plante moran | Audit. Tax. Consulting. Wealth Management.

Internal Controls Checklist

Protect your organization from risk. This quarterly checklist will help you stay on track with SOX compliance.

Q1 checklist	Internal controls
☐ Assess your organizational risk.	**Conduct an organizational risk assessment, and make updates to reflect changes in your risk profile and tolerance.** Your organizational risk profile may have changed since your last risk assessment. Are you focusing on the right processes and the most important controls? Avoid investing resources in "same-as-last-year" activities.
☐ Leverage the power of people.	**Identify internal control owners and champions.** Has anyone recently left the organization? Does everyone still understand requirements and responsibilities? Reinforce ownership and accountability through proactive discussions regarding the current year. Highlight the importance of maintaining strong internal controls, especially in times of change and uncertainty.
☐ Leverage the power of technology.	**Identify any new technologies that are used to manage your business.** In addition to changes in accounting software, procurement management, and transaction processing systems, other software platforms (both on- and off-premises) may have been utilized to manage recent organizational changes. Further, those systems may have been used in a contingency design environment.
☐ Focus on what is important.	**Identify in-scope processes and high-risk areas.** Prioritize key areas where controls will matter the most. Complete and accurate financial data in accordance with GAAP is crucial for contingent operations.
☐ Empower your staff through education.	**Educate control owners on minimum expectations, consistency, etc.** Internal control effectiveness and SOX requirements haven't changed, even when operating under a contingent operational framework. Confirm your control owners understand that control activities should remain present and effective.

Q2 checklist	Internal controls
☐ Address the basics.	**Document process and internal controls, and communicate them to others in your organization.** Be sure to consider differing levels of governance — specifically enterprise-level controls and IT system controls. Consider the governing process and transaction-level activities for those controls.
☐ Update your controls.	**Understand ineffective controls that were discovered in your risk assessment, and update or create controls as necessary.** Your risk assessment results may have revealed new risks or uncovered existing risks. Make sure you update existing controls or create new ones to address these issues.
☐ Widen the moat around your controls.	**Protect your organization by ensuring established controls cannot be overridden by management.** Management override of controls is one of the most dangerous risk factors that organizations face. The deliberate circumvention and established control activities not only exposes your organization to significant risk but it promotes bad control practices to your entire organization. Your controls were put in place for a reason, so management needs to uphold the established activities to promote a risk-conscious culture.
☐ Deploy agents of change.	**Identify temporary and permanent changes in your control environment resulting from changes to operating conditions.** Absent control owners, incomplete processes, and incomplete information that are necessary to perform controls are real risks that may prevent your organization from achieving your business objectives. Confirm the existence and effectiveness of compensating controls to address obvious internal control shortfalls.
☐ Check for bugs.	**Validate the consistent design of internal controls, identify deficiencies, and isolate the root cause of those deficiencies.** Ensure the design of your internal controls addresses all the identified risks. For any gaps or deficiencies identified, isolate the root cause and establish a management action plan to address the issue. **Deploy monitoring and evaluation techniques to assess where things may have gone wrong.** Not all control issues will be identified in a single design test. In order to fully assess the effectiveness of your internal control framework, your organization should execute an ongoing testing program to determine the overall operating effectiveness. **Assess IT systems and ensure those controls maintain a reliable IT environment that supports financial reporting requirements.** Your key IT systems aren't only critical to the operation of the business, but also critical to the success of your internal control framework. Performing testing procedures to determine the effectiveness of these systems can help identify potential causes for control deficiencies.

Q3 checklist	Internal controls
☐ Engage your team.	**Work with team members and subject-matter experts to develop meaningful, actionable risk management practices.** These should include updating review and approval procedures, configuration of system roles for better access restrictions, enhanced visibility, and control over key analyses and spreadsheets.
☐ Reinforce the structure.	**Remediate deficiencies identified as a result of recent monitoring activities.** Monitoring activities are designed to uncover deficiencies and gaps in your internal control framework. Are you taking action to remediate these deficiencies and strengthen your internal control framework? **Deploy risk management practices in a clear, deliberate fashion so your organization can work toward a common goal: better risk management.** A top-down and bottom-up approach ensures that information flows through all organizational departments in a clear and concise manner. Risk management processes should be evaluated and deliberately deployed to increase alignment with organizational objectives. **Apply updated control practices to ensure reliability of information coming from IT systems, as well as clearly documented procedures to validate the system output reliability.** You must take action to ensure the necessary information needed to execute an internal control is complete and accurate. Information produced by the entity (IPE) can only be reliable if general controls are effective over the IT systems utilized. **Identify and clearly note periods of time where internal controls may not have been effective. Note the starting period where newly implemented and corrected controls are in place, and ensure all involved have a clear understanding of the requirements to maintain effectiveness.** Have your internal controls been ineffective during a portion of the testing period? The SOX testing period must be adjusted to reflect the effective date of the control to ensure testing is performed on effective samples.
☐ Trust, but verify.	**Ensure that controls are designed to do what they are supposed to do and that they're functioning properly.** Internal controls may not have functioned as expected during certain periods throughout the year, even following efforts to problem-solve and implement improved internal control techniques.

Q4 checklist	Internal controls
☐ Plan for the year-end wrapup.	**Ensure disclosure controls and procedures are updated for material information related to market, credit, and liquidity risks.** Your organization may have experienced significant and unpredicted changes in the past. Management should ensure the appropriate effort has been directed at identifying, documenting, and disclosing these changes on periodic financial statements, subject to the appropriate level and precision of review. Factor in any discontinued operations, M&A activity, divestiture of business, renegotiation of debt or lease agreements, federal loans and relief, as well as any other significant and unusual transactions.
☐ Finish strong.	**Verify that all internal control activities have been assessed for effectiveness.** Are your internal controls functioning as intended? Testing the operational effectiveness of controls isn't a one-time event, but an ongoing process. Controls should be continuously tested to ensure they are operation consistently to prevent or detect errors or fraud that could result in a material misstatement. **Shift focus to controls that ensure financial information presentation and disclosure is complete, accurate, and fairly presented in accordance with U.S. GAAP.** You should have formal processes in place for financial reporting and disclosure development and review so that you can assess the effectiveness of controls related to these areas. Do you have documented requirements for reporting and disclosure, and are they updated frequently? Continuously evaluate critical reporting and disclosure processes to ensure the underlying controls are adequate to report complete and accurate information. The company's disclosure controls should be effective in addressing new developments as they arise. **If necessary, consult with subject-matter experts and advisors on the final application of business environment changes and how those should appear in financial reports.** Design a process to identify changes in your business environment that could impact the adequacy of controls and disclosures. Is there a designated protocol for monitoring and applying changes requiring evaluation such as new related party transactions, contingencies, mergers and acquisitions, system changes, laws and regulations, or personnel changes? Material events should be evaluated for alignment with existing controls and disclosures.

Are you confident in your internal controls and on track with SOX compliance requirements?

Consult us today for further guidance.