemented - Risk Nominal Not Implemented - Risk Moderate Not Implemented - Risk Accepted Not Implemented - Planned Not Implemented - Unplanned Not Applicable 	

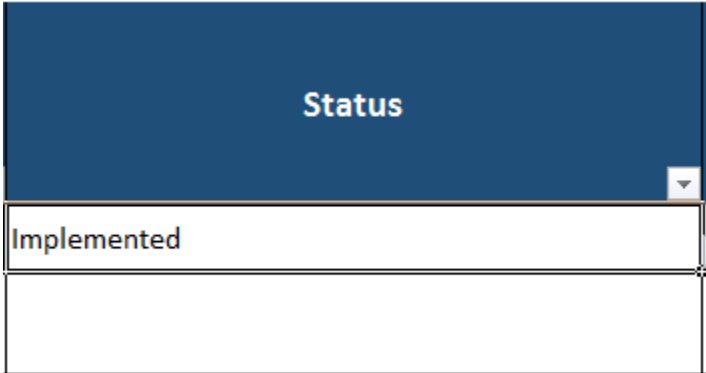
- Refer to Control_Status_def worksheet for descriptions and scores for each status

Document Marking

Official Use Only

This document belongs to the Internal Revenue Service. It may not be released without the express permission of IRS. Refer requests and inquiries for the document to: Michael Anthony, IRS IT Cybersecurity, 1111 Constitution Ave NW, Washington, DC 20224, 202.317.3028

- Official Use Only by default
 - Once the status is changed for any test case the document marking updates
- Sensitive But Unclassified (SBU)
 - SBU is for any self-assessment that now contains organizational data (i.e. self-assessment results)



The image shows a screenshot of a web interface. At the top is a dark blue header with the word "Status" in white text. Below the header is a dropdown menu with a white background and a black border. The word "Implemented" is displayed in the dropdown menu. To the right of the dropdown menu, there are small, faint icons for zooming in and out.

Sensitive But Unclassified

This document belongs to the Internal Revenue Service. It may not be released without the express permission of IRS. Refer requests and inquiries for the document to: Michael Anthony, IRS IT Cybersecurity, 1111 Constitution Ave NW, Washington, DC 20224, 202.317.3028

Appendix B – Sample Narratives for Critical Controls

Background:

The Strategic Threat Assessment and Response Working Group (STAR WG) was established in 2015 in order to facilitate the protection of taxpayer Personally Identifiable Information (PII) and to enhance the overall security posture of all those involved in the filing of tax returns. The initial focus (years 1 through 3) of the group was on “What” selected security features would be implemented by industry members. Starting in Year 4 (due January 2020) members will provide self-assessments focused on “How” selected security features were implemented.

The STAR WG identified 10 (see attachment) of the original set of 139 controls derived from NIST SP 800-53, Rev 4 to be reviewed as part of the Year 4 Self-Assessment. Each industry member will be asked to provide a summary narrative on how they implemented these 10 selected security controls or “Critical Controls”. The purpose of this template is described below.

Purpose:

To assist industry members (especially those with limited cybersecurity resources) in responding to the Year 4 Self-Assessment requirements, this STAR WG Year 4 Self-Assessment Template (hereafter referred to as the ‘Template’) is provided. It identifies and describes the information to be included in the submission.

The goal is to reduce the level of effort expended by members to complete this process by leveraging this template, and/or existing documentation, whether internally developed or vendor-produced, regarding system operations, maintenance or acquisition. As such, previously issued STAR WG guidance and Templates may be referenced.

Organization:

Industry members are expected to address each selected NIST identified security family (i.e., AU, RA, SA, SC and SI) in a separate section. Also, as AU-1 is listed as a separate control, please provide the member’s governing “Auditing Policies and Procedures” document. As a reminder, the STAR WG has published and distributed a Policies and Procedures Template for those members needing to organize and consolidate their existing policies and procedures. For the remaining identified NIST security families, please either provide the existing and relevant policy and procedures documents or insert relevant excerpts in the appropriate narrative sections.

