Office of Safeguards

New Publication 1075:

September 2021 Revision

September 2021 Office Hour Call

Agenda

- Overview & General Updates
- Updates By Area
  - FTI, Review, and Other Requirements
  - Physical Security Requirements
  - Cybersecurity Requirements
  - NIST 800-53 Security and Privacy Controls
- Next Steps
- Q&A

Overview

Highlights for September 2021 Revision

- There are **86** highlighted changes
- This publication revises and supersedes Publication 1075 (November 2016) will be effective approximately 6 months after publication
- Have feedback? Email comments to SafeguardReports@irs.gov, using "Publication 1075 comment/feedback" in the subject line

Pub. 1075

2016 Version

Introduction - FTI – Reviews

Recordkeeping

Secure Storage

Restricting Access

Training/Internal Inspections/Disclosure Awareness

Reporting Requirements

Disposal

Computer Security

General

Disclosure to Others

Return information in Statistical Reports

2021 Version

1. Federal Tax Information, Reviews and Other Requirements
2. Physical Security Requirements
3. Cybersecurity Requirements
4. NIST 800-53 Security and Privacy Controls

Review Types

On-Site Review **–**

Safeguard Staff conducts an on-site evaluation of the security and privacy controls implemented by the agency and all supporting parties.

Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.

Remote Review **–**

Safeguard Staff conducts a remote evaluation of the security and privacy controls implemented by the agency using secured collaborative technologies (for example screen-sharing capabilities, teleconferences, video enabled software, etc.)

Hybrid Review **–**

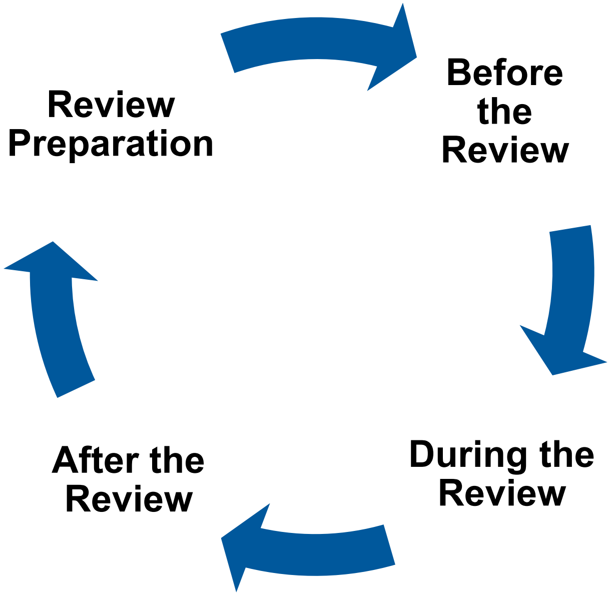
leverages a hybrid of both on-site and remote reviews. Reduces the IRS footprint during the on-site review and includes improved efficiency of the review workflow by enabling data collection to occur pre-visit and during on-site visit

Safeguard Reviews

Before the Review – Engagement (Notification) Letter, Other information request, what type of review (on-site or remote, PSE call)

During the Review – Employee Interviews, Facility Tours, Document Review, Automated and Manual testing, Closing conference

After the Review – Safeguard Review Report and Corrective Action Plan.



Federal Tax Information Logs

FTI Log									
Date Requested	Date Received	Taxpayer Identifier	Tax Year(s)	Type of Information	Reason for Request	Exact Location	Who has access?	Disposition Date	Disposition Method

FTI Bulk Transfer Log								
Date Received	Control Number/File Name	Content (do not include FTI)	Recipient/Title Location	Number of Records	Movement Date	Recipient/Title Location	Disposition Date	Disposition Method

Visitor Access Log

Date	Name & Org of Visitor	Form of Visitor ID	Purpose of Visit	Name & Org of Person Visited	Time of Entry	Time of Departure	Signature of Visitor

Language in the new Publication 1075 says log **must** include the above information, must be closed out at the end of each month and retained for 5 years.

Minimum Protection Standards (MPS)

Multifunction Devices (MFDs) or High-Volume Printers must be locked with a mechanism to prevent physical access to the hard disk or meet MPS.

Policies and Procedures

- Alternate Work Site
- FTI Disposal/Destruction
- Disclosure Awareness
- Access Control
- Fax Policy
- Email Policy
- Media Protection
- Personnel Security
- Access Control
- Background Investigation
- Physical and Environmental

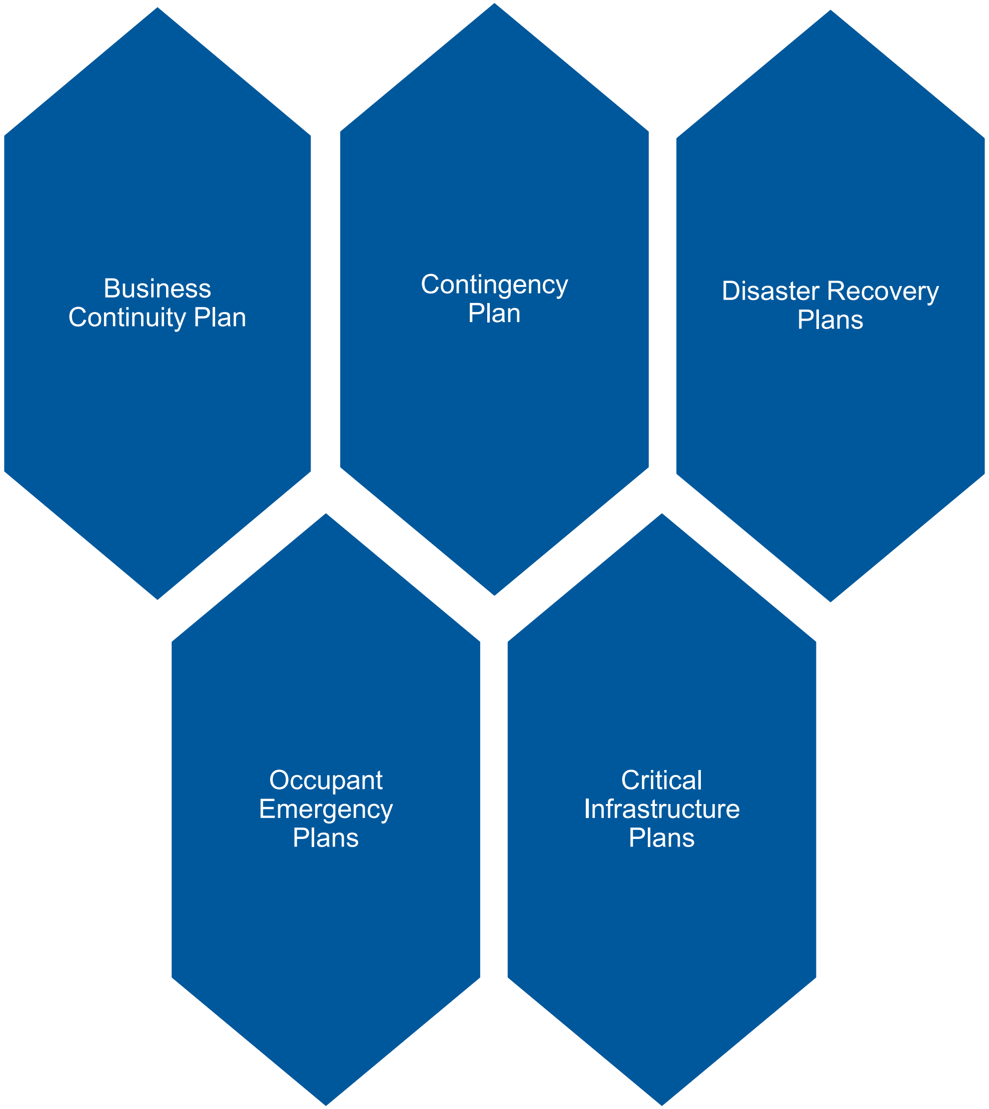
Both Policy and Procedures must be updated every 3 years.

