Leadership Accountability Risk Catalog

Revised September 2023

This page intentionally blank to facilitate double-sided printing

Leadership Accountability Risk Catalog
Table of Contents

Introduction **1**

Risk Category 3

Risk Categories 4

Risk Subcategories 4

Operations **5**

Internal 5

External 11

Reporting **17**

Internal 17

External 21

Compliance **24**

Internal 24

External 27

This page intentionally blank to facilitate double-sided printing

Leadership Accountability Risk Catalog

Introduction

This document is a tool to provide a statewide, standardized risk language for Leadership Accountability (previously State Leadership Accountability Act or SLAA) reporting. The examples provided are not intended to be all inclusive but rather to aid the reporting entity in understanding the definitions. Application of this tool will vary by entity and may include:

- Categorizing an entity's most significant risks for the Leadership Accountability report (required for web portal)
- Compiling risks identified from various units within an entity to identify common risk areas
- Providing ideas during brainstorming sessions

The standardized risk language is grouped into the following three units:

- Risk categories—current internal control standards for objectives
- Risk subcategories—internal or external source of the risk
- Risk factors—specific categories with definitions and examples

Several sources were consulted during the development and updates of the risk factors. We used the *Internal Control—Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission, the *Standards for Internal Control in the Federal Government* (Green Book) issued by the Comptroller General of the United States, previous cycles of Leadership Accountability reports, audit reports, focus groups, stakeholder feedback, and a variety of other sources. We appreciate the feedback provided, which has helped improve the usability of the Leadership Accountability Risk Catalog.

This page intentionally blank to facilitate double-sided printing.

Leadership Accountability Risk Catalog

Risk Category	Risk Subcategory	Risk Factors	
Operations	Internal	1	FI$Cal Implementation, Maintenance, or Functionality
		2	New System Implementation (Other Than FI$Cal)
		3	Organizational Structure
		4	Oversight, Monitoring, Internal Control Systems
		5	Physical Resources—Maintenance, Upgrades, Replacements, Security
		6	Program/Activity—Changes, Complexity
		7	Resource Management—Allocation, Leave Balance
		8	Staff—Key Person Dependence, Workforce Planning
		9	Staff—Safety
		10	Staff—Training, Knowledge, Competence
		11	Technology—Data Security, Cybersecurity
		12	Technology—Support, Tools, Design, or Maintenance
		13	Technology—Compatibility
		14	Workplace Environment
		15	Other
		16	Pandemic, Pandemic Related Response (ONLY FOR 2021)
	External	1	Business Interruption, Safety Concerns
		2	Economic Volatility
		3	FI$Cal Implementation, Maintenance, Functionality, or Support
		4	Fraud, Theft, Waste, Misconduct, Vandalism
		5	Funding—Sources, Levels
		6	Litigation
		7	New System Implementation (Other Than FI$Cal)
		8	Oversight of or Program Coordination with Others
		9	Political, Reputation, Media
		10	Service Provider—Internal Control System Adequacy
		11	Staff—Recruitment, Retention, Staffing Levels
		12	Technology—Data Security, Cybersecurity
		13	Technology—Compatibility
		14	Other
		15	Pandemic, Pandemic Related Response (ONLY FOR 2021)
Reporting	Internal	1	Distribution Limitations
		2	FI$Cal Implementation, Maintenance, or Functionality
		3	Information Collected—Adequacy, Accuracy, Interpretation, Timeliness
		4	Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness
		5	New System Implementation (Other Than FI$Cal)
		6	Other
		7	Pandemic, Pandemic Related Response (ONLY FOR 2021)
	External	1	Distribution Limitations
		2	FI$Cal Implementation, Maintenance, or Functionality
		3	Information Collected—Adequacy, Accuracy, Interpretation, Timeliness
		4	Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness
		5	New System Implementation (Other Than FI$Cal)
		6	Other
		7	Pandemic, Pandemic Related Response (ONLY FOR 2021)
Compliance	Internal	1	Priorities Affecting Laws or Regulations
		2	Resource Limitations
		3	Staff Adherence to Policies, Procedures, or Standards
		4	Other
		5	Pandemic, Pandemic Related Response (ONLY FOR 2021)
	External	1	Complexity or Dynamic Nature of Laws or Regulations
		2	Funding—Sources, Levels
		3	Priorities Affecting Laws or Regulations
		4	Service Provider—Internal Control System Adequacy
		5	Responsibilities of Laws or Regulations Clarification
		6	Other
		7	Pandemic, Pandemic Related Response (ONLY FOR 2021)