The selected controls, by NIST security families, and sample draft narrative sections are provided below. Note: “XXXX” was inserted as a placeholder for member reference documents.

Audit Narrative [Addressing Year 4 critical controls AU-2(3), AU-3(1) & AU-4)]

The member narrative should address the following:

- What system components or other components are implementing the required audit capabilities?
- Is the implementation consistent with the selected controls as defined by the identified NIST guidance?
- Is the implementation performed in a manner consistent with the organization's governing policy regarding audit generation, audit retention and audit review?

Sample Narrative:

The organization uses MS Windows Server 2019, Release 10.0.13763 to implement its auditing policy. As documented in the MS Windows Server Manual (located on-line at <https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance>), the MS Windows Server 2019 has the capability and functionality to implement the selected auditing requirements.

Also, the organization attests that this system component is configured to properly enforce the organization's auditing policy defined in XXXX (see attachment).

Vulnerability Scanning [Addressing Year 4 Critical Control RA-5(1)(2)(5)]

The narrative should address the following:

- What is the automated tool performing the vulnerability scans?
- What is the process to review and resolve findings?
- Identify and describe the roles of employees designated to support this function.

[The narrative shall identify the member policy/procedure that addresses what scanning products are used, the organization's official designated to review the scans, the frequency of the scans, what information is produced by the scans and how the organization resolves any findings produced by the scans.]

Sample Narrative:

The organization uses the NISSUS Professional tool to conduct monthly scans of the entire organization's IT infrastructure. The tool is configured to scan for FISMA compliance (see on-line documentation at <https://www.tenable.com/solutions/fisma>).

One of our goals is to develop a Plan of Actions and Milestones (POA&Ms) for all findings and resolve all findings rated as "High" within thirty days. As described in the organization's related policy, all findings will be documented along with any implemented or planned mitigation actions. The official designated to accept the risk of operating our IT infrastructure is identified in our policy. In addition, all workstations, servers, network, or mobile devices shall undergo more frequent vulnerability scanning if it processes, stores or transmits/receives taxpayer information and the risk level warrants it.

Allocation of Resources (System Acquisition) [Addressing Year 4 critical control SA-2]

The narrative should address the following:

- Proof that any system component acquired to support security operations can, if necessary, support a security posture at the Moderate level of NIST SP 800-53 requirements. For instance, a product used to encrypt Taxpayer PII while stored or transmitted meets the appropriate NIST encryption standard.
- Document that resources are allocated, at the Capital Planning level, for securing Taxpayer PII. Discussion: What should be the proper document or documentation?
- Document that resources are allocated, at the line item level, for securing Taxpayer PII. Discussion: What should be the proper document or documentation?
- Possible replacement: Document that adequate resources are identified and allocated for securing Taxpayer PII.

Sample Narrative:

Prior to acquiring/purchasing IT components to host, transmit or process Taxpayer PII, the organization has a review process in place. This process requires a designated official (such as the organization's CISO) responsible for maintaining the organization's security posture to review and approve all acquisitions/purchases that impact our security posture. The expectation is the acquisition/purchase supports the organization's goal of maintaining a security posture that reflects, at least, the NIST SP 800-53 at the Moderate security level. This process is documented in our XXXX.

In terms of protecting PII, this process is used during our 'Capital Planning' activities and is documented in our XXXX document at the line item level.

System Communications [Addressing Year 4 Critical Control SC-8 (1), SC-12, SC- 28]

The narrative should address the following:

- If data is protected in transit, document how it is being protected. If it is being encrypted, identify the product and how it is configured.
- If not using encryption, please document other implemented safeguards.

- If applicable, how does the organization safeguard cryptographic keys?
- Explain how the organization protects data at rest.

Sample Narrative:

To protect Taxpayer PII, the organization limits Taxpayer PII to designated Virtual Machines (VMs) within our Windows Server infrastructure. As described in the MS documentation (see <https://docs.microsoft.com/en-us/windows-server/networking/sdn/vnet-encryption/sdn-vnet-encryption>), we enabled MS Virtual Network Encryption feature to encrypt virtual network traffic between our virtual machines containing PII that communicate with each other within subnets marked as 'Encryption Enabled.' It also utilizes Datagram Transport Layer Security (DTLS) on the virtual subnet to encrypt packets. DTLS protects against eavesdropping, tampering, and forgery by anyone with access to the physical network.

