SOLUTION BRIEF

IRS 1075 Compliance with Tripwire

How Tripwire Enterprise Keeps Federal Income Tax Information Safe and Secure

> "To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure."
>
> — IRS Publication 1075
>
> Tripwire Enterprise gives you out-of-the-box compliance with portions of IRS 1075 and NIST 800-53. It's that simple.

The IRS 1075 publication lays out a framework of compliance regulations to ensure federal tax information (FTI) is treated with adequate security provisioning to protect its confidentiality. This may sound simple enough, but IRS 1075 puts forth a complex set of managerial, operational and technical security controls you must continuously follow in order to maintain ongoing compliance.

Any organization that handles FTI is beholden to comply with IRS 1075 regulations in order to avoid being saddled with a substantial fine. But crossing your compliance "T"s and dotting your cybersecurity "I"s is prohibitively time-consuming without an automated solution to take care of it for you.

IRS 1075 is comprised of the following sections:

- Introduction
- Federal Tax Information and Reviews
- Recordkeeping Requirement: IRC 6103(p)(4)(A)
- Secure Storage: IRC 6103(p)(4)(B)
- Restricting Access: IRC 6103(p)(4)(C)
- Other Safeguards: IRC 6103(p)(4)(D)
- Reporting Requirements: IRC 6103(p)(4)(E)
- Disposing of FTI: IRC 6103(p)(4)(F)
- Computer System Security
- Reporting Improper Inspections or Disclosures
- Disclosure to Other Persons
- Return Information in Statistical Report

Who Needs to Comply?

Any organization or agency that receives FTI needs to prove that they're

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

protecting that data properly with IRS 1075 compliance. Federal, state, county and local entities—as well as the contractors they employ—are all within its scope. And FTI doesn't just come from the IRS itself, either. The Social Security Administration, Federal Office of Child Support Enforcement, Bureau of Fiscal Service and Centers for Medicare and Medicaid Services may also furnish FTI data that must be protected.

Tripwire® Enterprise offers out of the box support for IRS 1075. The hardening guidelines supported by Tripwire for IRS 1075 include MS Windows server platforms (2003–2016), Windows desktops, VMware ESXi, RHEL, AIX and more.

IRS 1075 Requirements

IRS 1075 requires organizations and agencies to protect FTI using core cybersecurity best practices like file integrity monitoring (FIM) and security configuration management (SCM). Both of these technologies depend upon a known, secure baseline. Any deviations from this baseline signal authorized or unauthorized changes that bring your systems out of compliance or expose them to attacks.

IRS 1075 requires organizations and agencies to "… develop, document, and maintain under configuration control, a current baseline configuration of the information system." Agencies are then required to review and update that baseline at least annually, as well as anytime a system upgrade or patch becomes available.

According to IRS 1075, all organizations and agencies that handle FTI must do the following:

- » Determine the types of changes to the information system that are configuration controlled
- » Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses
- » Document configuration change decisions associated with the information system
- » Implement approved configuration-controlled changes to the information system
- » Retain records of configuration-controlled changes to the information system for the life of the system
- » Audit and review activities associated with configuration-controlled changes to the information system
- » Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur
- » Test, validate and document changes to the information system before implementing the changes on the operational system

IRS 1075 Compliance with Tripwire Enterprise

Tripwire Enterprise, an enterprise-class FIM and SCM solution, directly fulfills the above IRS 1075 requirements. Rest easy knowing this piece of IRS 1075 compliance is automated and that any changes that take you away from your secure baseline can be brought to your attention quickly. Tripwire Enterprise makes IRS 1075 compliance even less of a hassle by ensuring the configured state matches the hardening guidelines of IRS 1075 and allowing for waivers when your organization cannot meet those guidelines. Waivers signal to an auditor that a business justification and mitigation plan exist for failed policy tests.

One of Tripwire Enterprise's most fundamental capabilities is establishing a secure baseline configuration for your system and tracking all changes against that baseline. That's the core value of FIM combined with SCM. Tripwire Enterprise ensures the integrity of your files and systems, and keeps a record of all historical changes that take place and producing audit-ready reports to make proof of compliance easier.

> "An unauthorized disclosure has occurred when FTI is knowingly or due to gross negligence provided to an individual who does not have the statutory right to have access to it under the IRC."
>
> — IRS Publication 1075

Tripwire Enterprise also integrates with the following:

- » Systems of record such as ServiceNow, Cherwell, Jira and Remedy
- » Tripwire Event Sender, for exporting rich change data to SIEMs like QRadar and Splunk
- » Governance, Risk, Compliance (GRC) frameworks

These capabilities are important for a number of reasons:

- » Planned changes are often documented in a system of record such as ServiceNow. But proving that only the expected changes happened is difficult without a tool like Tripwire Enterprise in place to confirm expected changes and to report on unexpected ones.
- » Organizations often use a SIEM in their SOC (Security Operations Center) as the single pane of glass representing potential security incidents. Tripwire's change data and security state data often play a role in identifying and mitigating security incidents.
- » GRC tools are often used to consolidate and report on cybersecurity data like that provided by Tripwire Enterprise. Integration shortens the time-to-value provided by the GRC.

Tripwire Policy Manager supports over 1,000 policy combinations across all verticals and regulatory bodies, making compliance one less thing your teams need to stress over. Tripwire's dedicated policy team ensures that any new additions to regulatory frameworks are rapidly updated. By automatically tracking policy drift and making proof of compliance a given, Tripwire Enterprise provides significant cost savings while mitigating compliance risk.

Risks of Noncompliance

The repercussions of being found noncompliant with IRS 1075 are severe, so it's not worth the risk to put off compliance efforts. As is often the case, meeting these compliance criteria help you align with other compliance frameworks as well. For example, IRS 1075 is largely derived from NIST 800-53, meaning that meeting IRS 1075 compliance automatically aligns your systems more closely with NIST guidelines.

Criminal penalties and fines

As IRS 1075 is all about protecting FTI, it also includes codes that prescribe serious repercussions if FTI isn't properly safeguarded. Certain codes within IRS 1075 come with their own penalties. IRS Code 7213 states that it's a felony offense to disclose federal returns and the information they contain. IRS Code 7213A makes any unauthorized inspection of FTI—even accidental—a misdemeanor. It also explains that you can be fined $1,000 for each act of FTI disclosure, a sum that adds up quickly for organizations that handle large volumes of this data. In addition, it gives taxpayers the right to bring civil action against any organization that doesn't protect their information.

Summary

If your organization or agency handles federal income tax information of any sort, you are required to stay in compliance with IRS 1075. Failure to do so can lead to heavy fines and even criminal charges, but Tripwire technology makes ongoing compliance simple and keeps you audit-ready at all points in time.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc