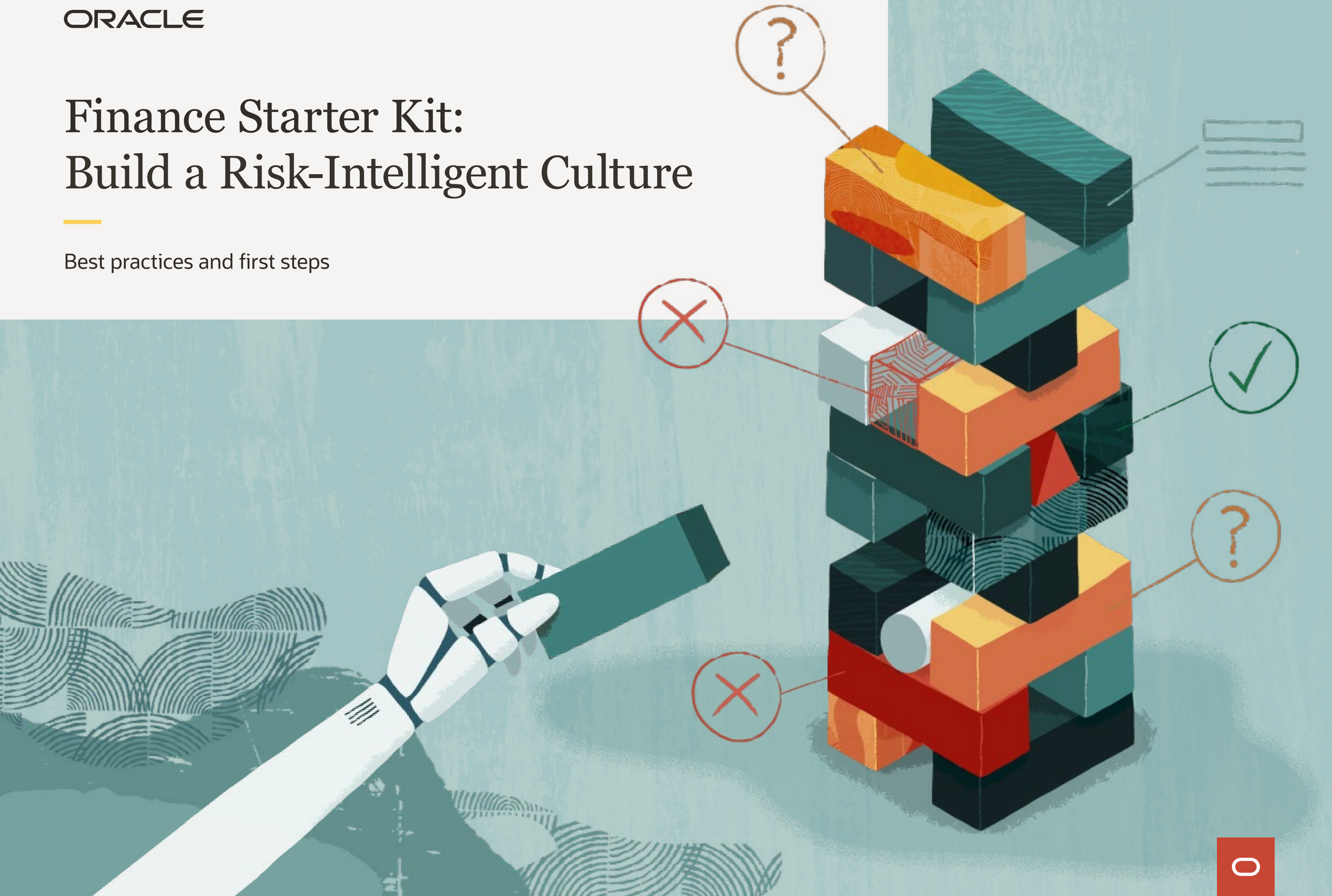
ORACLE

Finance Starter Kit: Build a Risk-Intelligent Culture

Best practices and first steps



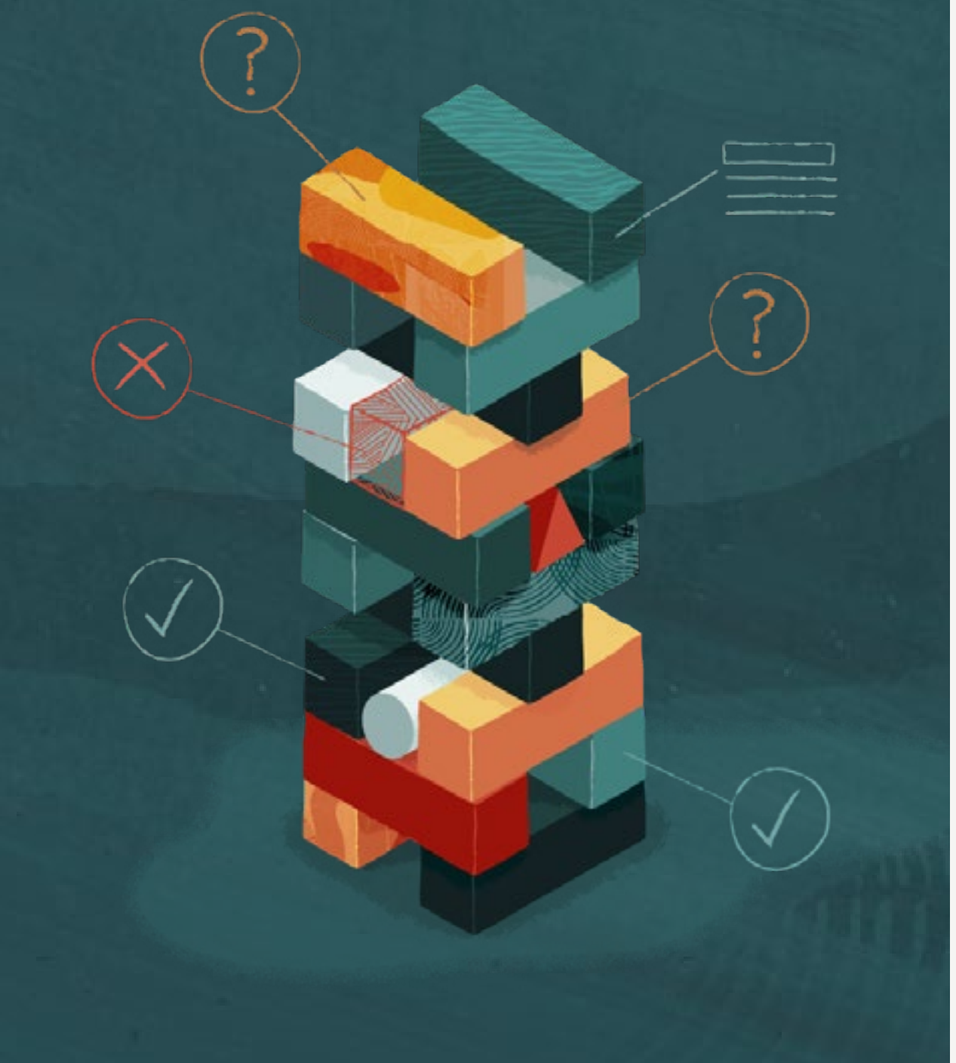
Build a risk-intelligent culture

Disruptions to your business, whether internal or external, are constantly challenging the efficacy of your risk management policies and functions. Organizations need to be agile and coordinated in their approach to security, risk, and compliance.

A scalable, centralized approach, connecting risk functions across your enterprise to your larger business, will ensure the best business outcomes. Security, risk, and compliance remain resilient throughout business changes and disruptions. You connect business results to business risks for better financial oversight, and increase the confidence needed to make timely, risk-based decisions.

A centralized risk management approach also supports collaboration and information sharing among control owners and governance teams, necessary for coordinated efforts and heightened awareness. Risk intelligence within your organization leads to stronger security, streamlined internal controls, better risk awareness, more efficient audits, and ultimately, better business outcomes.

Five best practices for risk management



1 Streamline and integrate your audit, compliance, enterprise risk management, and business continuity planning processes

Break down silos to boost the efficiency and effectiveness of security, audit, and risk management. Identify the critical areas of risk and exposure in your enterprise and the business process owners who play a role in risk detection and prevention. Shift finance and compliance resources to higher value-add activities by giving business process owners automated tools to perform risk management and internal controls activities, such as assessments. In addition, understand how automated collaboration and communication can drive coordinated action and response. This should be a strategic exercise that involves audit, security, and compliance stakeholders from across the business.

2 Use native integrated risk management to engage key stakeholders and business process owners

Integrated risk management (IRM) helps to promote a risk-intelligent culture by providing a single, comprehensive, enterprisewide view of risks within an organization. ***Native*** integrated risk management helps business process owners to automatically detect security issues when and where they originate, preventing delays that can be costly and disruptive. Having access to timely data is also crucial for a complete analysis of user access for the separation of duties and other controls. It enforces compliance and provides the collaboration necessary for risk-based decisions and quick response. Organizations can achieve significant strategic value by embedding risk management into business processes to promote a culture of risk-awareness.