Incident Response Procedures

Must test the incident response capability annually using tabletop exercises

Must track and document system security and privacy incidents

Must notify TIGTA and IRS immediately, but no later than 24 hours of discovery of disclosure or breach



Business Continuity Plan

Contingency Plan

Disaster Recovery Plans

Occupant Emergency Plans

Critical Infrastructure Plans

Background Investigation Minimum Requirements

- **Reinvestigation requirements have been changed from being conducted every 10 years to every 5 years.**
  - Requires Fingerprinting
  - Local Law Checks
  - Citizenship/Residency Status

Disclosure Awareness Training

Disclosure awareness training (including role-based training) must provide personnel who have access to FTI with initial and annual training on:

- Organizational authority for receiving FTI
- Authorized uses of FTI
- Disclosure of FTI with external parties only when authorized
- Consequences of unauthorized access, use or disclosure of FTI

Employees, contractors and subcontractors must be advised of the penalty provisions of IRC §§ 7431, 7213, and 7213A

Agencies must make employees, contractors and subcontractors aware that disclosure restrictions and penalties apply even after employment and contract with the agency has ended.

Cybersecurity Updates

Emphasizes on **privacy**, **expanded the security controls catalog** addressing the need for more proactive and systematic approach to cybersecurity. Two new control families: (PT) Personally Identifiable Information Processing and Transparency, (SR) Supply Chain Risk Management.

- Security controls cover management, operational and technical actions that are designed to deter, delay, detect, deny malicious attacks.

- Restructures the **new security controls** to be new outcome-based and shifted away from implementation

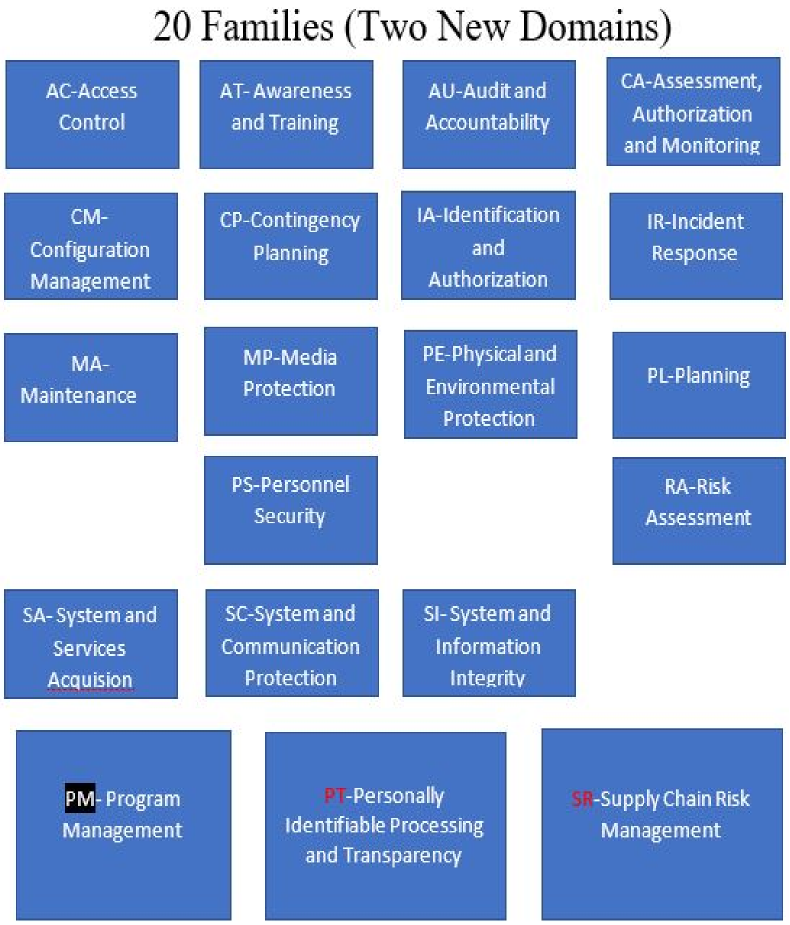
  - Updates the **Information Flow Enforcement** (AC-4) process

    – Former Pub 1075

    ➢ The information system must enforce approved authorization for controlling the flow of FTI within the system and between interconnected systems based on the technical Safeguards in place to protect FTI

