



---

# **State Leadership Accountability Act Risk Catalog**

---

This page intentionally blank to facilitate double-sided printing

**State Leadership Accountability Act (SLAA) Risk Catalog  
Table of Contents**

**Introduction ..... 1**

**SLAA Risk Categories Overview**

SLAA Risk Categories Overview ..... 3

Risk Categories..... 4

Risk Subcategories ..... 4

**Operations**

Internal..... 5

External..... 11

**Reporting**

Internal..... 16

External ..... 19

**Compliance**

Internal..... 22

External ..... 24

# SLAA Risk Catalog

This page intentionally blank to facilitate double-sided printing

# SLAA Risk Catalog

## Introduction

This document is a tool to provide a statewide, standardized risk language for 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 SLAA 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 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, four cycles of previous SLAA 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 SLAA Risk Catalog.

# SLAA Risk Catalog

This page intentionally blank to facilitate double-sided printing

## SLAA Risk Categories Overview

Risk Category	Risk Subcategory	Risk Factors
<b>Operations</b>	<b>Internal</b>	<ol style="list-style-type: none"> <li>1 FI\$Cal Implementation, Maintenance, or Functionality</li> <li>2 New System Implementation (Other Than FI\$Cal)</li> <li>3 Organizational Structure</li> <li>4 Oversight, Monitoring, Internal Control Systems</li> <li>5 Physical Resources—Maintenance, Upgrades, Replacements, Security</li> <li>6 Program/Activity—Changes, Complexity</li> <li>7 Resource Management—Allocation, Leave Balance</li> <li>8 Staff—Key Person Dependence, Workforce Planning</li> <li>9 Staff—Safety</li> <li>10 Staff—Training, Knowledge, Competence</li> <li>11 Technology—Data Security</li> <li>12 Technology—Support, Tools, Design, or Maintenance</li> <li>13 Technology—Compatibility</li> <li>14 Workplace Environment</li> <li>15 Other</li> </ol>
	<b>External</b>	<ol style="list-style-type: none"> <li>1 Business Interruption, Safety Concerns</li> <li>2 Economic Volatility</li> <li>3 FI\$Cal Implementation, Maintenance, Functionality, or Support</li> <li>4 Fraud, Theft, Waste, Misconduct, Vandalism</li> <li>5 Funding—Sources, Levels</li> <li>6 Litigation</li> <li>7 New System Implementation (Other Than FI\$Cal)</li> <li>8 Oversight of or Program Coordination with Others</li> <li>9 Political, Reputation, Media</li> <li>10 Service Provider—Internal Control System Adequacy</li> <li>11 Staff—Recruitment, Retention, Staffing Levels</li> <li>12 Technology—Data Security</li> <li>13 Technology—Compatibility</li> <li>14 Other</li> </ol>
<b>Reporting</b>	<b>Internal</b>	<ol style="list-style-type: none"> <li>1 Distribution Limitations</li> <li>2 FI\$Cal Implementation, Maintenance, or Functionality</li> <li>3 Information Collected—Adequacy, Accuracy, Interpretation, Timeliness</li> <li>4 Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness</li> <li>5 New System Implementation (Other Than FI\$Cal)</li> <li>6 Other</li> </ol>
	<b>External</b>	<ol style="list-style-type: none"> <li>1 Distribution Limitations</li> <li>2 FI\$Cal Implementation, Maintenance, or Functionality</li> <li>3 Information Collected—Adequacy, Accuracy, Interpretation, Timeliness</li> <li>4 Information Communicated—Adequacy, Accuracy, Interpretation, Timeliness</li> <li>5 New System Implementation (Other Than FI\$Cal)</li> <li>6 Other</li> </ol>
<b>Compliance</b>	<b>Internal</b>	<ol style="list-style-type: none"> <li>1 Priorities Affecting Laws or Regulations</li> <li>2 Resource Limitations</li> <li>3 Staff Adherence to Policies, Procedures, or Standards</li> <li>4 Other</li> </ol>
	<b>External</b>	<ol style="list-style-type: none"> <li>1 Complexity or Dynamic Nature of Laws or Regulations</li> <li>2 Funding—Sources, Levels</li> <li>3 Priorities Affecting Laws or Regulations</li> <li>4 Service Provider—Internal Control System Adequacy</li> <li>5 Responsibilities of Laws or Regulations Clarification</li> <li>6 Other</li> </ol>