Leadership Accountability   Risk Catalog

Risk: The possibility that an event will occur and adversely affect the achievement of objectives.[1]

Risk Categories

What is being affected?	
Operations	Effective and efficient functions to achieve an entity's mission or objectives.
Reporting	Preparation and communication of information for use by the entity, stakeholders, or other external parties
Compliance	Activities and actions adhering to applicable laws or regulations.

Risk Subcategories

Where does the risk originate?

Operations	
Internal	Risks originating within an entity affecting its ability to effectively and efficiently achieve its mission or objectives.
External	Risks originating outside of an entity affecting its ability to effectively and efficiently achieve its mission or objectives.

Is the report used internally or externally?

Reporting	
Internal	Risks relating to information needed within an entity to support decision making and performance evaluation.
External	Risks relating to information used outside an entity in accordance with standards, regulations, and stakeholder expectations.

Where does the risk originate?

Compliance	
Internal	Risks within an entity affecting its ability to comply with laws or regulations.
External	Risks outside an entity affecting its ability to comply with laws or regulations.

[1] Standards for Internal Control in the Federal Government, September 2014 (Green Book)

Operations – Internal

Risk Category	Operations

Risk Subcategory	Internal	
Risk Factors	1.	FI$Cal Implementation, Maintenance, or Functionality
	2.	New System Implementation (Other Than FI$Cal)
	3.	Organizational Structure
	4.	Oversight, Monitoring, Internal Control Systems
	5.	Physical Resources—Maintenance, Upgrades, Replacements, Security
	6.	Program/Activity—Changes, Complexity
	7.	Resource Management—Allocation, Leave Balance
	8.	Staff—Key Person Dependence, Workforce Planning
	9.	Staff—Safety
	10.	Staff—Training, Knowledge, Competence
	11.	Technology—Data Security, Cybersecurity
	12.	Technology—Support, Tools, Design, or Maintenance
	13.	Technology—Compatibility
	14.	Workplace Environment
	15.	Other
	16.	Pandemic, Pandemic Related Response (ONLY FOR 2021)

Operations – Internal

Operations— Internal

Risk Category - What is being affected?

Operations: Effective and efficient functions to achieve an entity's mission or objectives

Risk Subcategory - Where does the risk originate?

Internal: Risks originating within an entity affecting its ability to effectively achieve its mission or objectives.

Risk Factor - What is or may be the risk?

Risk Factors	
1. FI$Cal Implementation, Maintenance, or Functionality	Internal implementation or use of FI$Cal causes limitations of staff availability, information accuracy, security, or compatibility. Examples: • Operating inefficiency of system or user error • Lack of sufficient self-service features • Critical accounting functions not performed timely • Time spent learning FI$Cal and unexpected implementation challenges • Incompatibility with internal information systems • Timing of updates does not align with user expectations, creating data entry error
2. New System Implementation (Other Than FI$Cal)	Design or implementation of a system does not provide required information or output. Examples: • Inefficiencies created or availability reduced from errors or lack of familiarity with new system • Unanticipated conditions impact design and result in inefficiency or not achieving desired outcomes • Incompatible with legacy system • Complexity creating higher-than-anticipated costs • Timing of information updates does not align with user expectations, creating data entry errors • Users may not understand the purpose/benefits of system, which may lead to reduced participation, resistance, and/or less effort in implementing changes Note: Include the name of new system in the risk description.

