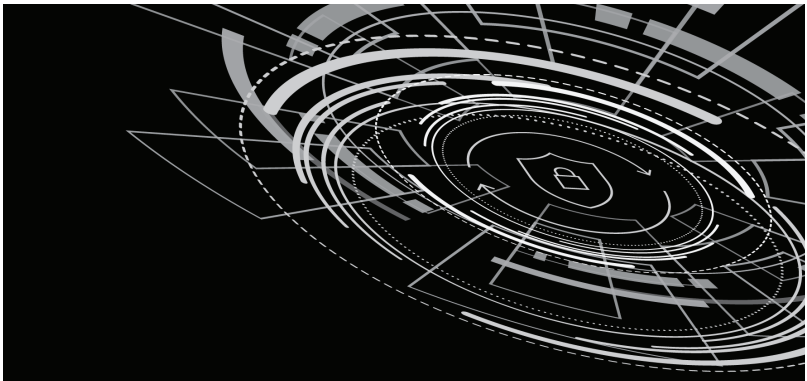
CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity
With Compliance To Defend Your Business
From Invisible Cyber Predators

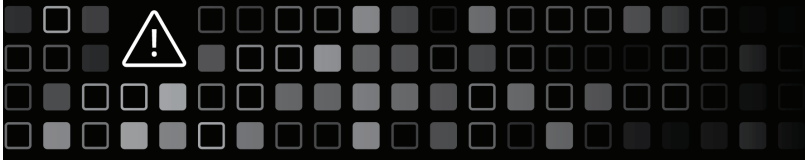
ANDREW D. RAMSEY

FEATURING CYBERSECURITY
EXPERTS FROM AROUND THE WORLD



CYBERSECURITY:
THE SILENT BATTLEFIELD

Leverage The Power Of Cybersecurity With Compliance To Defend Your Business From Invisible Cyber Predators



FEATURING CYBERSECURITY EXPERTS FROM AROUND THE WORLD

BigRedMedia
a TMT company

Nashville, Tennessee

Chapter 13:
Deciphering IRS 1075: Navigating Compliance Requirements

Andrew D. Ramsey
CEO and owner of Precision Solution Group

Compliance never seems easy. And when it's for the federal government, namely the Internal Revenue Service, well, the level of difficulty goes to a whole new level. And that's precisely the case with IRS 1075 Safeguards.

As an MSP and MSSP working in compliance, interacting with several types of sensitive government data on networks, I follow NIST SP 800-53, a comprehensive set of privacy and security controls that protect federal information systems. IRS Publication 1075 is a synopsis of 800-53. It's kind of like CliffsNotes. But you need to look at all the thousands of settings involved, depending on what technology you are utilizing.

Achieving IRS 1075 compliance now makes 800-53 look like child's play. If you handle Federal Tax Information (FTI) and you have to meet these requirements, have you even read Publication 1075? It's 216 pages long! And, as you drill down into those 216 pages, there are thousands of pages with even more information you need to know

and comply with. You have an agency or business to run, and keeping up with or even understanding the controls is probably more than you want to handle. Don't worry—there are people out there like me who specialize in this type of compliance, so you don't have to be an expert. But first, let's unravel the mysteries of IRS 1075.

What The Heck Is It And Who Has To Comply?

People who file and pay taxes want to feel confident that the personal and financial information they pass along to the IRS is protected. I mean, if it weren't, we'd all just stop paying our taxes, and Uncle Sam doesn't want that to happen. So, the IRS came up with Publication 1075, a set of regulatory guidelines for U.S. government agencies and their agents, to protect Federal Tax Information. Publication 1075 provides detailed requirements for safeguarding FTI received from the IRS or a secondary source that originates from the IRS. It outlines specific controls and security measures that must be implemented to protect FTI from unauthorized access, disclosure, or misuse. This includes physical security, system security, and administrative controls. Information security management is a fundamental component of IRS 1075, and it provides guidelines for managing risks associated with storing, processing, and transmitting FTI, including access controls, encryption standards, audit logs, and incident response protocols. In all, hundreds of security and privacy controls must be implemented under IRS 1075. And hundreds of sub-controls under those.