[Back to Top](#)

# SLAA Risk Categories

<b>Risk</b>	The possibility that an event will occur and adversely affect the achievement of objectives <sup>1</sup>
-------------	--

## Risk Categories

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

## Risk Subcategories

Where does the risk originate?	
Operations	
<b>Internal</b>	Risks originating within an entity affecting its ability to effectively and efficiently achieve its mission or objectives.
<b>External</b>	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	
<b>Internal</b>	Risks relating to information needed within an entity to support decision making and performance evaluation.
<b>External</b>	Risks relating to information used outside an entity in accordance with standards, regulations, and stakeholder expectations.

Where does the risk originate?	
Compliance	
<b>Internal</b>	Risks within an entity affecting its ability to comply with laws or regulations.
<b>External</b>	Risks outside an entity affecting its ability to comply with laws or regulations.

<sup>1</sup> Standards for Internal Control in the Federal Government, September 2014 (Green Book)



## Operations – Internal

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

# 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 and efficiently achieve its mission or objectives.

**Risk Factor—What is or may be the risk?**

**Risk Factors**

<p>1. FI\$Cal Implementation, Maintenance, or Functionality</p>	<p>Internal implementation or use of FI\$Cal causing limitations of staff availability, information accuracy, security, or compatibility.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Operating inefficiency as a result of system or user error</li> <li>• Lack of sufficient self-service features</li> <li>• Critical accounting functions not performed timely</li> <li>• Staff availability is reduced by time spent learning FI\$Cal and applying temporary fixes for any unexpected challenges of implementation</li> <li>• FI\$Cal system incompatibility with internal information systems</li> <li>• Timing of FI\$Cal updates do not align with user expectations, creating data entry error</li> </ul>
<p>2. New System Implementation (Other Than FI\$Cal)</p>	<p>Design or implementation of a system failing to provide required information or output.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Inefficiencies created as a result of user errors or lack of familiarity with new system</li> <li>• Unanticipated conditions impacting the design of the new system, causing it to function inefficiently or fail to achieve desired outcomes</li> <li>• New system is incompatible with legacy system, resulting in loss of data</li> <li>• Complexity of a program creating higher-than-anticipated costs</li> <li>• Staff availability reduced by time spent training for new system</li> <li>• Timing of system information updates does not align with user expectations, creating data entry errors</li> </ul> <p>Note: Include the name of new system in the risk description.</p>

## Operations – Internal

<b>3. Organizational Structure</b>	<p>Roles or responsibilities influencing efficient or effective operations including supervision and communication.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Work duplicated/incomplete due to unclear roles, a new program, an entity reorganization, or new objectives</li><li>• Strategic plan is not developed, updated, or followed</li><li>• Silos within an entity hinder efficient communication</li><li>• Inefficiencies created by the tone at the top (such as information sharing limitations created by the organizational structure)</li><li>• Lack of coordination among units, programs, or areas</li></ul>
<b>4. Oversight, Monitoring, Internal Control Systems</b>	<p>Monitoring, design, or evaluation of the internal control systems to identify and correct deficiencies.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Policies and procedures are not current, established, followed, or enforced</li><li>• Controls have become outdated and are no longer effective because of changes in environment or objectives</li><li>• Opportunity for theft, loss, or misuse of state resources as a result of a poorly designed internal control system or lack of oversight and monitoring</li><li>• Lack of adequate monitoring to prevent or identify procedures not being followed</li><li>• Entity is not monitoring grant expenditures as required</li><li>• Tone at the top (such as the tone set by management for ethical behavior and the control environment)</li></ul>
<b>5. Physical Resources—Maintenance, Upgrades, Replacements, Security</b>	<p>Administration of physical resources to ensure proper functionality and security.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Competing priorities delaying allocation of resources for maintenance or upgrades</li><li>• Lacking long-term plans for asset maintenance</li><li>• Jeopardizing funding from misuse of resources purchased with grant funds</li><li>• Code violations caused by inadequate building maintenance</li><li>• Unsecured work area allowing unauthorized access to dangerous conditions or confidential records</li></ul>

