Governance, Risk, and Compliance Council (GRCC)

November 5, 2025

1:00 p.m. – 2:30 p.m.

Virtual

Welcome!

Lynn Bashaw, GRCC Co-Chair,
California State Teachers Retirement System
(CalSTRS)

GRCC

Today’s Agenda

Topic	Presenter/Facilitator	Time
Welcome	Lynn Bashaw	1:00 – 1:10
Local Government Perspectives on ERM and Internal Controls	Albert Beltran	1:10 – 1:40
SLAA Implementation at Finance	Frances Parmelee	1:40 – 1:55
SLAA Updates 1. SLAA Portal Access—MFA 2. New SAM 20080 reporting 3. Portal New Look 4. Report Layout - New Look 5. Top Risks and Controls	Edwina Troupe/ Brian Dunham/ Carla Villa	1:55 – 2:25
What’s Next!	Anthony Martin	2:25 – 2:30

About the GRCC

To advance adaptive and integrative governance, risk, and compliance management principles

- Sponsored by the Government Operations Agency (GovOps)
- Advance sound governance, risk, and compliance management principles for California public entities
- Member-driven, share knowledge and resources
- Meetings include:
  - Presentations and sharing best practices (e.g., risk appetite/tolerance, addressing top SLAA risks, etc.)
  - Guest speakers
  - GovOps and DOF announcements

Governance, Risk Management and Compliance Council | GovOps (ca.gov)

GRCC Co-Chairs

Lynn Bashaw
Director of Enterprise Risk & Compliance
California State Teachers' Retirement System (CalSTRS)

Vaishali Dwarka
Director of Enterprise Strategy Management
California State Teachers' Retirement System (CalSTRS)

Sam Malla
Information Security Program Auditor
Office of Information Security
California Department of Technology

David Gordon
Principal Engineer
Strategic Risk Management
Department of Water Resources/State Water Project

GRCC Advisors

John Hanafee
Chief, Advisory Services Program
Office of Information Security
Department of Technology

Anthony Martin
Enterprise Risk Manager
Department of Industrial Relations

GRCC Sponsor

Alicia Albornoz, Assistant Equity Officer

Government Operations Agency
(GovOps)

AFERM

Melissa Thomson, AFERM

Albert Beltran, AFERM

Local Government Perspectives on ERM and Internal Controls

Mel Thomson, ARM, CRMP-FED, ERMCP

Association of Federal Enterprise Risk Management (AFERM) - Chair, State and Local Committee

Cybersecurity Risk Strategist, City of Phoenix

Albert Beltran Jr, CIA, CISA, CRMA, CC, CRISC

Association of Federal Enterprise Risk Management (AFERM) - Member, State and Local Committee

IIA San Jose Chapter, Advocacy Chair

Internal Audit Division-Finance Agency, County of Santa Clara

Presentation for the California Government Operations Agency (CalGovOps),

Governance, Risk Management and Compliance Council (GRCC)

Wednesday, November 5, 2025

Survey
https://forms.office.com/g/LdEim3FD88

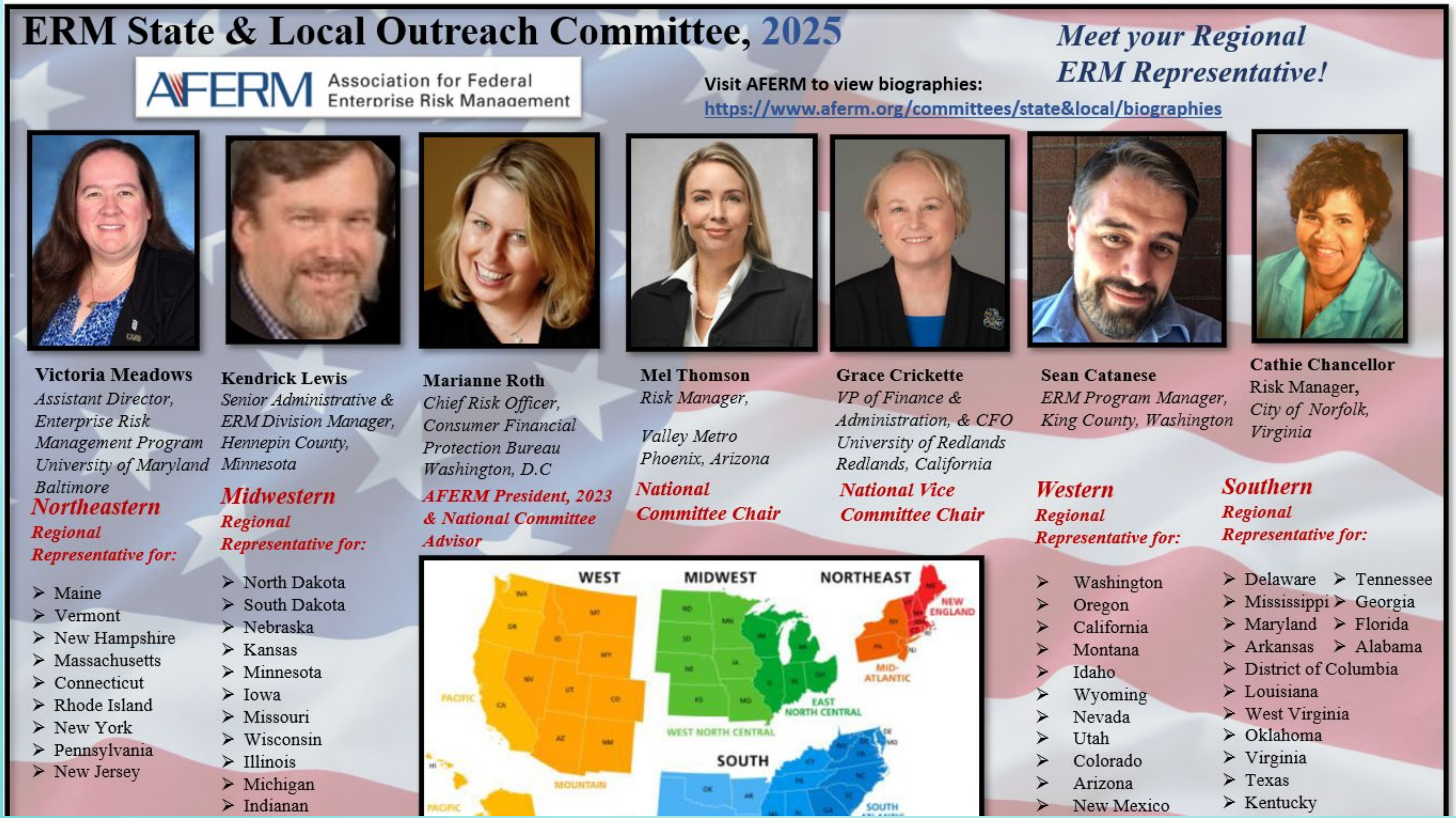
- ✓ What is your main role? (Risk, Controls, Audit)
- ✓ Do you work with others to understand risk across your entity?
- ✓ Have you read an ERM framework, word for word?
- ✓ Have you read the GAO Green Book, word for word?
- ✓ For Auditors - How many times has your client provided current and complete management objectives and policies and procedures?

Today’s Objectives

- ✓ Introduction to AFERM
- ✓ Enterprise Risk *Mindset*
- ✓ ERM (& AFERM) Alignment
  - ✓ 2025 GAO Green Book (Updated)
  - ✓ IIA Global Internal Audit Standards (GIAS)

Association of Federal Enterprise Risk Management (AFERM)

State and Local Committee



ERM State & Local Outreach Committee, 2025

AFERM Association for Federal Enterprise Risk Management

Visit AFERM to view biographies:
https://www.aferm.org/committees/state&local/biographies

Meet your Regional ERM Representative!

Victoria Meadows
Assistant Director,
Enterprise Risk
Management Program
University of Maryland
Baltimore

Northeastern Regional Representative for:

- Maine
- Vermont
- New Hampshire
- Massachusetts
- Connecticut
- Rhode Island
- New York
- Pennsylvania
- New Jersey

Kendrick Lewis
Senior Administrative &
ERM Division Manager,
Hennepin County,
Minnesota

Midwestern Regional Representative for:

- North Dakota
- South Dakota
- Nebraska
- Kansas
- Minnesota
- Iowa
- Missouri
- Wisconsin
- Illinois
- Michigan
- Indianan

Marianne Roth
Chief Risk Officer,
Consumer Financial
Protection Bureau
Washington, D.C

AFERM President, 2023 & National Committee Advisor

Mel Thomson
Risk Manager,

Valley Metro
Phoenix, Arizona

National Committee Chair

Grace Crickette
VP of Finance &
Administration, & CFO
University of Redlands
Redlands, California

National Vice Committee Chair

Sean Catanese
ERM Program Manager,
King County, Washington

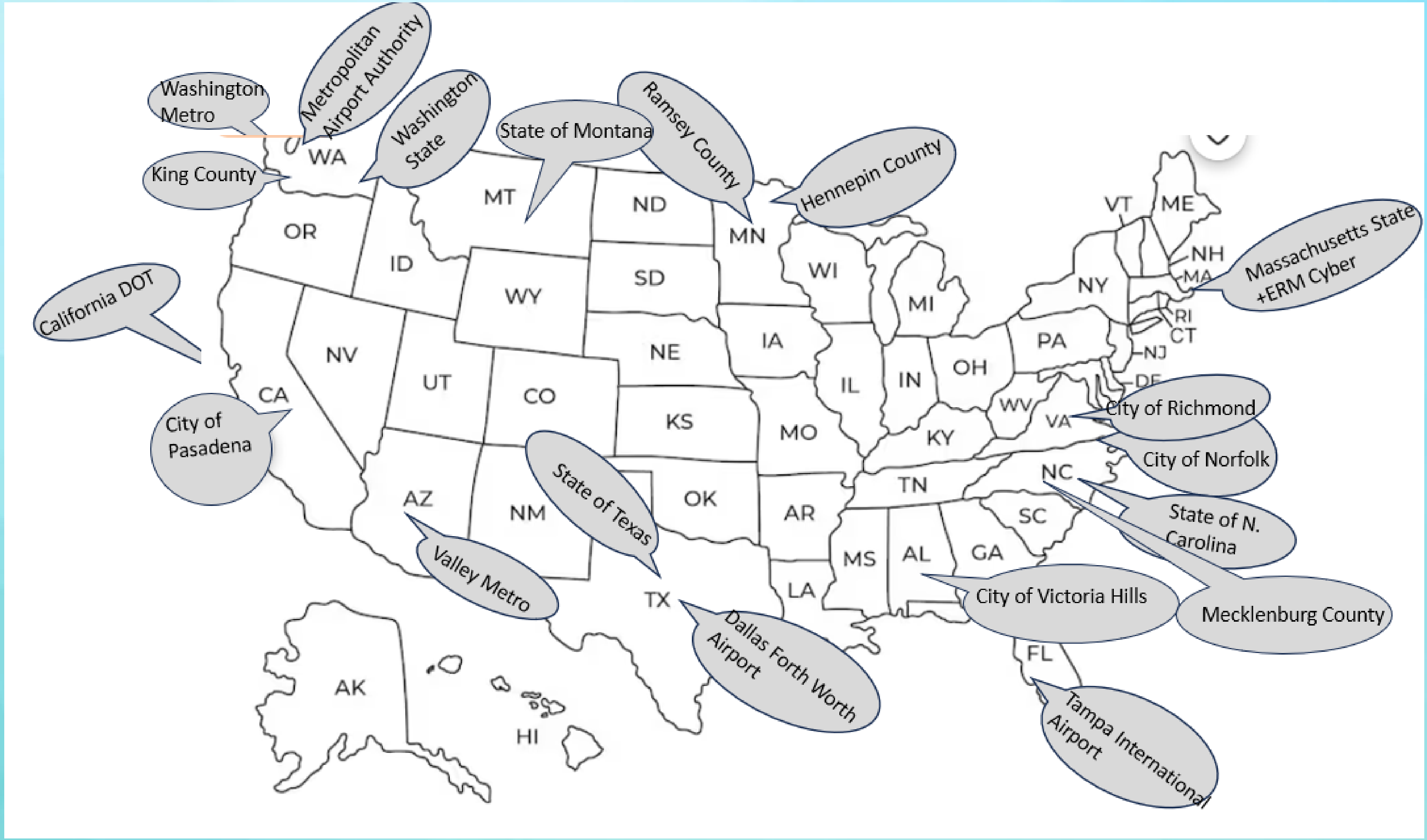
Western Regional Representative for:

- Washington
- Oregon
- California
- Montana
- Idaho
- Wyoming
- Nevada
- Utah
- Colorado
- Arizona
- New Mexico

Cathie Chancellor
Risk Manager,
City of Norfolk,
Virginia

Southern Regional Representative for:

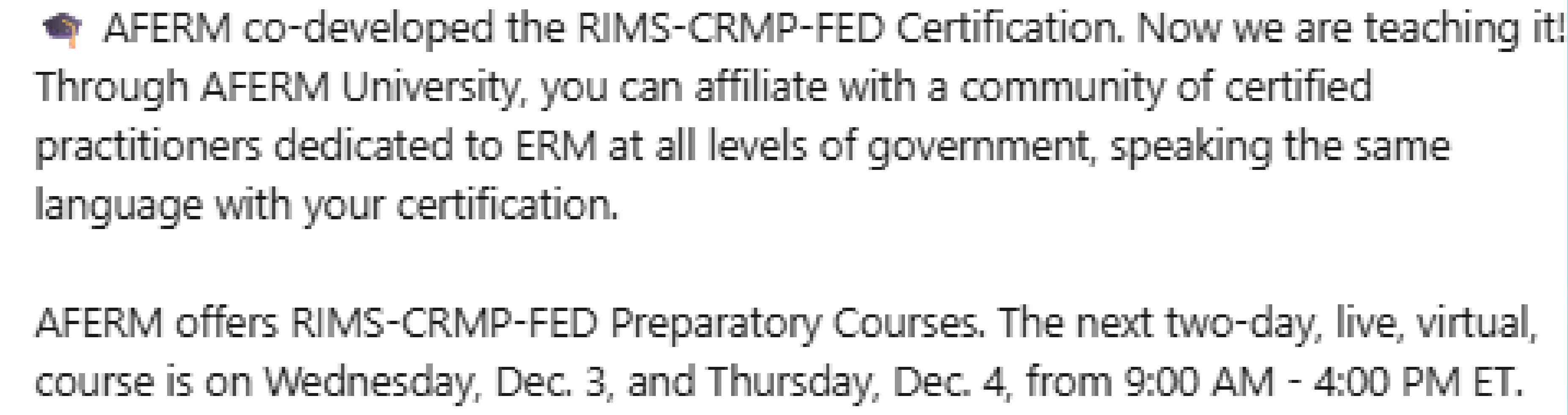
- Delaware
- Mississippi
- Maryland
- Arkansas
- District of Columbia
- Louisiana
- West Virginia
- Oklahoma
- Virginia
- Texas
- Kentucky
- Tennessee
- Georgia
- Florida
- Alabama


Washington Metro
Metropolitan Airport Authority
Washington State
State of Montana
Ramsey County
Hennepin County
King County
Massachusetts State +ERM Cyber
California DOT
City of Pasadena
State of Texas
City of Richmond
City of Norfolk
State of N. Carolina
Valley Metro
City of Victoria Hills
Mecklenburg County
Dallas Forth Worth Airport
Tampa International Airport
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
ME
NH
MA
RI
CT
NJ
DE
AK
HI

AFERM

Resources - Guidance

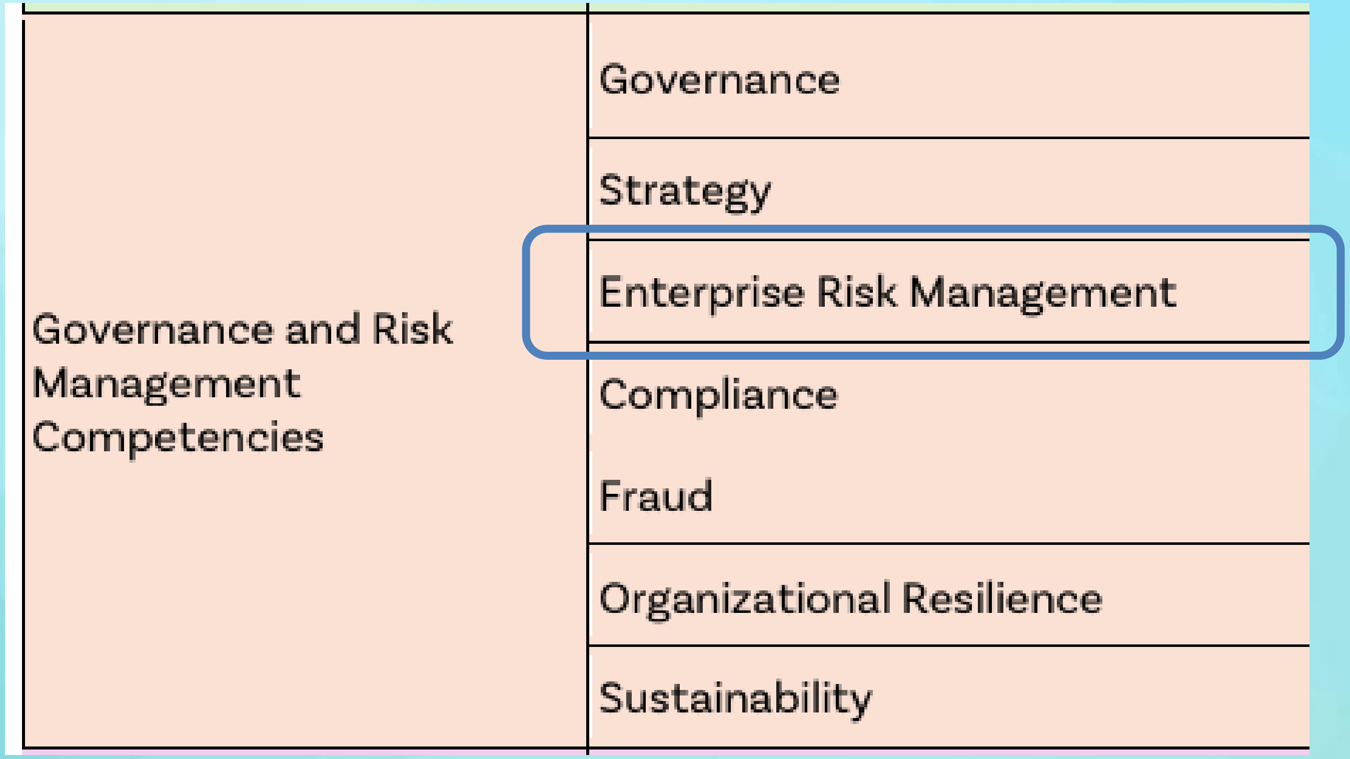
Training – Aligned with RIMS/IIA



🎓 AFERM co-developed the RIMS-CRMP-FED Certification. Now we are teaching it! Through AFERM University, you can affiliate with a community of certified practitioners dedicated to ERM at all levels of government, speaking the same language with your certification.

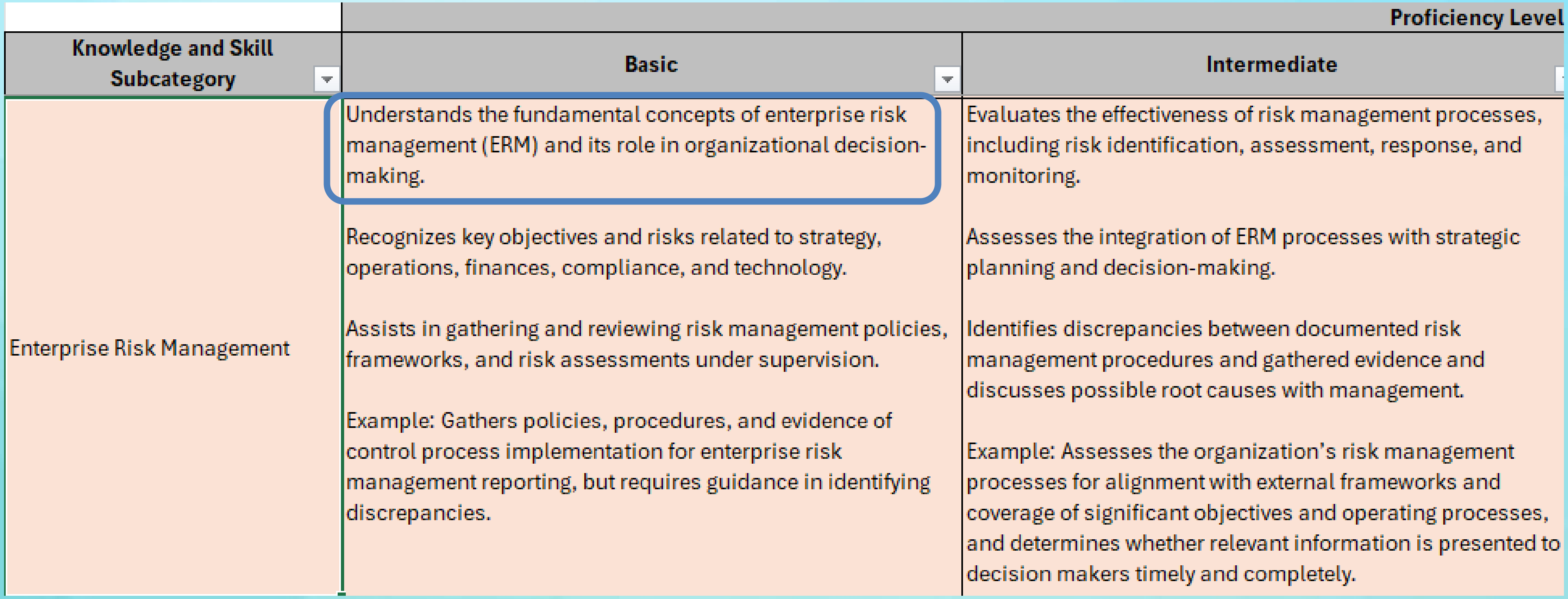
AFERM offers RIMS-CRMP-FED Preparatory Courses. The next two-day, live, virtual, course is on Wednesday, Dec. 3, and Thursday, Dec. 4, from 9:00 AM - 4:00 PM ET.