FTI Defined

So, when we talk about Federal Tax Information, you might wonder what all that entails. Here is how IRS Publication 1075 defines FTI:

- *FTI is categorized as Sensitive But Unclassified (SBU) information and may contain Personally Identifiable Information (PII).*
- *FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as the Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement.*
- *FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.*
- *FTI may not be masked to change the character of information to circumvent IRC § 6103 confidentiality requirements.*

And when we talk about FTI, we're also talking about personally identifiable information, which may include the name of the person(s) filing the return, taxpayer mailing address, taxpayer identification number, email addresses, phone numbers, Social Security numbers, bank account numbers, date and place of birth, mother's maiden name, biometric data (e.g., height, weight, eye color, fingerprints), or any combination of these items. It's all a gold mine for a cyberattacker!

Now that you know what it is, are you required to comply?

If you are a federal agency that receives, stores, processes, or transmits FTI, yes. If you are a state or local government agency accessing FTI, then yes. That includes departments of revenue, social services, and child support enforcement. If you are a contractor or vendor who works with government agencies and handles FTI, yes. This includes IT service providers, like me, data storage companies, and other third-party vendors. Also, some nongovernment organizations have access to FTI through their contracts with federal and state agencies that also need to comply. Basically, if you touch FTI, you must comply!

At my firm, we work with a lot of special councils, which are third-party law offices that work for the State of Ohio's Attorney General's Office, handling collections for the State of Ohio government agencies. Say someone in Ohio owes the state $10,000. The AG's office gets the federal tax info from the feds and may utilize that information for their collection efforts. However, they have a very small in-house collection unit, so they turn around and farm it out to the special councils. All three entities manage FTI. All three are subject to IRS 1075, and all three are subject to IRS 1075 Safeguards audits.

Not Your Basic Cyber Security

At its core, IRS 1075 requires organizations to use essential cybersecurity best practices to keep FTI confidential. Remember at the beginning of the chapter when I said that achieving IRS 1075 makes NIST SP 800-53 look like child's play? While IRS 1075 is based on the same set of security standards as NIST SP 800-53, Publication 1075 isn't completely identical. It's a combination of several other NIST standards like zero trust and Federal Information Processing Standard 140 (FIPS 140) encryption requirements, which is a topic for another day. But you get the point. It's like cybersecurity on steroids.

Let's take a look at six of the key sections of IRS Publication 1075.

1. **Record Keeping:** Any agency receiving FTI is required to establish a permanent and secure record-keeping system. It has to include internal and external requests and be able to identify and track the location of electronic and nonelectronic FTI from receipt or creation until it is destroyed.
2. **Secure Storage:** Any physical or digital location where tax information is kept must be protected from unauthorized access. This includes using locked cabinets or secure rooms for paper records and encrypted drives or secure servers for digital data. The goal is to ensure that only authorized individuals can access the information, keeping it safe from theft, loss, or accidental exposure.
3. **Access Controls:** IRS 1075 requires strict measures to control who has access to FTI. These include user authentication, role-based access, and the principle of least privilege, ensuring that only authorized personnel can access sensitive information.
4. **Reporting:** A Plan of Action and Milestones (POA&M) and Corrective Action Plan (CAP) must be periodically created and sent to your IRS point of contact for an internal review or, in our case, the Ohio Attorney General's Office.
5. **Disposal:** Once your agency is finished with the data, both physical and electronic forms of FTI must be destroyed or disposed of properly by burning, shredding, or following DoD standards in accordance with IRS 1075 guidelines.
6. **Training:** Education for employees, contractors, and subcontractors is critical to properly protecting FTI. The IRS 1075 guidelines outline training in disclosure awareness, security and privacy awareness, role-based training, contingency training, incident

response training, and insider threat awareness training. There is an initial certification and an ongoing annual certification.

The Journey To IRS 1075 Compliance In 5 Steps

There is no definitive answer to how long it takes to become IRS 1075 compliant because it depends on various factors, like the current state of your security environment, the number and complexity of the security controls you need to implement, the availability and cooperation of your staff and stakeholders, and the frequency and intensity of the IRS audits and reviews. But here is an overview of the process:

- **Step 1: Establish A Safeguards Program.** This formal document outlines how your organization will protect FTI and comply with the IRS Safeguards 1075 compliance standards. It should include the roles and responsibilities of your staff, the security policies and procedures you will follow, the security controls you will implement, and the security training and awareness you will provide.
- **Step 2: Conduct A Safeguards Review.** This is an assessment not only for you, your IT support, and your compliance provider, but it will also be reviewed by the IRS and Ohio Attorney General's Office to evaluate your current security posture and identify any gaps or weaknesses that need to be addressed to meet the IRS Safeguards 1075 compliance standards. You should use the IRS Safeguards Review Checklist and the IRS Safeguards Security Report Template to guide you through this process.
- **Step 3: Implement The Safeguards Recommendations.** This is the CAP that details how you will remediate the findings and recommendations from the Safeguards review. You should prioritize the most critical and urgent issues and document your progress and evidence of compliance.