## Operations – Internal

<b>6. Program/Activity— Changes, Complexity</b>	<p>Dynamic or complicated processes creating opportunity for errors, omissions, or inefficiencies.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Highly complex time keeping process causes overpayment to employees</li><li>• Workload backlogs from program changes inhibit program roll-out or effectiveness</li><li>• Implementation of plan or design changes produce unanticipated or undesired effects to secondary processes</li><li>• Complex interactions between various funding sources and the rules governing each creating inefficiencies</li></ul>
<b>7. Resource Management— Allocation, Leave Balance</b>	<p>Level or management of fiscal resources, creating inefficiencies or preventing completion of objectives.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Leave balance liabilities</li><li>• Difficult-to-forecast or unplanned expenses exceed budgeted levels</li><li>• Fees from users either not collected or collected inefficiently</li></ul>
<b>8. Staff—Key Person Dependence, Workforce Planning</b>	<p>Loss of key personnel or changes in work environments and processes causing a gap between staff skills and the critical needs of the entity.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Limited positions create challenges cross-training backups</li><li>• Large percentage of workforce nearing retirement age without suitable replacements</li><li>• Staff expert is relied upon exclusively without any backup to assist in his/her absence</li><li>• Changes in workforce skills needed to accomplish the mission</li></ul>
<b>9. Staff—Safety</b>	<p>Conditions presented by the inherent nature of the work performed or by work location.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Workplace violence or retaliation</li><li>• Safety concerns impact ability to recruit and retain staff, increasing the risk of an accident</li><li>• Safety risks to operating machinery</li></ul>

## Operations – Internal

<b>10. Staff—Training, Knowledge, Competence</b>	<p>Operational impacts to efficiency due to adequacy of training or other limitations of staff knowledge.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Inadequate or outdated training resources</li><li>• Staff resistant to change</li><li>• Lack of commitment or resources to train staff</li><li>• Process or procedure change not communicated to existing staff</li><li>• Staff knowledge and ability not in line with job requirements</li><li>• Staff does not use or apply the training/resources provided</li></ul>
<b>11. Technology—Data Security</b>	<p>Internal acts threatening the integrity, safety, or privacy of information.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Staff accidentally altering important files</li><li>• Unintentional release of confidential information</li><li>• Failing to follow internal security procedures such as inappropriate password sharing or failing to lock computer</li><li>• Access levels allow users to view unauthorized information</li><li>• Inadequate process to discourage or identify unauthorized access</li></ul>
<b>12. Technology—Support, Tools, Design, or Maintenance</b>	<p>Design or resources causing system functionality issues.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Disruption of operations due to system failure</li><li>• Inadequate back up of a system, causing loss of information</li><li>• Lack of IT personnel or expertise</li><li>• Lack of appropriate software to efficiently complete assignments</li></ul>
<b>13. Technology—Compatibility</b>	<p>Existing systems do not meet current needs of the entity.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• A legacy system does not work with other software within the entity</li><li>• Updates and support are no longer available</li></ul>

## Operations – Internal

<b>14. Workplace Environment</b>	<p>Factors impacting working relationships and organizational culture, such as physical environment, workplace behavior, or shared values.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Organization is slow to adapt to changes</li><li>• Low staff morale resulting from workplace culture or perception of favoritism</li><li>• No incentive to improve performance</li><li>• Lack of discipline for poor performance</li><li>• Unit A refuses to collaborate with Unit B due to different workplace cultures</li><li>• Discrimination and harassment issues</li></ul>
<b>15. Other</b>	<p>A risk that cannot be clearly defined in another category.</p>