IIA Competency Standards (UPDATED)



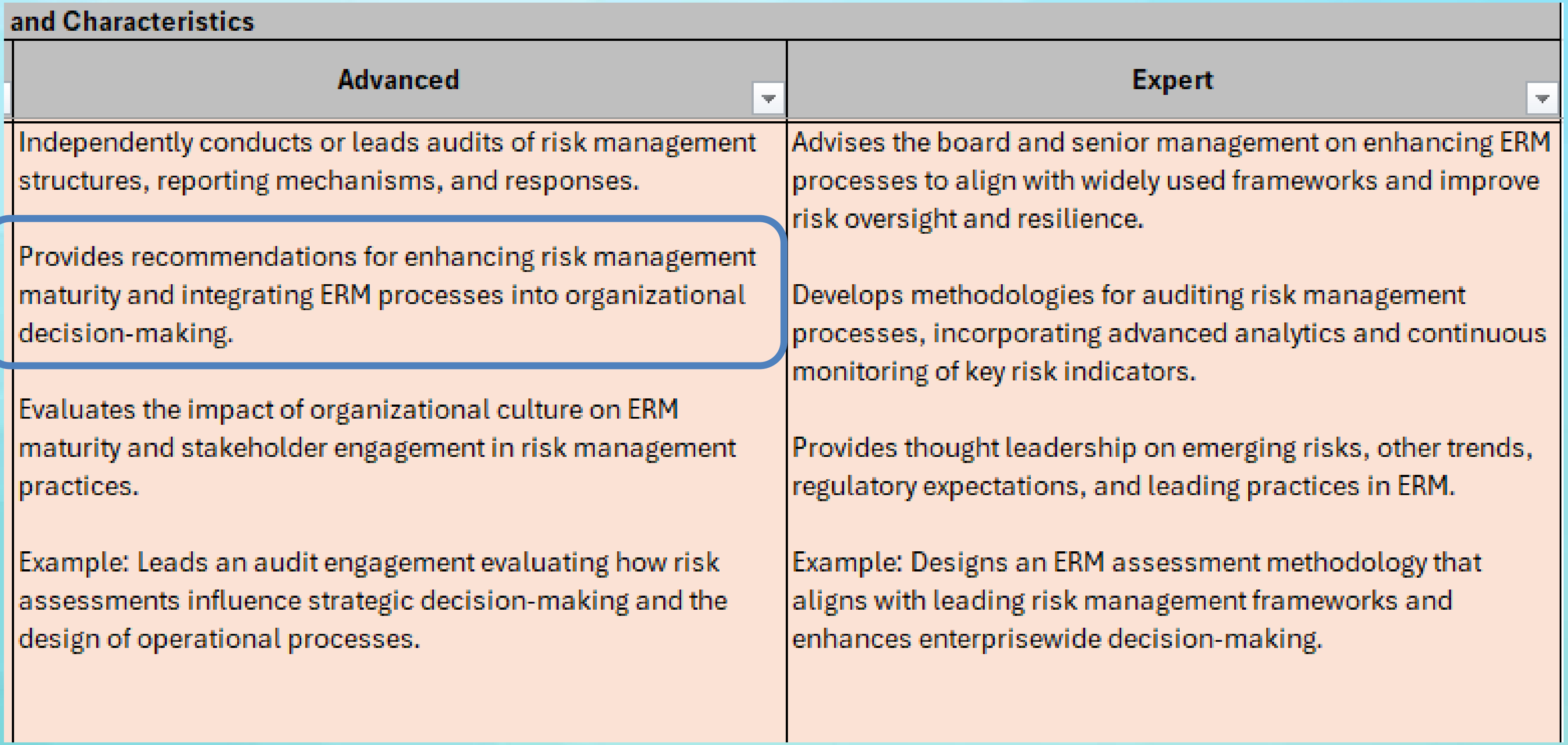
Governance and Risk Management Competencies	Governance
	Strategy
	Enterprise Risk Management
	Compliance Fraud
	Organizational Resilience
	Sustainability

IIA Competency Standards (UPDATED)



	Proficiency Level	
Knowledge and Skill Subcategory	Basic	Intermediate
Enterprise Risk Management	Understands the fundamental concepts of enterprise risk management (ERM) and its role in organizational decision-making. Recognizes key objectives and risks related to strategy, operations, finances, compliance, and technology. Assists in gathering and reviewing risk management policies, frameworks, and risk assessments under supervision. Example: Gathers policies, procedures, and evidence of control process implementation for enterprise risk management reporting, but requires guidance in identifying discrepancies.	Evaluates the effectiveness of risk management processes, including risk identification, assessment, response, and monitoring. Assesses the integration of ERM processes with strategic planning and decision-making. Identifies discrepancies between documented risk management procedures and gathered evidence and discusses possible root causes with management. Example: Assesses the organization's risk management processes for alignment with external frameworks and coverage of significant objectives and operating processes, and determines whether relevant information is presented to decision makers timely and completely.

IIA Competency Standards (UPDATED)



and Characteristics

Advanced	Expert
Independently conducts or leads audits of risk management structures, reporting mechanisms, and responses. Provides recommendations for enhancing risk management maturity and integrating ERM processes into organizational decision-making. Evaluates the impact of organizational culture on ERM maturity and stakeholder engagement in risk management practices. Example: Leads an audit engagement evaluating how risk assessments influence strategic decision-making and the design of operational processes.	Advises the board and senior management on enhancing ERM processes to align with widely used frameworks and improve risk oversight and resilience. Develops methodologies for auditing risk management processes, incorporating advanced analytics and continuous monitoring of key risk indicators. Provides thought leadership on emerging risks, other trends, regulatory expectations, and leading practices in ERM. Example: Designs an ERM assessment methodology that aligns with leading risk management frameworks and enhances enterprisewide decision-making.

ISO

ISO 31000

Playbook:
Enterprise Risk Management for the U.S. Federal Government

Developed and issued in collaboration with Federal Government organizations to provide guidance and support for ERM.

CFO
UNITED STATES
CHIEF FINANCIAL OFFICERS COUNCIL

FORUM ON TAX ADMINISTRATION

OECD Tax Administration Maturity Model Series

Enterprise Risk Management Maturity Model

OECD
BETTER POLICIES FOR BETTER LIVES

FEATURED TOOL

RIMS Risk Maturity Model

The RIMS Risk Maturity Model® is a self-assessment for risk professionals to identify strengths and weaknesses in their risk strategy. The RIMS RMM® was built for risk professionals, by risk professionals.

READ MORE →

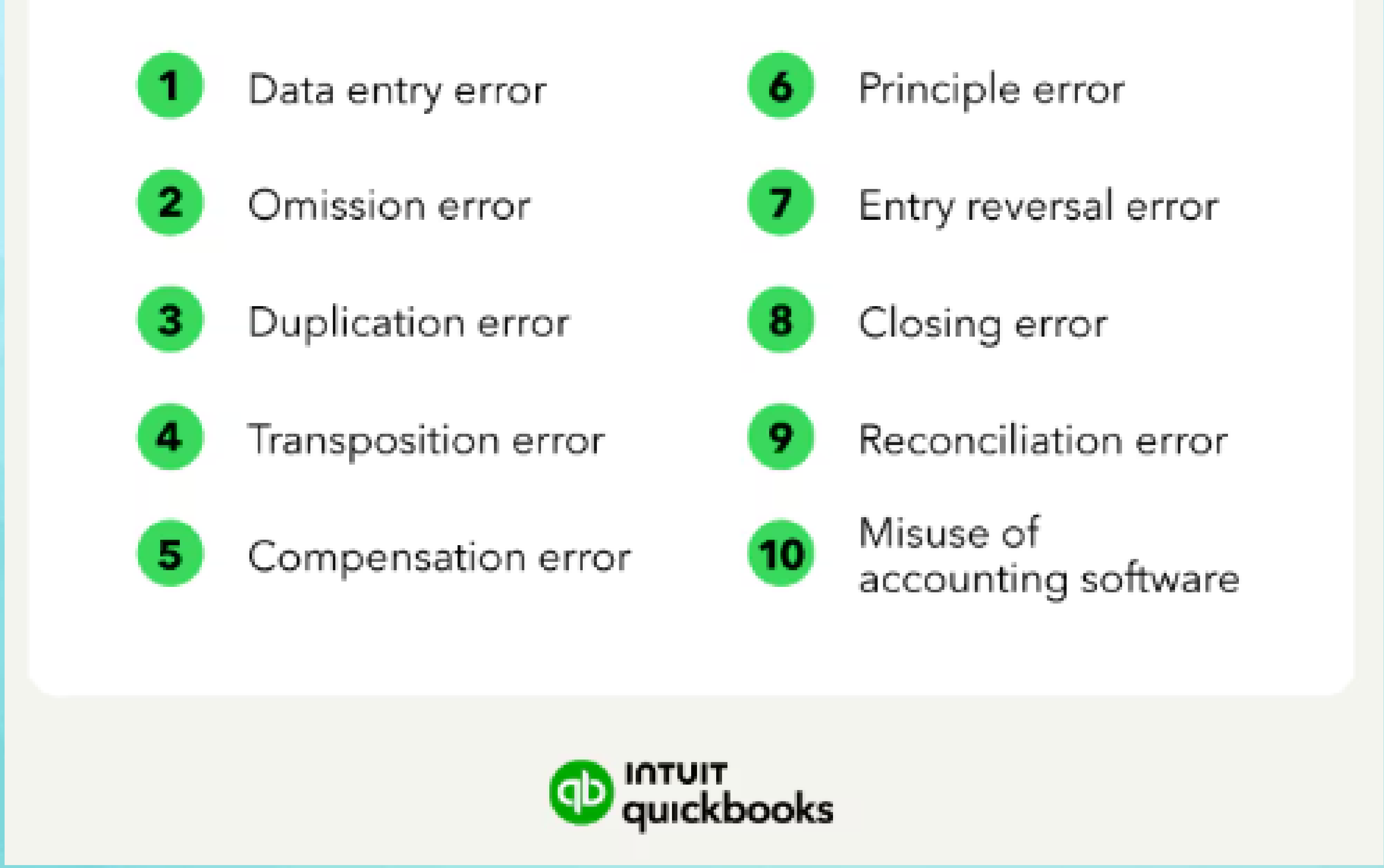
RIMS Risk Maturity Model®

Created by risk professionals for risk professionals

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

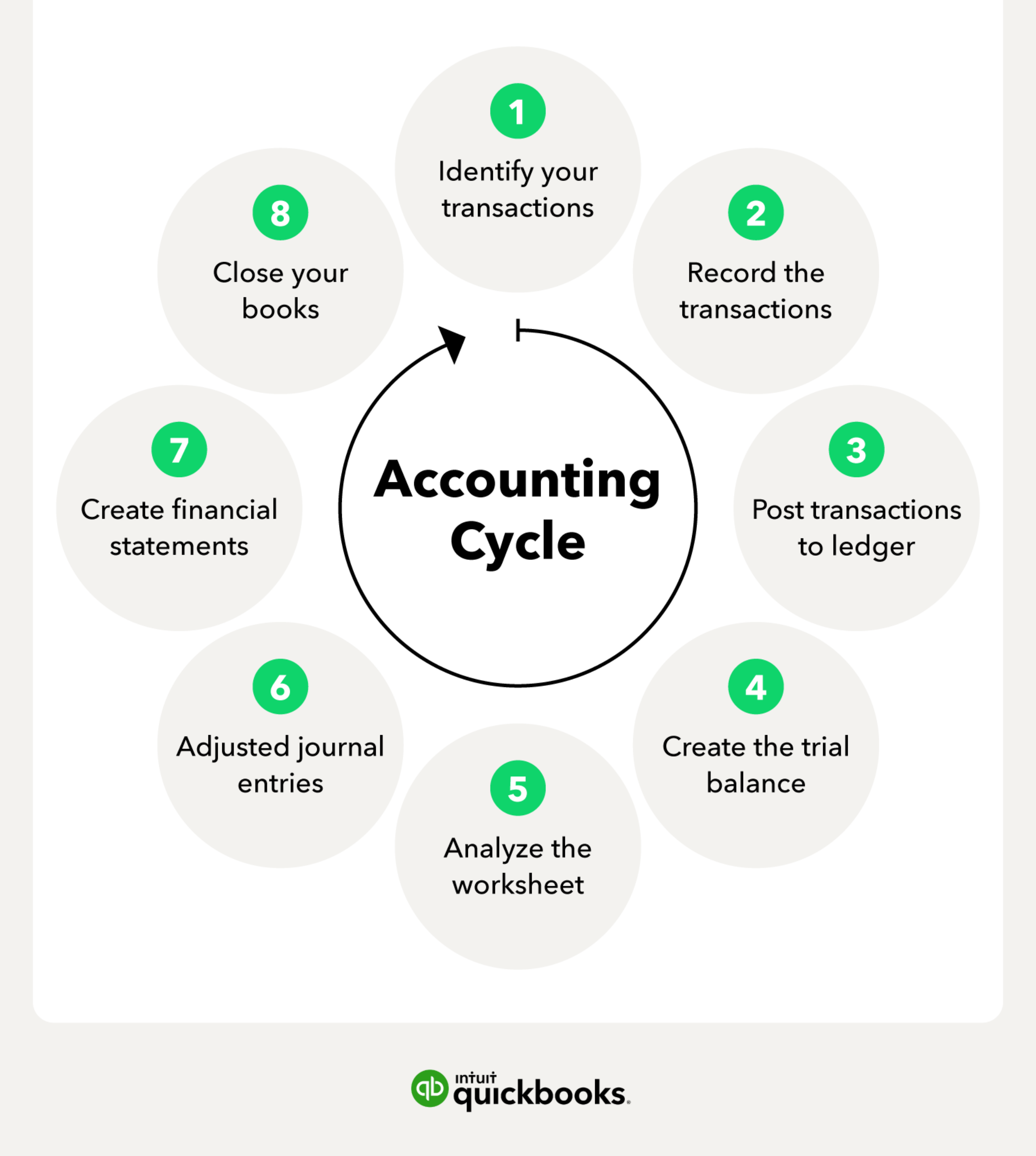
Guidance for management & auditors
to identify and assess risks
across all operational activities of an entity

Financial Accounting Errors as “Risk”



1. Data entry error
2. Omission error
3. Duplication error
4. Transposition error
5. Compensation error
6. Principle error
7. Entry reversal error
8. Closing error
9. Reconciliation error
10. Misuse of accounting software