Operations – Internal

Risk Factors	
3. Organizational Structure	Roles or responsibilities influencing efficient or effective operations, including supervision and communication. Examples: • Work duplicated/incomplete due to unclear roles, new program, reorganization, or new objectives • Strategic plan not developed, updated, followed, or does not address inclusive practices • Silos hinder communication or representation in decision-making process • Inefficiencies created by the tone at the top (such as information-sharing limitations created by the organizational structure) • Lack of coordination among units, programs, or areas
4. Oversight, Monitoring, Internal Control Systems	Monitoring, design, or evaluation of the internal control systems to identify and correct deficiencies. Examples: • Policies and procedures are not current, established, followed, monitored, or enforced • Controls are outdated and not effective because of changes in environment or objectives • Opportunity for theft, loss, or misuse of state resources because of internal control design or lack of monitoring • Entity is not monitoring grant expenditures as required • Tone at the top does not emphasize ethical behavior and the control environment • Insufficient or homogeneous feedback on issues from those within the organization
5. Physical Resources—Maintenance, Upgrades, Replacements, Security	Administration of physical resources to ensure proper functionality and security. Examples: • Competing priorities delay maintenance or upgrades • Lacking long-term plans for asset maintenance • Jeopardizing funding from misuse of resources purchased with grant funds • Code violations caused by inadequate building maintenance • Unsecured work area allowing unauthorized access to dangerous conditions or confidential records

Operations – Internal

Risk Factors	
6. Program/Activity—Changes, Complexity	Dynamic or complicated processes may create errors, omissions, or inefficiencies. Examples: • Workload backlogs from program changes inhibit program roll-out or effectiveness • Implementation of plan or design changes produces unanticipated or undesired effects on secondary processes • Complex interactions between various funding sources and the rules governing each create inefficiencies • Addressing multiple concerns simultaneously creates implementation challenges
7. Resource Management—Allocation, Leave Balance	Level or management of fiscal resources, creating inefficiencies, timing challenges, or preventing completion of objectives. Examples: • Leave balance liabilities • Difficult-to-forecast or unplanned expenses exceed budgeted levels • Fees from users either not collected or collected inefficiently • Pressure to identify or fund projects timely
8. Staff—Key Person Dependence, Workforce Planning	Loss of key personnel or changes in work environments and processes cause a gap between staff skills and the critical needs of the entity. Examples: • Limited positions create challenges in cross-training backups • Large percentage of workforce nearing retirement age without suitable replacements • Staff expert is relied upon exclusively without any backup to assist in his/her absence • Changes in workforce skills needed to accomplish the mission
9. Staff—Safety	Conditions presented by the inherent nature of the work performed or by work location. Examples: • Workplace violence or retaliation • Safety concerns impact the ability to recruit and retain staff, increasing the risk of an accident • Safety risks to operating machinery

Operations – Internal

Risk Factors	
10. Staff—Training, Knowledge, Competence	Operational impacts to efficiency due to adequacy of training or other limitations of staff knowledge. Examples: • Inadequate or outdated training resources • Staff resistant to change, does not apply provided training or resources • Lack of commitment or resources to train staff • Process or procedure change not communicated • Staff knowledge/ability not in line with job requirements • Unconscious biases
11. Technology—Data Security, Cybersecurity	Internal acts (accidental or intentional) threaten the integrity, confidentiality, availability, or ownership of information. Examples: • Alteration, loss, disclosure, or loss of control of important, or sensitive information may compromise operations • Evolving conditions hinder timely updates, maintenance, and or security protocols • System controls fail to prevent, detect, or protect from unauthorized access, devices, or software • Clicking on phishing emails • Artificial intelligence applications result in unintended consequences or unwanted results
12. Technology—Support, Tools, Design, or Maintenance	Design or resources causing system functionality issues. Examples: • Disruption of operations due to system failure • Inadequate backup of a system, causing loss of information • Lack of IT personnel or expertise • Lack of appropriate software to efficiently complete assignments
13. Technology—Compatibility	Existing systems do not meet current needs of the entity. Examples: • A legacy system does not work with other software within the entity • Updates and support are no longer available

