WHITEPAPER

IRS WISP Compliance Using RidgeBot Continuous Security Validation

Protect Taxpayer Information (PII) with Continuous Threat Exposure Management

RIDGE SECURITY

Ridge Security's RidgeBot technology can help you comply with the IRS Written Information Security Plan (WISP) requirements with its capabilities including asset discovery and inventory, vulnerability scanning, penetration testing with exploitation, and vulnerability remediation.

U.S. Federal law requires professional tax preparers—regardless of the size of the firm or the number of clients, including solo practitioners—to create and maintain a WISP.

Identity thieves are increasingly focusing on tax professionals and accountants to acquire taxpayer information to file fraudulent tax returns to gain illegal refunds. The IRS Security Summit organization enacts measures to combat tax fraud—one of its measures requires tax preparer firms and individuals to establish and maintain a WISP.

Introduction

Data thefts at tax professionals' offices are on the rise, leading to increased filing of fraudulent tax returns and other identity theft crimes.

The Internal Revenue Service (IRS) is the U.S. government department that oversees the collecting and monitoring of tax payments by businesses and individuals.

The IRS Security Summit is a public-private partnership formed in 2015 to protect taxpayers and the tax system against identity theft refund fraud. The Security Summit consists of the IRS, state tax agencies and the tax community, including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations and financial institutions.

As the series of security safeguards enacted by the IRS Security Summit makes an impact on fraud, identity thieves need ever more detailed taxpayer data to enable them to file fraudulent tax returns. These bad actors are focusing increasingly on tax practitioners, making data security a necessity for every tax professional—whether a partner in a large firm or a sole practitioner, and for every Authorized IRS e-File Provider.

IRS WISP Overview

The Gramm-Leach-Bliley Act (GLBA) of November 1999 requires financial institutions to protect customer data. Under this law, all tax and accounting professionals are considered financial institutions, regardless of size. U.S. federal law—enforced by the Federal Trade Commission (FTC)—requires professional tax preparers to implement and maintain a WISP. The first version of the WISP requirements was released in 2022, and an updated version became available in August 2024.

The GLBA law, the FTC Safeguards Rule, and IRS Publication 4557 "Safeguarding Taxpayer Data" collectively create some of the main measures ensuring the security and protection of Personally Identifiable Information (PII) data for financial firms. The FTC Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place—amongst others a WISP—to keep PII secure. In addition to developing their own safeguards, companies covered by the FTC Safeguards Rule are responsible for taking steps to ensure that their affiliates and service providers also safeguard the customer information in their care.

A WISP helps tax and accountant firms identify actions to take in the event of a security incident, data loss or theft—acting as the first line of defense in protecting taxpayer PII. individual, managing operational and technical matters requires automated technical solutions that find, report on, and help prioritize found security vulnerabilities.

WISP Requirements

There In its implementation of the GLBA law, the FTC issued several measures required to keep customer PII safe. One requirement is implementing a WISP, and as a part of the plan, the FTC requires each firm to:

1. Designate a qualified individual to coordinate its information security program.
2. Identify and assess the risks to customer PII in each relevant area of the firm's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
3. Design and implement a safeguards program, and regularly monitor and test it.
4. Select service providers that can maintain appropriate safeguards by ensuring the firm's contract with the provider(s) requires their maintaining safeguards and overseeing handling of customer PII.
5. Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.
6. Implement multi-factor authentication for any individual accessing any information system, unless the qualified individual has approved in writing the use of reasonably equivalent or more secure access controls.
7. Report a security event affecting 500 or more people to the FTC as soon as possible, but no later than 30 days from the date of discovery.

Requirement #2 entails a risk assessment for each relevant component of your firm's operations:

- Evaluating how effective current information safeguards are
- Creating an asset inventory to pinpoint potential shortcomings within those safeguards
- Understanding the landscape of data vulnerabilities within and external to the firm
- Establishing targeted risk mitigation strategies

Requirement #3 requires that analyses and tests are performed on a regular basis.

RidgeBot technology can help you to comply with both requirements #2 and #3.

A WISP is intended to be an evergreen document—it requires regular reviews and updates. To maintain compliance, security measures deployed must be periodically verified and corrected where necessary.