INTUIT quickbooks



Accounting Cycle

1 Identify your transactions

2 Record the transactions

3 Post transactions to ledger

4 Create the trial balance

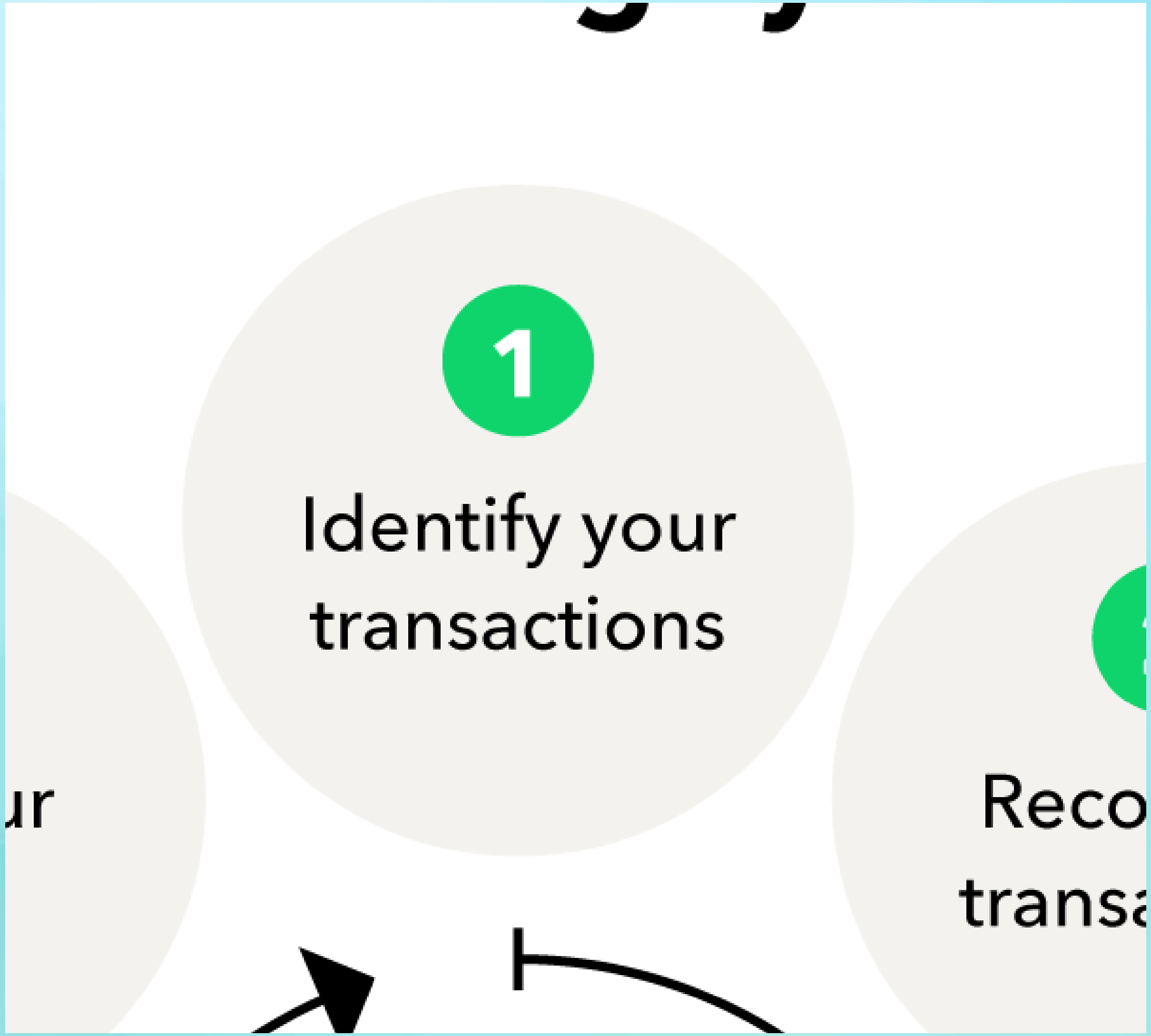
5 Analyze the worksheet

6 Adjusted journal entries

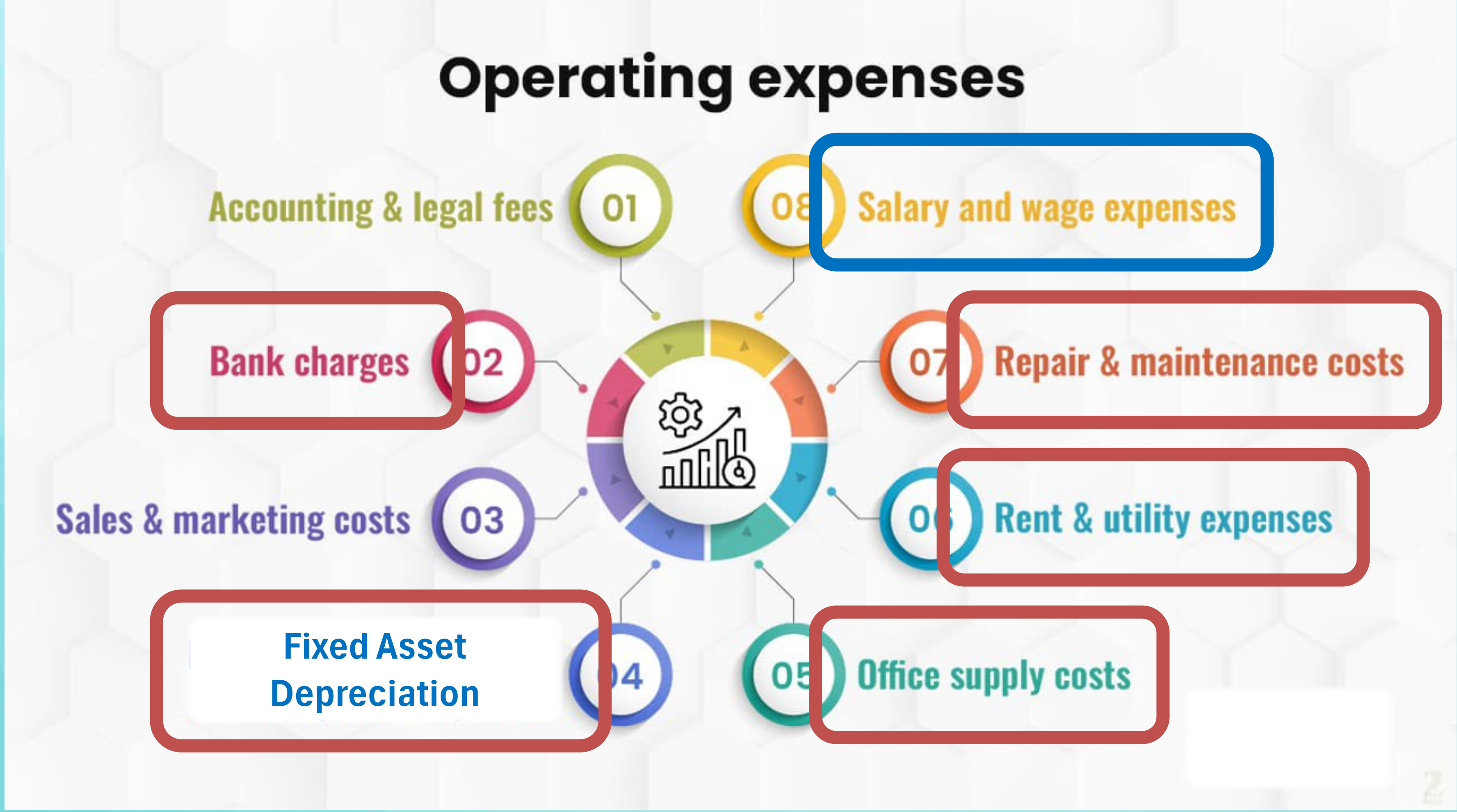
7 Create financial statements

8 Close your books

Transactions = Operational Activity & Expenses



Enterprise Risk *Mindset = Total Operational Risk*



Operating expenses

01 Accounting & legal fees

02 Bank charges

03 Sales & marketing costs

04 Fixed Asset Depreciation

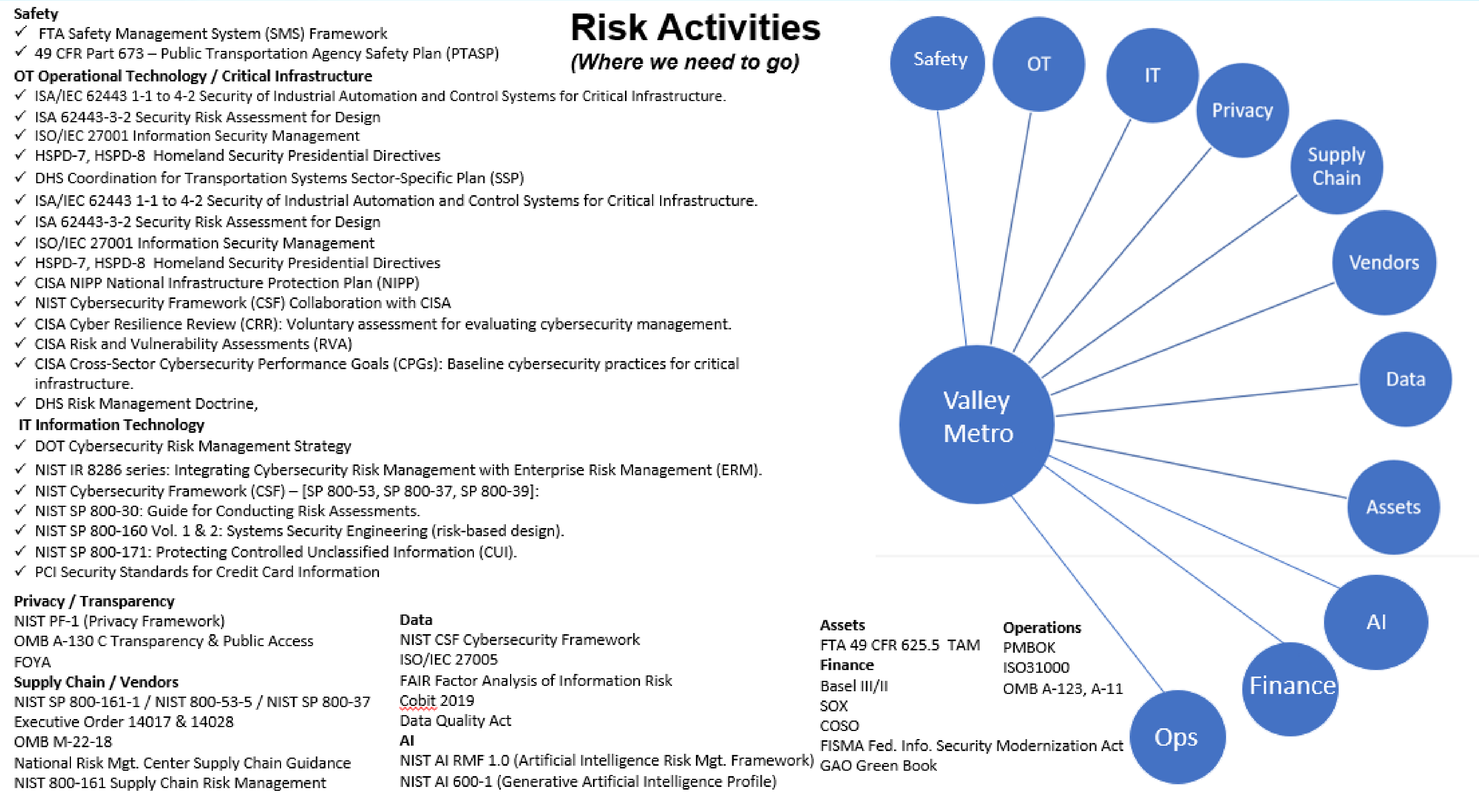
05 Office supply costs

06 Rent & utility expenses

07 Repair & maintenance costs

08 Salary and wage expenses

ERM Mindset into ERM Reality – Valley Metro



Risk Activities

(Where we need to go)

Safety
- ✓ FTA Safety Management System (SMS) Framework
- ✓ 49 CFR Part 673 – Public Transportation Agency Safety Plan (PTASP)

OT Operational Technology / Critical Infrastructure
- ✓ ISA/IEC 62443 1-1 to 4-2 Security of Industrial Automation and Control Systems for Critical Infrastructure.
- ✓ ISA 62443-3-2 Security Risk Assessment for Design
- ✓ ISO/IEC 27001 Information Security Management
- ✓ HSPD-7, HSPD-8 Homeland Security Presidential Directives
- ✓ DHS Coordination for Transportation Systems Sector-Specific Plan (SSP)
- ✓ ISA/IEC 62443 1-1 to 4-2 Security of Industrial Automation and Control Systems for Critical Infrastructure.
- ✓ ISA 62443-3-2 Security Risk Assessment for Design
- ✓ ISO/IEC 27001 Information Security Management
- ✓ HSPD-7, HSPD-8 Homeland Security Presidential Directives
- ✓ CISA NIPP National Infrastructure Protection Plan (NIPP)
- ✓ NIST Cybersecurity Framework (CSF) Collaboration with CISA
- ✓ CISA Cyber Resilience Review (CRR): Voluntary assessment for evaluating cybersecurity management.
- ✓ CISA Risk and Vulnerability Assessments (RVA)
- ✓ CISA Cross-Sector Cybersecurity Performance Goals (CPGs): Baseline cybersecurity practices for critical infrastructure.
- ✓ DHS Risk Management Doctrine,

IT Information Technology
- ✓ DOT Cybersecurity Risk Management Strategy
- ✓ NIST IR 8286 series: Integrating Cybersecurity Risk Management with Enterprise Risk Management (ERM).
- ✓ NIST Cybersecurity Framework (CSF) – [SP 800-53, SP 800-37, SP 800-39]:
- ✓ NIST SP 800-30: Guide for Conducting Risk Assessments.
- ✓ NIST SP 800-160 Vol. 1 & 2: Systems Security Engineering (risk-based design).
- ✓ NIST SP 800-171: Protecting Controlled Unclassified Information (CUI).
- ✓ PCI Security Standards for Credit Card Information

Privacy / Transparency
NIST PF-1 (Privacy Framework)
OMB A-130 C Transparency & Public Access
FOYA

Supply Chain / Vendors
NIST SP 800-161-1 / NIST 800-53-5 / NIST SP 800-37
Executive Order 14017 & 14028
OMB M-22-18
National Risk Mgt. Center Supply Chain Guidance
NIST 800-161 Supply Chain Risk Management

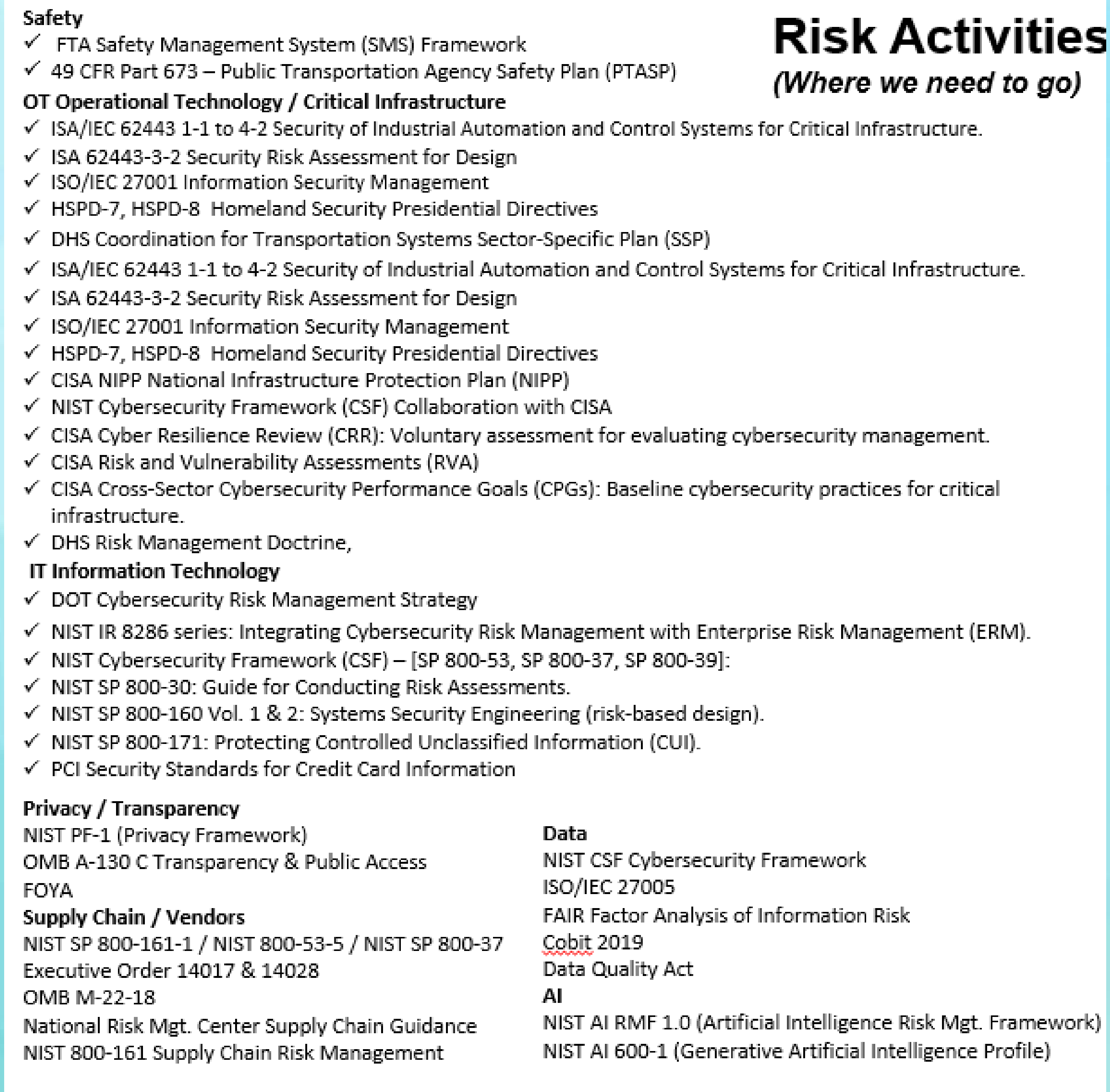
Data
NIST CSF Cybersecurity Framework
ISO/IEC 27005
FAIR Factor Analysis of Information Risk
Cobit 2019
Data Quality Act

AI
NIST AI RMF 1.0 (Artificial Intelligence Risk Mgt. Framework)
NIST AI 600-1 (Generative Artificial Intelligence Profile)

Assets
FTA 49 CFR 625.5 TAM

Finance
Basel III/II
SOX
COSO
FISMA Fed. Info. Security Modernization Act
GAO Green Book

Operations
PMBOK
ISO31000
OMB A-123, A-11



Risk Activities

(Where we need to go)

Safety

- ✓ FTA Safety Management System (SMS) Framework
- ✓ 49 CFR Part 673 – Public Transportation Agency Safety Plan (PTASP)

OT Operational Technology / Critical Infrastructure

- ✓ ISA/IEC 62443 1-1 to 4-2 Security of Industrial Automation and Control Systems for Critical Infrastructure.
- ✓ ISA 62443-3-2 Security Risk Assessment for Design
- ✓ ISO/IEC 27001 Information Security Management
- ✓ HSPD-7, HSPD-8 Homeland Security Presidential Directives
- ✓ DHS Coordination for Transportation Systems Sector-Specific Plan (SSP)
- ✓ ISA/IEC 62443 1-1 to 4-2 Security of Industrial Automation and Control Systems for Critical Infrastructure.
- ✓ ISA 62443-3-2 Security Risk Assessment for Design
- ✓ ISO/IEC 27001 Information Security Management
- ✓ HSPD-7, HSPD-8 Homeland Security Presidential Directives
- ✓ CISA NIPP National Infrastructure Protection Plan (NIPP)
- ✓ NIST Cybersecurity Framework (CSF) Collaboration with CISA
- ✓ CISA Cyber Resilience Review (CRR): Voluntary assessment for evaluating cybersecurity management.
- ✓ CISA Risk and Vulnerability Assessments (RVA)
- ✓ CISA Cross-Sector Cybersecurity Performance Goals (CPGs): Baseline cybersecurity practices for critical infrastructure.
- ✓ DHS Risk Management Doctrine,

IT Information Technology

- ✓ DOT Cybersecurity Risk Management Strategy
- ✓ NIST IR 8286 series: Integrating Cybersecurity Risk Management with Enterprise Risk Management (ERM).
- ✓ NIST Cybersecurity Framework (CSF) – [SP 800-53, SP 800-37, SP 800-39]:
- ✓ NIST SP 800-30: Guide for Conducting Risk Assessments.
- ✓ NIST SP 800-160 Vol. 1 & 2: Systems Security Engineering (risk-based design).
- ✓ NIST SP 800-171: Protecting Controlled Unclassified Information (CUI).
- ✓ PCI Security Standards for Credit Card Information

Privacy / Transparency

NIST PF-1 (Privacy Framework)
OMB A-130 C Transparency & Public Access
FOYA

Supply Chain / Vendors

NIST SP 800-161-1 / NIST 800-53-5 / NIST SP 800-37
Executive Order 14017 & 14028
OMB M-22-18
National Risk Mgt. Center Supply Chain Guidance
NIST 800-161 Supply Chain Risk Management

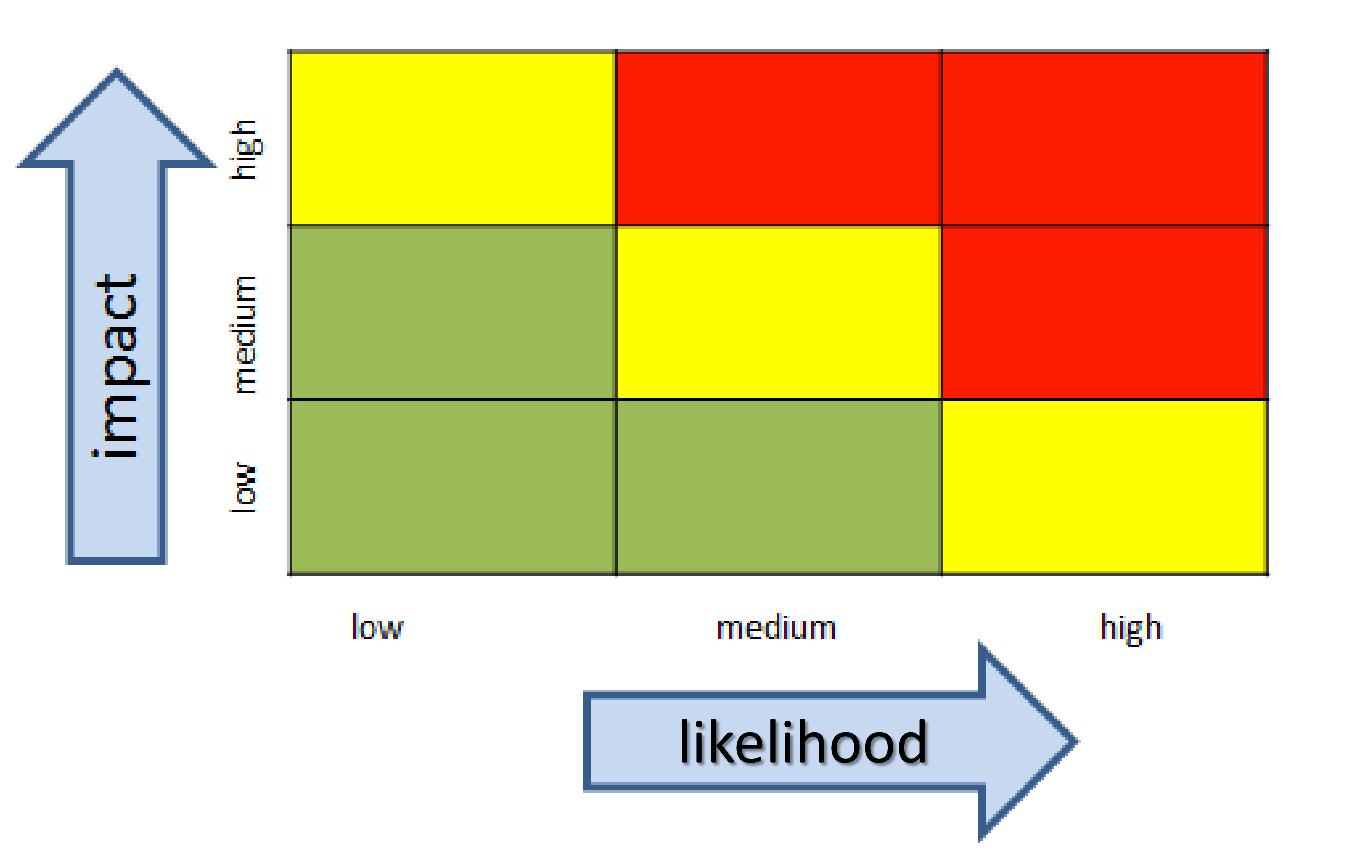
Data

NIST CSF Cybersecurity Framework
ISO/IEC 27005
FAIR Factor Analysis of Information Risk
Cobit 2019
Data Quality Act

AI

NIST AI RMF 1.0 (Artificial Intelligence Risk Mgt. Framework)
NIST AI 600-1 (Generative Artificial Intelligence Profile)