## Operations – External

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

# 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 and efficiently achieve its mission or objectives.

**Risk Factor—What is or may be the risk?**

## Risk Factors

<p><b>1. Business Interruption, Safety Concerns</b></p>	<p>Disruption to operational objectives, endangerment, or threat to the public or resources due to external acts or natural disasters.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Terrorist or criminal acts/threats</li> <li>• Natural disasters such as droughts, earthquakes, floods, and wildfires</li> <li>• Communicable disease outbreaks</li> <li>• Agricultural contamination from unsafe water runoff</li> <li>• Riots, protests, and other forms of civil unrest</li> <li>• Irate customer disrupting operations</li> </ul>
<p><b>2. Economic Volatility</b></p>	<p>Market factors having an effect on entity objectives.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Rise in capital gains creating temporary tax surplus</li> <li>• Sharp decrease in financial market creating a deficit for retirement funding</li> <li>• Decrease in disposable income leading to lower sales tax revenue</li> <li>• Increasing demand for unemployment benefits</li> <li>• Operating expenses increasing due to a spike in energy prices</li> </ul>
<p><b>3. FI\$Cal Implementation, Maintenance, Functionality, or Support</b></p>	<p>Design, implementation, maintenance, operation, or support of FI\$Cal causing limitations of information availability, security, or access.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Loss of information, lack of availability, server down time, or slow response</li> <li>• Information security breaches on FI\$Cal servers</li> <li>• Inadequate system support</li> <li>• System maintenance having unanticipated effects on other FI\$Cal functions</li> </ul>



## Operations – External

<p><b>4. Fraud, Theft, Waste, Misconduct, Vandalism</b></p>	<p>Anyone other than staff causing damage or loss of the entity’s property.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Medi-Cal fraud and abuse</li> <li>• Public stealing equipment from entity’s work site</li> <li>• Grantee using grant funds for a purpose other than intended</li> <li>• Visitors to a state park damage property</li> </ul>
<p><b>5. Funding—Sources, Levels</b></p>	<p>Resources used to finance an entity objective may be reduced, discontinued, or difficult to obtain.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Entity is heavily reliant on nonguaranteed federal funds</li> <li>• Depletion of available bond funds</li> <li>• Decline in private donations</li> <li>• Complex grant application requirements create challenges for an entity</li> </ul>
<p><b>6. Litigation</b></p>	<p>Possible legal action by an outside party in response to an entity’s actions, inactions, services, or other events.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• Public interest groups sue entity due to implementation of a new law they believe violates civil rights</li> </ul>
<p><b>7. New System Implementation (Other Than FI\$Cal)</b></p>	<p>Level of information availability, security, or access caused by design or implementation of a new system managed by another entity.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Information loss, lack of availability, server down time, or slow response for systems managed by another entity</li> <li>• Information security breaches on other entity’s servers</li> </ul> <p>Note: Include the name of new system in the risk description.</p>
<p><b>8. Oversight of or Program Coordination with Others</b></p>	<p>Program complexity, level of understanding, or differences in goals, which prevent or create inefficiencies in meeting objectives.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Communication deficiency with oversight agency</li> <li>• Local regulations conflict with entity goals</li> <li>• Grantee does not complete grant deliverables due to conflicting priorities</li> </ul>

## Operations – External

<b>9. Political, Reputation, Media</b>	<p>Disruption to operations due to perceptions of an entity, changes in political climate, or publicity.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Negative media attention</li><li>• Protests due to controversial practices of an entity</li><li>• Diminishing public confidence due to appearance of mismanagement</li><li>• Political pressure to change entity operations or objectives</li><li>• Collective bargaining process impacting public opinion or interrupting operations</li></ul>
<b>10. Service Provider—Internal Control System Adequacy</b>	<p>Adequacy of oversight of a service provider (defined below) creating inefficiencies or preventing accomplishment of entity mission or objectives.</p> <p>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.</p> <p>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.</p> <p>Example:</p> <ul style="list-style-type: none"><li>• 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</li></ul>
<b>11. Staff—Recruitment, Retention, Staffing Levels</b>	<p>Staffing levels creating inefficiencies or preventing achievement of entity mission or objectives.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Inability to find or retain viable candidates due to pay, location, experience, promotional advancement, or worker fatigue from overtime</li><li>• Lengthy hiring process</li><li>• Backlog or reduced quality of work due to inadequate staff levels</li></ul>
<b>12. Technology—Data Security</b>	<p>Intentional external acts threatening the integrity, safety, or privacy of information.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Hacking into an entity's database</li><li>• Inadequate process to discourage or identify unauthorized access</li></ul>

