State Leadership Accountability Act Risks and Definitions

California Department of Finance

Revised 7/2015

State Leadership Accountability Act (SLAA) Risks and Definitions Table of Contents

This page intentionally blank to facilitate double-sided printing

Introduction

This document is a tool to provide state entities with standardized risk language for use during the risk assessment process. This tool can be employed throughout an entity to assist those working in locations away from headquarters and in diverse programs and operations. The standardized risk language is grouped into three units. The three units are risk categories, risk subcategories, and risk factors. The risk categories follow current internal control standards. The risk subcategories allow entities to identify the source of the risk as either internal or external. In the third grouping, the risk factors are defined.

Several sources were consulted during the development of the risk factors. We use the *Internal Control—Integrated Framework* of the Committee of Sponsoring Organization of the Treadway Commission, the *Standards for Internal control in the Federal Government* (Green Book) issued by the Comptroller General of the United States, three cycles of previous SLAA reports, audit reports, newspapers, the internet, and a variety of other sources. Additionally, we were assisted by focus groups during the development of the document. We appreciate the assistance and the feedback provided by the focus groups.

This page intentionally blank to facilitate double-sided printing

SLAA Risk Categories Overview

Risk Category	Risk Subcategory	Risk Factors	
Operations	Internal	1	FI$Cal Conversion
		2	New System Implementation (Other Than FI$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
		8	Staff-—Key Person Dependence, Succession Planning
		9	Staff—Safety
		10	Staff—Training, Knowledge, Competence
		11	Technology-—Data Security
		12	Technology—Inadequate Support, Tools, Design, or Maintenance
		13	Technology—Outdated, Incompatible
		14	Workplace Environment
		15	Other
	External	1	Business Interruption, Safety Concerns
		2	Economic Volatility
		3	FI$Cal Conversion
		4	Fraud, Theft, Waste, Misconduct, Vandalism
		5	Funding—Sources, Levels
		6	Litigation
		7	New System Implementation (Other Than FI$Cal)
		8	Partner Agencies/Grantees—Conflicting Objectives, Program Coordination
		9	Political, Reputation, Media
		10	Service Provider—Inadequate Internal Control System
		11	Staff—Recruitment, Retention, Staffing Levels
		12	Technology—Data Security
		13	Technology—Incompatibility
		14	Other
Reporting	Internal	1	Distribution Limitations
		2	FI$Cal Conversion
		3	Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely
		4	Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely
		5	New System Implementation (Other Than FI$Cal)
		6	Other
	External	1	Distribution Limitations
		2	FI$Cal Conversion
		3	Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely
		4	Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely
		5	New System Implementation (Other Than FI$Cal)
		6	Other
Compliance	Internal	1	Priorities Conflicting with Laws or Regulations
		2	Resource Limitations
		3	Staff Not Adhering to Policies, Procedures, or Standards
		4	Other
	External	1	Complexity or Dynamic Nature of Laws or Regulations
		2	Funding—Sources, Levels
		3	Priorities Conflicting with Laws or Regulations
		4	Service Provider—Inadequate Internal Control System
		5	Unclear Responsibilities of Laws or Regulations
		6	Other

SLAA Risk Categories

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.

