


RISK MANAGEMENT


Any student use of these slides is subject to the same License Agreement that governs the student's use of the SHRM Certification Prep System materials.


1


SRM
COSO



The Committee of Sponsoring Organizations of the Treadway Commission (COSO)


- Provide thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.




 American Accounting Association
Thought Leaders in Accounting

 American Institute of Certified Public Accountants


 Financial Executives International

 The Association of Accountants and Financial Professionals in Business

 The Institute of Internal Auditors

© SHRM 2026 2


2

SRM
Risk and Risk Management


Risk	<p>"The effect of uncertainty on objectives" (from ISO 31000)</p> <hr/> <p>Could take the form of threats or opportunities</p>
Risk management	<p>"Coordinated activities to direct and control an organization with regard to risk"</p> <hr/> <p>Change probabilities or magnitude of impact on objectives</p>

© SHRM 2026 3


3

SIRM Categories of Risk 

- Known unknowns and unknown unknowns
- Kaplan and Mikes's categories
 - Internal and preventable
 - Strategy
 - External
- Enterprise perspective:
 - Strategic
 - Operational
 - Financial
 - Hazard

© SHRM 2026 4


4

SIRM Benefits and Barriers 

Benefits of Risk Management	Barriers to Risk Management
<ul style="list-style-type: none"> ▪ Positive impact to customer satisfaction, reputation, and employee engagement. ▪ Financial risks can be more easily identified. ▪ Attractiveness to prospective employees and customers, including Certified B Corp status. ▪ Easier to remain in compliance. ▪ Antifragility 	<ul style="list-style-type: none"> ▪ Structural—silo organizational structures. ▪ Cognitive—lack of imagination and openness to change. ▪ Cultural—inadequate communication of the culture's risk approach.

© SHRM 2026 5

5

SIRM ISO 31000 

- 11 principles—for example:
 - Focused on value and continual improvement
 - Integrated into all processes and decision making
 - Transparency
 - Responsive to change
- Framework
 - Management commitment
 - Design
 - Implementing risk management
 - Periodic monitoring/review
 - Continual improvement

© SHRM 2026 6

6

SIRM ISO 31000

ISO International Organization for Standardization
When the world agrees

In London, in 1946, 65 delegates from 25 countries meet to discuss the future of International Standardization. In 1947, ISO officially comes into existence

26052 **175** **829**

International Standards and other deliverables covering almost all aspects of technology, management and manufacturing. Members representing ISO in their country. There is only one member per country. Technical committees and subcommittees to take care of standards development.

© SHRM 2026 7

7

SIRM ISO 31000

ISO International Organization for Standardization
When the world agrees

ISO standards are internationally agreed by experts
Think of them as a formula that describes the best way of doing something.

Quality management standards to help work more efficiently and reduce product failures.	Energy management standards to help cut energy consumption.
Environmental management standards to help reduce environmental impacts, reduce waste and be more sustainable.	Food safety standards to help prevent food from being contaminated.
Health and safety standards to help reduce accidents in the workplace.	IT security standards to help keep sensitive information secure.

© SHRM 2026 8

8

SIRM Risk Management Process

1 **Establish the context of risk.**
Define risk appetite and set risk management goals.

2 **Identify and analyze risks.**
Gather information in order to accurately evaluate and prioritize risk.

3 **Manage risks.**
Adopt and implement risk responses appropriate to each risk.

4 **Evaluate.**
Audit risk controls, review effectiveness, and monitor for changes in risks.

Communication and Consultation
Monitor and Review

© SHRM 2026 9

9

SIRM Risk Management

Step 1: Establish the context of risk.

- Establish the role risk plays in the organization, where it resides, and what the typical sources are.
- May use various tools, including SWOT, PESTLE, or others.
- Determine risk position, which is influenced by risk appetite or tolerance.

© SHRM 2026 10

10

SIRM Strength of Organization's Governance

© SHRM 2026 11

11

SIRM Loss Expectancy

Single Loss Expectancy = Asset Value X Exposure Factor (% of Value)

SLE \$66 = \$100 X .66
(if loss occurs, 2/3rds of the asset will be lost)

Annualized Loss Expectancy = SLE X Annual rate of occurrence (ARO)

ARO \$33 = \$66 X .5
(This loss is expected to occur once every 2 years)

© SHRM 2026 12

12

SIRM Common Misaligned Risks

Moral hazard
One party engages in risky behavior knowing that another party will incur any resulting loss.

Principal-agent problem
An agent makes decisions on behalf of a principal but has personal incentives not aligned with those of the principal.

Conflict of interest
A person or organization has the potential to be influenced by two opposing sets of incentives.

© SHRM 2026 13

13

SIRM Effectiveness of Current Risk Controls

- Risk controls are actions taken to manage a risk.
- Establish by asking first if there are controls in place for identified risk.
- Then ask if there is data showing that the controls are effective.

© SHRM 2026 14

14

SIRM Risk Management

Step 2: Identify and analyze risks.