- **Step 4: Submit The Safeguards Security Report.** This final report summarizes your Safeguards program, your Safeguards review results, and your Safeguards recommendations implementation status. You should submit this report to the IRS Safeguards Office or the Ohio Attorney General's office within 90 days of receiving FTI or annually thereafter. However, this can be more frequent based on many factors, such as whether you received the FTI from the IRS directly or from the Ohio Attorney General's Office.
- **Step 5: Prepare For The IRS Safeguards Audit.** This is your POA&M, the external audit that verifies your compliance with the IRS Safeguards 1075 compliance standards. You should cooperate with the IRS Safeguards auditors and provide them with the necessary documentation and access to your systems and networks. You should also address any findings and recommendations from the audit and submit a Corrective Action Plan (CAP) to the IRS Safeguards Office or, in our case, the Ohio Attorney General's Office.

Slap On The Wrist? Maybe Not

Maybe you're thinking, what's the harm in a tiny slipup if a couple of records fall through the cracks? Well, the IRS doesn't take it lightly. In fact, if you fail to comply with any of Publication 1075's FTI requirements, you could be looking at monetary fines and criminal penalties, including prison time. Additionally, you could face civil charges by taxpayers once they're notified that a criminal indictment or an unauthorized inspection or disclosure has occurred. How, you ask, will the IRS know? Audits.

Are You Upholding Your End Of The FTI Bargain?

An IRS 1075 audit is how the IRS assesses your business's compliance with the security guidelines for protecting FTI, as outlined in the 1075 Publication. The purpose of the audit is to prove that 1) you are meeting the required standards of IRS 1075, 2) you are committed to a secure data environment, 3) you appreciate the sensitivity of the data and want to maintain the public's trust, and 4) you are dedicated to your business's operational resilience. That's what the IRS wants to know. And here are two crucial things you need to know: Passing the audit means you can keep providing services. Failing the audit could mean no more access to FTI until you can pass the next audit, as well as forfeiture of the FTI you already have. *It's hard to get it back!*

IRS 1075 audits typically happen annually but could occur randomly. I could write an entire chapter just on the IRS 1075 audit process. But that's a chapter for another day. I'll just hit the high notes here.

1. **Preaudit Preparation**
    - *Self-Assessment:* You'll want to conduct an internal audit against the IRS 1075 requirements to help you understand your system's current security posture and identify any gaps.
    - *Documentation Review:* You'll need to prepare and provide documentation demonstrating compliance with the security and privacy requirements. This includes policies, procedures, and other relevant documentation.
2. **Audit Process**
    - *Entrance Conference:* The audit begins with an entrance conference, during which the IRS and/or agency from which

you received the FTI explains the audit scope, objectives, and procedures.

- *Review Of Policies And Procedures:* Auditors will review your policies, procedures, and practices related to the handling, storage, transmission, and destruction of FTI.
- *Physical Security Inspection:* Auditors will examine the physical security measures you have put in place to protect FTI, including access controls, security cameras, and locked storage areas.
- *Technical Security Controls:* The audit will assess the technical controls you use to protect FTI, including encryption, access controls, logging, and monitoring.
- *Employee Training And Awareness:* They'll evaluate your training programs and ensure that your employees understand their responsibilities for safeguarding FTI.
- *Incident Response:* Auditors will review your organization's incident response procedures, including how you handle security breaches involving FTI.
- *Interviews:* Auditors may interview key personnel to verify compliance and an understanding of FTI protection requirements.

3. **Audit Findings And Report**
    - *Exit Conference:* After the audit, the IRS and/or state agency will hold an exit conference to discuss the preliminary findings and potential areas of noncompliance.
    - *Audit Report:* The IRS and/or state agency will issue a formal audit report detailing any findings, recommendations, and required corrective actions.

