Risk Assessment Template

This risk assessment template, which aligns with the Fraud Risk Management Framework developed by the U.S. Government Accountability Office (GAO),[1] is intended as a guidance document to support Centers for Medicare & Medicaid Services (CMS) program efforts to identify and address program risks. This risk assessment template provides a suggested step-by-step approach for identifying, assessing, prioritizing, and addressing program integrity risks.

When using this template, please note the following:

- This template serves as a starting point and can be tailored as needed to fit each associated CMS program area.
- Examples included in this template are derived from the Medicaid program only, but the template can be used to fit any major program area.
- This is a dynamic tool that can be continually updated and maintained to identify new and emerging risks and update mitigation strategies as needed.
- CMS does not require users to implement the risk assessment process outlined in this document but provides a proven approach to support the evaluation of program integrity risks. Users may choose instead to continue to use existing processes or leverage other approaches for identifying and addressing program risks.

[1] U.S. Government Accountability Office (GAO) (2015). A Framework for Managing Fraud Risks in Federal Programs. Retrieved from: https://www.gao.gov/products/GAO-15-593SP.

Disclaimer: The contents of this document do not have the force and effect of law and are not meant to bind the public in any way, unless specifically incorporated into a contract. This document is intended only to provide clarity to the public regarding existing requirements under the law. This tool is intended to assist program managers with completing standardized risk assessments of programs and the internal controls needed to mitigate potential risks. It is not intended to be used in legal proceedings.

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES CENTER FOR PROGRAM INTEGRITY

Step 1. Identify vulnerability, theme, and sources

The first step in identifying program integrity risks is to identify vulnerabilities, including new federal requirements, and assign an appropriate vulnerability theme. Since vulnerabilities may cover a wide range of CMS program areas, there may be more than one topic that applies. When identifying the policy source of these vulnerabilities, it may be helpful to include an attachment or hyperlink for accessibility for review. This will support the completion of **Step 2 (identifying inherent risks)** and help ensure that all related risks have been comprehensively identified. If available, include any relevant federal regulations as this will help reorient stakeholders to the direct regulation(s).

Note: Users can modify this step as needed when applying this template to other scenarios.

Table 1: Identify Vulnerability, Theme and Sources

Vulnerability #	CMS Program Area(s)	Vulnerability	Vulnerability Theme(s)	Policy Source(s)[2]	Relevant Federal Regulations[3]
1	**EXAMPLE**: Medicaid	**EXAMPLE**: As a condition of receiving the increased 6.2 federal medical assistance percentage (FMAP) under the Families First Coronavirus Response Act (FFCRA) through the end of the month in which the public health emergency (PHE) ends, states may not terminate coverage for validly enrolled individuals found ineligible based on a redetermination of eligibility at renewal (unless the beneficiary requests a voluntary termination of eligibility, or the state determines that the individual is no longer considered to be a resident of the state).	**EXAMPLE**: Beneficiary Eligibility	**EXAMPLE**: Section 6008(b)(3) of the Families First Coronavirus Response Act	**EXAMPLE:** • 42 CFR § 435.916: Periodic Renewal of Medicaid Eligibility
2	--	--	--	--	--

[2] Policy source(s) for the COVID-19 Public Health Emergency may include (but are not limited to) Medicaid and CHIP State Plan Amendments (SPAs), Medicaid and CHIP Disaster Relief SPAs, Medicaid and CHIP Modified Adjusted Gross Income (MAGI)-Based Disaster Relief Addendums, Section 1115 Waivers, Section 1135 Waivers, 1915 (c) Waivers, Appendix K amendments, legislation, guidance, and other state policy changes.
[3] Relevant federal regulations and other authorities for disaster-related flexibilities may be found in the Medicaid and CHIP Disaster Response Toolkit, Inventory of Medicaid and CHIP Flexibilities and Authorities in the Event of a Disaster, available at https://www.medicaid.gov/resources-for-states/disaster-response-toolkit/index.html .

Step 2. Identify inherent risks affecting the program

This step involves identifying and documenting all program risks (related to the vulnerability identified in **Table 1**). To fully identify all potential inherent risks, this step may include engagement with a diverse range of stakeholders. Relevant stakeholders are individuals who can understand and recognize potential risks to the programs being assessed. These could be internal stakeholders, such as other departments or divisions within the agency, or external stakeholders such as other federal agencies and contractors. To ensure stakeholder efforts are focused on the program risks most relevant to them, it may be helpful to group and assign inherent risks together based on their designated category of the risk.