Perceptions of Risk

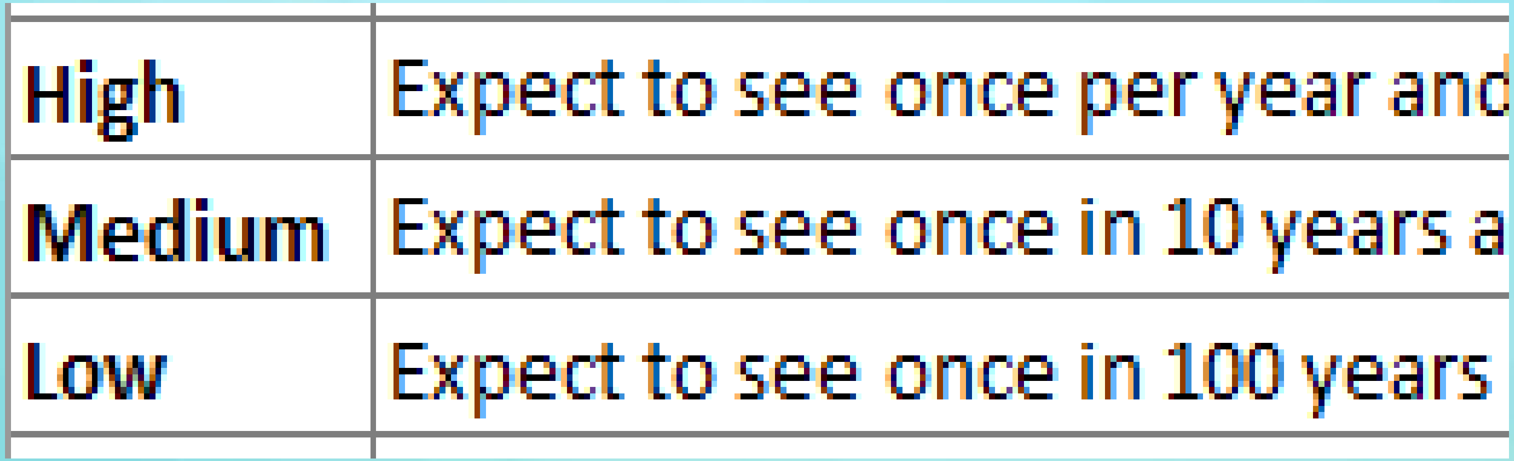


	low	medium	high
high	🟨	🟥	🟥
medium	🟩	🟨	🟥
low	🟩	🟩	🟨

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

Data-based Reality of Risk

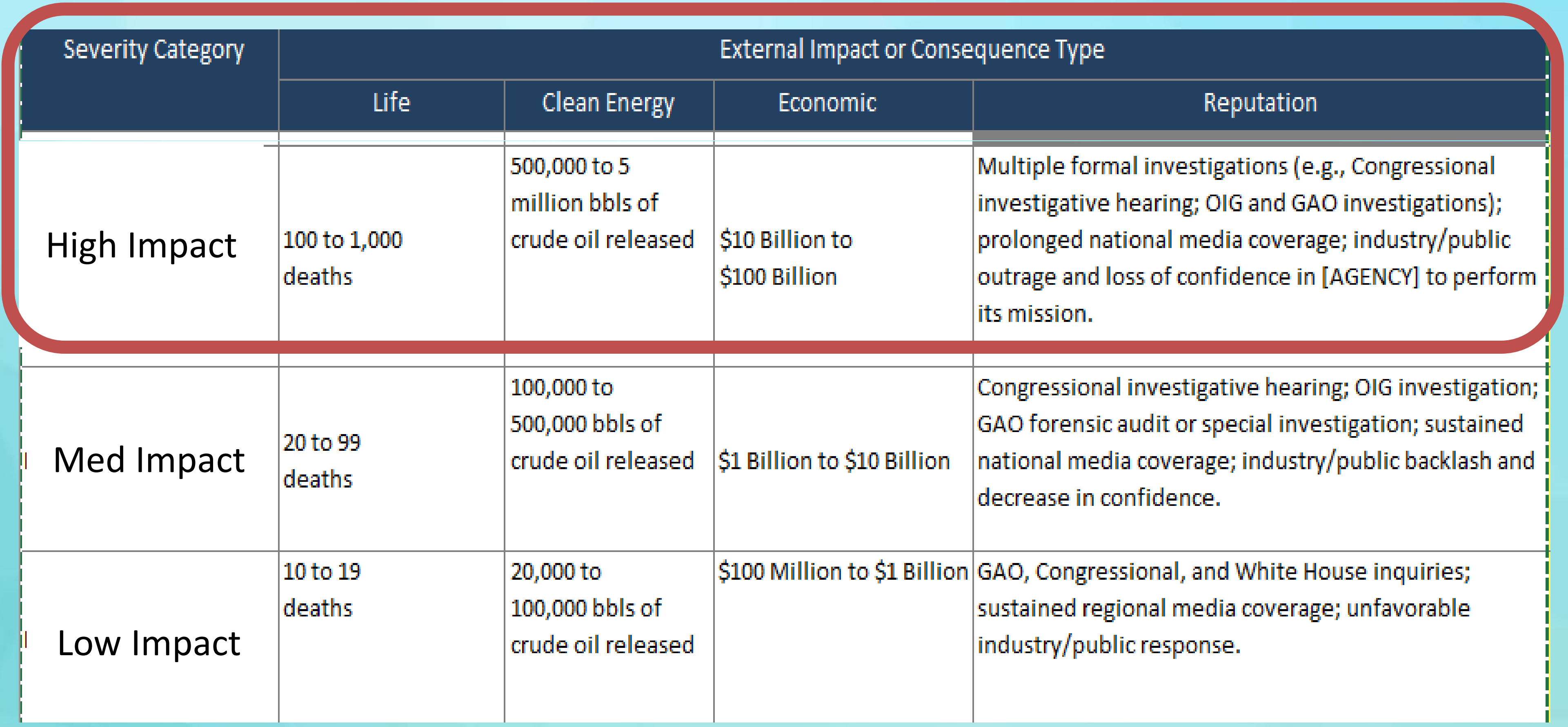
Likelihood/Cause of a Risk Event



High	Expect to see once per year and
Medium	Expect to see once in 10 years a
Low	Expect to see once in 100 years

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

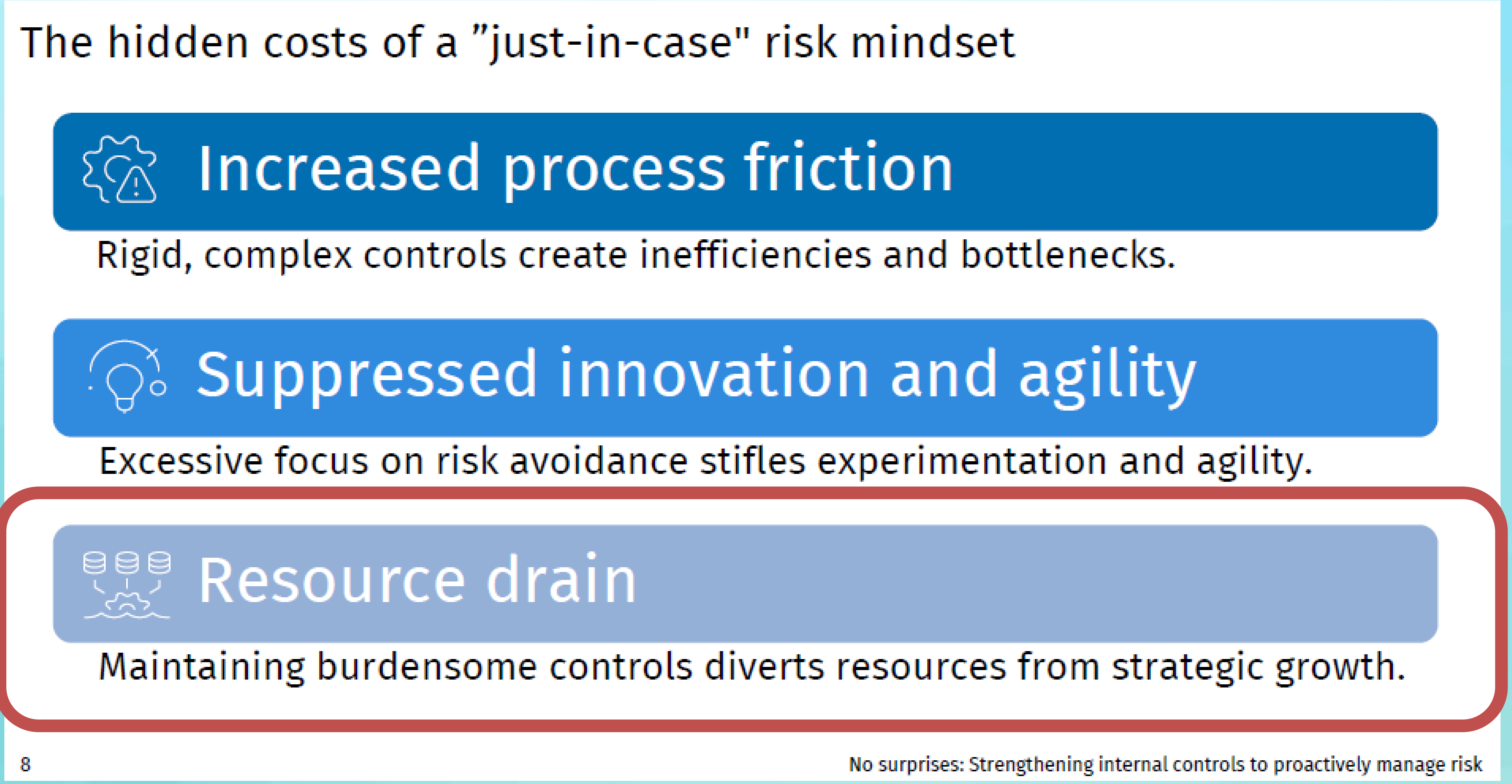
Impact/Consequence of a Risk Event



Severity Category	External Impact or Consequence Type			
	Life	Clean Energy	Economic	Reputation
High Impact	100 to 1,000 deaths	500,000 to 5 million bbls of crude oil released	$10 Billion to $100 Billion	Multiple formal investigations (e.g., Congressional investigative hearing; OIG and GAO investigations); prolonged national media coverage; industry/public outrage and loss of confidence in [AGENCY] to perform its mission.
Med Impact	20 to 99 deaths	100,000 to 500,000 bbls of crude oil released	$1 Billion to $10 Billion	Congressional investigative hearing; OIG investigation; GAO forensic audit or special investigation; sustained national media coverage; industry/public backlash and decrease in confidence.
Low Impact	10 to 19 deaths	20,000 to 100,000 bbls of crude oil released	$100 Million to $1 Billion	GAO, Congressional, and White House inquiries; sustained regional media coverage; unfavorable industry/public response.

How do we talk about risk?

First a Change in mindset



The hidden costs of a ”just-in-case" risk mindset

Increased process friction

Rigid, complex controls create inefficiencies and bottlenecks.

Suppressed innovation and agility

Excessive focus on risk avoidance stifles experimentation and agility.

Resource drain

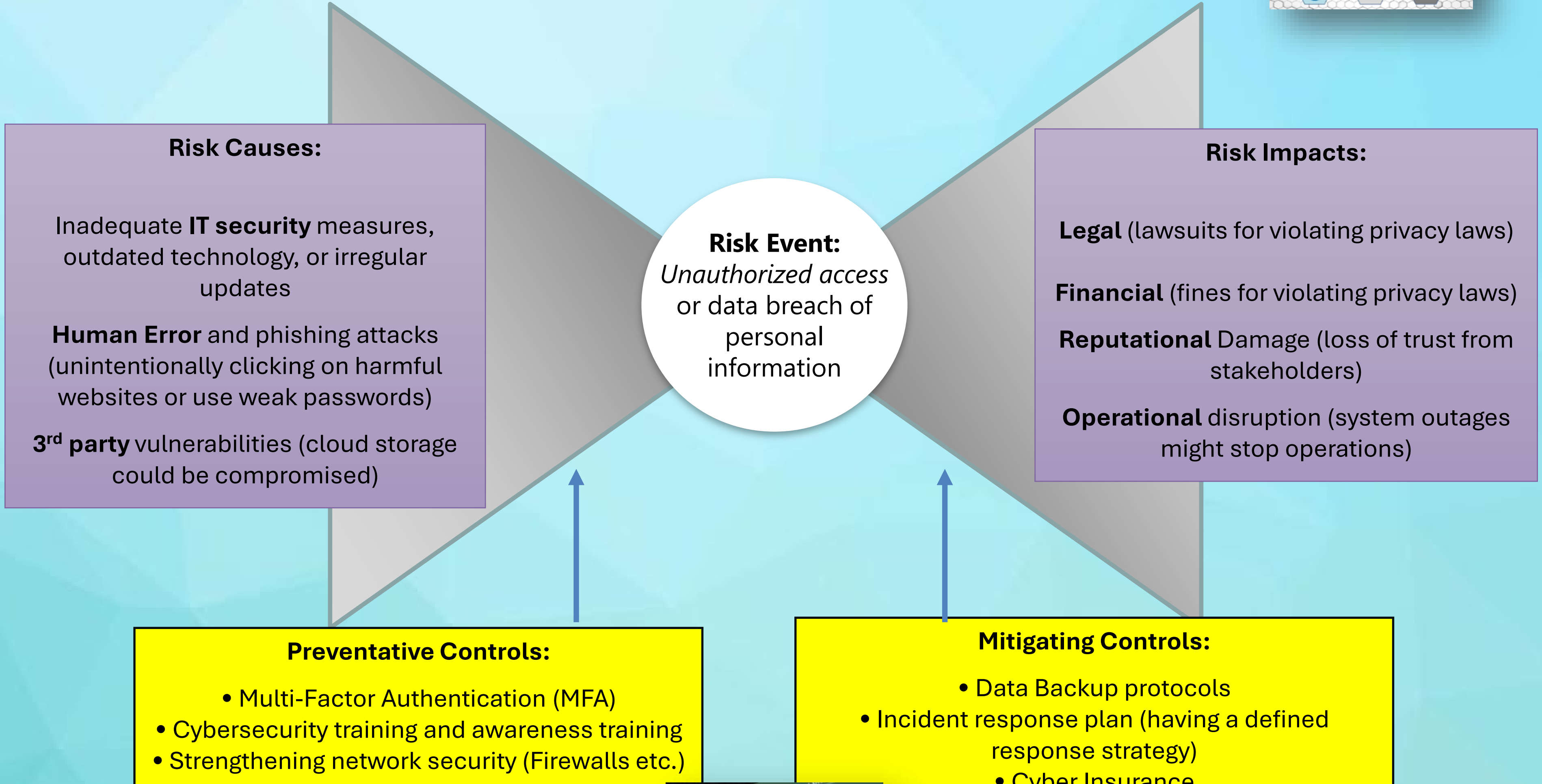
Maintaining burdensome controls diverts resources from strategic growth.

8

No surprises: Strengthening internal controls to proactively manage risk

Bow Tie Analysis (EXAMPLE)

Playbook:
Enterprise Risk Management
for the U.S. Federal Government



Risk Causes:

Inadequate **IT security** measures, outdated technology, or irregular updates

Human Error and phishing attacks (unintentionally clicking on harmful websites or use weak passwords)

3rd party vulnerabilities (cloud storage could be compromised)

Risk Event:
Unauthorized access or data breach of personal information

Risk Impacts:

Legal (lawsuits for violating privacy laws)

Financial (fines for violating privacy laws)

Reputational Damage (loss of trust from stakeholders)

Operational disruption (system outages might stop operations)

Preventative Controls:

- Multi-Factor Authentication (MFA)
- Cybersecurity training and awareness training
- Strengthening network security (Firewalls etc.)

Mitigating Controls:

- Data Backup protocols
- Incident response plan (having a defined response strategy)
- Cyber Insurance

United States Government A

Internal Control

GAO

2014

Standards for
Internal Control
in the Federal
Government

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

GAO

Internal Control

2014

Standards for
Internal Control
in the Federal
Government

ERM & Green Book

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

GAO

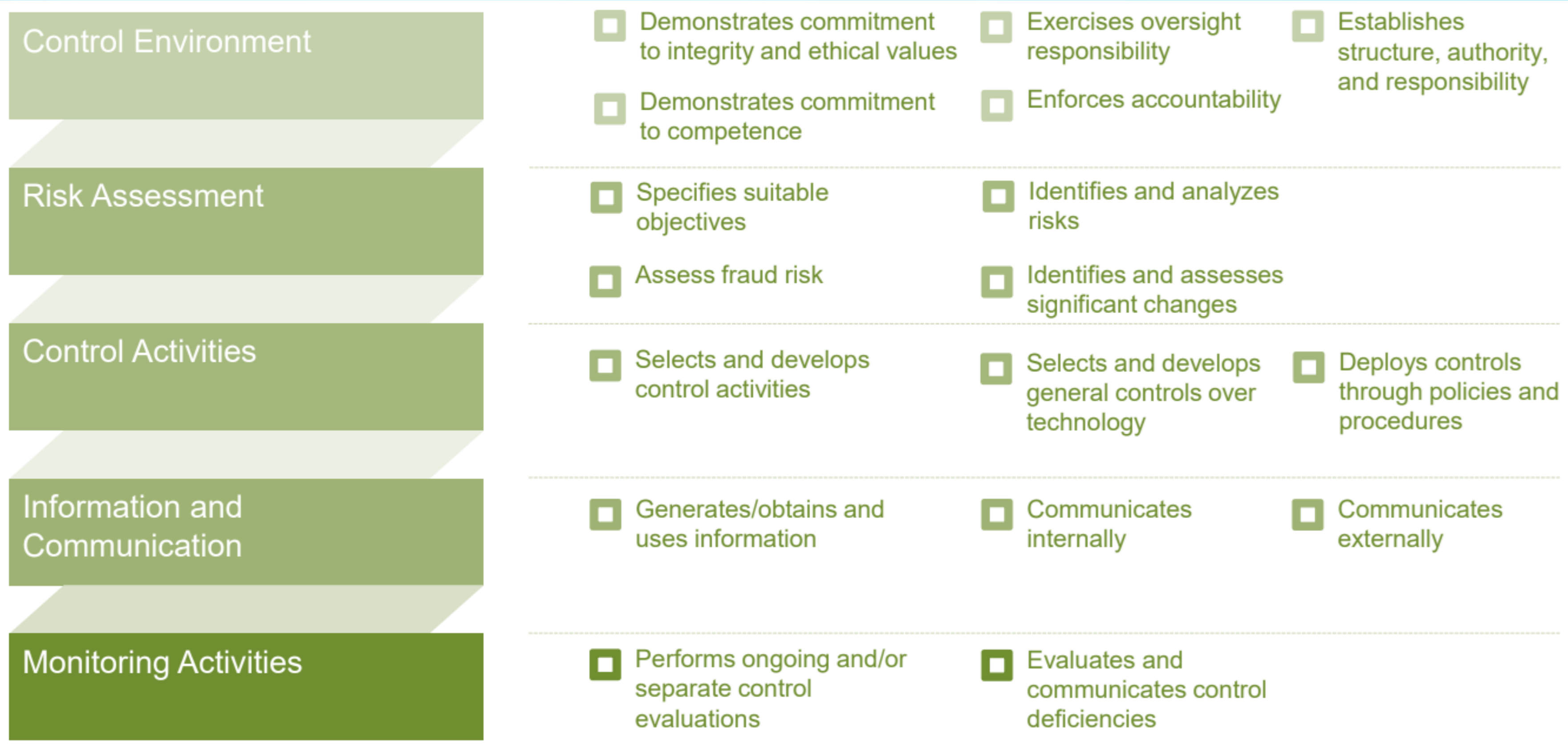
Internal Control

Standards for
Internal Control
in the Federal
Government

2014

Risk Categories	Green Book Principles
Governance Risks	P1, P2
Strategy Risks	P6, P7, P9
Technology Risks	P11
Reporting Risks	P13-P17
Financial Risks	P8
Operations Risks	P3, P10, P12
People Risks	P4, P5

5 Components: The Full Picture



Control Environment	□ Demonstrates commitment to integrity and ethical values □ Demonstrates commitment to competence	□ Exercises oversight responsibility □ Enforces accountability	□ Establishes structure, authority, and responsibility
Risk Assessment	□ Specifies suitable objectives □ Assess fraud risk	□ Identifies and analyzes risks □ Identifies and assesses significant changes	
Control Activities	□ Selects and develops control activities	□ Selects and develops general controls over technology	□ Deploys controls through policies and procedures
Information and Communication	□ Generates/obtains and uses information	□ Communicates internally	□ Communicates externally
Monitoring Activities	□ Performs ongoing and/or separate control evaluations	□ Evaluates and communicates control deficiencies	

GAO Update July 2025

documentation requirements for **risk assessments** and **change assessments**

Including risks related to fraud, improper payments, and **information security**

prioritizing **preventive controls**

OV 4.08 → OV 2.10-2.13

OV 2.11 - Minimum Documentation Requirements

7.15 – Risk Assessment

9.05 – Change Assessment Process

12.02 – Policies and Procedures

17.05 – Control Deficiencies

OV 1.06 → OV 1.07

"**People** are what make internal control work."

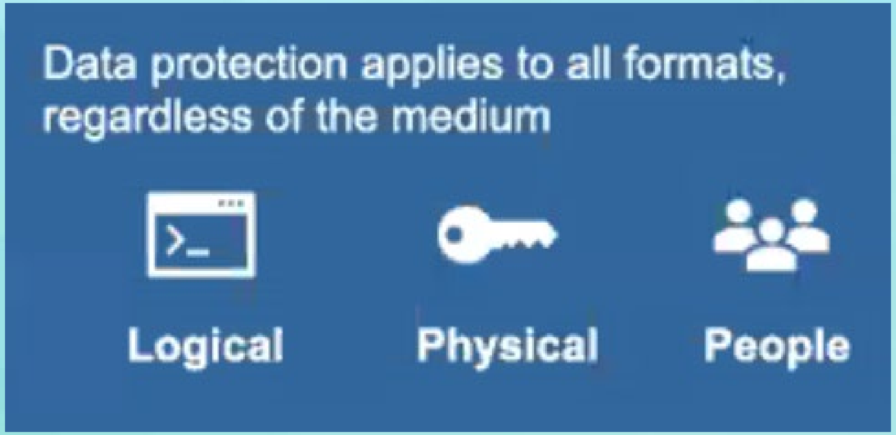
NEW: OV 4.08 – OV 4.12

Information Technology

"…refers more broadly to the people, processes, data…

that management uses …

to support the entity's business processes."

