

Interim Guidance Memorandum

Control Number: PGLD-10-0220-0001
Expiration Date: 02-28-2022
Affected IRM: 10.10.2

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: Peter Wade
Director, Privacy Policy & Compliance

SUBJECT: Interim Guidance on Risk Management for Authentication in
Non-Electronic Channels

This memorandum issues guidance on Risk Management for Authentication in Non-Electronic Channels until it is added as the proposed IRM 10.10.2. Please ensure that this information is distributed to all affected management officials within your organization who are responsible for setting policy related to authentication of taxpayers interacting with IRS.

Purpose: This policy establishes requirements for conducting risk assessments for telephone, in-person, and correspondence channels for authentication. This IG memo is intended to help personnel understand the concepts behind the authentication risk assessment process, while additional policy is written to detail the steps needed to complete the risk assessment.

Background/Source(s) of Authority: As a result of a Government Accountability Office (GAO) recommendation (*GAO 18-418, recommendation 3*), this guidance builds on existing requirements to establish a policy for conducting risk assessments for telephone, in-person, and correspondence channels for authentication. This policy applies NIST Risk Management Framework concepts to IRS authentication processes, as a baseline for completing these risk assessments.

Procedural Change: As of the publication of this IG, **there is no change to current authentication procedures.** Most IRS programs include continuous monitoring processes similar to this guidance. However, additional procedural guidance, following a related GAO recommendation (*GAO 18-418, recommendation 4*), will be published within the coming months, detailing a plan for performing risk assessments in accordance with this policy. That guidance will include further details on any changes to existing authentication procedures.

Effect on Other Documents: This guidance will be incorporated as a section of IRM 10.10, Identity Assurance, **by February 28, 2022.**

Effective Date: February 28, 2020

Contact: If you have any questions, please contact me, or a member of your staff may contact Greg Ricketts, Associate Director, Privacy Policy and Knowledge Management, at 901-707-6176, or Gregory.T.Ricketts@irs.gov.

Distribution:

[IRS.gov \(http://www.irs.gov\)](http://www.irs.gov)

Commissioner of Internal Revenue
Deputy Commissioner for Operations Support
Deputy Commissioner for Services & Enforcement
Commissioner, Large Business and International Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax-Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief of Staff
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Communications and Liaison
Chief Counsel
Chief, Criminal Investigation Chief Financial Officer
Chief, Planning, Programming & Audit Oversight
Chief Privacy Officer
Chief Risk Officer
Chief Technology Officer
Director, Affordable Care Act Office
Director, Office of Compliance Analytics
Director, Office of Online Services
Director, Office of Professional Responsibility
Director, Office of Research, Analysis and Statistics
Director, Return Preparer Office
Director, Whistleblower Office
Executive Director, Equity, Diversity and Inclusion
IRS Human Capital Officer
National Taxpayer Advocate
Treasury Inspector General for Tax Administration (TIGTA)
Associate Chief Information Officer, Cybersecurity

The following changes are hereby effective February 28, 2020 for IRM 10.10.2 (proposed)

Risk Management for Authentication in Non-Electronic Channels

1 Risk Management for Authentication Channels Overview

- (1) This policy applies to assessing the risk in the authentication process of telephone, in-person, and correspondence exchanges of sensitive information with individuals in authenticated customer contact channels. Management officials who lead programs described in this policy must follow these guidelines for continuous monitoring of new and ongoing authentication policy related to these channels.

NOTE: For interactions with non-sensitive information, refer to guidance applicable to the exchange, such as providing forms, general information or public releases.

- (2) This policy does not cover risk assessments for online interactions. For information about risk assessments of online services, contact *IT Cyber CPO DIRA (it.cyber.cpo.dira@irs.gov).

- (3) Confidentiality regulations such as IRC 6103 and other Federal guidelines require the IRS to authenticate the identity of individuals with whom it exchanges sensitive but unclassified (SBU) information (including PII and tax information), regardless of the channel. Management officials bear the responsibility to conduct risk assessments of factors, procedures, and processes used to authenticate individuals interacting with the IRS.

NOTE: In the context of this policy, a customer contact “**channel**” is the means by which IRS interacts with external stakeholders. Channel examples include:

- telephone
- in-person
- correspondence.

- (4) This risk assessment policy operates in conjunction with other review processes, such as System Security Plans, Privacy and Civil Liberties Impact Assessments (PCLIA), Chief Risk Office reviews, and regular operational review processes.

Example: Program owners may use the time dedicated to the Annual Assurance Reviews required by the Federal Managers’ Financial Integrity Act to include additional questions related to the review and assessment of risks relevant to taxpayer interactions taking place as part of their programs. Documentation of the annual discussion that would support the continuous monitoring requirement.

- (5) For determining whether an individual needs authentication, see also IRM 11.3.2, *Disclosure of Official Information, Disclosure to Persons with a Material Interest*, and IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*.

1.1 Authentication Risk Assessment Procedures

- (1) The National Institute of Standards and Technology (NIST) defines a risk assessment as “[t]he process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

NOTE: See the Terms and Acronyms section for definitions of terms in this quote.