A comprehensive assessment of inherent risks may involve a variety of information gathering activities, such as staff interviews, environmental scans, and reviews of program audits and evaluation reports; however, not all these activities may be feasible when evaluating vulnerability risks. Users should balance the need for a thorough assessment with the speed and urgency needed to conduct the assessment, existing resources, and other priorities when determining an approach for information gathering.

At a minimum, the following details should be noted for each identified inherent risk:

- **Description of the risk**: This column captures the nature of the risk (e.g., beneficiaries enrolled through the optional COVID-19 testing category are improperly enrolled into other eligibility categories; improperly restrictive eligibility standards may result in adverse audit findings triggering a recovery of federal funds). Users may also choose to note the specific number or numbers of the vulnerability associated with the inherent risk in parenthesis from **Table 1** to allow for easy reference throughout each step. However, if users re-number the vulnerability, it may cause issues with numbering in **Table 1** not aligning with **Tables 2-8**.
- **Category of risk:** This column captures the broad type of risk with respect to the program (e.g., improper enrollment or reenrollment determination; receipt of category of services for which beneficiary is not eligible; claiming of FFP at an improper FMAP match rate). Risks that fall within the same category in many instances may be mitigated by the same or similar mitigations. One or more risk categories can be assigned as needed.
- **Primary Source(s) of risk**: This column captures the primary source within the agency's organizational structure and mechanisms of the risk. Select one or more relevant sources of risk including:
  - **Policy**: The course of action adopted by the agency or imposed by legislation or other authority.
  - **Processes**: The sequence of steps the agency has developed to carry out a policy or task.
  - **Operations**: How one or more of those process steps are executed, by whom, and when.

Table 2: Identify Inherent Risks

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Category of Risk	Primary Source(s) of Risk		
			Policy	Processes	Operations
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	**EXAMPLE:** Improper continued enrollment	X	X	X
2	**EXAMPLE:** Higher likelihood of eligibility errors because of the increased workload associated with re-determining eligibility for many beneficiaries on a compressed time frame (1).	**EXAMPLE:** Receipt of category of services for which beneficiary is not eligible	X	X	X
3	--	--	--	--	--

Step 3. Identify potential outcomes and assess and score inherent risks

This step involves assessing each identified risk and assigning a risk score for each inherent risk type for the following categories:

- **Likelihood**: The level of possibility that a risk will occur.
- **Beneficiary Harm**: The level of possibility that the risk could inflict harm on beneficiaries.
- **Dollars**: The level of possibility that the risk could lead to financial impacts for the CMS program.
- **Overall**: The average score of the scores for the preceding risk categories.

Before determining risk scores, users should identify the potential outcome(s) associated with each inherent risk. This important step supports users in better understanding the magnitude and nature of the impact of each risk. Users can use these insights when deciding how to score the inherent risk. This process can ultimately assist users when determining risk prioritization in the subsequent steps.

Note: There are many ways to determine risks scores, and users may tailor this part of the process to fit their program and needs. For instance, risk scores can be quantitative (i.e., use a numeric scoring methodology, such as a 5-point or 10-point scale), or consist of qualitative factors to assign a category of risk (e.g., low, medium, high). In the example in this template, risk scores are calculated using a qualitative scale of low, medium, and high to allow for ease in calculating the overall risk score. However, this can be adjusted as needed based on internal preferences. Additionally, users may choose to use other or additional categories to score risk, such as program reputation. Finally, users may utilize various methodologies for establishing the overall risk score including weighing certain risks or risk types based on specific priorities.

Table 3: Identify Potential Outcomes and Assess Inherent Risks

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Potential Outcomes	Inherent Risk Scoring			
			Likelihood	Harm	Dollars	Overall
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	**EXAMPLES:** • Improper continued enrollment, if state does not appropriately or timely redetermine eligibility based on identified changes based on change of circumstances or renewal. • Potential adverse audit finding	Medium	Low	Medium	Medium
2	--	--	--	--	--	--

Step 4. Determine risk tolerance

In general, the goal of risk management is to achieve as low a risk level as possible; however, it is generally difficult to eliminate all risk. Understanding that not all risk can be eliminated in most cases, risk tolerance represents the level of risk an entity will accept when trying to achieve a goal. The acceptable level of risk tolerance depends on the circumstances within each CMS program and other objectives besides mitigating fraud risks. This is an essential step when determining which risks to address and to prioritize.