To support this installation, we:

- Installed encryption certificates on each of the SDN-enabled Hyper-V hosts.
- Used a credential object in the Network Controller to reference the thumbprint of that certificate.
- Properly configured, for each of the Virtual Networks, the subnets enforcing the required encryption.

As a note: Once encryption is enabled on a subnet, all network traffic within that subnet is encrypted automatically, in addition to any application-level encryption that may also take place. Traffic that crosses between subnets, even if marked as encrypted, is sent unencrypted automatically. Any traffic that crosses the virtual network boundary also gets sent unencrypted.

System Integrity [Addressing Year 4 Critical Control SI-5]

The narrative should address the following:

- How the organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

Sample Narrative:

To protect taxpayer PII, the organization receives information system security alerts, advisories, and directives from external sources (such as the IDTTRF ISAC and list any other sources). The ISAC provides information as it receives it. We have designated an official (someone needs to be designated to review and implement, when feasible/necessary) to review, evaluate and resolve these alerts, advisories, and directives as they are received.

Table 1 - Year 4 STAR WG Adopted Controls

Controls	Control Description	Implementation Criteria
AU-1	Audit and Accountability Policy and Procedures	AU-1
AU-2	Audit Events	AU-2 (3)
AU-3	Content of Audit Records	AU-3 (1)
AU-4	Audit Storage Capacity	AU-4
RA-5	Vulnerability Scanning	RA-5 (1) (2) (5)
SA-2	Allocation of Resources	SA-2
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)
SC-12	Cryptographic Key Establishment and Management	SC-12
SC-28	Protection of Information at Rest	SC-28
SI-5	Security Alerts, Advisories, and Directives	SI-5

Appendix C – Tax Ecosystem Selected Security Controls

NIST SP 800-53 (Rev 4)		Cybersecurity Framework
No.	Control Name	
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	AC-1
AC-2	ACCOUNT MANAGEMENT	AC-2
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7
AC-17	REMOTE ACCESS	AC-17
AC-18	WIRELESS ACCESS	AC-18
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	AT-1
AT-3	ROLE-BASED SECURITY TRAINING	AT-3
CA-5	PLAN OF ACTION AND MILESTONES	CA-5
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	PE-1
PL-4	RULES OF BEHAVIOR	PL-4
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	PS-1
PS-4	PERSONNEL TERMINATION	PS-4
SC-13	CRYPTOGRAPHIC PROTECTION	SC-13
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	SI-1
SI-2	FLAW REMEDIATION	SI-2
SI-3	MALICIOUS CODE PROTECTION	SI-3
AC-3	ACCESS ENFORCEMENT	AC-3
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	IA-1
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	IR-1
IR-6	INCIDENT REPORTING	IR-6
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	MP-1
MP-2	MEDIA ACCESS	MP-2
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	RA-1
RA-2	SECURITY CATEGORIZATION	RA-2
RA-3	RISK ASSESSMENT	RA-3
RA-5	VULNERABILITY SCANNING	RA-5
SC-7	BOUNDARY PROTECTION	SC-7
SI-4	INFORMATION SYSTEM MONITORING	SI-4
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5
AC-6	LEAST PRIVILEGE	AC-6
AT-2	SECURITY AWARENESS TRAINING	AT-2
PE-3	PHYSICAL ACCESS CONTROL	PE-3
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	SC-1
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8
SC-28	PROTECTION OF INFORMATION AT REST	SC-28
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9
IR-5	INCIDENT MONITORING	IR-5
MP-6	MEDIA SANITIZATION	MP-6
PE-6	MONITORING PHYSICAL ACCESS	PE-6