Operations – Internal

Risk Factors	
14. Workplace Environment	Factors impacting working relationships and organizational culture, such as physical environment, workplace behavior, or shared values. Examples: • Organization is slow to adapt to changes • Low staff morale resulting from workplace culture or perception of favoritism • No incentive to improve performance • Lack of discipline for poor performance • Unit A refuses to collaborate with Unit B due to different workplace cultures • Discrimination, harassment, accessibility issues • In/out-group dynamics hindering working relationships
15. Other	A risk that cannot be clearly defined in another category.
16. Pandemic, Pandemic Related Response (ONLY FOR 2021)	Disruption to internal function resulting from pandemic conditions. Examples: • Impacts to internal communication methods and timing, collaboration, teamwork, camaraderie, morale, employee wellbeing, mental health, changes to employee childcare and eldercare circumstances • Adherence to policies and procedures; updates to policies and procedures cannot keep up with need to address changing circumstances; electronic document version control, document routing procedures • Long-term office lease commitments, underutilized office space; obtaining scheduling software for conference rooms for collaborative work; employee health and safety in the field or office (distancing), compliance with OSHA & other guidelines, exposure to communicable diseases • Data security concerns, access and connectivity limitations; IT support backlog, use of personal equipment to conduct business • Increasing retirements; changes to recruiting, hiring, onboarding new hires, and ongoing training programs • Staffing limitations due to staff being redirected, quarantined, or otherwise not available

Operations – External

Risk Category	Operations

Risk Subcategory	External
Risk Factors	1. Business Interruption, Safety Concerns
	2. Economic Volatility
	3. FI$Cal Implementation, Maintenance, Functionality, or Support
	4. Fraud, Theft, Waste, Misconduct, Vandalism
	5. Funding—Sources, Levels
	6. Litigation
	7. New System Implementation (Other Than FI$Cal)
	8. Oversight of or Program Coordination with Others
	9. Political, Reputation, Media
	10. Service Provider—Internal Control System Adequacy
	11. Staff—Recruitment, Retention, Staffing Levels
	12. Technology—Data Security, Cybersecurity
	13. Technology—Compatibility
	14. Other
	15. Pandemic, Pandemic Related Response (ONLY FOR 2021)

Operations – External

Operations—External

Risk Category - What is being affected?

Operations: Effective and efficient functions to achieve an entity's mission or objectives.

Risk Subcategory - Where does the risk originate?

External: Risks originating outside an entity affecting its ability to effectively achieve its mission or objectives.

Risk Factor - What is or may be the risk?

Risk Factors	
1. Business Interruption, Safety Concerns	Disruption to operational objectives, endangerment, or threat to the public or resources due to external acts or natural disasters. Examples: • Terrorist or criminal acts/threats • Natural disasters such as droughts, earthquakes, floods, and wildfires • Communicable disease outbreaks • Agricultural contamination from unsafe water runoff • Riots, protests, and other forms of civil unrest • Irate customer disrupting operations
2. Economic Volatility	Market factors have an effect on entity objectives. Examples: • Rise in capital gains creating temporary tax surplus • Sharp decrease in financial market creating a deficit for retirement funding • Decrease in disposable income leading to lower sales tax revenue • Increasing demand for unemployment benefits • Operating expenses increasing due to a spike in energy prices
3. FI$Cal Implementation, Maintenance, Functionality, or Support	Design, implementation, maintenance, operation, or support of FI$Cal causing limitations of information availability, security, or access. Examples: • Loss of information, lack of availability, server downtime, or slow response • Information security breaches on FI$Cal servers • Inadequate system support • System maintenance having unanticipated effects on other FI$Cal functions