Determining a risk tolerance level may require engagement with management to determine what level of risk tolerance is acceptable for each risk. When faced with limited time and/or resources, users may choose to prioritize risk tolerance discussions on those risks with high-risk scores. Additionally, management may revisit risk tolerances over time as needed.

Additionally, when assessing risk tolerance, consideration should be given to whether risk tolerances allow for the appropriate design of internal controls that adequately support mitigation of each risk. To do this, the user may determine risk tolerances in the context of applicable laws, regulations, standards as well as standards of conduct, oversight structure, organizational structure, and expectations of competence.[4]

Table 4: Determine Risk Tolerance

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Potential Outcomes	Inherent Risk Scoring				Risk Tolerance
			Likelihood	Harm	Dollars	Overall	
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	**EXAMPLES:** • Improper continued enrollment, if state does not appropriately or timely redetermine eligibility based on identified changes based on change of circumstances or renewal • Potential adverse audit finding	Medium	Low	Medium	Medium	Low
2	--	--	--	--	--	--	--

[4] For example, allowing individuals to remain enrolled when they are no longer eligible to receive benefits may lead to improper payments and/or adverse findings during audits. This may result in a financial impact to the state's Medicaid program if it is determined that the state will need to refund the Federal Government and may also impact the program's reputation with one or more stakeholders. Given these large potential impacts, management may determine that the tolerance for this type of risk is low (that is, the risk is very concerning). Conversely, allowing temporarily enrolled providers to remain enrolled beyond the permitted timeframe could expose the state to potential fraud, waste, and abuse by unscrupulous providers. However, in this example, if a provider's access to the billing system expires automatically every 365 days, the potential risk is time limited. Furthermore, other program integrity controls exist to monitor providers for potential fraud, waste, and abuse. Because management recognizes other routine processes exist to prevent a fraudulent provider from billing indefinitely, management may determine their tolerance for this risk is higher (that is, the risk is not very concerning).

Step 5. Examine suitability of current controls and prioritize remaining risks

After all potential inherent risks have been identified, the next step is to analyze these risks and determine a potential response. This involves the following two sub-steps:

5.1 Compare inherent risks to existing controls to determine remaining (e.g., residual) risks and how to prioritize

This step focuses on connecting existing risk management activities and controls to the identified risks so that the user can determine the likelihood and impact of the remaining risks on the program. This step can be completed in two stages: first, determine what risk control activities (e.g., "existing controls"), if any, are currently in place that in some way mitigate each inherent risk; second, assess how successfully the existing controls are working: that is, how much inherent risk remains despite the existing controls. The user then assigns a residual risk level score based on this assessment.[5] Based on this analysis, the user then determines how to prioritize each risk.

Note: Risk prioritization can be determined using a defined quantitative method (e.g., ranking, or assigning a high/medium/low score) or by simply noting whether one or more risks are prioritized or not.

Table 5: Examine Existing Controls and Determine/Prioritize Residual Risks

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Score	Risk Tolerance	Existing Controls	Residual Risk Level	Risk Prioritization
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	Medium	Low	**EXAMPLES:** • Eligibility offices are pulling reports to identify cases with changes reported by beneficiaries. • Eligibility and waiver determination office is running reports to identify cases with upcoming and past due renewals during the PHE. • State is processing all redeterminations that can be completed with available information, before the end of the PHE, to reduce the volume of post-PHE work.	Medium	High

[5] For example, the state may conduct regular audits of a sample of eligibility determinations. Those audits serve as an existing control. The state may have residual risk to the extent that those audits and other data indicate that erroneous determinations are still occurring. If so, the state may decide the rate of errors is higher than it is willing to accept. If the state determines the rate of errors exceeds its risk tolerance, the state may come up with mitigation strategies that will reduce the issue to an acceptable level of tolerance.