NIST SP 800-53 (Rev 4)		Cybersecurity Framework
No.	Control Name	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	PL-1
PL-2	SYSTEM SECURITY PLAN	PL-2
PS-2	POSITION RISK DESIGNATION	PS-2
PS-5	PERSONNEL TRANSFER	PS-5
CA-8	PENTRATION TESTING	CA-8
IR-8	INCIDENT RESPONSE PLAN	IR-8
MP-4	MEDIA STORAGE	MP-4
SC-18	MOBILE CODE	SC-18
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	CA-1
CA-2	SECURITY ASSESSMENTS	CA-2
CM-2	BASELINE CONFIGURATION	CM-2
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	CM-8
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	MA-1
PS-3	PERSONNEL SCREENING	PS-3
SA-8	SECURITY ENGINEERING PRINCIPLES	SA-8
AC-4	INFORMATION FLOW ENFORCEMENT	AC-4
IA-11	RE-AUTHENTICATION	IA-11
MP-5	MEDIA TRANSPORT	MP-5
MP-7	MEDIA USE	MP-7
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	PE-5
CM-7	LEAST FUNCTIONALITY	CM-7
IA-5	AUTHENTICATOR MANAGEMENT	IA-5
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8
MA-2	CONTROLLED MAINTENANCE	MA-2
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19
AC-21	INFORMATION SHARING	AC-21
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-1
AU-8	TIME STAMPS	AU-8
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9
AU-11	AUDIT RECORD RETENTION	AU-11
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	CM-1
CM-3	CONFIGURATION CHANGE CONTROL	CM-3
IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	IA-10
PE-16	DELIVERY AND REMOVAL	PE-16
PL-8	INFORMATION SECURITY ARCHITECTURE	PL-8
MA-5	MAINTENANCE PERSONNEL	MA-5
AC-5	SEPARATION OF DUTIES	AC-5
AU-2	AUDIT EVENTS	AU-2
AU-3	CONTENT OF AUDIT RECORDS	AU-3

NIST SP 800-53 (Rev 4)		Cybersecurity Framework
No.	Control Name	
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-6
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	IA-3
IA-6	AUTHENTICATOR FEEDBACK	IA-6
PS-7	THIRD-PARTY PERSONNEL SECURITY	PS-7
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	SA-9
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SA-10
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	SA-11
SA-12	SUPPLY CHAIN PROTECTION	SA-12
SA-15	DEVELOPMENT PROCESS STANDARDS AND TOOLS	SA-15
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	SA-17
CA-3	SYSTEM INTERCONNECTIONS	CA-3
AU-4	AUDIT STORAGE CAPACITY	AU-4
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	AU-5
AU-12	AUDIT GENERATION	AU-12
CM-4	SECURITY IMPACT ANALYSIS	CM-4
IA-4	IDENTIFIER MANAGEMENT	IA-4
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION	IA-9
IR-4	INCIDENT HANDLING	IR-4
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	PE-18
PS-8	PERSONNEL SANCTIONS	PS-8
SC-31	COVERT CHANNEL ANALYSIS	SC-31
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	SI-7
CM-11	USER-INSTALLED SOFTWARE	CM-11
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	AC-20
AU-7	AUDIT REDUCTION AND REPORT GENERATION	AU-7
AU-10	NON_REPUDIATION	AU-10
CA-7	CONTINUOUS MONITORING	CA-7
MA-4	NONLOCAL MAINTENANCE	MA-4
PS-6	ACCESS AGREEMENTS	PS-6
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	SA-1
SA-4	ACQUISITION PROCESS	SA-4
SA-5	INFORMATION SYSTEM DOCUMENTATION	SA-5
SA-14	CRITICALITY ANALYSIS	SA-14
PM-1	INFORMATION SECURITY PROGRAM PLAN	PM-1
PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	PM-6
PM-14	TESTING, TRAINING, AND MONITORING	PM-14
PM-16	THREAT AWARENESS PROGRAM	PM-16
CM-6	CONFIGURATION SETTINGS	CM-6
CM-9	CONFIGURATION MANAGEMENT PLAN	CM-9
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10
MA-3	MAINTENANCE TOOLS	MA-3