    – New Pub 1075

    ➢ Enforce approved authorization for controlling the flow of information within the system and between interconnected systems based on the technical safeguards in place to protect FTI



20 Families (Two New Domains)

AC-Access Control

AT- Awareness and Training

AU-Audit and Accountability

CA-Assessment, Authorization and Monitoring

CM-Configuration Management

CP-Contingency Planning

IA-Identification and Authorization

IR-Incident Response

MA-Maintenance

MP-Media Protection

PE-Physical and Environmental Protection

PL-Planning

PS-Personnel Security

RA-Risk Assessment

SA- System and Services Acquision

SC-System and Communication Protection

SI- System and Information Integrity

PM- Program Management

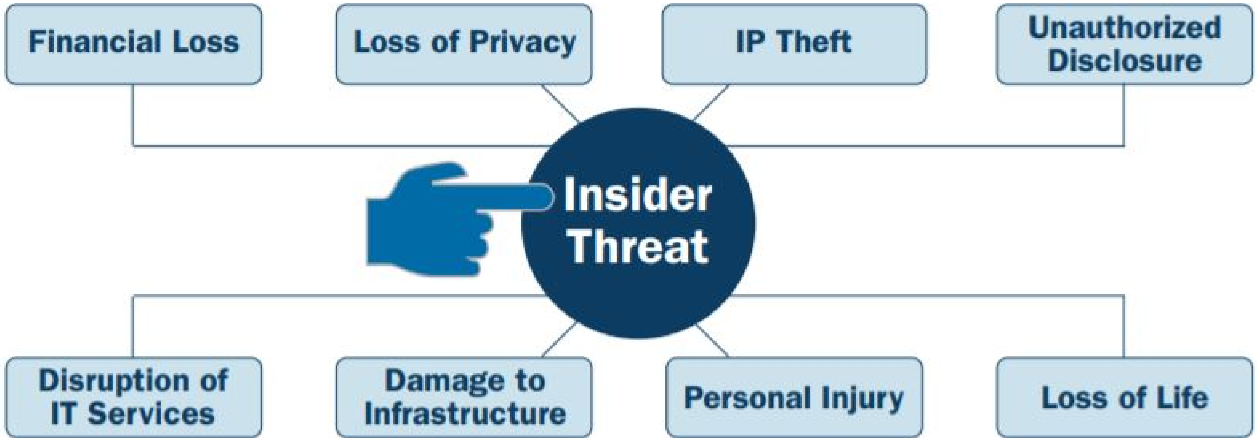
PT-Personally Identifiable Processing and Transparency

SR-Supply Chain Risk Management

Cybersecurity Updates

4.13 Program Management

- PM-12 Insider Threat Program
  - Implement an insider threat program that includes a cross-discipline insider threat incident handling team.



4.8 Incident Response

- CE-6 Insider Threats: Implement an incident handling capability for incidents involving insider threats

Cybersecurity Updates

4.2 AT-2: Awareness and Training

- Agency must include practical exercises in awareness training that simulate security and privacy incidents
- (CE-1) Practical Exercises
  - Practical exercises may include, for example, no-notice social engineering
  - IRS-Defined: Conduct phishing email simulation exercises on at least a quarterly basis.