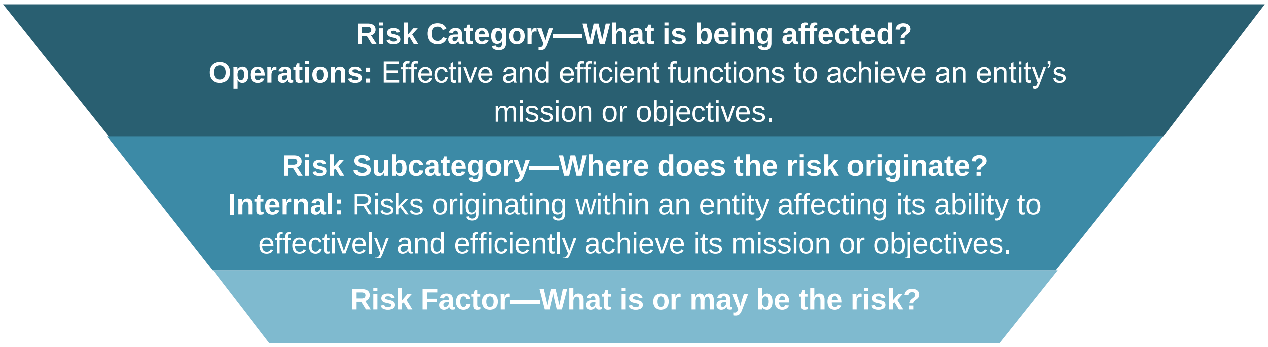
Where does the risk originate?	
Compliance	
Internal	Risks within an entity affecting its ability to comply with laws or regulations.
External	Risks outside an entity affecting its ability to comply with laws or regulations.

[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$Cal Conversion
	2. New System Implementation (Other Than FI$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
	8. Staff—Key Person Dependence, Succession Planning
	9. Staff—Safety
	10. Staff—Training, Knowledge, Competence
	11. Technology—Data Security
	12. Technology—Inadequate Support, Tools, Design, or Maintenance
	13. Technology—Outdated, Incompatible
	14. Workplace Environment
	15. Other

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

1. FI$Cal Conversion	Internal implementation of FI$Cal causing limitations of staff availability, information accuracy, security, or compatibility. Examples: • Operating inefficiency as a result of system or user error from implementation of FI$Cal • Staff availability is reduced by time spent training for FI$Cal conversion • FI$Cal system incompatibility with internal information systems • Timing of FI$Cal updates do not align with user expectations, creating data entry errors
2. New System Implementation (Other Than FI$Cal)	Design or implementation of a system failing to provide required information or output. Examples: • Inefficiencies created as a result of user errors or lack of familiarity with new system • Unanticipated conditions impacting the design of the new system, causing it to function inefficiently or fail to achieve desired outcomes • New system is incompatible with legacy system, resulting in loss of data • Complexity of a program creating higher-than-anticipated costs • Staff availability reduced by time spent training for new system • Timing of system information updates does not align with user expectations, creating data entry errors Note: Include the name of new system in the risk description.

Operations – Internal

3. Organizational Structure	Unclear/undefined roles or responsibilities creating inefficient or ineffective operations including supervision and communication. Examples: • Work duplicated/incomplete due to unclear roles, a new program, an entity reorganization, or new objectives • Strategic plan is not developed, updated, or followed • Silos within an entity hinder efficient communication • 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	Insufficient monitoring, design, or evaluation of the internal control systems to identify and correct deficiencies. Examples: • Policies and procedures are not current, established, followed, or enforced • Controls have become outdated and are no longer effective because of changes in environment or objectives • 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 • Lack of adequate monitoring to prevent or identify procedures not being followed • Entity is not monitoring grant expenditures as required • Tone at the top (such as the tone set by management for ethical behavior and the control environment)
5. Physical Resources—Maintenance, Upgrades, Replacements, Security	Inadequate administration of physical resources to ensure proper functionality and security. Examples: • Competing priorities delaying allocation of resources for 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