Operations – External

Risk Factors	
4. Fraud, Theft, Waste, Misconduct, Vandalism	Anyone other than staff causing damage or loss of the entity's property. Examples: • Medi-Cal fraud and abuse • Public stealing equipment from entity's work site • Grantee using grant funds for a purpose other than intended • Visitors to a state park damage property
5. Funding—Sources, Levels	Resources used to finance an entity objective may be reduced, discontinued, difficult to obtain, or have timing concerns. Examples: • Entity is heavily reliant on nonguaranteed federal funds • Depletion of available bond funds • Decline in private donations • Complex grant application requirements create challenges for an entity • Pressure to identify or fund projects timely
6. Litigation	Possible legal action by an outside party in response to an entity's actions, inactions, services, or other events. Example: • Group(s) sues entity due to implementation of a new law • Lawsuits filed due to perceived discrimination, reverse discrimination, or lack of reasonable accommodations
7. New System Implementation (Other Than FI$Cal)	Level of information availability, security, or access caused by design or implementation of a new system managed by another entity. Examples: • Information loss, lack of availability, server downtime, or slow response for systems managed by another entity • Information security breaches on other entity's servers • Limited access to subject matter expertise or system resources • Inadequate data or information sharing Note: Include the name of new system in the risk description.

Operations – External

Risk Factors	
8. Oversight of or Program Coordination with Others	Program complexity, level of understanding, or differences in goals, prevent or create inefficiencies in meeting objectives. Examples: • Communication deficiency with oversight agency • Local regulations conflict with entity goals • Grantee does not complete grant deliverables due to conflicting priorities • Third-party vendors fail to deliver on commitments, provide complete and accurate information, or engage in practices inconsistent with program principles
9. Political, Reputation, Media	Disruption to operations due to perceptions of an entity, changes in political climate, or publicity. Examples: • Negative media attention • Protests due to controversial practices of an entity • Diminishing public confidence due to appearance of mismanagement or inequities • Political pressure to change entity operations or objectives • Collective bargaining process impacting public opinion or interrupting operations • Public scrutiny of failures or perceived inconsistencies • Changes in federal, state, or local laws affecting goals of the operation
10. Service Provider—Internal Control System Adequacy	Adequacy of oversight of a service provider (defined below) creates inefficiencies or prevents accomplishment of entity mission or objectives. Entity management is responsible for the performance of processes assigned to the service provider. Risks exist when the entity does not sufficiently review the service provider's work. Insufficient review may be the result of lack of entity expertise, procedures, staff levels, or some other factor. Service Provider is defined as an organization performing certain operational processes for the entity, such as accounting and payroll processing, security services, or IT services. Example: • Service provider's weak internal controls result in erroneous expenditure reporting, which was not identified by the entity, causing the entity to pay incorrect claims

Operations – External

Risk Factors	
11. Staff—Recruitment, Retention, Staffing Levels	Staffing levels create inefficiencies or prevent achievement of entity mission or objectives. Examples: • Inability to find or retain viable candidates due to pay, location, experience, promotional advancement, or worker fatigue from overtime • Lengthy hiring process • Backlog or reduced quality of work due to inadequate staff levels
12. Technology—Data Security, Cybersecurity	External acts threaten the integrity, confidentiality, availability, or ownership of information. Examples: • Harm from artificial intelligence-enhanced attacks, malware, ransomware, phishing, spyware, or spoofing • Outdated or limited identity authorization • Cyber-attacks cause alteration, loss, disclosure, or loss of control of important, or sensitive information • Evolving conditions degrade system(s) performance, hinder timely updates, maintenance, or other security protocols • System controls fail to prevent, detect, or protect from unauthorized access, devices, or software
13. Technology—Compatibility	Information system limitations hinder communication. Examples: • Communication failure between two interdependent networks • Background check data not centralized • Counties' prisoner realignment population data is inconsistent with state data
14. Other	A risk that cannot be clearly defined in another category.