Cybersecurity Updates

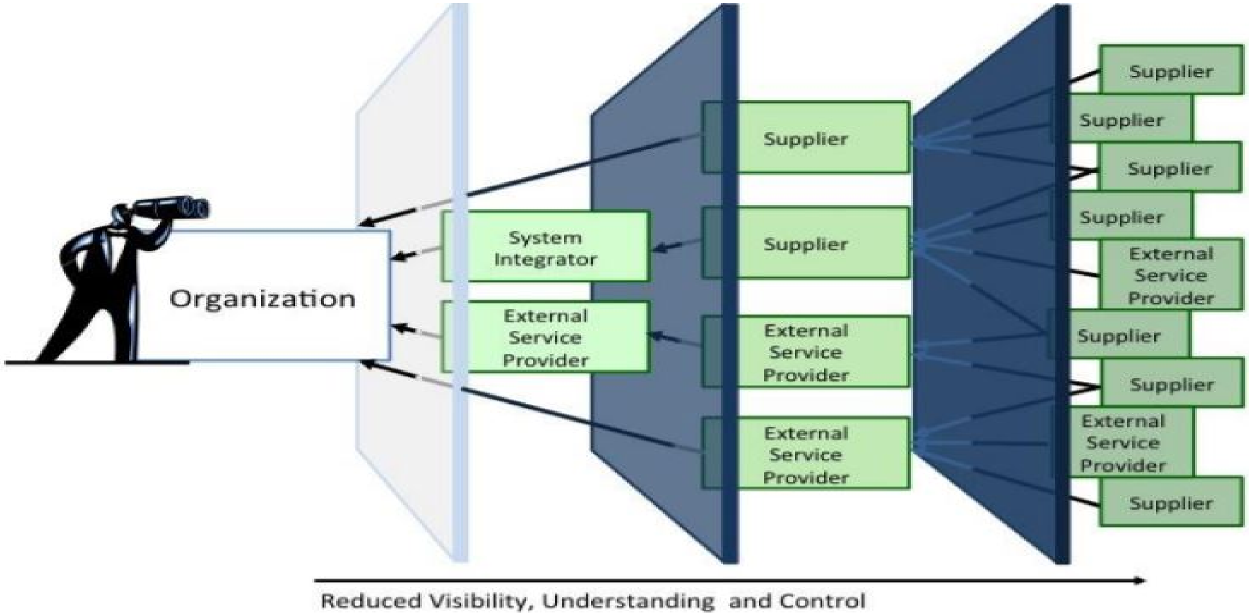
4.2 AT-2: Awareness and Training

- CE-3 Social Engineering and Mining
  - Provides literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.
  - According to the 2021 Verizon's Data Breach Investigation Report (DBIR), it was found that 85 percent of breaches involved a human element. The pandemic has expanded the attack surface and the human element is still the weakest link. Invest in educating your personnel about phishing. Ensure everyone involved in protecting FTI understands the red flags to look for and how to report suspicious messages.

Cybersecurity Updates

4.20 SUPPLY CHAIN RISK MANAGEMENT

- Publication 1075 establishes a new supply chain risk management (SCRM) control family and integrates supply chain risk management aspects throughout the other control families to help protect system components, products and services that are critical to protecting FTI.


Organization
System Integrator
External Service Provider
Supplier
Supplier
External Service Provider
External Service Provider
Supplier
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

Cybersecurity Updates

4.20 SUPPLY CHAIN RISK MANAGEMENT

- 20 plus additional security controls elements and enhancements
  - SR-2 Supply Chain Risk Management Plan
    - Develops a plan for managing supply chain risk associated with the systems, system components and system services that process, store or transmit FTI
  - SR-6 Supplier Assessment and Reviews
    - Assess and review the supply chain-related risks associated with suppliers, contractors and the system at a minimum annually
  - SR-11 Component Authenticity
    - Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system
    - SR-11 (CE-1) Anti-counterfeit training: Train agency personnel on roles to detect counterfeit system components (including hardware, software, and firmware)

Cybersecurity Updates

3.3.8 Public-Facing Systems granting access to FTI identity proofing requirements:

- Requires IAL2, AAL2, FAL2 per NIST SP 800-63
  - Can use commercial identity provider

CA-8: Penetration Testing

- Required every 3 years
- SA-11 Developer Testing and Evaluation requires pen testing for developers as well

CM-7: Least Functionality

- Requires application whitelisting (*Authorized Software – Allow By Exception*)

IA-2: Identification and Authentication (Organizational Users)

- MFA required for all users (privileged and non-privileged) for all access types (for example, **local**, **network**, remote)
- AAL2 required for MFA, one factor must be from a device separate from the system gaining access

IA-5: Authenticator Management

- Passwords for most systems must be complex and at least 14 characters

Next Steps

- Safeguards will respond to any outstanding 1075 Pub questions from these Office Hour discussions
- Safeguards will publish the new Publication 1075 (1st qtr. FY22)
- Agencies will receive the official completed Publication 1075 via email

Q&A