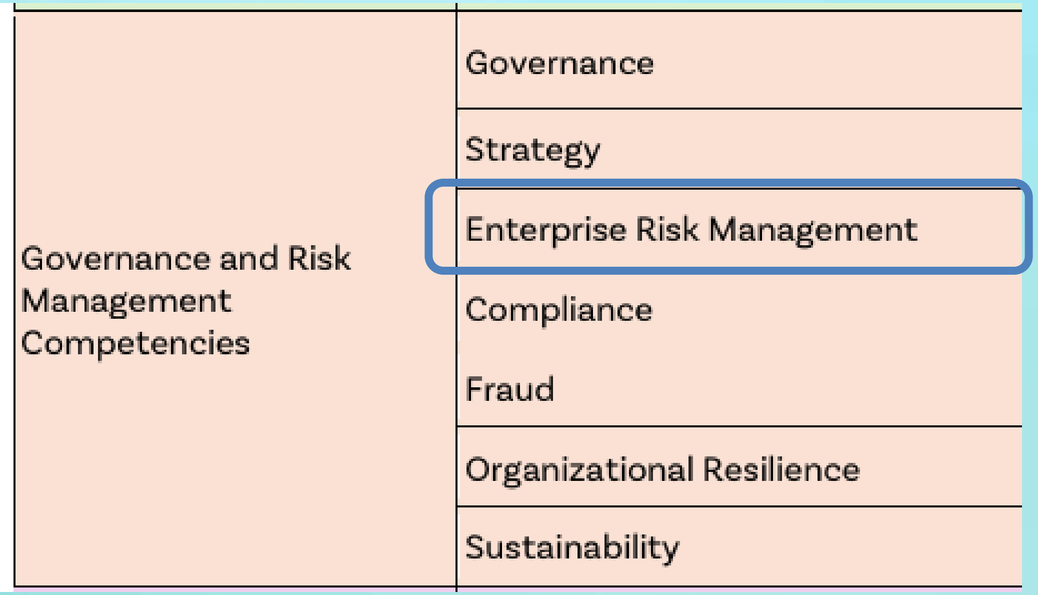


Data protection applies to all formats, regardless of the medium

NEW: OV 4.18 – OV 4.19

Enterprise Risk Management

"…more than internal control."



Governance and Risk Management Competencies	Governance
	Strategy
	Enterprise Risk Management
	Compliance Fraud
	Organizational Resilience
	Sustainability

NEW: Principle 8 - 8.02 – 8.05

Identify Risks Related to Fraud, Improper Payments, and Information Security

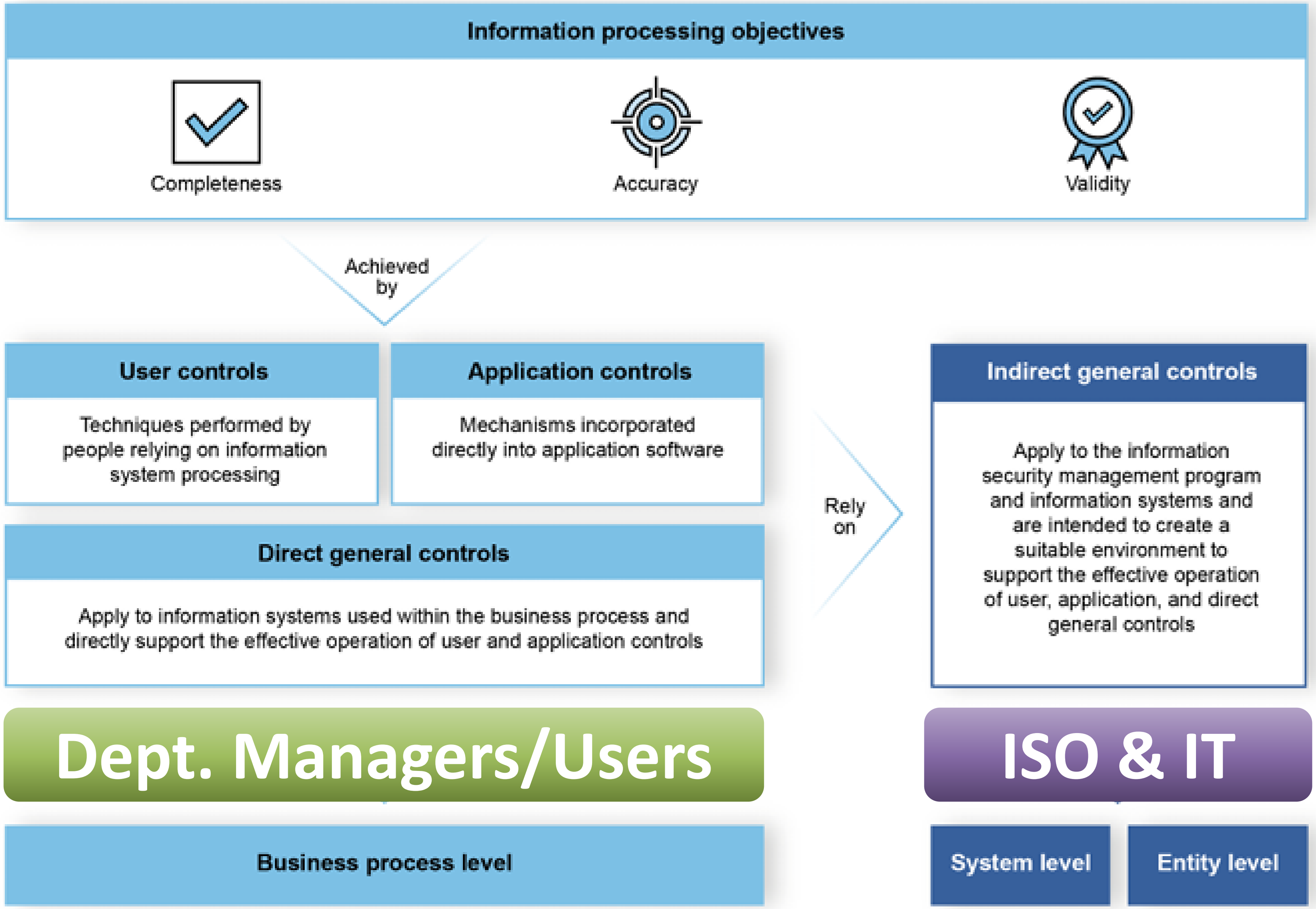
8.02 "…same risk identification process … for all analyzed risks."

Principle 10, 10.10 – 10.13

Design of Preventive and Detective Control Activities

Workflow diagrams are great for this!

Figure 4: Fundamental Information System Control Concepts



Information processing objectives

Completeness

Accuracy

Validity

Achieved by

User controls

Techniques performed by people relying on information system processing

Application controls

Mechanisms incorporated directly into application software

Direct general controls

Apply to information systems used within the business process and directly support the effective operation of user and application controls

Rely on

Indirect general controls

Apply to the information security management program and information systems and are intended to create a suitable environment to support the effective operation of user, application, and direct general controls

Dept. Managers/Users

ISO & IT

Business process level

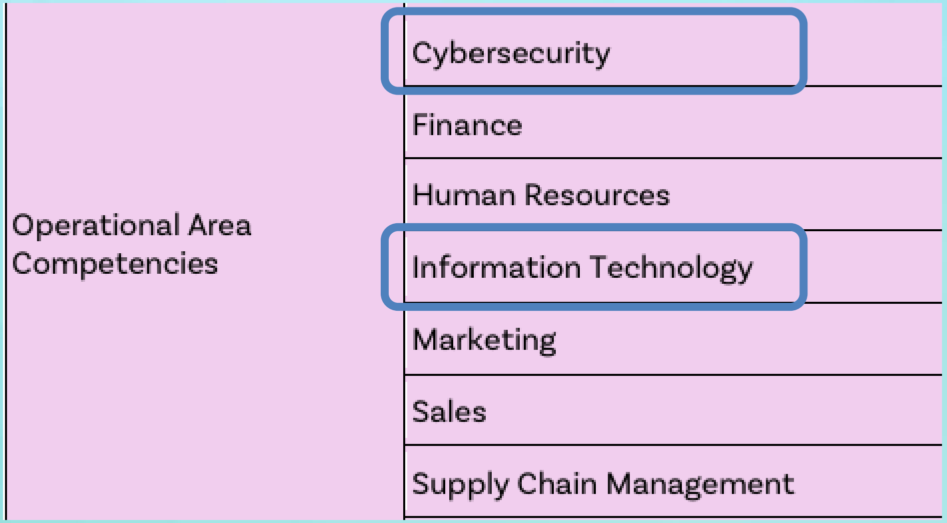
System level

Entity level

Principle 11, 11.06

Design of the Entity’s Information Technology

“…support the entity’s business processes.”



Operational Area Competencies	Cybersecurity
	Finance
	Human Resources
	Information Technology
	Marketing
	Sales
	Supply Chain Management

Principle 12, 12.02 – 12.04

Documentation of Control Activities Through Policies and Procedures

"…in policies what is expected

in procedures specified actions

… to mitigate risks

OV 1.06 → OV 1.07

“**People** are what make internal control work.”

ERM Alignment

with

Role and Authority of Internal Audit

Internal Audit Oversight Role

- **Our Authority in CA Gov Code**:
  - GC §26881, the Auditor –Controller has the responsibility to supervise and review **internal controls Countywide**.
  - GC §1236, Local Government Internal Auditors shall conduct work according to professional standards (i.e. Yellow Book or Red Book)
  - GC §13405 - State Leadership Accountability Act – Dept of Finance, State Auditor and SCO shall guide state agencies in conducting internal reviews of systems of internal control.
  - GC § 12422.5 - [SCO] may audit any local agency for purposes of determining whether the agency's internal controls are adequate to detect and prevent financial errors and fraud.
- **County of Santa Clara, County Charter Article VI, § 601, 602:**
  - "§ 601 (a)(b)(c)…The Auditor-Controller shall have the power and duty to:
    - (a) Keep accounts showing the financial ***transactions*** of all offices …
    - (c) Prepare…reports…necessary for information and use in the ***management and control of the operations*** of the county.
  - "§ 602…audit of the accounts and records of all offices and departments…"

Role as Facilitator and Change Agent

- **Our Mission**:
  - The Audit Division helps the County accomplish its objectives by using a systematic, disciplined approach to ***improve*** governance, risk management, and control processes.

Aligned Standards and Guidance

ISO

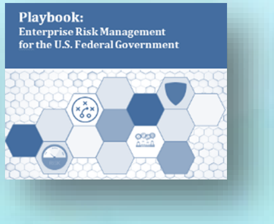
The Institute of Internal Auditors

GASB

GASB: Current Project: **Cybersecurity** Risk Disclosures

GFOA: Best Practice: **Enterprise Risk Management**

usa gov


Playbook:
Enterprise Risk Management
for the U.S. Federal Government

United States Government
Internal Control
GAO
2014
Standards for Internal Control in the Federal Government

2 CFR § 200.303

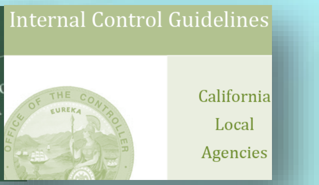
"The recipient and subrecipient must…

OMB A-123

CA.GOV

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

United States Government
Internal Control
GAO
2014
Standards for Internal Contr
in the Federal
Government


Internal Control Guidelines
Office of the Controller
Eureka
California
Local
Agencies

- financial focus -

Global
Internal Audit
Standards™

CA GC § 1236

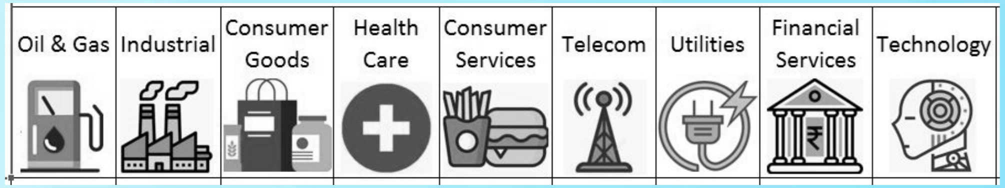
County Internal Control Policy & Methods

- financial focus -

Global
Internal Audit
Standards™

Objectives

OMB A-11, Grants, Budget Priorities



Oil & Gas	Industrial	Consumer Goods	Health Care	Consumer Services	Telecom	Utilities	Financial Services	Technology

Risks & ERM

ISO, GFOA, OMB A-123

Playbook:
Enterprise Risk Management
for the U.S. Federal Government

Controls

GASB, GAO, CA State Controller

United States Government Ac
Internal Control

GAO

2014

Standards for
Internal Control
in the Federal
Government

Audit

IIA, GAO, CA GOV CODE

Global
Internal Audit
Standards™

Local Government Perspectives on ERM and Internal Controls

Mel Thomson, ARM, CRMP-FED, ERMCP

Association of Federal Enterprise Risk Management (AFERM) - Chair, State and Local Committee

Cybersecurity Risk Strategist, City of Phoenix

Albert Beltran Jr, CIA, CISA, CRMA, CC, CRISC

Association of Federal Enterprise Risk Management (AFERM) - Member, State and Local Committee

IIA San Jose Chapter, Advocacy Chair

Internal Audit Division-Finance Agency, County of Santa Clara

Presentation for the California Government Operations Agency (CalGovOps),

Governance, Risk Management and Compliance Council (GRCC)

Wednesday, November 5, 2025

GOVERNANCE RISK AND COMPLIANCE COUNCIL

GRCC

SLAA Implementation at Finance

Frances Parmelee, Program Budget Manager, Department of Finance (DOF)

Implementing SLAA: A Department’s Approach

California Community Colleges

INSPECTOR GENERAL
California Department of Transportation

DEPARTMENT OF FINANCE
CALIFORNIA

My SLAA Journey

Finance’s Monitoring Framework

Monitoring Framework Components

- Monitoring Organizational Structure
- Roles & Responsibilities
- Communications Strategy

- Risk Assessment Process
- Risk Monitoring Tools
- Training
- Audits/Reviews

Framework still in draft and subject to change.

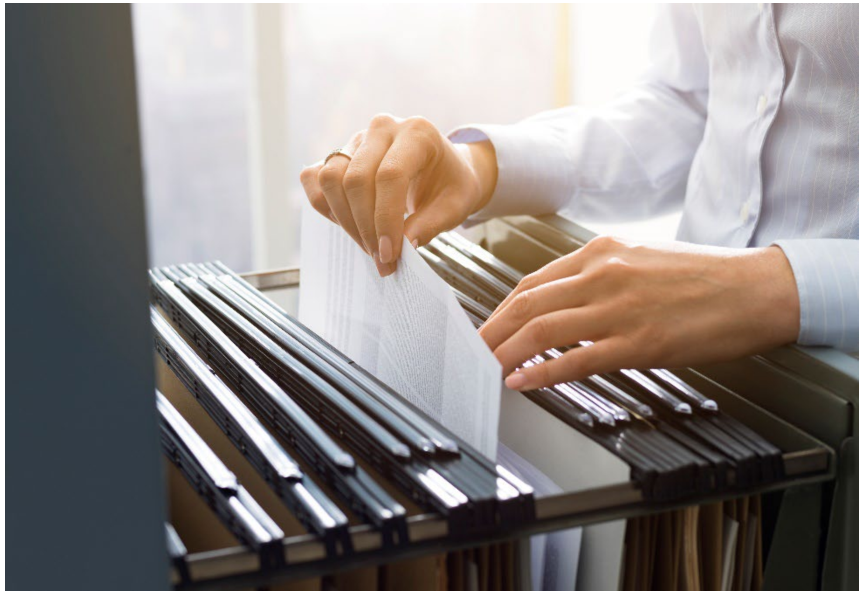
Monitoring Organizational Structure

Tier 1	Director	Director
Tier 2	Executive Monitoring Sponsor	COO
Tier 3	Executive Management	Chief Deputies, Deputies, and Legal
Tier 4	Operational Management	Program Budget Managers (PBMs) and DD of Admin
Tier 5	Middle Management	Assistant PBMs, Chiefs, Assistant Chiefs
Tier 6	Supervisors and Managers	PPA II/IIIs, Supervisors, and Managers
Tier 7	Staff	Budget, Administrative, Accounting, IT, and Audit staff

Communications Strategy

Communication Methods	Involved Parties	Frequency
Executive Meetings	Cap Office	Weekly
PBM Meetings	PBMs, DD of Admin & COO	Weekly
1:1 with COO	PBM and COO	1x month or as needed
PBM Offsites	PBMs & COO	2x year
Exec Offsite	Cap Office and PBMs	2x year
Daily Budget Check-Ins	Budget Management	As Needed
Unit Specific Meetings	Varies (All Staff, Teams, or 1:1s)	As Needed
Team Chats	All Staff	Daily

List is not all-inclusive.



Risk Monitoring Tools

- Risk Reporting Inbox
- Anonymous Reporting Portal on Finance’s Intranet
- Email Reminders about CSA’s Whistleblower Hotline and Finance’s Risk Monitoring Tools
- Suggestion Boxes
- Surveys

Trainings

Methods	Participants	Frequency
New Employee Orientation	New Employees	Once
IT Training	All Staff	Every year
Harassment Prevention	All Staff	Every 2 years
Cornerstone	All Staff	Varies
Defensive Driving	Certain Staff	Every 5 years
Mock Testimony Training	Budget Units, OSAE Management	Once
Various Leadership Training	Certain Staff	Once

List is not all-inclusive.

Resources

- Strategic Plan (in progress)
- Succession Plan (in progress)
- Workforce Plan
- Administrative Policy Manual
- Leadership Handbook
- New Employee Handbook
- Unit-Specific Policies and Procedures

Does Continuous Improvement Matter?

“You tried your best and you failed miserably. The lesson is: never try.”

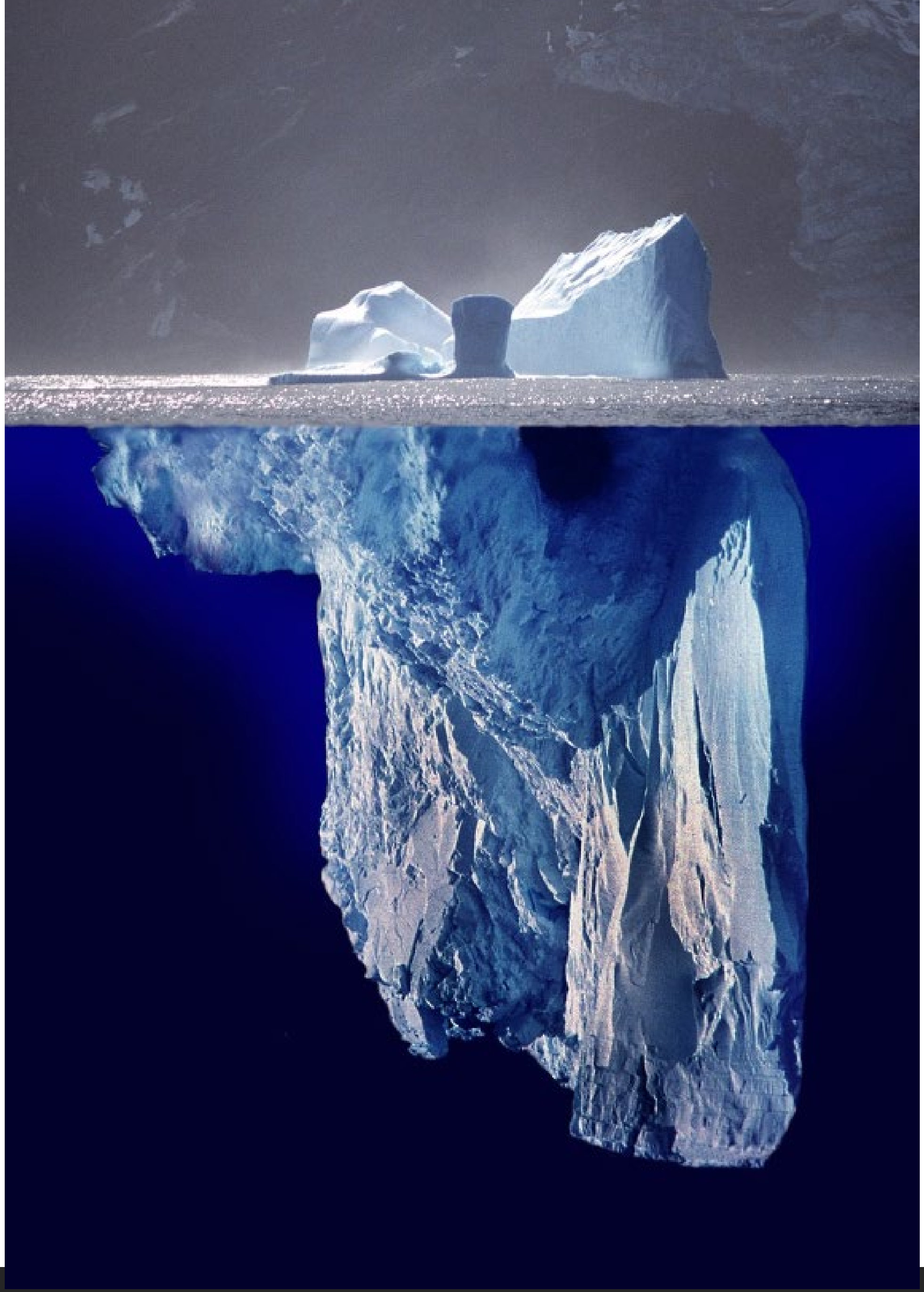
-Homer Simpson, The Simpsons Movie (2007)

Compliance to Continuous Improvement

“Compliance is doing things right; continuous improvement is doing the right things better.” *Philip B. Brosby*

“Without continual growth and progress, such words such as improvement, achievement, and success have no meaning.” *Benjamin Franklin*

“Compliance is the foundation; continuous improvement is the journey.” *W. Edwards Deming*



Thank you

Frances Parmelee, CPA, CIG

Program Budget Manager

Frances.Parmelee@dof.ca.gov

ph. 916-315-3330

OVERSIGHT & ACCOUNTABILITY UNIT
CALIFORNIA DEPARTMENT OF FINANCE

SLAA Updates

Edwina Troupe, Department of Finance
Brian Dunham, Department of Finance
Carla Villa, Department of Finance