WISP Outline

IRS publication 5708 “Creating a Written Information Security Plan for your Tax & Accounting Practice” provides a suggested outline for a WISP. The specific areas where Ridge Security Ridgebot’s capabilities can help you comply are highlighted in the Publication 5708 outline below.

I. Define the WISP objectives, purpose, and scope

II. Designate a qualified individual

III. Assess/Identify Risks

- List types of information your office handles
- List potential areas for data loss (internal and external)
- Outline procedures to monitor and test risks

IV. Inventory Hardware

- List description and physical location of each item
- Record types of information stored or processed by each item

V. Document Safety Measures in place

a. Suggested policies to include in your WISP:

- Data collection and retention
- Data disclosure
- Network protection
- User access
- Electronic data exchange
- Wi-Fi access
- Remote access
- Connected devices
- Reportable Incidents

b. Draft Employee Code of Conduct

VI. Draft an implementation clause

VII. Attachments

Request a demonstration of
RidegeBot and see it for yourself

Implementing a WISP

- Physical Safeguards: Keep your PII data safe from physical threats
- Technical Safeguards: Ensure that your device(s) and network are not compromised
- Administrative Safeguards: Manage and train your staff

RidgeBot can help in the Technical Safeguards area, by doing a risk assessment of your firm's digital and network operations, evaluating how effective current safeguards are, creating an inventory of your digital assets, pinpointing potential shortcomings within current safeguards and providing guidelines for targeted risk mitigation strategies.

Additional Resources

WISP requirements and guidelines for implementation can be found in IRS documentation, including:

- IRS publication 5708 "Creating a Written Information Security Plan for your Tax & Accounting Practice"
- IRS Publication 5709 "How to Create a Written Information Security Plan for Data Safety"
- IRS Publication 4557 "Safeguarding Taxpayer Data"
- IRS Publication 1345 "Authorized IRS e-file Providers of Individual Income Tax Returns"
- FTC Safeguards Rule
- News release from the IRS Security Summit in August 2024 regarding WISP requirements

How RidgeBot can Help

RidgeBot is a Continuous Threat Exposure Management technology that can help with the establishment, maintenance and updating of your WISP to keep your security compliance fresh at all times, and to immediately address high-priority vulnerabilities before bad actors can exploit them to steal PII data.

RidgeBot Overview

RidgeBot is an AI agent designed to do continuous security validation. It autonomously performs tests to continuously validate your firm's cybersecurity posture and offers prioritization and remediation guidance for any vulnerabilities found.

RidgeBot's key functions can assist you in WISP compliance.

- **Asset Discovery:** Automatically discovers all types of assets on your network, including devices, applications, and websites.
- **Attack Surface Discovery:** Utilizes smart crawling techniques and fingerprint algorithms to:
  - Discover broad types of IT assets, including IPs, domains, hosts, operating systems, applications, websites, databases, and network/IoT devices
  - Discover devices that have fallen behind in operating system or security updates and patches
  - Discover new (or existing) devices connected to the network which may not be properly secured
- **Vulnerability Scanning**: Automates penetration testing and vulnerability detection. Utilizes a rich knowledge base to identify potential vulnerabilities in your discovered assets.
- **Vulnerability Detection:** Employs a proprietary payload-based testing approach, a rich knowledge-base of vulnerabilities and security breach events, and various risk modeling techniques. Discover risks of obtaining PII that doesn't have that doesn't have security measures in place.
- **Vulnerability Exploitation:** Emulates adversary attacks. Employs built-in attack techniques to launch ethical attacks against identified vulnerabilities, documenting successful exploits for further analysis and remediation. Uses multi-engine technology to simulate real-world attacks with toolkits, collecting data for further analysis in a post-breach scenario.

Request a demonstration of
RidegeBot and see it for yourself

- **Reporting and Remediation:** Provides a comprehensive report with risk assessments, remediation advice, and tools for patch verification.
- **Risk Prioritization:** Prioritizes vulnerabilities based on exploitability with remediation guidance. Automatically forms an analytical view, visualizes the kill chain, and displays a hacker's script. It shows hacking results like compromised object data and escalated privileges.

Use RidgeBot to Help Implement and Maintain IRS WISP Compliance

IRS publication 5708 "Creating a Written Information Security Plan for your Tax & Accounting Practice" provides a sample template for a WISP. The text of this template refines specific requirements.