Operations – External

Risk Factors	
15. Pandemic, Pandemic Related Response (ONLY IN 2021)	Disruption to the operational mission, goals, and/or objectives resulting from pandemic conditions. Examples: • Application processing for public services and benefits delayed; backlog of applications for public services exceeded resource capacity • Impacts or delays to inspection schedules due to staff being redirected or otherwise not available; gaps in services were exacerbated • Procurement delays in obtaining equipment and supplies • Data security concerns, access and connectivity limitations • Tracking equipment assigned to remote workforce and risk of loss when staff separate from state employment; use of state cameras within an employee's private residence • Outreach efforts with stakeholders and other community members impacted; the public’s experience with government negatively impacted; erosion of government’s reputation from inability to meet the public need • Concern for employee or consumer health and safety while in a state facility or in the field

Reporting – Internal

Risk Category	Reporting

Risk Subcategory	Internal
Risk Factors	1. Distribution Limitations
	2. FI$Cal Implementation, Maintenance, or Functionality
	3. Information Collected—Adequacy, Accuracy, Interpretation, Timeliness
	4. Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness
	5. New System Implementation (Other Than FI$Cal)
	6. Other
	7. Pandemic, Pandemic Related Response (ONLY IN 2121)

Reporting – Internal

Reporting—Internal

Risk Category - What is being affected?

Reporting: Preparation and communication of information for use by the entity, stakeholders, or other external parties.

Risk Subcategory - Is the report used internally or externally?

Internal: Risks related to information needed within an entity to support decision making and performance evaluation.

Risk Factor - What is or may be the risk?

Risk Factors	
1. Distribution Limitations	Inadequate or outdated system/method exists to disseminate information within the organization. Examples: • Inadequate process to inform employees of new policies • Inadequate process to update and maintain distribution lists
2. FI$Cal Implementation, Maintenance, or Functionality	Internal FI$Cal reports are inadequate, inaccurate, misinterpreted, or untimely to meet internal user needs. Examples: • Information is not available or not structured in a way that is useful for management decision-making • Information in FI$Cal reports is inadequate, inaccurate, misinterpreted, or untimely • Staff not aware of FI$Cal reporting capabilities, causing inefficient methods to gather or present needed information • FI$Cal update frequency does not match user expectations or understanding, resulting in misinterpretation of available information • System functionality affects ability to access information or enter data used for management decision making

Reporting – Internal

Risk Factors	
3. Information Collected—Adequacy, Accuracy, Interpretation, Timeliness	Information gathered is inadequate, inaccurate, misinterpreted, or untimely to generate a reliable report. Examples: • Shared information has errors • Incorrect inputs produce inaccurate results • Manual process for gathering data causes delays • System downtime causes delays • Insufficient records retained to support decision making • Interpretation biases introduce assumptions, perspectives, or preconceived notions that influence the interpretation of information • Terminology inaccurately captures information, unintentionally excluding individuals from reporting or resulting in insensitive reporting
4. Information Communicated — Adequacy, Accuracy, Interpretation, Timeliness	Information distributed to users is inadequate, inaccurate, misinterpreted, or untimely to convey the intended message. Examples: • Inaccurate air quality report • Unemployment report does not include underemployed workers • Reports take a long time to produce • Communication channels are ineffective or inaccessible to employees
5. New System Implementation (Other Than FI$Cal)	Internal reports are inadequate, inaccurate, misinterpreted, or untimely to meet internal user needs. Examples: • Information is not available or not structured in a way that is useful for management decision making • Staff not aware of reporting capabilities, causing inefficient methods to gather or present needed information • System update frequency does not match user expectations or understanding, resulting in misinterpretation of available information • Inadequate analysis and interpretation causing limited insights or disregard for crucial patterns and trends Note: Include the name of new system in the risk description.

Reporting – Internal

Risk Factors	
6. Other	A risk that cannot be clearly defined in another category.
7. Pandemic, Pandemic Related Response (ONLY IN 2021)	Information gathered or distributed for internal purposes does not satisfy the intended purpose. Examples: • User report may be impacted or delayed resulting from staff shortages or telework environment • Report may be impacted by data security concerns, data access or quality, or connectivity limitations • Tracking relief funding and outcomes

Reporting – External

Risk Category	Reporting

Risk Subcategory	External
Risk Factors	1. Distribution Limitations
	2. FI$Cal Implementation, Maintenance, or Functionality
	3. Information Collected— Adequacy, Accuracy, Interpretation, Timeliness
	4. Information Communicated— Adequacy, Accuracy, Interpretation, Timeliness
	5. New System Implementation (Other Than FI$Cal)
	6. Other
	7. Pandemic, Pandemic Related Response (ONLY IN 2021)

Reporting – External

Reporting—External

Risk Category - What is being affected?

