



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.10.2

FEBRUARY 17, 2023

EFFECTIVE DATE

(02-17-2023)

PURPOSE

- (1) This transmits revised IRM 10.10.2, Identity Assurance, Authentication Risk Assessments in Non-Digital Channels.

BACKGROUND

- (1) This policy applies to the assessment of risk(s) in the authentication process of telephone/voice, in-person, remote in-person, and correspondence exchanges of sensitive information with individuals in authenticated customer contact channels.

MATERIAL CHANGES

- (1) IRM 10.10.2.1, 10.10.2.1.7, and 10.10.2.2 - Editorial change to update Form 15295 to current version 2022.

EFFECT ON OTHER DOCUMENTS

IRM 10.10.2, Authentication Risk Assessments in Non-Digital Channels, dated August 5, 2022 is superseded.

AUDIENCE

The intended audience is Executives and management officials responsible for setting policy related to the authentication of taxpayers, representatives or other third-parties interacting with the IRS over non-digital channels (telephone/voice, in-person, remote in-person, and correspondence).

Angela R. Gartland
Director, Identity Assurance

10.10.2

Authentication Risk Assessments in Non-Digital Channels

Table of Contents

10.10.2.1 Program Scope and Objectives

10.10.2.1.1 Background

10.10.2.1.2 Authority

10.10.2.1.3 Roles and Responsibilities

10.10.2.1.4 Program Management and Review

10.10.2.1.5 Program Controls

10.10.2.1.6 Terms and Acronyms

10.10.2.1.7 Related Resources

10.10.2.2 Non-Digital Authentication Risk Assessments

10.10.2.2.1 Prepare

10.10.2.2.2 Categorize

10.10.2.2.3 Select

10.10.2.2.4 Implement

10.10.2.2.5 Assess

10.10.2.2.6 Monitor

10.10.2.2.7 Authorize

10.10.2.1
(02-17-2023)
**Program Scope and
Objectives**

- (1) **Purpose.** Industry best practices for authentication, authorization, and access (A3) promote the use of omni-channel integration across service channels. An omni-channel approach means having an enterprise A3 environment that is streamlined, integrated, consistent and accurate across digital and non-digital channels. This policy applies to the assessment of risk(s) in the authentication process of non-digital telephone/voice, in-person, remote in-person, and correspondence exchanges of sensitive information with individuals in authenticated customer contact channels. The assessment and mitigation of risks in these channels serves to promote consistency and accuracy across digital and non-digital channels.

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

- a. Establishes policy for assessing and documenting risk in authentication processes over non-digital customer contact channels (telephone/voice, in-person, remote in-person, and correspondence) where sensitive information is exchanged with individuals.

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/voice, in-person, remote in-person, and correspondence (fax, mail).

- b. Creates Non-Digital Authentication Risk Assessment (NDARA) process to ensure consistent risk assessment procedures are used across Business Units.
- c. Provides link to the Form 15295, Non-Digital Authentication Risk Assessment (NDARA) <https://core.publish.no.irs.gov/forms/internal/pdf/f15295--2022-10-00.pdf>
- d. Establishes three-year frequency for completing the risk assessment.
- e. Establishes time-frame for addressing deficiencies or risks identified during assessment process. The follow-up timeframe for addressing identified acceptable deficiencies or risks is every three years until resolved. The follow-up timeframe for addressing identified deficiencies or risks is every six months until determined acceptable or resolved.
- f. Applies National Institute of Standards and Technology (NIST) Risk Management Framework concepts to IRS authentication processes as a baseline for completing the NDARA.
- g. List related resources for completing the risk assessment.
- h. This risk assessment policy operates in conjunction with other review processes, such as System Security Plans (SSP), Privacy and Civil Liberties Impact Assessments (PCLIA), Chief Risk Office reviews, and regular operational review processes.

Note: For example,

the Federal Managers’ Financial Integrity Act (FMFIA) Annual Assurance Questionnaire includes an assessment of compliance with the risk assessments required by this policy. Front Line Manager (FM) Question 24: FM-24. I ensure sensitive information, including Federal Tax Information, is only shared when authorized with properly authenticated individuals and,

when required, I conduct risk assessments of telephone/voice, in-person, remote in-person, and correspondence channels for authentication and/or identity proofing.