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Score	Risk Tolerance	Existing Controls	Residual Risk Level	Risk Prioritization
				• State is sending request for information to renewals that cannot be confirmed with ex parte information before the end of the PHE to reduce the volume of work post-PHE.		
2	--	--	--	--	--	--

5.2 Determine potential mitigation strategies to address each residual risk, assign responsibilities, and determine an estimated go-live date for each mitigation strategy

After determining the priority of the inherent risk, next describe the risk response by identifying potential risk mitigation strategies and/or actions to mitigate residual risks. It may be helpful to identify the broad nature of each mitigation strategy taken in response to risks. Such categories may include—

- **Acceptance**: No action is taken to respond to the risk based on the insignificance of the risk.
- **Avoidance**: Action needs to be taken to stop the operational process or the part of the operational process causing the risk.
- **Reduction**: Action needs to be taken to reduce the likelihood or magnitude of the risk.
- **Sharing**: Action is taken to transfer or share risks across the entity or with external parties.

This step also includes identifying a responsible entity, either individuals or divisions, assigned to manage implementation of mitigation strategies, and an estimated go-live date (EGD), or a proposed implementation date (e.g., 07/01/2021 or Q1 2021). Please note, for activities that have a single date when they become effective, such as the issuance of a regulation, the EGD is that date. For mitigations that will be ongoing for an indeterminate period of time, such as data monitoring, the EGD is the date the activity began. The idea is to capture the date the mitigation begins to have an effect on the risk.

Note: Multiple mitigation strategies for a given risk may be needed to reduce the risk to an acceptable level.

Table 6: Determine Mitigation Strategies

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Score	Risk Tolerance	Residual Risk Level	Mitigation Strategies	Responsible Entity	Estimated Go-Live Date
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given	Medium	Low	Medium	**EXAMPLES:** **1.1 Avoidance:**	• Relevant agency component	02/15/2021

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Score	Risk Tolerance	Residual Risk Level	Mitigation Strategies	Responsible Entity	Estimated Go-Live Date
	the volume of cases to process and limited time to do so (1).				• To the extent permissible during the PHE, act on changes in circumstances and process renewals based on available information. • Structure workforce tasks to focus on difficult cases that require manual review. • If the state has sufficient information to renew eligibility when redetermining eligibility based on a change, complete the renewal and provide the beneficiary with a new 12-month (or other) eligibility period. • Prior to the end of the PHE, Submit SPA to expand renewal timeframe for non-MAGI renewals from # months to 12 months.	(or person within component) • Relevant agency component (or person within component) • Relevant agency component (or person within component) • Relevant agency component (or person within component)	
					1.2 Reduction: • Use additional electronic data verification sources and consider additional verification flexibilities in	• Relevant agency component (or person within component)	Beginning ASAP post-PHE

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Score	Risk Tolerance	Residual Risk Level	Mitigation Strategies	Responsible Entity	Estimated Go-Live Date
					order to reduce amount of outreach required for beneficiaries and improve successful ex parte renewals. • Submit SPA to expand renewal timeframe for non-MAGI renewals from 6 months to 12 months. • Process renewals at highest risk for ineligibility first (i.e., individuals determined ineligible during the PHE but were never terminated d/t FFCRA, individuals who may have aged out of coverage during the PHE, or individuals who gained coverage only because of a temporary eligibility flexibility).	• Relevant agency component (or person within component) • Relevant agency component (or person within component)	
2	--	--	--	--	--	--	--

Step 6. Document the risk profile

An effective risk assessment includes documenting all findings and conclusions from the previous steps, including the analysis of the types of risks, their perceived likelihood and impact, risk tolerance, and proposed risk response and mitigation strategies. A "risk profile," the summation of these findings, is a critical component of the risk assessment process that helps inform the specific control activities implemented by management.

The final format of the risk profile will likely vary. Users can choose to create their own risk profile or alternatively use the two additional supplemental templates provided below.

- **Table 7: Summary Profile View:** This template provides a high-level view of each risk and their associated overall risk score, risk tolerance, prioritization, likelihood that the risk can be addressed, and the estimated resources required to address each risk.
- **Table 8: Individual Risk Profile:** This template provides a place to compile findings and determinations from all previous steps for each inherent risk identified. This template can be copied and pasted as many times as needed until this has been completed for all inherent risks, or as many as deemed necessary.