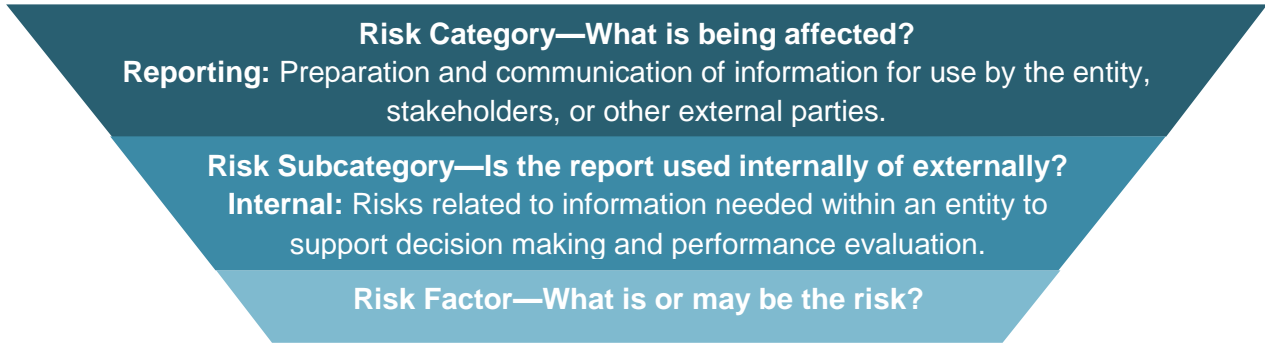
## Operations – External

<b>13. Technology— Compatibility</b>	Information system limitations hindering communication.  Examples: <ul style="list-style-type: none"><li>• Communication failure between two interdependent entities' networks</li><li>• Background check data not centralized</li><li>• Counties' prisoner realignment population data is inconsistent with state data</li></ul>
<b>14. Other</b>	A risk that cannot be clearly defined in another category.

## 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

# Reporting—Internal



### Risk Factors

<b>1. Distribution Limitations</b>	<p>Inadequate or outdated system/method exists to disseminate information within the organization.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Inadequate process to inform employees of new policies</li> <li>• Inadequate process to update and maintain distribution lists</li> </ul>
<b>2. FI\$Cal Implementation, Maintenance, or Functionality</b>	<p>Internal FI\$Cal reports are inadequate, inaccurate, misinterpreted, or untimely to meet internal user needs.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Information is not available or not structured in a way that is useful for management decision making</li> <li>• Information in FI\$Cal reports is inadequate, inaccurate, misinterpreted, or untimely</li> <li>• Staff not aware of FI\$Cal reporting capabilities, causing inefficient methods to gather or present needed information</li> <li>• FI\$Cal update frequency does not match user expectations or understanding, resulting in misinterpretation of available information</li> <li>• System functionality affects ability to access information or enter data used for management decision making</li> </ul>
<b>3. Information Collected—Adequacy, Accuracy, Interpretation, Timeliness</b>	<p>Information gathered is inadequate, inaccurate, misinterpreted, or untimely to generate a reliable report.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Shared information has errors</li> <li>• Incorrect inputs produce inaccurate results</li> <li>• Manual process for gathering data causes delays</li> <li>• System downtime causes delays</li> <li>• Insufficient records retained to support decision making</li> </ul>