Leadership Accountability Updates

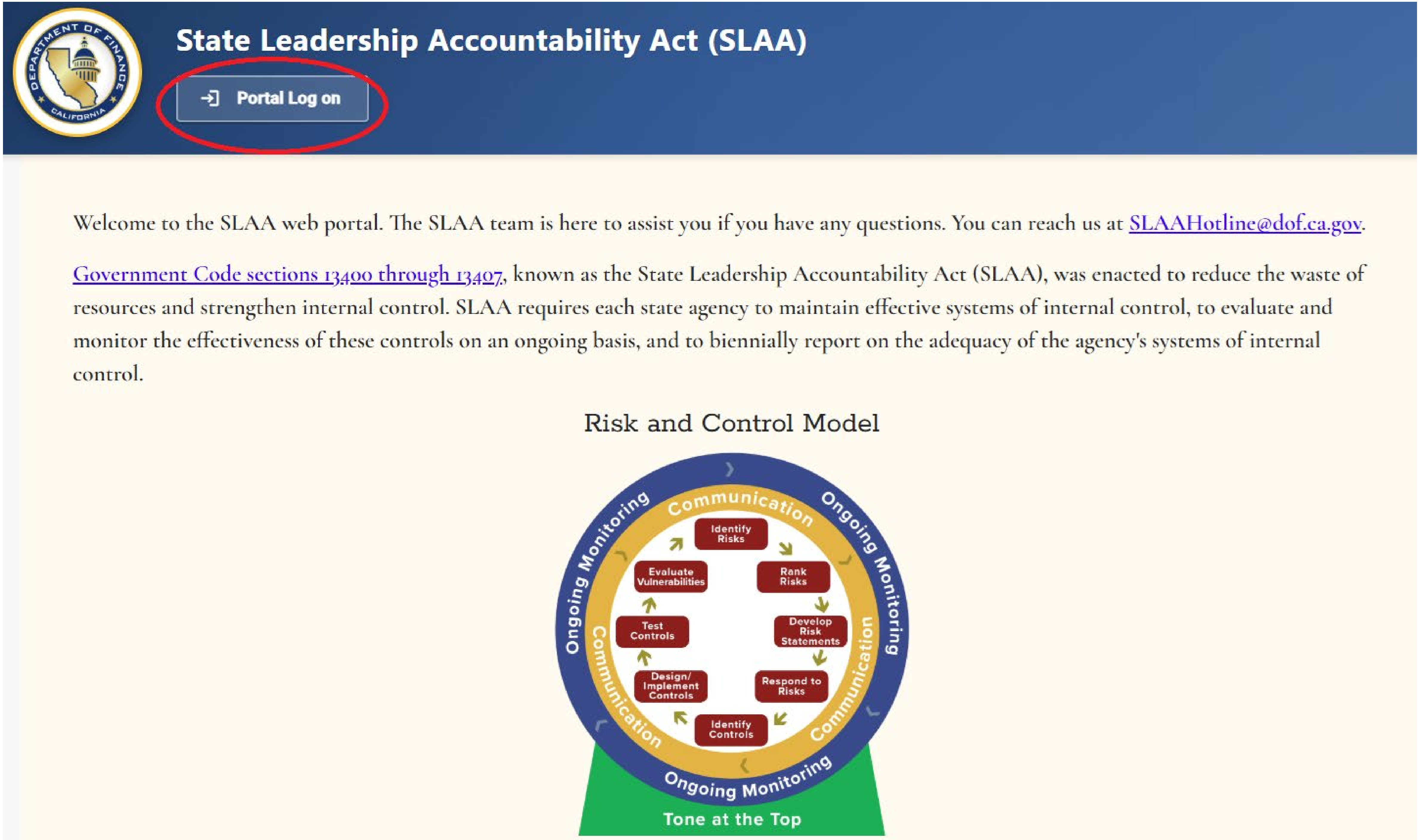
Agenda

1. SLAA Portal Access—MFA
2. New SAM 20080 reporting
3. Portal New Look
4. Report Layout - New Look
5. Top Risks and Controls
   a. Risk Statements
   b. Common Controls

SLAA Portal Access

Multi-Factor Authentication (MFA) for first-time access.

slaa.dof.ca.gov

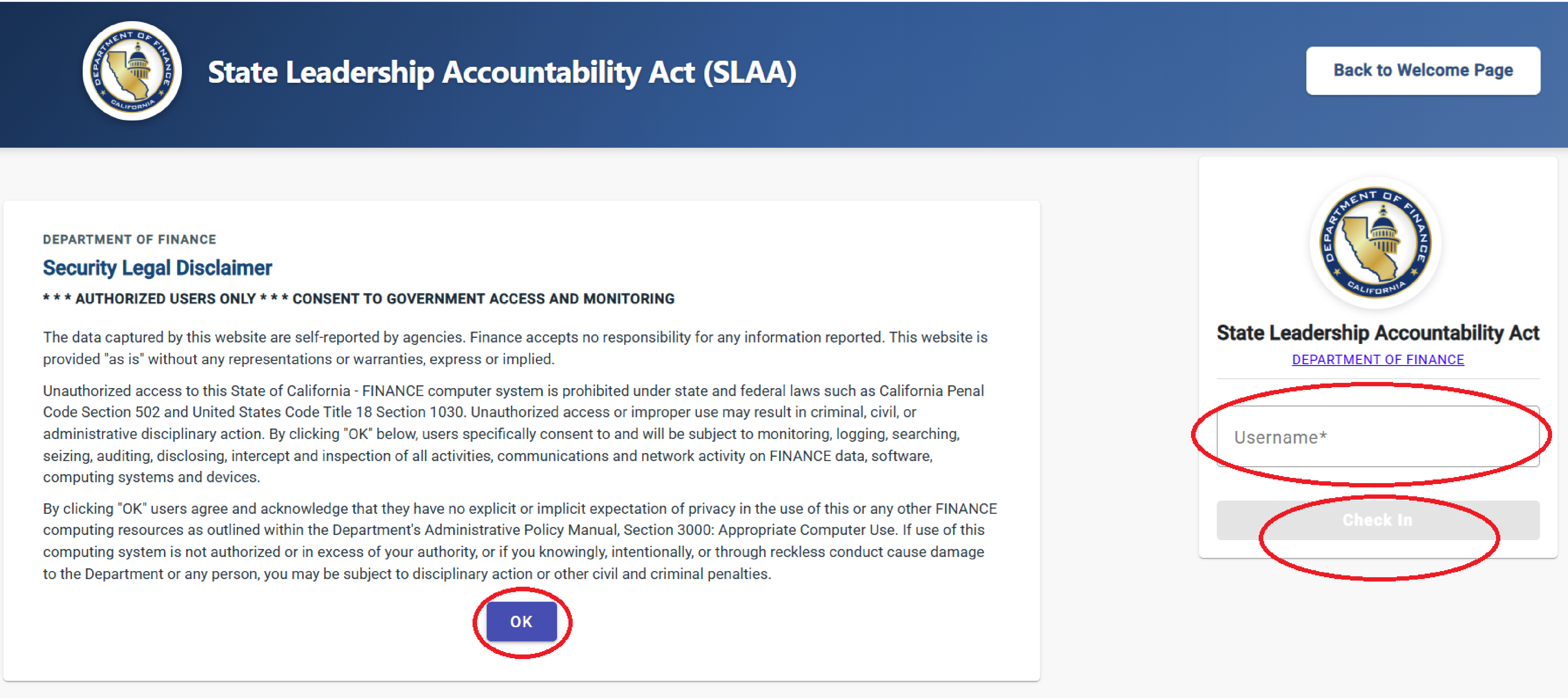


State Leadership Accountability Act (SLAA)

Welcome to the SLAA web portal. The SLAA team is here to assist you if you have any questions. You can reach us at SLAAHotline@dof.ca.gov.

Government Code sections 13400 through 13407, known as the State Leadership Accountability Act (SLAA), was enacted to reduce the waste of resources and strengthen internal control. SLAA requires each state agency to maintain effective systems of internal control, to evaluate and monitor the effectiveness of these controls on an ongoing basis, and to biennially report on the adequacy of the agency's systems of internal control.

Risk and Control Model



DEPARTMENT OF FINANCE

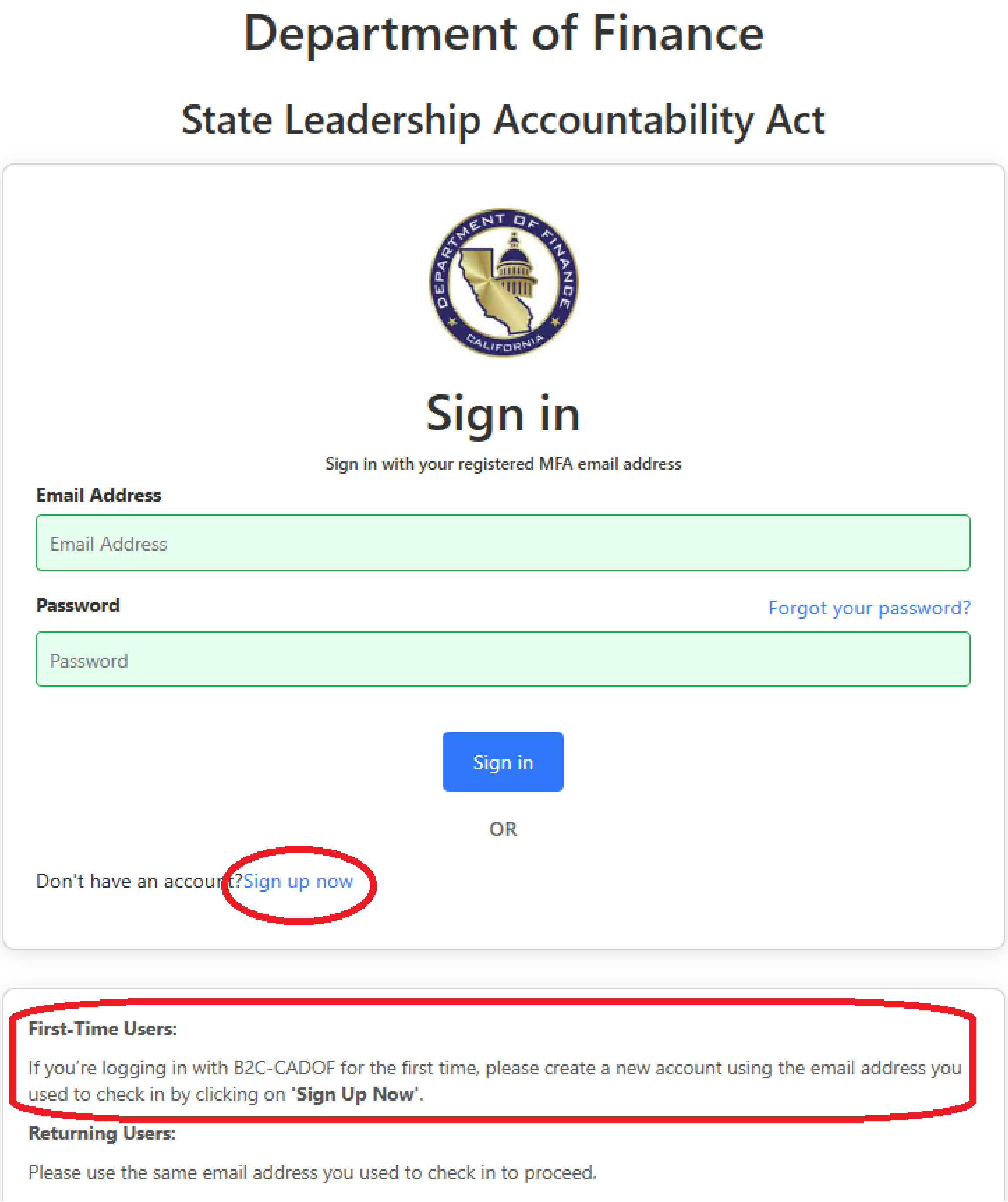
Security Legal Disclaimer

*** * * AUTHORIZED USERS ONLY * * * CONSENT TO GOVERNMENT ACCESS AND MONITORING**

The data captured by this website are self-reported by agencies. Finance accepts no responsibility for any information reported. This website is provided "as is" without any representations or warranties, express or implied.

Unauthorized access to this State of California - FINANCE computer system is prohibited under state and federal laws such as California Penal Code Section 502 and United States Code Title 18 Section 1030. Unauthorized access or improper use may result in criminal, civil, or administrative disciplinary action. By clicking "OK" below, users specifically consent to and will be subject to monitoring, logging, searching, seizing, auditing, disclosing, intercept and inspection of all activities, communications and network activity on FINANCE data, software, computing systems and devices.

By clicking "OK" users agree and acknowledge that they have no explicit or implicit expectation of privacy in the use of this or any other FINANCE computing resources as outlined within the Department's Administrative Policy Manual, Section 3000: Appropriate Computer Use. If use of this computing system is not authorized or in excess of your authority, or if you knowingly, intentionally, or through reckless conduct cause damage to the Department or any person, you may be subject to disciplinary action or other civil and criminal penalties.



Sign in

Sign in with your registered MFA email address

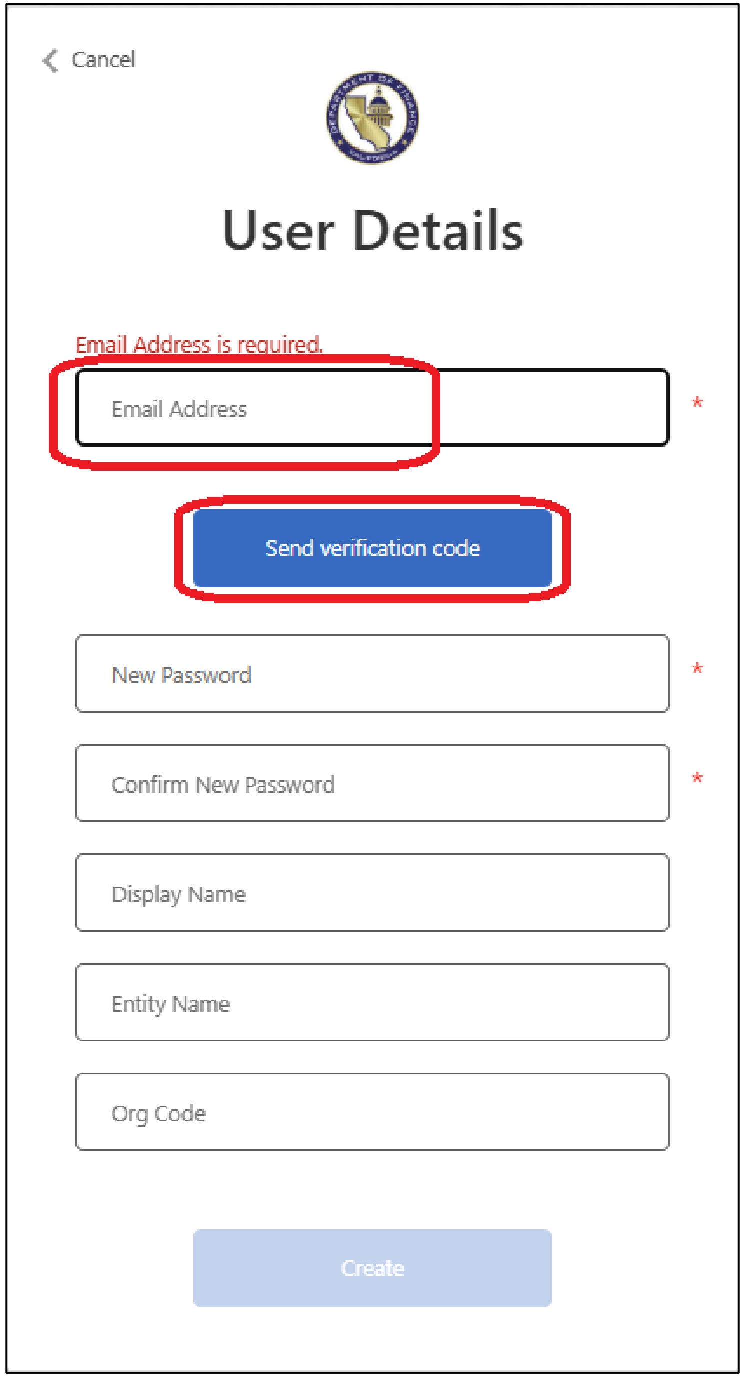
Don't have an account?Sign up now

First-Time Users:

If you're logging in with B2C-CADOF for the first time, please create a new account using the email address you used to check in by clicking on **'Sign Up Now'**.

Returning Users:

Please use the same email address you used to check in to proceed.



User Details

Email Address is required.

Email Address *

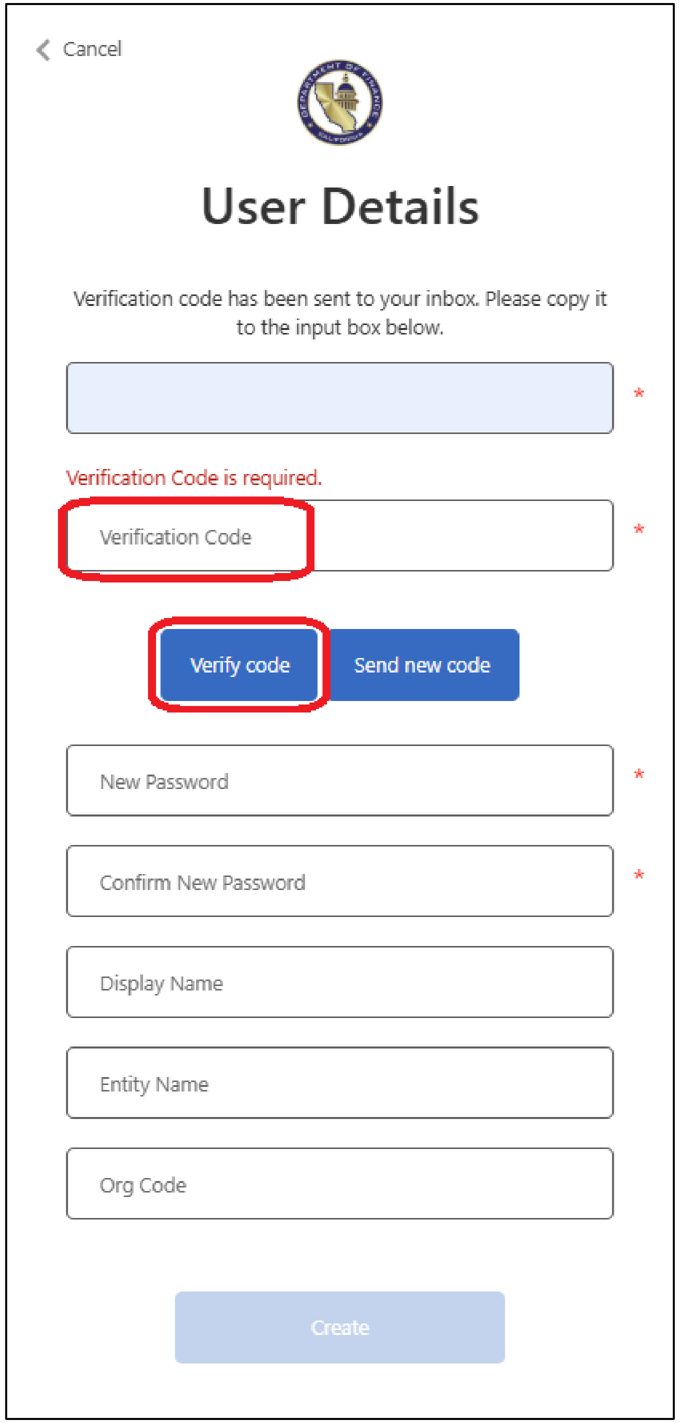
New Password *

Confirm New Password *

Display Name

Entity Name

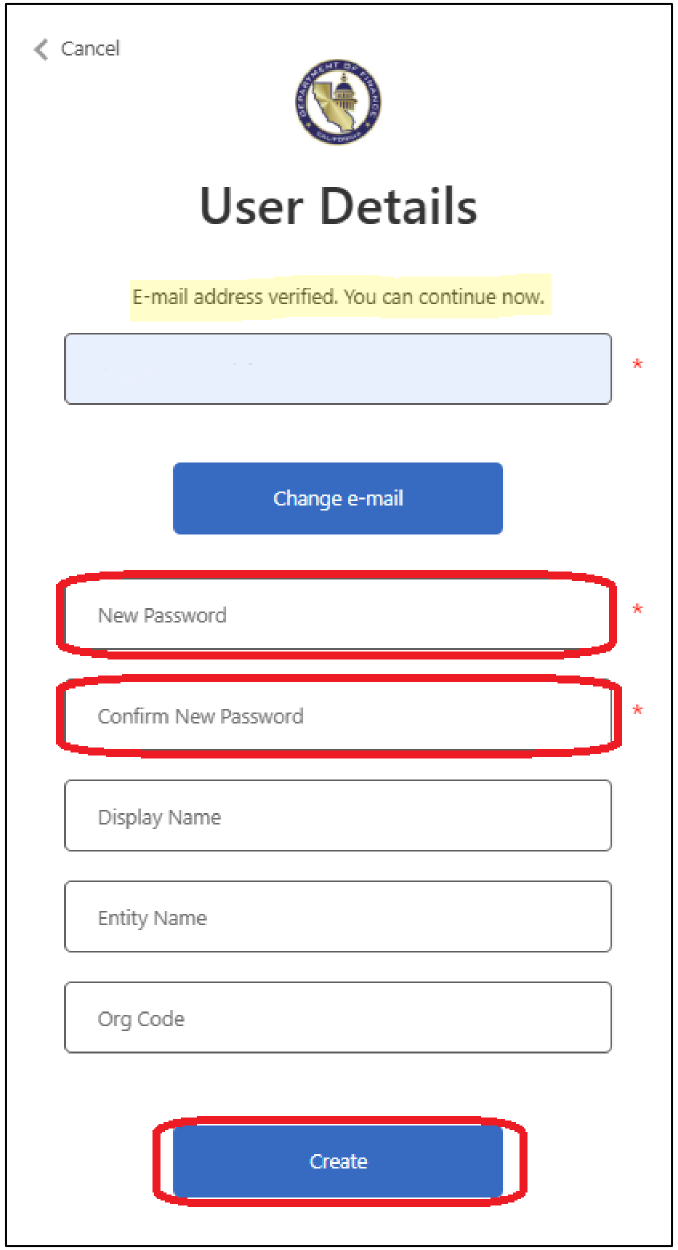
Org Code



User Details

Verification code has been sent to your inbox. Please copy it to the input box below.

