# Security Assessment Report and Attestation Guideline

**August 2023**

TEXAS
Health and Human Services

# Table of Contents

# Purpose

This document supplements the Texas Health and Human Services Information Security Controls, specifically the following requirements as they apply to external entities:

- CA-02 Control Assessments
- CA-06 Authorization
- CA-07 Continuous Monitoring

This document meets state requirements in Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24, in the Agency Information Security Program. These requirements include protections based on risk for all information and information resources, including resources outsourced to an external entity.

# Scope

This document affects external entities responsible for complying with the HHS information security requirements and HHS employees who are responsible for monitoring external entity compliance.

# Definitions

**External Entity -** Individuals or organizations external to HHS who have an existing or potential contracting relationship that permits the individual or organization to access, create, disclose, receive, transmit, maintain, or store HHS data.

**Independent Assessments -** Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations.

**Independent Assessor -** Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

# Guidance

## Authority to Receive HHS Data

Before an external entity receives HHS data, the external entity must comply with HHS information security requirements as documented in the contractual agreement between the external entity and HHS and must be authorized to receive data in accordance with IS Controls CA-06, Authorization.

To be granted the authority to connect or authority to operate, the external entity must comply with the security compliance requirements outlined below.

## Complying with HHS Information Security Requirements

The following requirements represent IS Controls CA- 02, Control Assessments. [a]An external entity's compliance requirements vary depending on the types of HHS data that it accesses, creates, discloses, receives, transmits, maintains, or stores.

**Security Compliance Requirements**

| Security Control Baseline or Overlay[b] | Required Documents | Frequency | Mandated by IS Controls |
|---|---|---|---|
| Low or Low Plus[c] | Security Assessment Report | Biennial (only submit upon request) | CA-02 |
| Moderate | Security Assessment Report by an Independent Assessor | Biennial | CA-02, CA-02(01) |
| High | Security Assessment Report by an Independent Assessor | Annual | CA-02, CA-02(01) |
| IRS, CMS- MARS-E, or CJIS | Security Assessment Report by an Independent Assessor | Annual | CA-02, CA-02(01) |

[a]However, an external entity's contractual agreement with HHS may provide more restrictive compliance requirements

[b]Refer to Framework for Understanding the IS Controls for a full explanation of all security overlays and control baselines.

[c]HHS requires external entities who must comply with the "low" or "low plus" security baselines to complete a Security Assessment Report on a biennial basis. However, external entities are not required to submit the required documentation to HHS unless otherwise stipulated in the contractual agreement, or unless requested by HHS. If HHS requests the required documentation, the external entity must submit it within 90 days of the request.

# Security Assessment Report

The external entity must complete a Security Assessment Report as proof of compliance with HHS information security requirements. For HHS to accept the Security Assessment Report, the external entity must do the following:

1. Submit the Security Assessment Report using the HHS template.
2. Attest that the external entity is compliant with all HHS information security controls required per the external entity's contractual agreement with HHS.

# Moderate and High Security Control Baseline Additional Requirements

An independent assessment must validate that the external entity meets security compliance requirements. "Independent assessment" is defined in the definition section of this document and described in IS Controls CA-02(01), Independent Assessors supplemental guidance.

# Regulatory or Federal Overlays Additional Requirements

The external entity may receive some data from HHS that originates from another regulatory or federal source that has additional assessment requirements beyond what is mentioned above. The external entity must refer to its contractual agreement with HHS for any added requirements.

# Reporting Non-Compliance with HHS Requirements

External entities must submit additional documentation to HHS for each documented instance of non-compliance with HHS information security requirements.

External entities must submit one of the following applicable forms for each instance of non-compliance to document how they will address the reported non-compliance.

## Plan of Action and Milestone (POA&M) Form

The external entity must complete a separate Plan of Action and Milestone (POA&M) Form for each non-compliant information security control that will be remediated.

The external entity must use this form to explain how and when they will become compliant and should include timelines and a remediation plan.

### Risk Exception Request Form

If the external entity cannot remediate the risk posed by their non-compliance, the external entity must complete a Risk Exception Request Form for each non-compliant information security control that cannot be remediated. The external entity must use the form to explain why they cannot comply with information security requirements and include alternative solutions to reduce the risk posed by the non-compliance.

## How to Submit Documentation

All information security documentation concerning HHS data is classified as confidential. The external entity must send this documentation in a manner compliant with IS Controls SC-08, Transmission Confidentiality and Integrity, and IS Controls SC-28, Protection of Information at Rest. The external entity should contact the HHS point-of-contact identified in the contractual agreement for further guidance on how to securely submit the documents to HHS.

The external entity must submit a Security Assessment Report, along with any of the following document(s) if applicable:

- POA&M forms
- Risk Exception Request Forms
- Any other required security documentation identified in the contractual agreement

HHS reserves the right to request additional information from the external entity to confirm that the applicable information security requirements are in place.

Failure by the external entity to comply with information security requirements may result in consequences including, but not limited to, liquidated damages, contract termination, regulatory fines, or other remedies.

# Guidance Documents

Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24

Establishes requirements that each agency shall develop, document, and implement an agency-wide information security program that includes protections, based on risk, for all information and information resources.

**HHS Information Security Controls**

Includes safeguards or countermeasures that, when implemented and enforced, satisfy the information security compliance requirements defined in applicable federal and state laws, executive orders, directives, policies, HHS regulations, and standards.

# Revision History

| Date | Change | Department Owner |
|---|---|---|
| 08/31/2023 | Updated to correspond with revised IS Controls | Chief Information Security Office |
| 03/03/2021 | Document renamed and issued as Security Assessment Report & Attestation Guideline | Chief Information Security Office |
| 06/17/2019 | Revised and replaced IS-RAMP | Chief Information Security Office |
| 08/31/2015 | Issued as IS-RAMP | Chief Information Security Office |