- *Corrective Action Plan:* If you were found to be noncompliant, you have to submit a CAP outlining how you will address the issues identified in the audit.

4. **Follow-Up**
   - *Follow-Up Audits:* The IRS or state agency may conduct follow-up audits to ensure you have implemented the corrective actions and are maintaining compliance with Publication 1075 requirements.
5. **Ongoing Compliance**
   - *Continuous Monitoring:* It's never a one-and-done. You're expected to continuously monitor and update your security and privacy controls to maintain compliance.
   - *Annual Review:* You'll need to conduct an annual review of your compliance with IRS 1075 and report any significant changes to the IRS.

What's the best way to ensure a successful Publication 1075 Audit? Work with an expert.

Outsource Your IRS 1075 Compliance… But To Who?

Maintaining 1075 compliance is not just cybersecurity as usual. Remember, Publication 1075 is 216 pages long, with nearly 190 security and privacy controls to implement. Partnering with an expert MSP and MSSP to navigate IRS 1075 requirements can help you sleep at night. However, not just any old MSP or MSSP will do.

Staying compliant and protecting FTI can take hundreds of hours. And while many MSPs and MSSPs are great at basic cybersecurity and

protecting your IT infrastructure, IRS 1075 requires higher security acumen and expertise from someone with extensive experience and knowledge in not just cybersecurity but also compliance.

As you are looking for a compliance partner, there is one other very important thing to remember outside of expertise. You want the best, not the cheapest.

When it comes to third-party IT partnerships, many businesses are driven by price instead of looking at the big picture. If an MSP or MSSP charges you half the price of another provider for IRS 1075 compliance, it's because they're only doing half of what should be done. You need to ask these questions: Why? And what am I not getting?

With IRS 1075, there is a paper component and a technical component to compliance. Maybe the provider charging half-price only handles the paper documentation or the technical side. That means you're outsourcing the other side to another vendor or multiple vendors. Or worse, not doing it at all. So, now you're getting a bill from two vendors or maybe more.

What else are you not getting with the cheaper price? Is the software required by the IRS included in the bargain-basement fee schedule? What about hardware? What happens if you go over the allotted support hours and need help? Does this vendor have the capability of automating the IRS 1075 compliance requirements? The takeaway is that you need an MSP and MSSP with a one-stop-shop support platform. While they're keeping you IRS 1075 compliant, the MSP or MSSP across the street is too busy nickel-and-diming you. How much

time are you spending managing all those vendors? Time is money and the only resource you can't create more of!

Something else you want to consider when choosing an MSP or MSSP for your IRS 1075 compliance: How many times have they been audited, and what were your scores? I can tell you that I have participated in over 50 Ohio Attorney General compliance audits. And we've been requested by the Ohio AG to participate and represent the Special Counsel community in every scheduled IRS 1075 compliance audit performed by the Federal IRS Auditors since 2013. Why? Because we have delivered a perfect scores on several compliance Safeguards Computer Security Evaluations across several audits.

With your agency or business's livelihood resting on being able to process FTI, it's just not worth it to cut corners. Sure, you can drive without car insurance and save money until you get into an accident and find yourself not covered or under covered. But why would you?

Conclusion

As I said before, IRS 1075 compliance isn't easy, and you don't want an MSP or MSSP who just dabbles in it to be your guy (or girl) because that actually puts more work back on you in the long run. Work with someone who specializes in IRS 1075 compliance, with a proven process, a good track record for audits, and a reasonable time frame to compliance so you can meet your contractual requirements—and contract someone reputable and responsive. IRS 1075 compliance isn't something you or a third-party provider can do overnight. It's a serious, painstaking business where the consequences are high. This is no time to penny-pinch!

About Andrew D. Ramsey

Andrew D. Ramsey is the CEO and owner of Precision Solution Group (PSG). The Columbus, Ohio-based IT firm was founded in 2002 to provide a one-stop shop and flexible managed IT services to small and medium-sized Ohio businesses. For over 20 years, Andrew has gained extensive knowledge and experience in the cybersecurity and compliance arenas, including IRS Publication 1075, HIPAA/HITECH, PCI, and SOC 2 standards, to mention just a few.