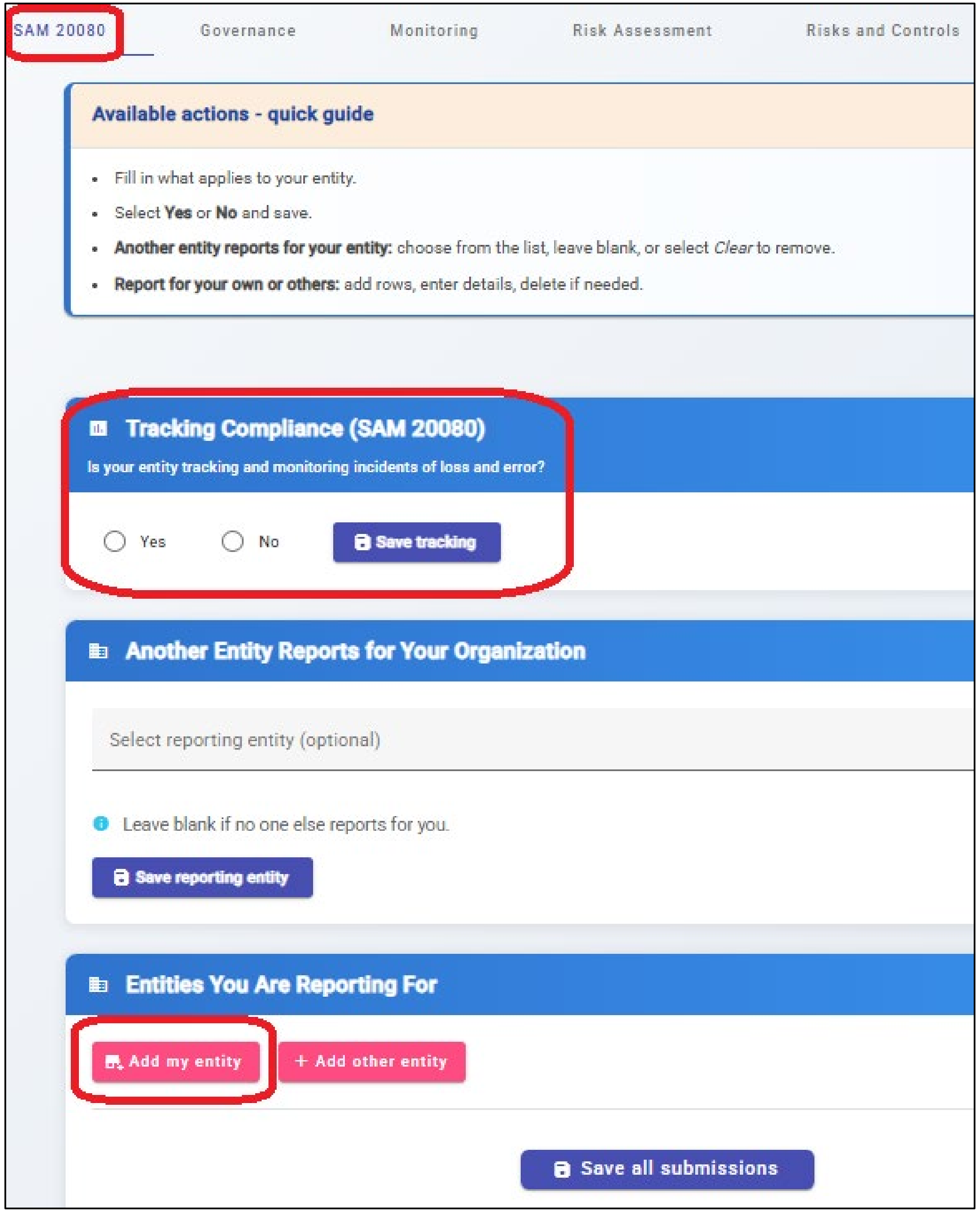
Verification Code is required.



User Details

E-mail address verified. You can continue now.

New SAM 20080 Reporting



Available actions - quick guide

- Fill in what applies to your entity.
- Select **Yes** or **No** and save.
- **Another entity reports for your entity:** choose from the list, leave blank, or select *Clear* to remove.
- **Report for your own or others:** add rows, enter details, delete if needed.

Tracking Compliance (SAM 20080)

Is your entity tracking and monitoring incidents of loss and error?

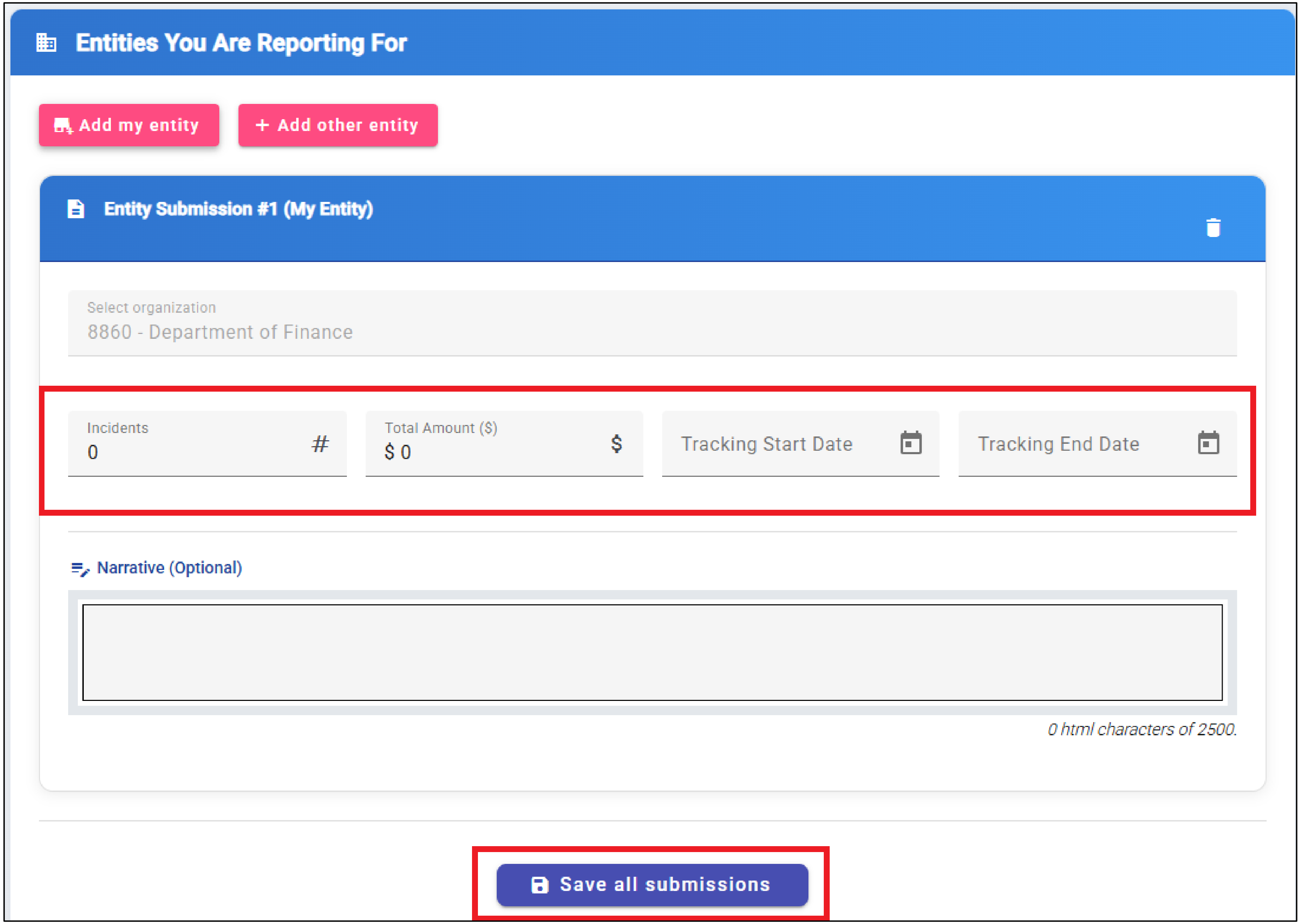
○ Yes ○ No

Another Entity Reports for Your Organization

Select reporting entity (optional)

Leave blank if no one else reports for you.

Entities You Are Reporting For



Entities You Are Reporting For

Add my entity

+ Add other entity

Entity Submission #1 (My Entity)

Select organization
8860 - Department of Finance

Incidents
0 #

Total Amount ($)
$ 0 $

Tracking Start Date

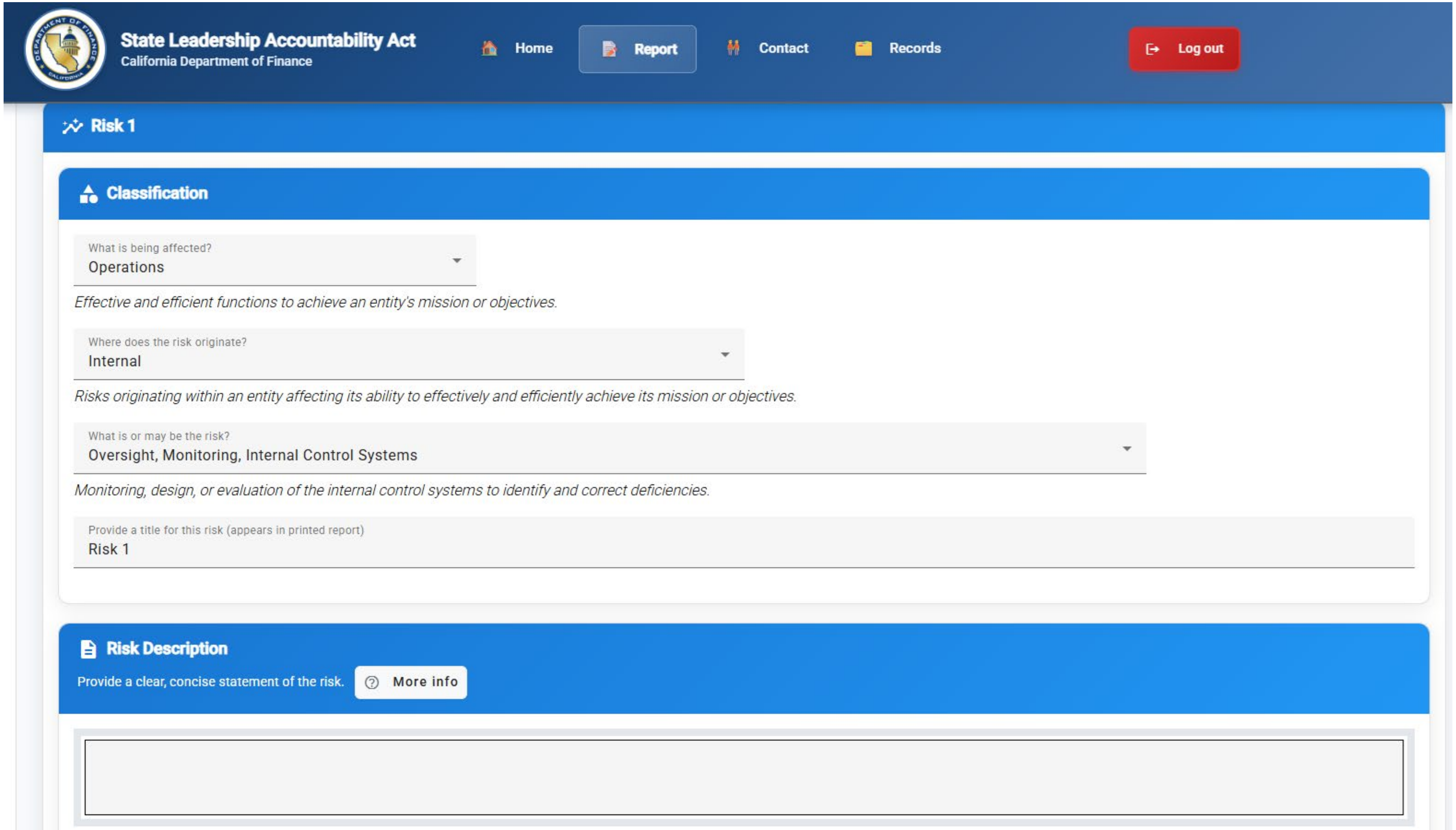
Tracking End Date

Narrative (Optional)

0 html characters of 2500.

Save all submissions

A New Look for the Portal



State Leadership Accountability Act
California Department of Finance
Home
Report
Contact
Records
Log out

Risk 1

Classification

What is being affected?
Operations

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

Where does the risk originate?
Internal

Risks originating within an entity affecting its ability to effectively and efficiently achieve its mission or objectives.

What is or may be the risk?
Oversight, Monitoring, Internal Control Systems

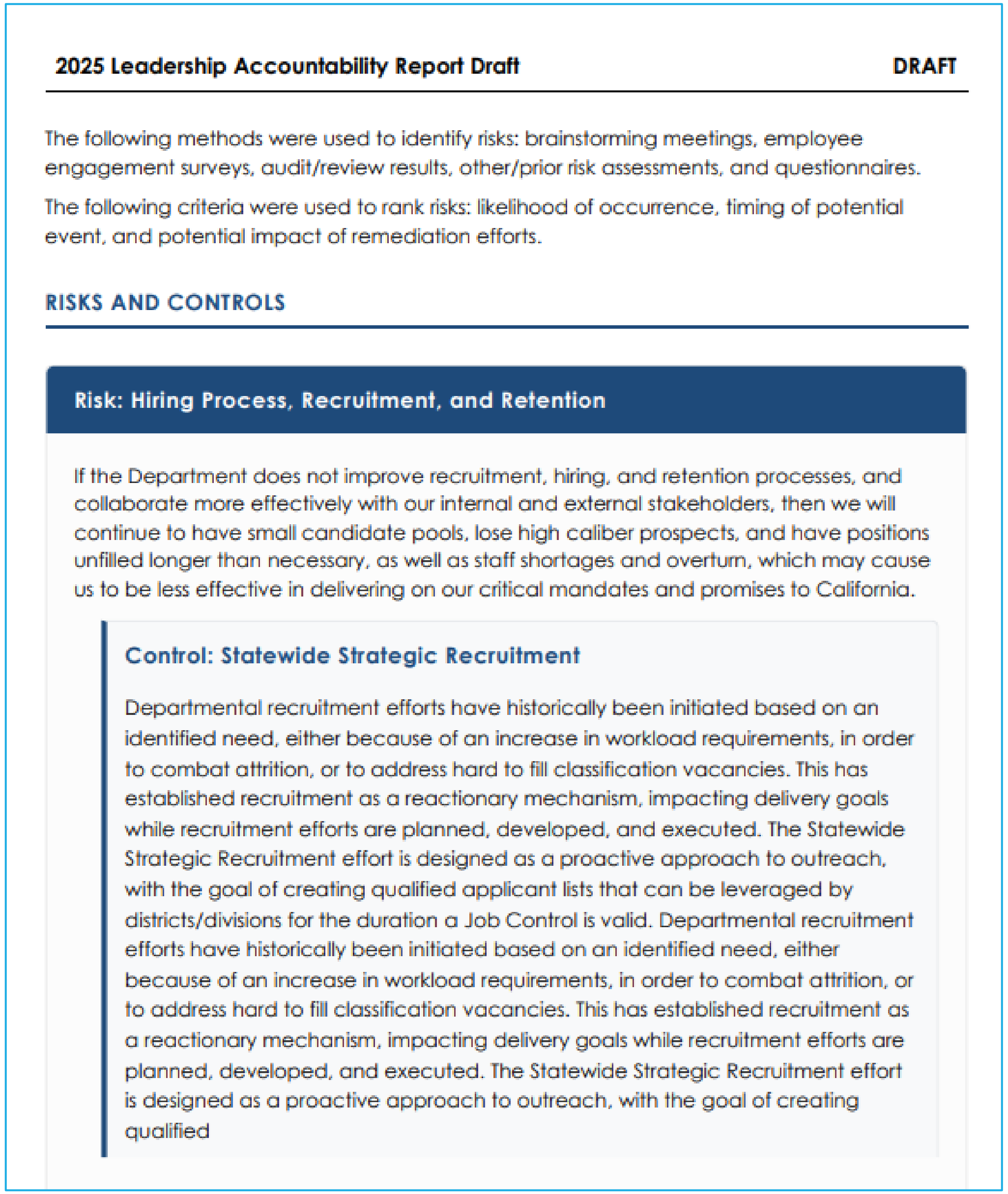
Monitoring, design, or evaluation of the internal control systems to identify and correct deficiencies.

Provide a title for this risk (appears in printed report)
Risk 1

Risk Description

Provide a clear, concise statement of the risk.

Report – New Look



2025 Leadership Accountability Report Draft **DRAFT**

The following methods were used to identify risks: brainstorming meetings, employee engagement surveys, audit/review results, other/prior risk assessments, and questionnaires.

The following criteria were used to rank risks: likelihood of occurrence, timing of potential event, and potential impact of remediation efforts.

RISKS AND CONTROLS

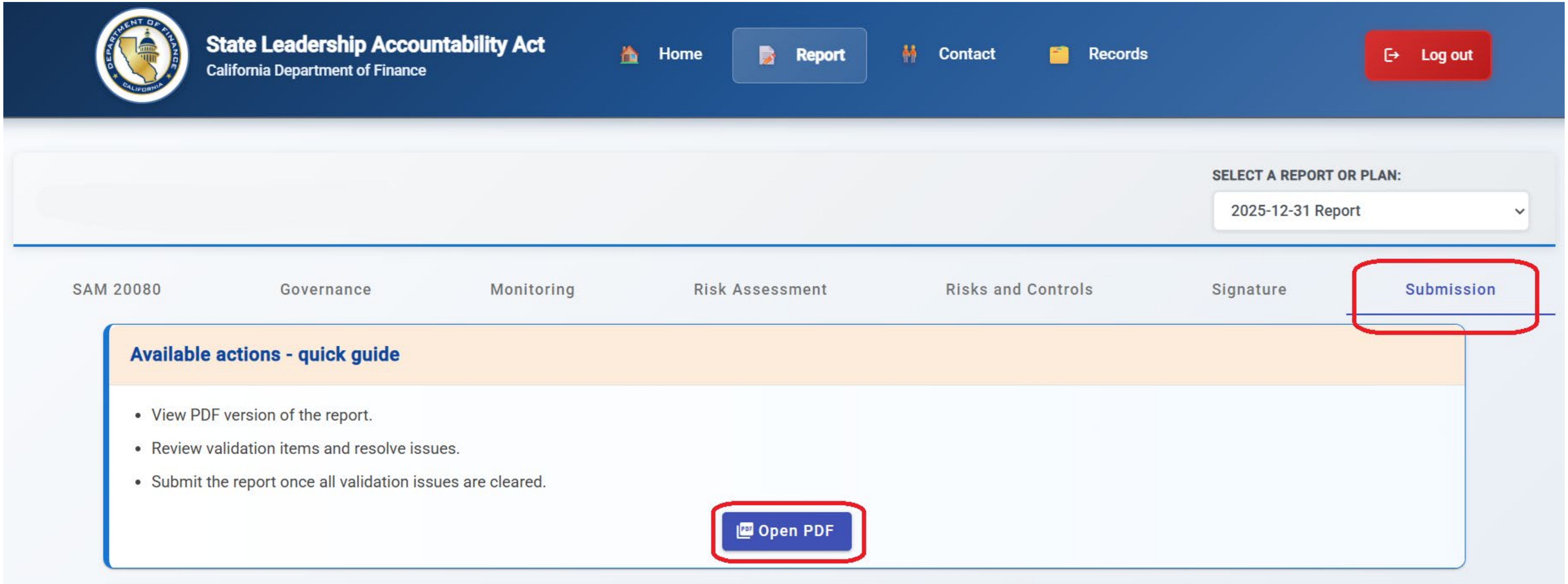
Risk: Hiring Process, Recruitment, and Retention

If the Department does not improve recruitment, hiring, and retention processes, and collaborate more effectively with our internal and external stakeholders, then we will continue to have small candidate pools, lose high caliber prospects, and have positions unfilled longer than necessary, as well as staff shortages and overturn, which may cause us to be less effective in delivering on our critical mandates and promises to California.