- i. 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.
- j. This policy does not cover risk assessments for online interactions. For information about risk assessments of online services mail to: *it.cyber.cpo.dira@irs.gov*

- (2) **Audience.** The intended audience is management officials responsible for determining policy related to the authentication of taxpayers, representatives or other third-parties interacting with the IRS on non-digital channels (telephone/voice, in-person, remote in-person, and correspondence).
- (3) **Policy Owner.** Identity Assurance (IA), under Privacy, Governmental Liaison and Disclosure (PGLD), is the program office responsible for oversight, policies and procedures for Authentication Risk Assessments for Non-Digital Channels.
- (4) **Program Owner.** The Director, Identity Assurance reports to the Chief Privacy Officer and is responsible for IA program oversight.
- (5) **Primary Stakeholders.** All organizations and business units who authenticate taxpayers, representatives or other third-parties over non-digital channels (telephone/voice, in-person, remote in-person, and correspondence).
- (6) **Contact Information.** To recommend changes or make any other suggestions to this IRM section mail to: *os.p.gld.ia.risk.assessments@irs.gov*

10.10.2.1.1 (07-29-2021) Background

- (1) This IRM builds on existing policy by adding processes for assessing, documenting, and addressing authentication risks for telephone/voice, in-person, remote in-person, and correspondence channels. This policy applies NIST Risk Management Framework concepts to IRS authentication processes as a baseline for completing these risk assessments.

10.10.2.1.2 (07-29-2021) Authority

- (1) By law, federal agencies are expected to document, publish and maintain records of policies, authorities, procedures and organizational operations. The IRM is the source for the IRS. See IRM 1.11.1.1.2, Authority, for the authorities and legal obligations of Internal Management Documents (IMDs).
- (2) 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 personally identifiable information (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 taxpayers, representatives or other third-parties interacting with the IRS.
- (3) Privacy, Government Liaison and Disclosure's (PGLD) Privacy Policy and Knowledge Management (PPKM) implements relevant privacy statutes, regulations, guidelines, OMB Memoranda, and other requirements. Numerous statutes such as the Privacy Act, Federal Information Security Modernization Act (FISMA) and Paperwork Reduction Act are reinforced by OMB and NIST guidance and implemented by the IRS accordingly.

10.10.2.1.3
(08-05-2022)

Roles and Responsibilities

- (1) The Director, Identity Assurance (IA) is responsible for the Non-Digital Authentication Risk Assessment (NDARA) process.
- (2) Organization Executives and Management Officials who lead programs described in this policy are responsible for these guidelines for continuous monitoring of new and ongoing authentication policies related to these channels.
- (3) Executives of each IRS organization are responsible for ensuring an NDARA is completed every three years for each of their respective programs related to these channels. Any risks identified should be documented, mitigated and monitored.
- (4) Each IRS organization is responsible for establishing internal processes for managing their risk assessment procedures and monitoring based upon this guidance.
- (5) A copy of approved assessments will be emailed to *OS P GLD IA Risk Assessments, for policy team review and coordination on any identified risks.

10.10.2.1.4
(07-29-2021)

Program Management and Review

- (1) The Identity Assurance function manages and reviews the Authentication Risk Assessments in Non-Digital Channels Program.

10.10.2.1.5
(07-29-2021)

Program Controls

- (1) Business Units are responsible for completing an NDARA every three years and addressing any deficiencies identified. The follow-up timeframe for addressing identified acceptable deficiencies or risks is every three years until resolved. The follow-up timeframe for addressing identified deficiencies or risks is every 6 months until determined acceptable or resolved.
- (2) When risk assessments are completed and signed, they become an official record and must be maintained in accordance with Document 12829, *General Records Schedule* (GRS) 5.7 Item 020. Each office is responsible for reports and audits identifying internal administrative program weaknesses and risks, mitigation action plans, corrective actions, tracking records, correspondence, and other records held by the office responsible for coordinating internal control functions including risks. Destroy records five years after no further corrective action is needed.

10.10.2.1.6
(07-29-2021)

Terms and Acronyms

- (1) The tables lists commonly used terms and definitions:

Term	Definition
A3	A3 refers to authentication, identity proofing, authorization and access policies and capabilities across all service delivery channels (i.e., phone, in-person, remote in-person, correspondence and online/digital).