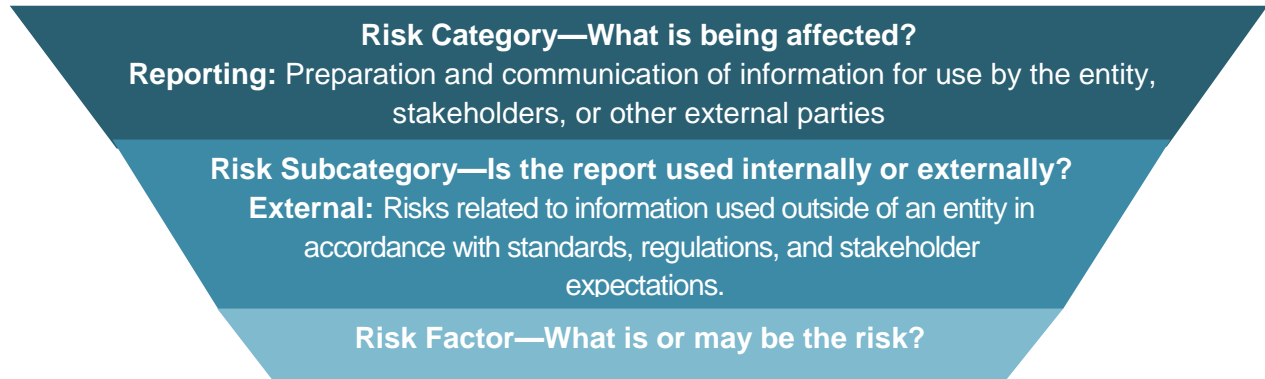
## Reporting – Internal

<b>4. Information Communicated— Adequacy, Accuracy, Interpretation, Timeliness</b>	<p>Information distributed to users is inadequate, inaccurate, misinterpreted, or untimely to convey the intended message.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Inaccurate air quality report</li><li>• Unemployment report does not include underemployed workers</li><li>• Reports take a long time to produce</li></ul>
<b>5. New System Implementation (Other Than FI\$Cal)</b>	<p>Internal reports are inadequate, inaccurate, misinterpreted, or untimely to meet internal user needs.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Information is not available or not structured in a way that is useful for management decision making</li><li>• Staff not aware of reporting capabilities, causing inefficient methods to gather or present needed information</li><li>• System update frequency does not match user expectations or understanding, resulting in misinterpretation of available information</li></ul> <p>Note: Include the name of new system in the risk description</p>
<b>6. Other</b>	<p>A risk that cannot be clearly defined in another category.</p>

## 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

# Reporting—External



### Risk Factors

<b>1. Distribution Limitations</b>	<p>Inadequate or outdated system/method exists to disseminate information outside the organization.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• New tools available for use but stakeholders are unaware of the information available</li> <li>• Email notifications go into spam folders</li> <li>• Inadequate processes to update and maintain distribution lists</li> </ul>
<b>2. FI\$Cal Implementation, Maintenance, or Functionality</b>	<p>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.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Vendors misinterpret reports generated from FI\$Cal because of a lack of experience reading the report</li> <li>• External parties provide the incorrect information as a result of a misunderstood report</li> <li>• System functionality affects ability to access or enter data needed to create a report for outside users</li> </ul>
<b>3. Information Collected—Adequacy, Accuracy, Interpretation, Timeliness</b>	<p>Information gathered is inadequate, inaccurate, misinterpreted, or untimely to generate a reliable report.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Shared interagency information has errors</li> <li>• Incorrect inputs produce inaccurate results</li> <li>• External parties provide incorrect information as a result of misunderstood report requirements</li> <li>• Insufficient records retained to support decision making</li> </ul>



## Reporting – External

<b>4. Information Communicated— Adequacy, Accuracy, Interpretation, Timeliness</b>	<p>Information distributed to users is inadequate, inaccurate, misinterpreted, or untimely to convey the intended message.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Inaccurate air quality report</li><li>• Unemployment report does not include underemployed workers</li><li>• Reports take a long time to produce</li></ul>
<b>5. New System Implementation (Other Than FI\$Cal)</b>	<p>Reports are inadequate, inaccurate, misinterpreted, or untimely to convey the intended message due to the implementation or design of a new system.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• Vendors misinterpret reports generated from a new system because of a lack of experience reading the report</li><li>• External parties provide incorrect information as a result of a misunderstood report</li></ul> <p>Note: Include the name of new system in the risk description</p>
<b>6. Other</b>	<p>A risk that cannot be clearly defined in another category.</p>

## Compliance – Internal

<b>Risk Category</b>	<b>Compliance</b>
<b>Risk Subcategory</b>	<b>Internal</b>
<b>Risk Factors</b>	1. <b>Priorities Affecting Laws or Regulations</b>
	2. <b>Resource Limitations</b>
	3. <b>Staff Adherence to Policies, Procedures, or Standards</b>
	4. <b>Other</b>