NIST SP 800-53 (Rev 4)		Cybersecurity Framework
No.	Control Name	
PE-20	ASSET MANAGEMENT AND TRACKING	PE-20
PM-13	INFORMATION SECURITY WORKFORCE	PM-13
PM-15	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	PM-15
IR-3	INCIDENT RESPONSE TESTING	IR-3
PE-19	INFORMATION LEAKAGE	PE-19
PM-9	RISK MANAGEMENT STRATEGY	PM-9
PM-4	PLAN OF ACTION AND MILESTONES PROCESS	PM-4
PM-8	CRITICAL INFRASTRUCTURE PLAN	PM-8
PM-12	INSIDER THREAT PROGRAM	PM-12
AC-16	SECURITY ATTRIBUTES	AC-16
PM-11	MISSION/BUSINESS PROCESS DEFINITION	PM-11
SC-5	DENIAL OF SERVICE PROTECTION	SC-5
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	CP-1
CP-2	CONTINGENCY PLAN	CP-2
SC-2	APPLICATION PARTITIONING	SC-2

Appendix D – Submission Instructions

Please contact support@taxadmin.org for a one-time link to upload the self-assessment to the secure State Exchange System.

Appendix E – Glossary

Term	Definition
Buyer	The people or organizations that consume a given product or service.
Adware	Computer advertising software that may or may not monitor computer use to target ads.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
Confidentiality	Restrictions placed on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Encrypt	To convert plain text to unintelligible text using a cryptographic algorithm.

Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Information Security	The process that ensures the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.
Intrusion Detection	The act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.
Keylogging	The action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored; often secretly downloaded by malware, keylogging enables the theft of usernames and passwords among other things.

Malware -	Refers to malicious software (malware) programs designed to damage or perform other unwanted actions on a computer system. Examples of malware are viruses, worms, Trojan horses, and spyware.
Management Safeguards	The security safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Operational Safeguards	Security for an information system that is primarily implemented and executed by people rather than by a system.
Phishing	An attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Ransomware -	A type of malicious software, or malware, designed to block access to a computer system until a ransom is paid. Ransomware is typically spread through phishing emails or by unknowingly visiting an infected website.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk	The likelihood that the unwanted impact of an incident will be realized.
Risk Assessment	The process of identifying risks and determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Management	The process of managing risks through risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process includes consideration of effectiveness, efficiency and constraints due to laws, directives, policies, or regulations.
Safeguard	Protective measures prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security and security of physical structures, areas, and devices.
Security Controls	Safeguards designed to protect the confidentiality, integrity and availability of a system and its information.
Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Social Engineering –	The manipulation of people into performing actions such as deviating from standard security practices or divulging confidential information that give attackers access to systems or confidential information.
Spear Phishing -	Phishing attempts directed at specific individuals or companies; attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the Internet today, accounting for 91% of attacks
Spyware	Software installed into an information system to gather information on individuals or organizations without their knowledge.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Supplier	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
Taxonomy	A scheme of classification.
Technical Safeguards	Controls for a system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact operations, assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
Trojan Horse	A computer program used to attack a computer system by secretly allowing, among other things, unauthorized access or alteration of data or software.
Virus	A computer program used to compromise a computer system by performing functions that may be destructive. A virus may alter other programs to include a copy of itself and execute when the host program or other executable component is executed.
Vulnerability	Weakness in a system through procedures, internal controls or implementation that could be exploited or triggered by a threat source.
Worm	A computer program used to compromise a computer system by impacting performance. A worm can travel from computer to computer across network connections replicating itself

Appendix F – References

See Federal Trade Commission, *Data Security*, <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security> (accessed October 7, 2016).

See National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, www.nist.gov/cyberframework (accessed August 20, 2019).

See NIST, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, <https://doi.org/10.6028/NIST.SP.800-53r4> (accessed August 20, 2019).

See NIST, additional cybersecurity resources: <http://csrc.nist.gov/> (accessed August 20, 2019).

See U.S. Small Business Administration SBA Learning Center, <https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses> (accessed October 7, 2016).