Term	Definition
Authentication	The process of establishing or confirming that someone is the previously identified person they claim to be.
Authorization	The process that establishes the rights or privileges of users to interact with the IRS on behalf of themselves or others (e.g., businesses, individuals). Allows those users to exercise rights that have previously been established. Authorization is required for any person or business conducting IRS business on another person's behalf (such as tax return preparers).
Access	The process of allowing an authenticated person to execute transactions or get to the data authorized by the taxpayer as provided through the Authorization process. Access allows individuals to exercise the rights or privileges defined during Authorization, based on successful Authentication.
Channel	The means by which IRS interacts with external stakeholders.
Correspondence (mail, fax)	Communications, through mail and fax.
Digital	Relating to, using, or storing data or information in the form of digital signals. Involving or relating to the use of computer technology.
In-person/remote in-person	In-person authentication to complete and/or request transactions. For example, a taxpayer requesting a transcript may visit an IRS site or through video conferencing, to provide in-person/remote in-person authentication with identification, such as a driver's license.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
National Institute of Standards and Technology (NIST)	Provides standards for federal agencies for implementing digital identity services. The guidelines cover identity proofing and authentication of users interacting with government IT systems over open networks as well as registration, authenticators, management processes, authentication protocols, federation and related assertions.

Term	Definition
Non-Digital	Not using the internet or computers. Not represented by numbers, especially binary codes; not digitized.
Omni-channel	Omni-channel refers to having a stream-lined, integrated and accurate understanding of current-state A3 (i.e., processes, data, risks, and user experience) across customer-contact channels.
Operational Reviews	Recurring reviews of programs performed at various operational and business unit levels.
Personally Identifiable Information	Any information that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Process	A series of actions or steps taken in order to achieve a particular end.
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.
Telephone / voice	Enterprise Architecture approved telephone and voice channels for external communications.

Term	Definition
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.

(2) The table list commonly used acronyms and definitions:

Acronym	Definition
DIRA	Digital Identity Risk Assessment
FTI	Federal Tax Information
IRC	Internal Revenue Code
IMD	Internal Management Document
NDARA	Non-Digital Authentication Risk Assessment
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PCLIA	Privacy and Civil Liberties Impact Assessment: See IRM 10.5.1
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

10.10.2.1.7
(02-17-2023)
Related Resources

- (1) The Non-Digital Authentication Risk Assessment Form 15295 may be accessed at <https://core.publish.no.irs.gov/forms/internal/pdf/f15295--2022-10-00.pdf>
- (2) Privacy Act of 1974 (as amended)
- (3) IRC 6103, Confidentiality and Disclosure of Returns and Return Information
- (4) NIST Special Publication 800-37, Risk Management Framework
- (5) GAO 15-593SP, A Framework for Managing Fraud Risks in Federal Programs

10.10.2.2
(02-17-2023)
**Non-Digital
Authentication Risk
Assessments**

- (1) The National Institute of Standards and Technology defines a risk assessment as "the 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 Terms and Acronyms section in this IRM for definitions of terms in this quote.

- (2) Business Units are recommended to use Form 15295 when conducting non-digital authentication risk assessments which was designed to assist with this process. The Non-Digital Authentication Risk Assessment Form 15295 may be accessed at <https://core.publish.no.irs.gov/forms/internal/pdf/f15295--2022-10-00.pdf>
- (3) The non-digital risk 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.

10.10.2.2.1
(07-29-2021)
Prepare

- (1) **Prepare** to consider risk of the authentication process in telephone/voice, in-person, remote 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/voice, in-person, remote 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 and Technical SMEs, if applicable.

10.10.2.2.2
(07-29-2021)
Categorize

- (1) **Categorize** the risks in IRS authentication channels, and consider the components of the customer contact. Review the information gathered in the Prepare step in this IRM and 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 complex in data categorization (such as outlining individual elements of a tax return, when a category for "return information" applies to all at the proper level of risk). Risks are added when too many categories increase levels of access. Additional levels create additional systemic burden, making it difficult to maintain sufficiently secure processes in a shifting threat landscape.

10.10.2.2.3
(07-29-2021)
Select

- (1) **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. Things to consider when selecting a set of controls:

- Examine generally accepted best practices.
- Review NIST, OMB or legislative guidance specific to the channel.
- Model industry best practices and available tools.
- Consider how this authentication process affects or is affected by other channels which 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.
- Inconvenience, distress or damage to standing or reputation.
- Financial loss or agency liability.
- Harm to agency programs or public interests.
- Personal safety.
- Civil or criminal violations.

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

10.10.2.2.4
(07-29-2021)
Implement

- (1) **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 individual. 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, Policy and Guidance for guidance on risk acceptance and risk-based decisions.

10.10.2.2.5
(07-29-2021)
Assess

- (1) **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, appropriate with the risk.

10.10.2.2.6
(07-29-2021)
Monitor

- (1) **Monitor** all non-digital authentication channels (i.e., telephone/voice, in-person, remote 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.

10.10.2.2.7
(07-29-2021)
Authorize

- (1) **Authorize** the process at the level of ownership for the authentication channel. Refer to the Prepare step's governance roles in this IRM.

