



Integrating internal control with Enterprise Risk Management (ERM)

What does internal control have to do with ERM?

The Office of Management and Budget (OMB) Circular A-123 requires that internal control activities be integrated under a larger ERM program. Integration of ERM with internal control helps agencies drive:

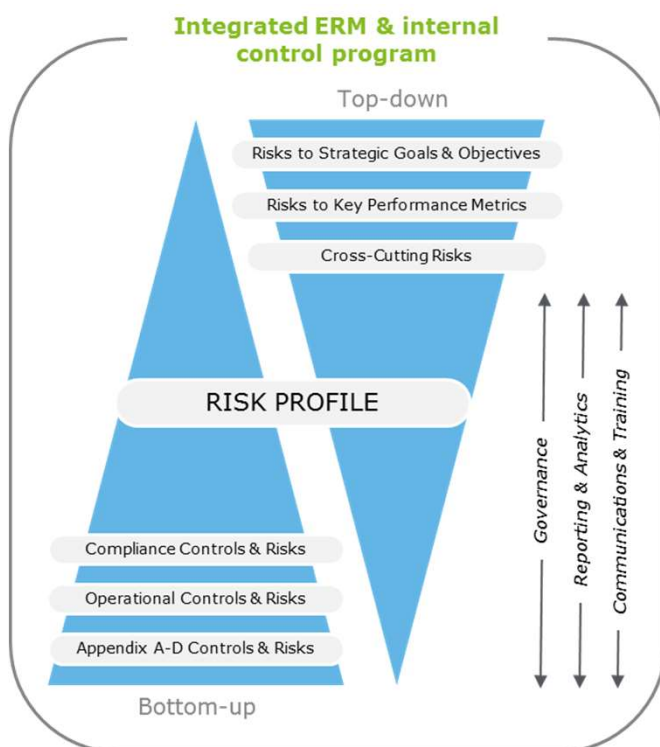
- **Chief Financial Officer (CFO) community collaboration:** Integration brings together the programmatic and operational community with the CFO and internal control community, which have historically been separate.
- **Enhanced risk response:** Internal controls are primarily a tool to manage risks (though control assessments can also help identify new risks). Aligning internal control with ERM helps harness internal control capabilities to create more effective risk responses.
- **Return on investment (ROI):** By leveraging the investments already in place for internal control and ERM functions, each community produces outputs—an assurance statement for internal control and a risk profile for ERM—that are more valuable because they build on each other's work.

The result? More impactful, targeted solutions to the risks affecting an agency's strategic, operations, compliance, and reporting objectives.

Points of integration

- 1 **Identify, assess, and prioritize risks**, using internal control data to measure risk likelihood and vulnerability
- 2 Develop risk **response** plans, including assessments on the effectiveness of controls and identification of gaps
- 3 **Monitor and report** on risk profile, aligning existing controls with risks and re-allocating resources as necessary

What does internal control and ERM integration look like for an agency?



An integrated ERM and internal control program provides awareness of an agency's full risk portfolio by aligning the top-down and bottom-up perspectives on risk:

- The ERM process provides a *top-down* approach to risk management and focuses on the *broader*, cross-cutting risks that affect the entire enterprise and should be front/center on leadership's agenda.
- Internal control provides a complementary *bottom-up* perspective based on in-depth assessment of an agency's business processes, its specific risks, and how those risks are being controlled.

Aligning the specific, transactional risk data from management's evaluation of internal control with the broader, enterprise-level risks from ERM creates a line of sight into what is causing an enterprise risk and where those causes should be mitigated. This also helps highlight existing gaps and where resources may be needed to reduce an agency's vulnerability.

Integrating internal control with ERM

Why integrate internal control and ERM?

Applying the rigor of internal control evaluation to enterprise risks can lead to better, evidence-based decisions and more targeted solutions that address the risks that affect an agency's mission.

Without integration, agencies may...	With integration, agencies can...
<ul style="list-style-type: none"> • Make risk response decisions that overlook the design and operating effectiveness of existing controls and their alignment to enterprise risks 	<ul style="list-style-type: none"> • Produce assurance statements giving leaders the confidence from knowing how effectively risks are being managed across the entire portfolio (top-down, bottom-up)
<ul style="list-style-type: none"> • Conduct separate ERM and internal control processes involving the same stakeholders and similar topics, resulting in duplication of effort and inefficient use of resources 	<ul style="list-style-type: none"> • Capitalize on internal control processes to produce better enterprise risk assessments and response plans while deploying internal control assets to the risks that matter most
<ul style="list-style-type: none"> • Operate internal control functions that focus on transactional, financial, and compliance-focused objectives instead of enterprise-level strategic and operational objectives 	<ul style="list-style-type: none"> • Identify risks to an agency's strategic plans and use internal controls to make strategic goals and objectives more resilient in the face of potential risk exposures
<ul style="list-style-type: none"> • Fail to consider internal control results when assessing enterprise risks, causing the wrong risks to be prioritized onto the risk profile 	<ul style="list-style-type: none"> • Respond to risks more proactively and in a more targeted manner based on results from testing the effectiveness of controls

What are OMB's integrated internal control and ERM requirements?

Internal control and ERM programs will continue to be responsible for their respective deliverables, but will now join forces to create the agency's integrated enterprise risk profile.



To find out more about integrating internal control and ERM, contact:

Alla Bishop
 Partner | Deloitte Risk and Financial Advisory
 Deloitte & Touche LLP
 + 571 814 7111 | aybishop@deloitte.com

Cynthia Vitters
 Managing Director | Deloitte Risk and Financial Advisory
 Deloitte & Touche LLP
 +571 858 0857 | cvitters@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.