6. Program/Activity—Changes, Complexity	Dynamic or complicated processes creating opportunity for errors, omissions, or inefficiencies. Examples: • Highly complex time keeping process causes overpayment to employees • Workload backlogs from program changes inhibit program roll-out or effectiveness • Implementation of plan or design changes produce unanticipated or undesired effects to secondary processes • Complex interactions between various funding sources and the rules governing each creating inefficiencies
7. Resource Management	Limitations or mismanagement of fiscal resources, creating inefficiencies or preventing completion of objectives. Examples: • Difficult-to-forecast or unplanned expenses exceed budgeted levels • Leave balance liabilities • Insufficient financial resources to achieve an objective • Fees from users either not collected or collected inefficiently
8. Staff—Key Person Dependence, Succession Planning	Loss of institutional knowledge due to heavy reliance on staff who may become temporarily or permanently unavailable. Examples: • Limited positions create challenges 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
9. Staff—Safety	Dangerous conditions presented by the inherent nature of the work performed or by work location. Examples: • Workplace violence or retaliation • Inherent safety concerns impact ability to recruit and retain staff, increasing the risk of an accident • Inherent safety risks to operating machinery

Operations – Internal

10. Staff—Training, Knowledge, Competence	Operational inefficiency due to inadequate or outdated training or other limitations of staff knowledge. Examples: • Inadequate or outdated training resources • Staff resistant to change • Lack of commitment or resources to train staff • Process or procedure change not communicated to existing staff • Staff knowledge and ability not in line with job requirements • Staff does not use or apply the training/ resources provided
11. Technology—Data Security	Internal acts threatening the integrity, safety, or privacy of information. Examples: • Staff accidently altering important files • Unintentional release of confidential information • Failing to follow internal security procedures such as inappropriate password sharing or failing to lock computer • Access levels allow users to view unauthorized information • Inadequate process to discourage or identify unauthorized access
12. Technology—Inadequate Support, Tools, Design, or Maintenance	Limitations in design or resources causing system functionality issues. Examples: • Disruption of operations due to system failure • Inadequate back up of a system, causing loss of information • Lack of IT personnel or expertise • Lack of appropriate software to efficiently complete assignments
13. Technology—Outdated, Incompatible	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

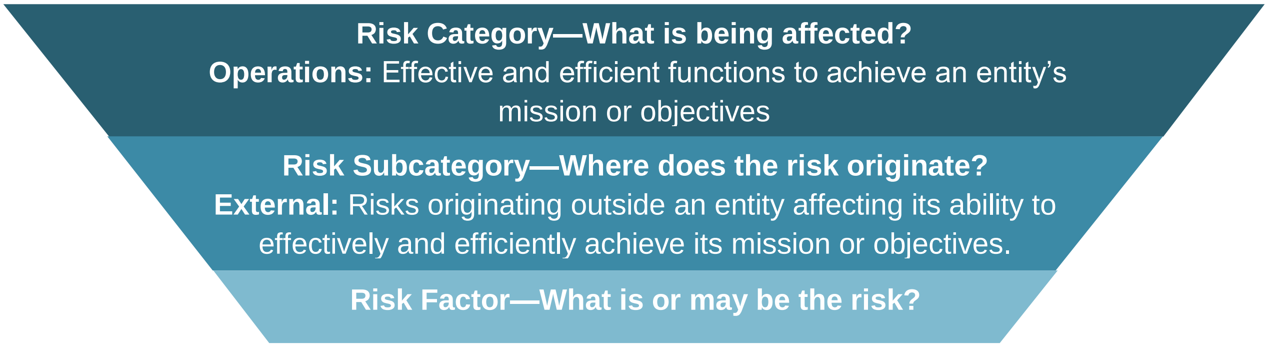
Operations – Internal

14. Workplace Environment	Factors impacting working relationships, such as physical environment, workplace behavior, or shared values. Examples: • 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 and harassment issues
15. Other	A risk that cannot be clearly defined in another category.