# 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?**

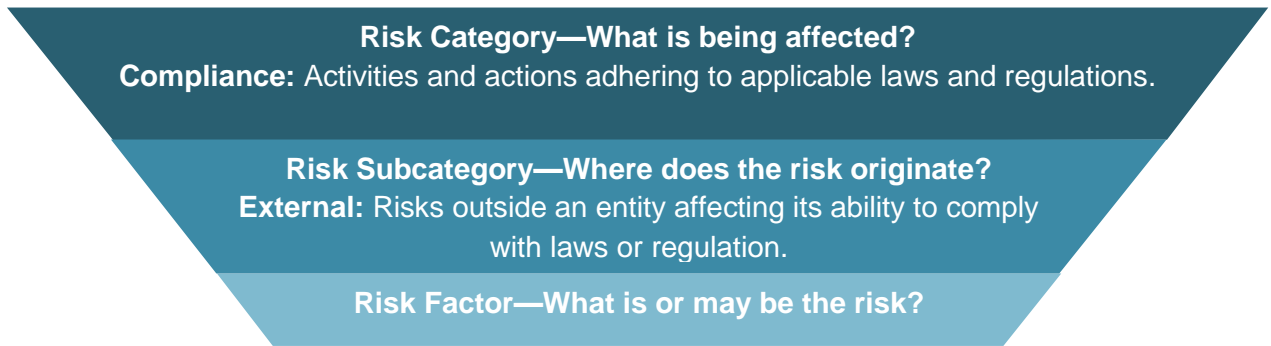
**Risk Factors**

<p>1. <b>Priorities Affecting Laws or Regulations</b></p>	<p>Directives, decisions creating financial, or timeline pressures to meet specific objectives.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Financial statement presentation requirements vary for different users</li> <li>• Project deadlines create incentives to not follow all requirements</li> </ul>
<p>2. <b>Resource Limitations</b></p>	<p>The ability to comply with laws or regulations is jeopardized by the level of resources such as staff, facilities, or funds.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Inadequate staff time to produce a report required by new legislation</li> <li>• Limited storage space to secure confidential documents required for compliance with a regulation</li> <li>• Insufficient funding to maintain pathways that comply with accessibility requirements</li> </ul>
<p>3. <b>Staff Adherence to Policies, Procedures, or Standards</b></p>	<p>Staff performing duties in a way that may affect compliance with laws or regulations.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Training or resource level, or insubordination</li> <li>• Changes to professional licensing, continuing education requirements, or construction standards</li> </ul>
<p>4. <b>Other</b></p>	<p>A risk that cannot be clearly defined in another category.</p>

## Compliance – External

<b>Risk Category</b>	<b>Compliance</b>
<b>Risk Subcategory</b>	<b>External</b>
<b>Risk Factors</b>	1. <b>Complexity or Dynamic Nature of Laws or Regulations</b>
	2. <b>Funding—Sources, Levels</b>
	3. <b>Priorities Affecting Laws or Regulations</b>
	4. <b>Service Provider—Internal Control System Adequacy</b>
	5. <b>Responsibilities of Laws or Regulations Clarification</b>
	6. <b>Other</b>

# Compliance—External



## Risk Factors

<p><b>1. Complexity or Dynamic Nature of Laws or Regulations</b></p>	<p>Difficult-to-interpret or changing requirements of laws or regulations.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Complex legal requirements creating interpretation concerns</li> <li>• Court rulings affecting interpretation of laws</li> </ul>
<p><b>2. Funding—Sources, Levels</b></p>	<p>Resources needed to comply with law being reduced, discontinued, or difficult to obtain.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• Funding limits full program implementation required by the law</li> </ul>
<p><b>3. Priorities Affecting Laws or Regulations</b></p>	<p>Financial or timeline pressures to meet specific objectives.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• Pressure from the public to meet a project deadline or budget creating an incentive to not follow guidelines</li> </ul>
<p><b>4. Service Provider—Internal Control System Adequacy</b></p>	<p>Adequacy of oversight of service provider (defined below) creating the risk of noncompliant services.</p> <p>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.</p> <p>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.</p> <p>Example:</p>

## Compliance – External

	<ul style="list-style-type: none"><li>• Inadequate review of payroll provider’s withholdings data which were processed improperly causing the entity to not comply with payroll laws</li></ul>
<b>5. Responsibilities of Laws or Regulations Clarification</b>	<p>Conflicting, inconsistent, or undefined requirements among governing bodies.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• 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</li><li>• State legalization of marijuana conflicting with federal law</li><li>• Undeveloped interagency cooperation preventing optimal enforcement of a law or regulation</li><li>• A new regulation is inconsistent with a preexisting regulation</li></ul>
<b>6. Other</b>	A risk that cannot be clearly defined in another category.