Control: Statewide Strategic Recruitment

Departmental recruitment efforts have historically been initiated based on an identified need, either because of an increase in workload requirements, in order to combat attrition, or to address hard to fill classification vacancies. This has established recruitment as a reactionary mechanism, impacting delivery goals while recruitment efforts are planned, developed, and executed. The Statewide Strategic Recruitment effort is designed as a proactive approach to outreach, with the goal of creating qualified applicant lists that can be leveraged by districts/divisions for the duration a Job Control is valid. Departmental recruitment efforts have historically been initiated based on an identified need, either because of an increase in workload requirements, in order to combat attrition, or to address hard to fill classification vacancies. This has established recruitment as a reactionary mechanism, impacting delivery goals while recruitment efforts are planned, developed, and executed. The Statewide Strategic Recruitment effort is designed as a proactive approach to outreach, with the goal of creating qualified

Draft SLAA Report

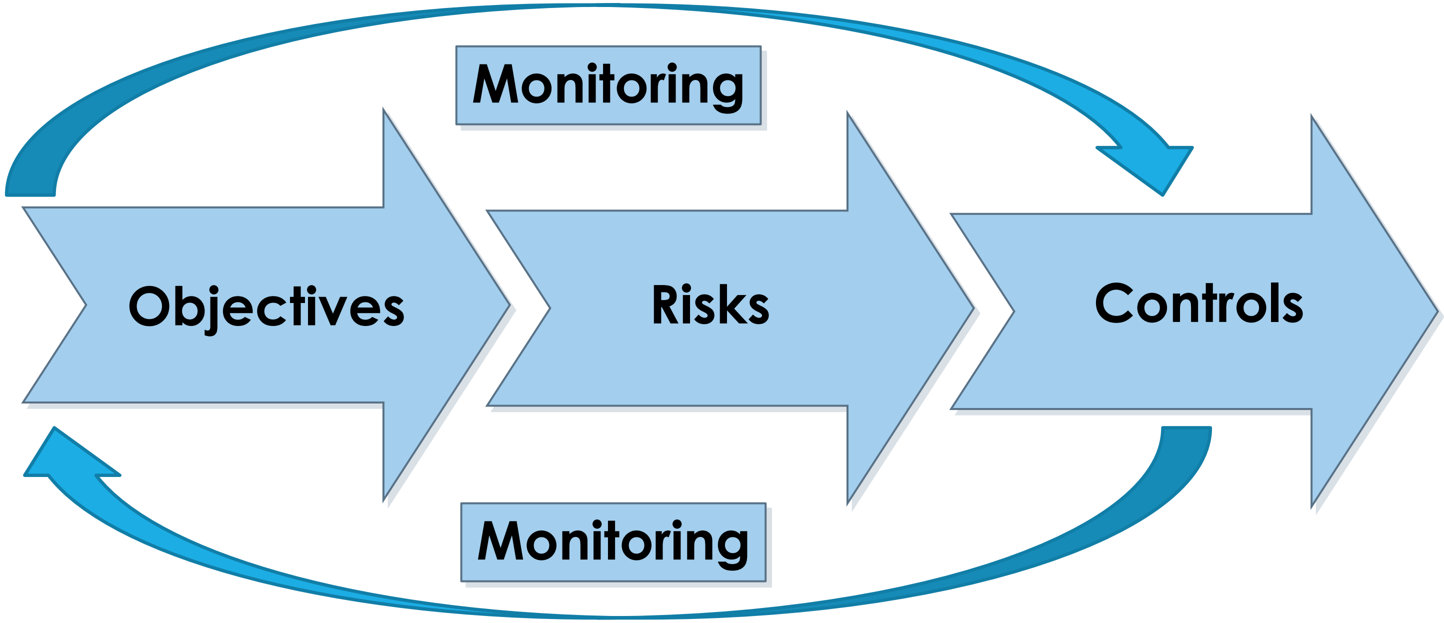


SELECT A REPORT OR PLAN: 2025-12-31 Report

Available actions - quick guide

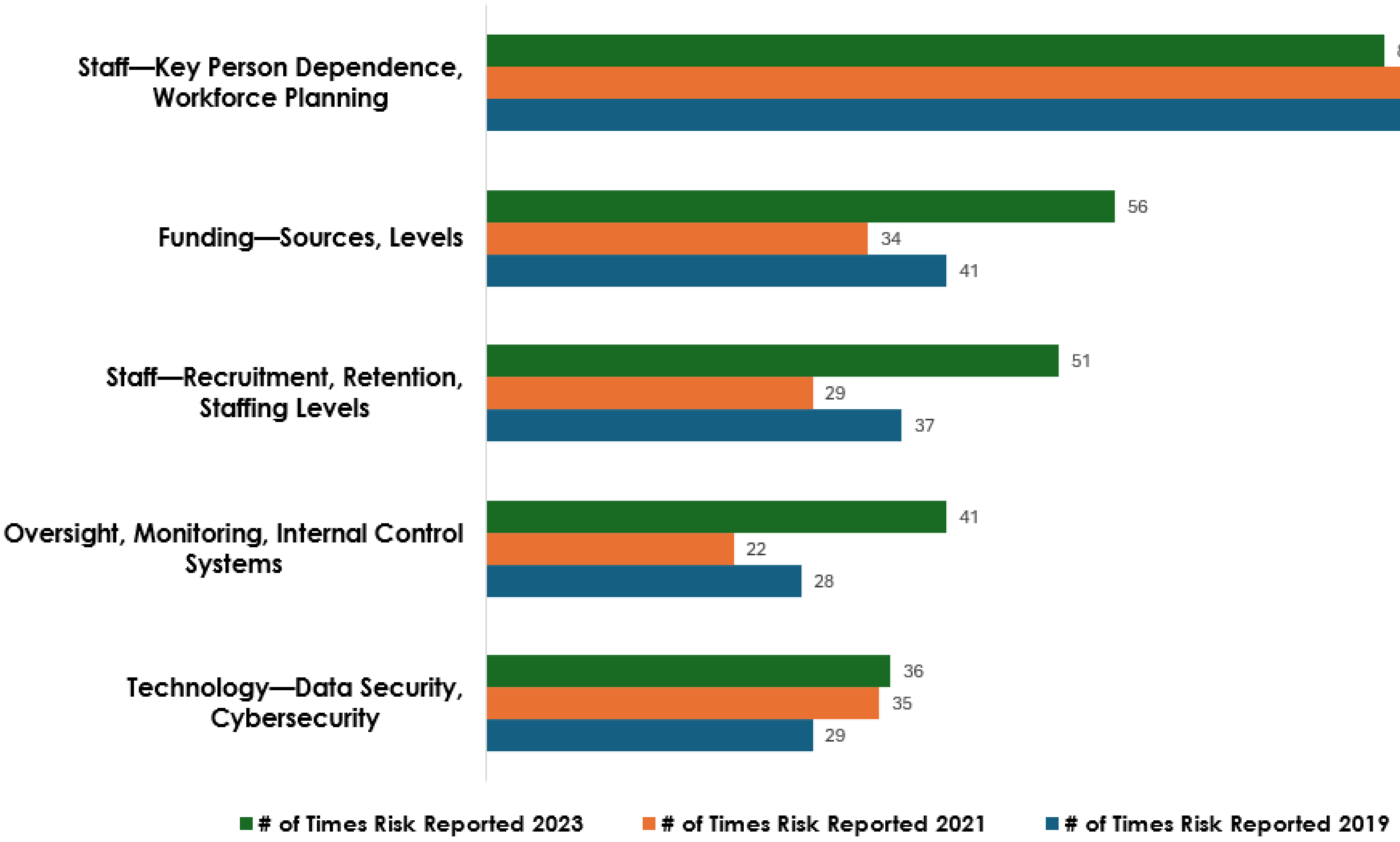
- View PDF version of the report.
- Review validation items and resolve issues.
- Submit the report once all validation issues are cleared.

Risk Management

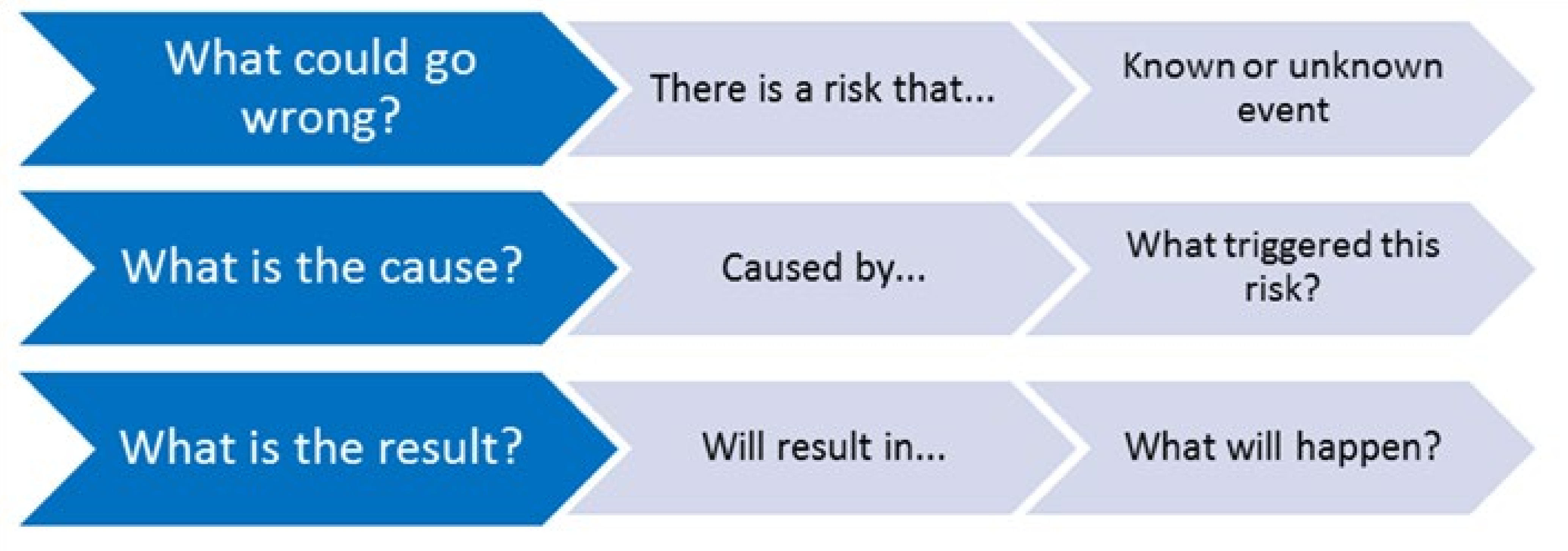


1. **Objective** – What are you aiming to accomplish?
2. **Risks** – What can stop you from achieving your goal?
3. **Controls** – What will you do to ensure success?
4. **Monitoring** – How do you know if it’s working?

Top 5 Statewide Risks 2019-2023



Risk Statement Elements



What could go wrong?	There is a risk that…	Known or unknown event
What is the cause?	Caused by…	What triggered this risk?
What is the result?	Will result in…	What will happen?

Risk Statement Examples

High employee turnover caused by high stress work environments can cause delays in completing objectives.

What could go wrong?

What is the cause?

What is the result?

Risk Statement Examples

Without proper employee training, staff can feel overwhelmed and ill-equipped to handle their workload, which can result in lower-quality work products.

What could go wrong?

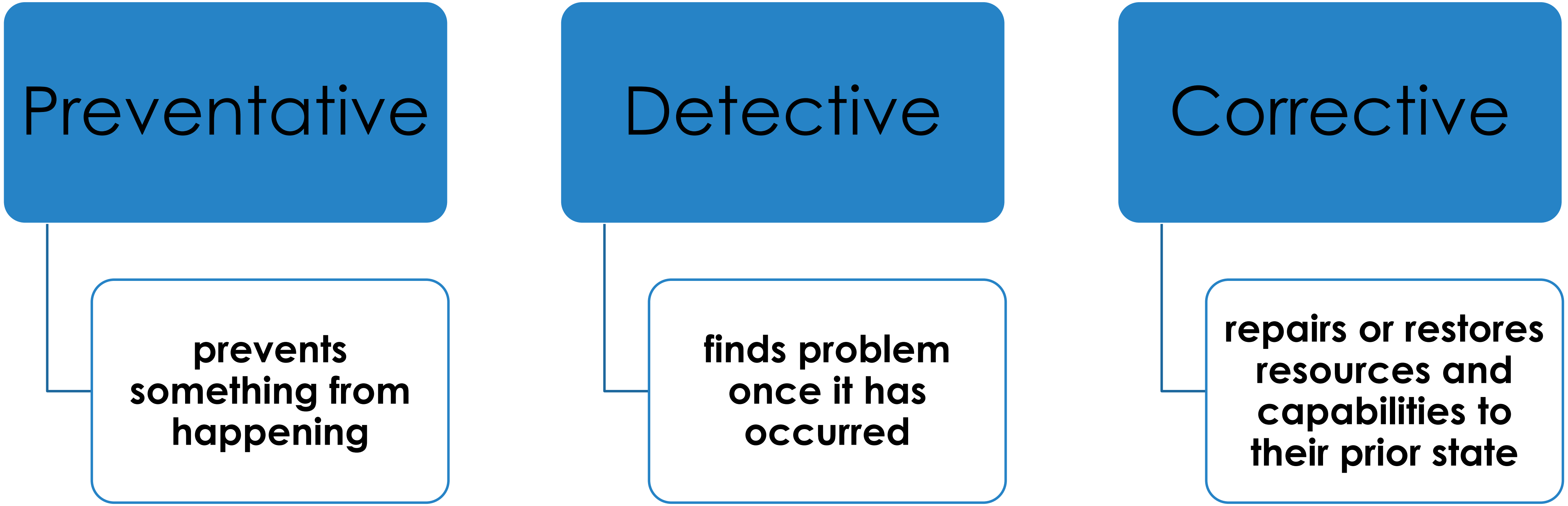
What is the cause?

What is the result?

Workforce Risk Example
Key Person Dependence

The agency has limited positions, personnel with training and expertise sufficient to provide backup for key positions, which leads to dependence upon key persons. The risk is that duties and tasks mandated or critical to completing the entity's mission may not be completed accurately or in a timely manner if key personnel are unavailable.

Types of Risk Responses



Preventative

prevents something from happening

Detective

finds problem once it has occurred

Corrective

repairs or restores resources and capabilities to their prior state

Risk Response Examples

- Standing agenda item
- Training
- Strategic & workforce plans
- Project scoring criteria
- Questionnaires
- Employee evaluations
- Grant application criteria
- Templates, checklist, route form
- Budget detail worksheets
- Documented policies, procedures, tasks, desk manual
- Meetings

Staff—Key Person Dependence, Workforce Planning, Recruitment, Retention, Staffing Levels

Controls:

- Use a focused recruitment and retention strategy to attract and keep qualified staff
- Advertising vacancies broadly
- Partner with CalHR to review classifications and pay

Staff—Key Person Dependence, Workforce Planning, Recruitment, Retention, Staffing Levels

Controls:

- Maintain a workforce and succession plan to identify key positions
- Capture institutional knowledge
- Prepare staff for future leadership through training and mentoring

Staff—Key Person Dependence, Workforce Planning, Recruitment, Retention, Staffing Levels

Controls:

- Identify a backup for all key personnel
- Document processes, procedures, and tasks
- Cross-train staff

Participant Poll

Risk Categories:

Key Person Dependence, Workforce Planning, Staffing Levels, Recruiting and Retention.

Question:

Will this be a risk in 2025?

Vote in the Chat:

Yes, No, or Not sure

Oversight, Monitoring, Internal Control Systems

Control:

- monitor operations to ensure compliance with internal controls and policies
- Staff perform reviews, asset checks, and compliance assessments

Participant Poll

Risk Categories:

Oversight, Monitoring, Internal Control Systems

Question:

Will this be a reported risk in 2025?

Vote in the Chat:

Yes, No, or Not sure

Cyber Risk Example

What could go wrong: privacy and security of the information assets and data subjects could be compromised

Caused by: cyber security incident

Results in: service delivery impacts

Cyber Risk Control Examples

- independent security assessments and information security program audits identify weaknesses to be addressed
- IT policies to protect information
- Personnel acknowledge IT policies & standards

Technology—Data Security, Cybersecurity

Control:

- Protect systems and data through a coordinated cybersecurity program led by the Information Security Officer
- Regular risk assessments, password and access controls, and multi-factor authentication help prevent unauthorized access
- Performs periodic audits and monitor for new threats to guard for safe and reliable systems

Technology—Data Security, Cybersecurity

Control:

- All employees complete annual cybersecurity and privacy training to stay aware of risks and best practices for protecting data
- Department provides reminders, phishing-awareness messages, and alerts about suspicious activity to promote safe habits

Cyber Risk Control Examples

- Conducts monthly phishing exercises
- Annual mandatory information security and privacy training.

Cyber Risk Control Examples

Information Security Incident and Event Response Plan and Technology Recovery Plan that describe requirements, expectations, roles, and responsibilities; define processes and procedures; and create channels for effective and timely communication.

Cyber Risk Control Examples

IT Strategic Plan: Establish measures and initiatives aimed at meeting information security goals and objectives and reducing information security risk across the organization.

Participant Poll

Risk Categories:

Technology, Data Security, Cyber Security

Question:

Will this be a reported risk in 2025?

Vote in the Chat:

Yes, No, or Not sure

Participant Poll

Questions:

1. Is your department having ‘Return to Office’ discussions?

2. Will your department need to lease more space?

3. Will ‘Return to Office’ efforts be a 2025 risk?

Leadership Accountability Tools and Resources

- ➢Department of Finance Public Website
  - State Leadership Accountability Act (SLAA)
  - SAM 20080 Frequently Asked Questions

- ➢SLAA Hotline SLAAHotline@dof.ca.gov

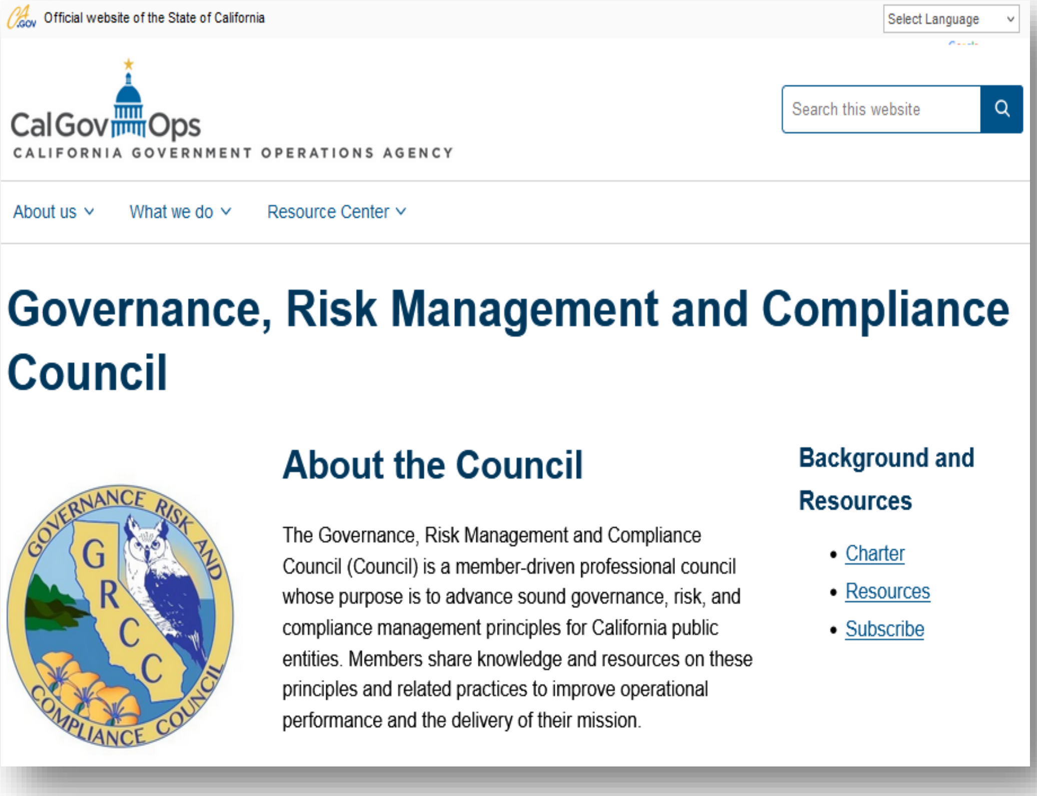
- ➢Free download, *Standards for Internal Control in the Federal Government (Green Book)* athttps://www.gao.gov/assets/gao-25-107721.pdf

What’s Next?

Anthony Martin, GRCC Advisor,
Department of Industrial Relations

GRCC Resources/Next Meeting

- GRCC on the GovOps Website
    - Subscribe to our ListServ
- Winter Newsletter/Survey
- Next Meeting – May 2026


Official website of the State of California
Select Language
CalGovOps
CALIFORNIA GOVERNMENT OPERATIONS AGENCY
Search this website
About us
What we do
Resource Center

Governance, Risk Management and Compliance Council

About the Council

The Governance, Risk Management and Compliance Council (Council) is a member-driven professional council whose purpose is to advance sound governance, risk, and compliance management principles for California public entities. Members share knowledge and resources on these principles and related practices to improve operational performance and the delivery of their mission.

Background and Resources

- Charter
- Resources
- Subscribe

Governance, Risk Management and Compliance Council | GovOps (ca.gov)