- (2) The risk management assessment process may begin at any of the steps described below, depending on the reason for assessment. However, for any initial review under this policy, of either an existing process or a newly developed customer contact channel, the steps must be followed in order.

- (3) **Prepare** to consider risk of the authentication process in telephone, in-person, and correspondence, depending on the risk. Key tasks applicable to assessing risk in IRS customer contact channels, include steps to:

- Describe the channel and how users gain access (i.e., telephone, in-person, and correspondence)
- List data potentially included in the exchange and its level of sensitivity (i.e., SBU data, FTI, PII, law enforcement, or non-sensitive items)
- Gather Subject Matter Experts (SMEs), appropriate to the tools used in the authentication process.
- Identify roles and responsibilities, which may include:
 - Process Owner
 - Assessment Reviewers
 - Business Unit SMEs
 - Technical SMEs, if applicable.

- (4) **Categorize** risks in IRS authentication channels by considering the components of the customer contact. Review the information gathered in the Prepare step. Include additional details to assess the level of risk associated with each factor.

- Review and list all data in the process required for authentication.
- Determine sensitivity of the data needed to authenticate
- Determine the data made available, if successfully authenticated
- Consider prior incidents and the potential for improper authentication of a taxpayer
- Consider the type of users accessing the data (individuals, businesses, third- or fourth-party representatives).

NOTE: Avoid becoming overly granular in data categorization (such as delineating individual elements of a tax return, when a category for “return information” applies to all at the proper level of risk). This may add risks, when too many categories create too many levels of access. Additional levels create additional systemic burden, making it difficult to

maintain sufficiently secure processes in a shifting threat landscape.

(5) **Select** an initial set of controls for the authentication process and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk. Tasks associated with selecting a set of controls include:

- Review generally accepted best practices, such as:
 - Internal Revenue Manual
 - NIST, OMB or legislative guidance specific to the channel
 - Industry best practices and available tools
- Consider how this authentication process affects or is affected by other channels. Other channels may provide support and, if appropriate, mitigate risks where they overlap.
- The availability of options to eliminate or mitigate a risk
- Cost of meeting the privacy and security requirements, compared to the cost of inadequate privacy and security. Such factors could include:
 - Inconvenience, distress or damage to standing or reputation
 - Financial loss or agency liability
 - Harm to agency programs or public interests
 - Unauthorized release of sensitive information
 - Personal safety
 - Civil or criminal violations

Example: An assessment of risks related to telephone authentication may consider mitigations based on the reliability of an automated system that helps confirm the identity of a caller, based on telephone service provider information.

(6) **Implement** controls at a level matching the risk to the channel. These controls must be adapted to the customer contact channel used to authenticate the person/entity. This includes information in physical, technological, and personal exchanges of information. Implementation may include application of commercially available solutions, new technology, adjustments to procedures, or new policies. Document any deviations from selected levels of risk.

Note: See IRM 10.8.1 for guidance on risk acceptance and risk-based decisions.

(7) **Assess** the controls once implemented to ensure they are operating as intended. Ongoing assessments, such as quality reviews and operational reviews, reduce overall risk by identifying problems before they may be exploited. These assessments may be performed at a variety of levels. Any newly identified risks must be analyzed using this process, beginning at the step most applicable to the nature of the risk and addressed within a reasonable timeframe, commensurate with the risk.

(8) **Authorize** the process at the level of ownership for the authentication channel. Refer to the Prepare step's governance roles.

(9) **Monitor** all authentication channels (i.e., telephone, in-person, and correspondence) at a level of frequency matching the level of sensitivity and

frequency of changes to the related channel.

- Program level continuous monitoring must provide for immediate response, when necessary, as well as periodic reviews of the program for new threats or vulnerabilities. The regularity for response must be commensurate with the level of risk in the interaction. This policy recommends completing a full risk assessment every one to three years, depending on the results of the initial assessment and any intervening events.
- Owners of this policy should review it at least every three years, when changes are made to the related processes, or an external event, such as large improper releases of information or legislative changes, prompts review. The review should ensure the policy remains consistent with NIST, OMB, and other related requirements for IRS and the government, in general.

1.2 Acronyms

(1) The following table contains definitions for the acronyms used in this IRM:

Acronym	Definition
DIRA	Digital Identity Risk Assessment
FTI	Federal Tax Information
IRC	Internal Revenue Code
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PCLIA	Privacy and Civil Liberties Impact Assessment. See IRM 10.5.2
PII	Personally Identifiable Information
RAFT	Risk Acceptance Form and Tool
SBU	Sensitive, But Unclassified Information. See IRM 10.5.1.
SME	Subject Matter Expert
SSP	System Security Plan

1.3 Terms

(1) The following table defines key terms found in this guidance:

Term	Definition
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
Channel	The means by which IRS interacts with external stakeholders

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Operational Reviews	Recurring reviews of programs performed at various operational and business unit levels.
Process Owner	The official responsible for oversight and management of a particular IRS process.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

1.4 Related Resources

- (1) Privacy Act of 1974 (as amended)
- (2) IRC 6103
- (3) NIST SP 800-37, Risk Management Framework
- (4) GAO 15-593SP, A Framework for Managing Fraud Risks in Federal Programs