Table 7: Summary Profile View

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Risk Score	Risk Tolerance	Risk Prioritization	Mitigation Strategies
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	Medium	Low	High	**EXAMPLES:** **1.1 Avoidance:** • To the extent permissible during the PHE, act on changes in circumstances and process renewals based on available information. • Structure workforce tasks to focus on difficult cases that require manual review. • If the state has sufficient information to renew eligibility when redetermining eligibility based on a change, complete the renewal and provide the beneficiary with a new 12-month (or other) eligibility period. • Prior to the end of the PHE, Submit SPA to expand renewal timeframe for non-MAGI renewals from 6 months to 12 months.

Risk #	Description of Inherent Risk (Associated Vulnerability Number[s])	Overall Risk Score	Risk Tolerance	Risk Prioritization	Mitigation Strategies
					1.2 Reduction: • Use additional electronic data verification sources and consider additional verification flexibilities in order to reduce amount of outreach required for beneficiaries and improve successful ex parte renewals. • Process renewals at highest risk for ineligibility first (i.e., individuals determined ineligible during the PHE but were never terminated d/t FFCRA, individuals who may have aged out of coverage during the PHE, or individuals who gained coverage only because of a temporary eligibility flexibility).
2	--	--	--	--	--

Table 8: Individual Risk Profile

Overview of Risk (Step 2)				
Risk #	**Description of Inherent Risk (Associated Vulnerability Number[s])**	**Category of Risk**		
1	**EXAMPLE:** Ineligible individuals remain enrolled in coverage after the permissible period, given the volume of cases to process and limited time to do so (1).	**EXAMPLE:** Improper continued enrollment		
Potential Outcomes		**Primary Source(s) of Risk**		
EXAMPLES: • Improper continued enrollment, if state does not appropriately or timely redetermine eligibility based on identified changes based on change of circumstances or renewal • Potential adverse audit finding		**Policy**	**Operations**	**Processes**
		X	X	X

Risk Assessment and Tolerance (Steps 3-4)				
Inherent Risk Scoring				Risk Tolerance
Likelihood	Harm	Dollars	Overall	
Medium	Low	Medium	Medium	Low

Proposed Response and Mitigation Strategies (Step 5)		
Existing Controls	Residual Risk Level	Risk Prioritization
EXAMPLES: • Eligibility offices are pulling reports to identify cases with changes reported by beneficiaries. • Eligibility and waiver determination office is running reports to identify cases with upcoming and past due renewals during the PHE. • State is processing all redeterminations that can be completed with available information, before the end of the PHE, to reduce the volume of post-PHE work. State is sending request for information to renewals that cannot be confirmed with ex parte information before the end of the PHE to reduce the volume of work post-PHE.	Medium	High

Mitigation Strategies	Responsible Entity	Estimated Go-Live Date
EXAMPLES: **1.1 Avoidance**: • To the extent permissible during the PHE, act on changes in circumstances and process renewals. • Structure workforce tasks to focus on difficult cases that require manual review; • If the state has sufficient information to renew eligibility when redetermining eligibility based on a change, complete the renewal and provide the beneficiary with a new 12-month (or other) eligibility. • Prior to the end of the PHE, Submit SPA to expand renewal timeframe for non-MAGI renewals from 6 months to 12 months.	**EXAMPLES:** • Relevant component of Medicaid agency (or person within component) • Relevant agency component (or person within component)	**EXAMPLE:** 02/15/2021

Mitigation Strategies	Responsible Entity	Estimated Go-Live Date
	• Relevant agency component (or person within component) • Relevant agency component (or person within component)	
1.2 Reduction: • Use additional electronic data verification sources and consider additional verification flexibilities to reduce amount of outreach required for beneficiaries and improve successful ex parte renewals. • Submit SPA to expand renewal timeframe for non-MAGI renewals from X# months to 12-months. • Process renewals at highest risk for ineligibility first (i.e. Individuals determined ineligible during the PHE but were never terminated d/t FFCRA, individuals who may have aged out of coverage during the PHE, or individuals who gained coverage only because of a temporary eligibility flexibility).	• Relevant agency component (or person within component) • Relevant agency component (or person within component) • Relevant agency component (or person within component) • Relevant agency component (or person within component)	Beginning ASAP post-PHE