Operations – External

Risk Category	Operations
Risk Subcategory	External
Risk Factors	1. Business Interruption, Safety Concerns
	2. Economic Volatility
	3. FI$Cal Conversion
	4. Fraud, Theft, Waste, Misconduct, Vandalism
	5. Funding—Sources, Levels
	6. Litigation
	7. New System Implementation (Other Than FI$Cal)
	8. Partner Agencies/Grantees—Conflicting Objectives, Program Coordination
	9. Political, Reputation, Media
	10. Service Provider—Inadequate Internal Control System
	11. Staff—Recruitment, Retention, Staffing Levels
	12. Technology—Data Security
	13. Technology—Incompatibility
	14. Other

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

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 having 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$Cal Conversion	Design or implementation of FI$Cal causing limitations of information availability, security, or access. Examples: • Loss of information, lack of availability, server down time, or slow response • Information security breaches on FI$Cal servers

Operations – External

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, or difficult to obtain. 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
6. Litigation	Possible legal action by an outside party in response to an entity’s actions, inactions, services, or other events. Example: • Public interest groups sue entity due to implementation of a new law they believe violates civil rights
7. New System Implementation (Other Than FI$Cal)	Limitations 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 down time, or slow response for systems managed by another entity • Information security breaches on other entity’s servers Note: Include the name of new system in the risk description.

Operations – External

8. Partner Agencies/Grantees—Conflicting Objectives, Program Coordination	Lack of understanding or difference in partner or grantee operation prevents or creates inefficiencies in meeting entity objectives. Examples: • Communication deficiency with oversight agency • Local regulations conflict with entity goals • Grantee does not complete grant deliverables due to conflicting priorities
9. Political, Reputation, Media	Disruption to operations due to negative perceptions of an entity, changes in political climate, or negative publicity. Examples: • Negative media attention • Protests due to controversial practices of an entity • Diminishing public confidence due to appearance of mismanagement • Political pressure to change entity operations or objectives • Collective bargaining process impacting public opinion or interrupting operations
10. Service Provider—Inadequate Internal Control System	Inadequate oversight of a service provider (defined below) creating inefficiencies or preventing 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

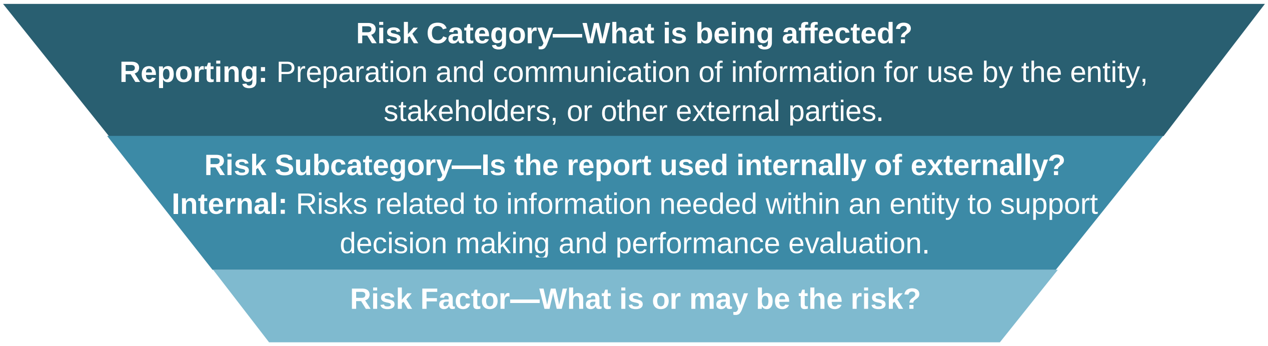
Operations – External

11. Staff—Recruitment, Retention, Staffing Levels	Staffing limitations creating inefficiencies or preventing 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	Intentional external acts threatening the integrity, safety, or privacy of information. Examples: • Hacking into an entity's database • Inadequate process to discourage or identify unauthorized access
13. Technology—Incompatibility	Information system limitations hindering communication. Examples: • Communication failure between two interdependent entities' 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.

Reporting – Internal

Risk Category	**Reporting**
Risk Subcategory	**Internal**
Risk Factors	**1. Distribution Limitations**
	2. FI$Cal Conversion
	3. Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely
	4. Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely
	5. New System Implementation (Other Than FI$Cal)
	6. Other

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 of 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$Cal Conversion	Internal FI$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
3. Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely	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

Reporting – Internal

4. Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely	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
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 Note: Include the name of new system in the risk description
6. Other	A risk that cannot be clearly defined in another category.