Reporting: Preparation and communication of information for use by the entity, stakeholders, or other external parties.

Risk Subcategory - Is the report used internally or externally?

External: Risks related to information used outside of an entity in accordance with standards, regulations, and stakeholder expectations.

Risk Factor – What is or may be the risk?

Risk Factors	
1. Distribution Limitations	Inadequate or outdated system/method exists to disseminate information outside the organization. Examples: • New tools available for use but stakeholders are unaware of the information available • Email notifications go into spam folders • Inadequate processes to update and maintain distribution lists • Lack of standardized reporting leading to inconsistent or fragmented reporting
2. FI$Cal Implementation, Maintenance, or Functionality	FI$Cal reports are inadequate, inaccurate, misinterpreted, or untimely to convey the intended message due to the implementation, design, maintenance, or functionality of FI$Cal. Examples: • Vendors misinterpret reports generated from FI$Cal because of a lack of experience reading the report • External parties provide incorrect information as a result of a misunderstood report • System functionality affects ability to access or enter data needed to create a report for outside users

Reporting – External

Risk Factors	
3. Information Collected—Adequacy, Accuracy, Interpretation, Timeliness	Information gathered is inadequate, inaccurate, misinterpreted, or untimely to generate a reliable report. Examples: • Shared interagency information has errors • Incorrect inputs produce inaccurate results • External parties provide incorrect information as a result of misunderstood report requirements • Insufficient records retained to support decision-making • Interpretation biases introduce assumptions, perspectives, or preconceived notions that influence the interpretation of information • Terminology inaccurately captures information, unintentionally excluding individuals from reporting or resulting in insensitive reporting
4. Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness	Information distributed to users is inadequate, inaccurate, misinterpreted, or untimely to convey the intended message. Examples: • Inaccurate air quality report • Unemployment report does not include underemployed workers • Reports take a long time to produce • Communication channels are ineffective or inaccessible to users
5. New System Implementation (Other Than FI$Cal)	Reports are inadequate, inaccurate, misinterpreted, or untimely to convey the intended message due to the implementation or design of a new system. Examples: • Vendors misinterpret reports generated from a new system because of a lack of experience reading the report • External parties provide incorrect information as a result of a misunderstood report Note: Include the name of new system in the risk description
6. Other	A risk that cannot be clearly defined in another category.
7. Pandemic, Pandemic Related Response (ONLY IN 2021)	Information gathered or distributed for external purposes does not satisfy the intended purpose. Examples: • Report may be impacted due to data security concerns, data access or quality, or connectivity limitations • Communication from and to stakeholders and other community members impacted by operating conditions . Tracking relief funding and outcomes

Reporting – External

Risk Category	Compliance

Risk Subcategory	Internal
Risk Factors	1. Priorities Affecting Laws or Regulations
	2. Resource Limitations
	3. Staff Adherence to Policies, Procedures, or Standards
	4. Other
	5. Pandemic, Pandemic Related Response (ONLY IN 2021)

Compliance – Internal

Compliance—Internal

Risk Category - What is being affected?
Compliance: Activities and actions adhering to applicable laws and regulations.

Risk Subcategory - Where does the risk originate?
Internal: Risks within an entity affecting its ability to comply with laws or regulations.

Risk Factor - What is or may be the risk?