In summary, the technically-focused requirements where RidgeBot can be helpful are stated below with references to specific extracts from template text:

III. SCOPE; A. Identify reasonably foreseeable internal and external risks to the security… RidgeBot can discover and map all the attack surfaces found in your digital assets and network.

III. SCOPE; C. Evaluate the sufficiency of existing… customer information systems, and other safeguards in place to control identified risks. A RidgeBot pentest can detect and prioritize vulnerabilities in your current assets to determine if safeguards are effective and sufficient. RidgeBot can discover risks of obtaining PII without that doesn't have security measures in place.

III. SCOPE; D. Design and implement this WISP to place safeguards to minimize those risks… RidgeBot pentest results document and prioritize vulnerabilities found along with remediation actions. Addressing the highest priority items can immediately lower your risk.

III. SCOPE; E. Regular monitoring and assessment of the effectiveness of aforementioned safeguards. RidgeBot is an automated tool that can continuously validate the security of your assets and pinpoint vulnerabilities introduced by:

- new devices connected to the network
- missing software and security updates or patches
- changes introduced by software upgrades or new installations that may affect open ports or other software attributes

IV. IDENTIFIED RESPONSIBLE OFFICIALS; Identifying all the firm's repositories of data… RidgeBot can discover and inventory all your digital assets. This assessment can be done on a regular or ongoing basis.

V. INSIDE THE FIRM RISK MITIGATION; C. …identify and document the locations where PII may be stored… a. Servers… c. PC Workstations, Laptop Computers… RidgeBot can discover and inventory all your digital assets that may store or contain PII. This assessment can be done on a regular or ongoing basis. RidgeBot can discover risks of obtaining PII without that doesn't have security measures in place.

V. INSIDE THE FIRM RISK MITIGATION; Reportable Event Policy; A. …determine if any changes in operations are required to improve the security of retained PII… RidgeBot pentest results document and prioritize vulnerabilities found along with remediation actions.

VI. OUTSIDE THE FIRM RISK MITIGATION; Network Protection Policy; A. Firewall protection, operating system security patches, and all software products shall be up to date…; B. All system security software, including anti-virus, anti-malware, and internet security, shall be up to date…; D. All computer systems will be continually monitored for unauthorized access…; E. The firm will maintain a firewall between the internet and the internal private network. This firewall will be secured and maintained by the firm's IT Service Provider. The Firewall will follow firmware/software updates per vendor recommendations for security patches. Workstations will also have a software-based firewall enabled.; F. Operating System (OS) patches and security updates will be reviewed and installed continuously. The DSC will conduct a top-down security review at least every 30 days. RidgeBot internal and external pentests can evaluate the efficacy and currency (updates and patches) of your firewall and anti-malware software and configurations. RidgeBot is an automated tool that can be run continuously or regularly, assisting in 30-day security review cycles. RidgeBot reports and documentation show vulnerability priority as well as remediation actions to address outdated software components or required patches.

VI. OUTSIDE THE FIRM RISK MITIGATION; Wi-Fi Access Policy; B. All devices with wireless capability such as printers, all-in-one copiers and printers, fax machines, and smart devices such as TVs, refrigerators, and any other devices with Smart Technology will have default factory passwords… RidgeBot can discover and map all the attack surfaces found in your digital assets and network, as well as regularly or continuously inventory all your assets.

VI. OUTSIDE THE FIRM RISK MITIGATION; Connected Devices Policy; A. Any new devices that connect to the Internal Network will undergo a thorough security review before they are added to the network… RidgeBot can discover and map all the attack surfaces found in your assets and network. New devices can be tested and verified in a sandbox environment to find and address vulnerabilities before they are deployed to your live network.

Get Access to RidgeBot Technology

If you are a Small or Midsize Enterprise (SME) firm, you may already have access to a Managed Security Service Provider (MSSP) program that can provide RidgeBot services. Smaller customers without MSSP coverage could potentially leverage professional services or consulting firms to do a periodic assessment and test.

Request a demonstration of

RidgeBot®

Designed for enterprises

RIDGE SECURITY

Ridge Security Technology Inc.

www.ridgesecurity.ai

Follow us online