Reporting – External

Risk Category	Reporting
Risk Subcategory	External
Risk Factors	1. Distribution Limitations
	2. FI$Cal Conversion
	3. Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely
	4. Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely
	5. New System Implementation (Other Than FI$Cal)
	6. Other

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
2. FI$Cal Conversion	FI$Cal reports are inadequate, inaccurate, misinterpreted, or untimely to convey the intended message due to the implementation or design of FI$Cal. Examples: • Vendors misinterpret reports generated from FI$Cal because of a lack of experience reading the report • External parties provide the incorrect information as a result of a misunderstood report
3. Information Collected—Inadequate, Inaccurate, Misinterpreted, Untimely	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

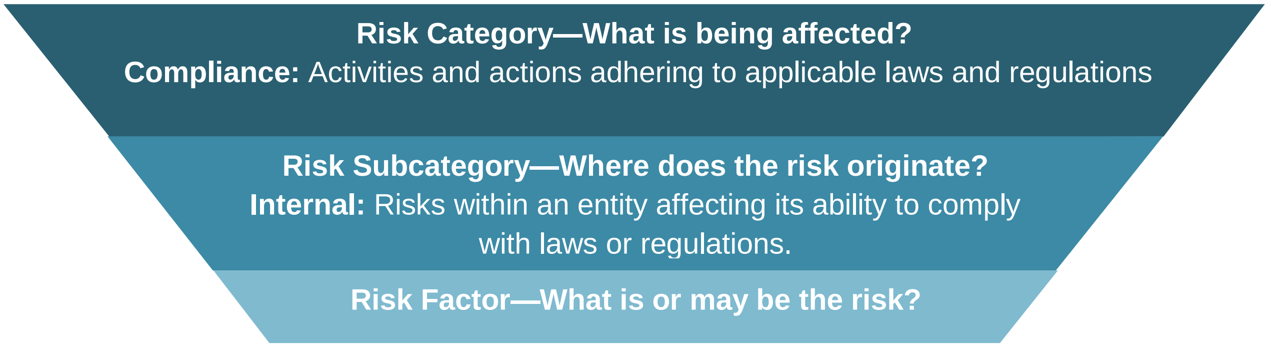
Reporting – External

4. Information Communicated—Inadequate, Inaccurate, Misinterpreted, Untimely	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
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.

Compliance – Internal

Risk Category	Compliance
Risk Subcategory	Internal
Risk Factors	1. Priorities Conflicting with Laws or Regulations
	2. Resource Limitations
	3. Staff Not Adhering to Policies, Procedures, or Standards
	4. Other

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 Conflicting with Laws or Regulations	Internal directives or 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
2. Resource Limitations	The ability to comply with laws or regulations is jeopardized by limited 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 Not Adhering to Policies, Procedures, or Standards	Staff performing duties in a way that does not ensure full compliance with laws or regulations. Examples: • Training issues, lack of resources, or insubordination • Changes to professional licensing, continuing education requirements, or construction standards
4. Other	A risk that cannot be clearly defined in another category.

Compliance – External

Risk Category	Compliance
Risk Subcategory	External
Risk Factors	1. Complexity or Dynamic Nature of Laws or Regulations
	2. Funding—Sources, Levels
	3. Priorities Conflicting with Laws or Regulations
	4. Service Provider—Inadequate Internal Control System
	5. Unclear Responsibilities of Laws or Regulations
	6. Other

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 regulation..

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. Example: • Funding limits full program implementation required by the law
3. Priorities Conflicting with Laws or Regulations	External stakeholders creating 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

4. Service Provider—Inadequate Internal Control System	Inadequate 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. Unclear Responsibilities of Laws or Regulations	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.