Growing up in Ohio, Andrew had a very modest upbringing, and his family was constantly moving. He didn't complete a single year at the same school until high school. On his own and providing for himself since he was 18, he was driven to succeed. His grandfather impressed upon him the importance of hard work, focus, and logic-based decision-making skills, which helped shape him into the determined, successful entrepreneur he is today.

Andrew graduated from DeVry Institute of Technology (now DeVry University) with a bachelor's in business administration. Applying his degree, talent, and "true calling" for designing, building, and implementing technology, Andrew began his career with companies such as Clark Refining, Nationwide Insurance, and Scotts. This enabled him to travel throughout Europe, Canada, and the United States. While at Scotts, Andrew launched Precision Solution Group and obtained a law firm as his first client.

Today, Andrew has grown PSG into one of Ohio's most successful and reliable IT firms, serving clients with five to 500 workstations, as well as Fortune 500 firms. His firm has become a household name within Ohio's special counsel law firm market and serves clients in the general legal markets, health care, manufacturing, financial institutions, accounting, and nonprofits.

With more than 14 years of compliance experience, Andrew understands the complexities, nuances, and time involved in managing a successful compliance program. It's what sets Precision Solution Group apart from other MSPs and MSSPs. Their team of experts is a leading IRS Safeguards 1075 compliance vendor in Ohio, participating in over 50 compliance audits for the Ohio Attorney General's Office and delivering scores of 100 on multiple compliance Safeguards Computer Security Evaluations Matrixes (SCSEMs) across several audits for their clients. Andrew's goal as an IT provider is to be a trusted partner to his clients with a one-stop-shop firm with cutting-edge technology solutions that empower and protect businesses across the State of Ohio.

As CEO and owner of Precision Solution Group, Andrew stays ahead of the compliance curve to ensure his entire firm delivers the right technology and knowledge to his clients to make their compliance journeys successful. As compliance rules evolve, PSG is in the know. With cyberattacks increasing in sophistication and frequency, one breach could interrupt operations or bring measurable financial losses. For these reasons, Andrew has made cybersecurity a core focus to help businesses maintain best cyber practices and protect the confidentiality and integrity of sensitive data, including federal tax and personally identifiable information.

When Andrew is away from the office, he enjoys spending time with friends and family and watching any John Wayne and Clint Eastwood movies he can find.

For more information, contact Andrew D. Ramsey at Precision Solution Group:
Phone: 614-465-3932
LinkedIn: linkedin.com/in/andrew-ramsey-92111a1
Email: andrew.ramsey@precisionsolution.com
Web: precisionsolution.com

CYBERSECURITY:
THE SILENT BATTLEFIELD

ABOUT ANDREW D. RAMSEY

Andrew D. Ramsey is the CEO and owner of Precision Solution Group (PSG), a leading Columbus, Ohio-based IT firm he founded in 2002. With over 20 years of experience in cybersecurity and compliance, Andrew has built PSG into a trusted provider for businesses across Ohio, specializing in IRS Publication 1075, HIPAA/HITECH, PCI, and SOC 2 compliance.

Growing up in Ohio, Andrew's upbringing was modest, with frequent moves that made adaptability essential. On his own since 18, he was driven to succeed, guided by his grandfather's lessons on hard work and logical decision-making. He earned a bachelor's in business administration from DeVry University and began his career at companies like Clark Refining, Nationwide Insurance, and Scotts, which took him across Europe, Canada, and the U.S. While at Scotts, he launched PSG, securing a law firm as his first client.

Today, PSG serves businesses with five to 500 workstations, including Fortune 500 firms, and has become a household name in Ohio's special counsel law firm market. The company also supports clients in healthcare, manufacturing, finance, accounting, and nonprofits. Andrew's deep compliance expertise sets PSG apart, making it Ohio's leading IRS Safeguards 1075 compliance vendor. His team has participated in over 50 compliance audits for the Ohio Attorney General's Office, earning perfect scores on multiple Safeguards Computer Security Evaluations Matrixes (SCSEMs).

Andrew is committed to keeping PSG at the forefront of cybersecurity and compliance, ensuring clients are protected against evolving cyber threats. He believes in being a trusted partner, delivering cutting-edge solutions that safeguard sensitive data and keep businesses secure.

Outside of work, Andrew enjoys spending time with friends and family and watching classic John Wayne and Clint Eastwood movies.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company