<p>Methods:</p> <ul style="list-style-type: none">▪ Experts and information sources▪ Focus groups and interviews▪ Surveys▪ Process analysis▪ Direct observation	<p>Example: Duty of care</p> <p>Employer's responsibility to take all reasonable steps to ensure the health, safety, and well-being of employees and protect them from foreseeable injury</p>
--	--

© SHRM 2026 15

15

Risk Analysis Tools

Risk formula
 Risk level = Probability of occurrence × Magnitude of impact

Risk matrix

Risk scorecard

Event/Threat	A: Event Probability	B: Speed of Onset	C: Existing Mitigation	D: Severity of Impact	Threat Ranking Index
Water supply interruption exceeding 4 hours	1	3	3	2	18
Chemical spill	1	3	2	1	6

© SHRM 2026 16

16

Evaluating Risks

© SHRM 2026 17

17

Key Risk Indicators

Key risk indicators (KRIs): Early signals of increasing risk exposure; critical part of preparedness.

- Strategically aligned.
- Develop KRIs by identifying root causes of risks and intermediate events.
- Monitor for changes in KRIs.

© SHRM 2026 18

18

SIRM Increase/Decrease Effect

Upside Risk Management Tactics	Downside Risk Management Tactics
Enhance	Mitigate
Uncertainty: Supervisor impact on employee engagement	Uncertainty: Vulnerability of employees to workplace violence
Tactic: Include communications skills training in supervisory career path.	Tactic: Provide training in identifying and responding to early warning signs.
Increase the likelihood	Decrease the likelihood

© SHRM 2026 25

25

SIRM Take No Action

Upside Risk Management Tactics	Downside Risk Management Tactics
Ignore	Accept
Uncertainty: Performance relative to goals	Uncertainty: Vulnerability of workplace to acts of terrorism
Tactic: Take no further action to produce performance that exceeds goals.	Tactic: Identify as low risk and operate with existing emergency response protocols.
Residual risk: the amount of risk that remains after all management efforts have been exhausted	

© SHRM 2026 26

26

SIRM Risk Management

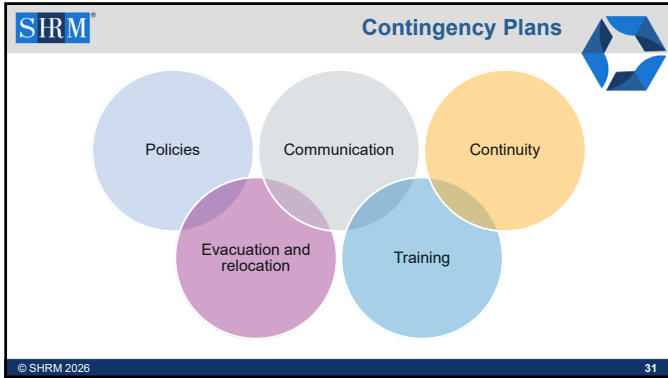
Step 3: Manage risk.

Implementing risk management plan

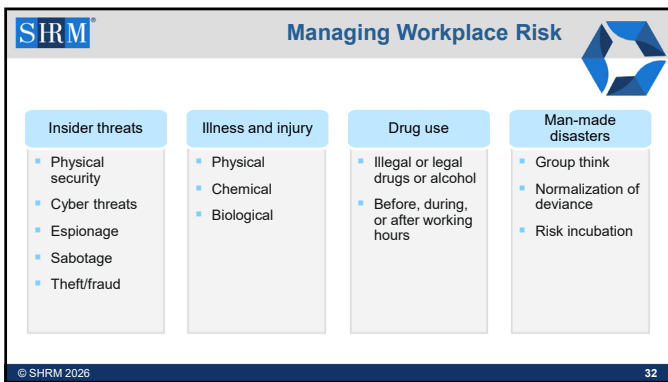
- Define objectives.
 - Be strategically focused.
 - Combine activities and results.
 - Combine lagging and leading metrics.
- Instill risk management principles in organization's members and processes.
- Integrate actions across organization.
- Communicate needs, expectations, and new policies and processes.
- Modify risks related to noncompliance.

© SHRM 2026 27

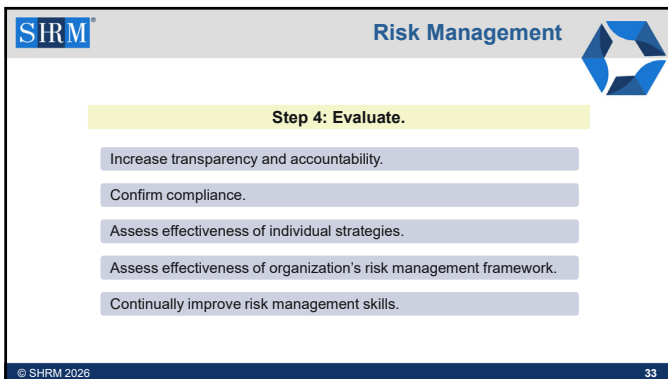
27




31



32



33


SIRM Risk Management 

- Conduct debriefs and incident investigations.
- Make sure process is in place that allows direct access to higher-level decision makers and protects whistleblowers from retaliation.
- Conduct audits.
 - Health and safety
 - Compliance
 - Process

“A crisis is a terrible thing to waste.”

© SHRM 2026 34

34

SIRM Quality Assurance and Continuous Improvement 

Quality assurance (QA)

- Helps to ensure that work is performed according to standards and that processes are used correctly and completely.
- Considers proactive, preventive, predictive, and preemptive actions.

Continuous improvement

- Equates to organizational approaches to improve and maintain the quality of risk management processes.

Risk management is not static; it is a continuous activity. Quality assurance and continuous improvement help an organization remain vigilant.

© SHRM 2026 35

35