Risk Factors	
1. Priorities Affecting Laws or Regulations	Directives, decisions creating financial, or timeline pressures to meet specific objectives. Examples: • Financial statement presentation requirements vary for different users • Project deadlines create incentives to not follow all requirements • Misrepresentation of performance or data
2. Resource Limitations	The ability to comply with laws or regulations is jeopardized by the level of resources such as staff, facilities, or funds. Examples: • Inadequate staff time to produce a report required by new legislation • Limited storage space to secure confidential documents required for compliance with a regulation • Insufficient funding to maintain pathways that comply with accessibility requirements
3. Staff Adherence to Policies, Procedures, or Standards	Staff performing duties in a way that may affect compliance with laws, regulations, or policies. Examples: • Training or resource level, or insubordination • Changes to professional licensing, continuing education requirements, or construction standards • Staff do not actively embed diversity, equity, inclusion, and accessibility principles in their work
4. Other	A risk that cannot be clearly defined in another category.

Compliance – Internal

Risk Factors	
5. Pandemic, Pandemic Related Response (ONLY IN 2021)	Pandemic conditions challenge the organizations efforts to comply with internal requirements. Examples: • Remote working environment challenges data security compliance measures • Changes to onboarding new staff and ongoing training programs to ensure staff meet licensing and other requirements • Compliance with OSHA & other guidelines for employee safety and health • Rapidly changing regulations and laws

Compliance – Internal

Risk Category	Compliance

Risk Subcategory	External
Risk Factors	1. Complexity or Dynamic Nature of Laws or Regulations
	2. Funding—Sources, Levels
	3. Priorities Affecting Laws or Regulations
	4. Service Provider—Internal Control System Adequacy
	5. Responsibilities of Laws or Regulations Clarification
	6. Other
	7. Pandemic, Pandemic Related Response (ONLY IN 2021)

Compliance – External

Compliance—External

Risk Category - What is being affected?
Compliance: Activities and actions adhering to applicable laws and regulations.

Risk Subcategory - Where does the risk originate?
External: Risks outside an entity affecting its ability to comply with laws or regulations.

Risk Factor - What is or may be the risk?

Risk Factors	
1. Complexity or Dynamic Nature of Laws or Regulations	Difficult-to-interpret or changing requirements of laws or regulations. Examples: • Complex legal requirements creating interpretation concerns • Court rulings affecting interpretation of laws
2. Funding—Sources, Levels	Resources needed to comply with law being reduced, discontinued, or difficult to obtain, or resources available have timing restrictions. Example: • Funding limits full program implementation required by the law • Pressure to identify or fund projects timely
3. Priorities Affecting Laws or Regulations	Financial or timeline pressures to meet specific objectives. Example: • Pressure from the public to meet a project deadline or budget creating an incentive to not follow guidelines

Compliance – External

Risk Factors	
4. Service Provider—Internal Control System Adequacy	Adequacy of oversight of service provider (defined below) creating the risk of noncompliant services. Entity management is responsible for the performance of processes assigned to the service provider. Risks exist when the entity does not sufficiently review the service provider's work. Insufficient review may be the result of lack of entity expertise, procedures, staff levels, or some other factor. Service Provider is defined as an organization performing certain operational processes for the entity, such as accounting and payroll processing, security services, or IT services. Example: • Inadequate review of payroll provider's withholdings data which were processed improperly causing the entity to not comply with payroll laws
5. Responsibilities of Laws or Regulations Clarification	Conflicting, inconsistent, or undefined requirements among governing bodies. Examples: • Law or regulations are not being updated timely to reflect changes in environment such as creation of a new entity or merging of two entities • State legalization of marijuana conflicting with federal law • Undeveloped interagency cooperation preventing optimal enforcement of a law or regulation • A new regulation is inconsistent with a preexisting regulation
6. Other	A risk that cannot be clearly defined in another category.

Compliance – External

Risk Factors	
7. Pandemic, Pandemic Related Response (ONLY FOR 2021)	Pandemic conditions challenge the organization's efforts to comply with externally imposed requirements. Examples: • Communication & outreach impacts to stakeholders or regulated community • Compliance with grant requirements impacted due to COVID related program delays • Data security concerns, access and connectivity limitations • Changes to onboarding new staff and ongoing training programs to ensure staff meet licensing and other requirements • Employee and citizen safety in the field or office (distancing), compliance with OSHA & other guidelines • Rapidly changing regulations and laws