Five best practices for risk management

3 Automate the analysis of application security for initial design, operation, certification, and evolution

Deep analysis, followed by automated monitoring of user access, periodic reviews or certification, lets you streamline internal controls to prevent Separation of Duties (SoD) violations and compliance issues. Being able to visually analyze and test roles during design or maintenance helps to minimize security weaknesses and audit findings. Automating the analysis of these processes eliminates off-line and vulnerable [spreadsheet-based or third-party] analyses. Ongoing, automated assessments and certifications, initiated when a change occurs in user role definitions, privileges, or responsibility levels, can significantly reduce the time and effort to identify issues for strong risk management and risk-based decisions.

4 Continuously monitor user activity to protect against fraud

Continuous monitoring of ERP processes (accounts payables, account receivables, general ledger) to analyze all data, including set-up data and transactions, reduces the incidence of fraud, error and policy violations, and cash leakage. Artificial intelligence is optimal for performing the fine-grain analysis necessary for risk detection and prevention.

Automated monitoring lets you eliminate time-consuming and error-prone manual data extraction (uncontrolled scripts and ad-hoc analysis), for more reliable transaction and configuration monitoring. Real-time prevention of unauthorized access to high-risk data and privileges is critical for strong risk management.

Five best practices for risk management

5 Grant external auditors self-service access to required data

Digitizing audit and compliance ensures your audit is more efficient and resilient, and protects against compliance and control failures due to changing regulations, staff, and operations. Your investment in automation of internal audit will enable you to adopt a virtual, self-service model for external auditors. Automation eliminates duplicate activities and reduces the need for requests for information and clarifications. Leverage a single source of data to ensure integrity and quality of audit. Reduce audit cycle times by enabling business process owners and auditors to work in parallel.

Steps to get started

The vast majority of organizations have considered, analyzed, and discussed transforming their risk management processes, but have struggled due to:

- Lack of executive sponsorship
- Spreadsheets and manual processes
- Disconnected, outdated tools
- Siloed risk functions and processes
- Manual controls/no automation

These steps are designed to help you avoid these pitfalls as you build the momentum necessary for transformation.

1. Get a quick win: start with a small to medium-sized project

Start with a well-defined financial compliance project to experience quick results and increase confidence in your strategy, as well as momentum in undertaking additional use cases. A financial compliance project lets you make a relatively low investment by leveraging your existing assets. This project will help you begin to identify the people and processes that play critical roles in strong risk management and risk-based decisions. You'll also begin to define the audit and collaborative aspects that will align to a larger risk management blueprint.

2. Leverage native risk automation capabilities for your most critical applications (ERP, SCM, HCM)

Start priming your organization by centralizing the risk repository and eliminating manual, spreadsheet-based, ad-hoc processes. Aggregate your processes for a well-integrated risk management approach to security, risk, and compliance. A centralized approach increases risk awareness and serves as a catalyst to promoting a risk-intelligent culture and collaboration. Insights into your risk metrics heighten awareness and provide for strengthened risk-based decisions and financial oversight.

3. Automate controls across your organization and processes to deliver timely analysis and insights

Assess risk management activities and controls within your organization to determine the automation needed for strong risk management and risk-based decisions. By engaging stakeholders at each level, you identify and better understand risks that can pose systemic threats. Continuous monitoring sets you up for ongoing protection against non-compliance and fraud.

Quick reminders

Do:

- Always take a risk-based approach to address your biggest risks first
- Centralize your risk repository for effective collaboration
- Prioritize native integrated risk management tools for control automation
- Engage and empower process owners to manage business risk

Don’t:

- Spread resources too thin on a poorly-defined scope—instead, focus on strategic value
- Start siloed efforts—instead, involve stakeholders early in the process
- Underestimate your risks—instead, adequately resource your risk management efforts

Looking forward

As leaders adopt best practices to ensure their security, risk, and compliance remain resilient throughout business changes and disruptions, they also set up the foundation necessary to connect risk functions across their enterprise for an end-to-end view. This enterprise view lets you connect business results to risks for more informed decision making. And, when you integrate risk management into your business processes, you achieve the agility and collaboration you need to respond quickly and efficiently. You increase risk-intelligence within your organization—and harness this intelligence to manage business risk proactively.

Visit our site to learn more about building a risk-intelligent culture and other big moves finance should make now, or take a quick product tour.

Visit site