JCONNER™

ASSURANCE INSIGHTS

# Internal Control Self-Assessment

A practical framework for financial reporting, operational accountability and technology-dependent controls

**CONTROLS SHOULD REDUCE RISK IN THE WAY WORK IS ACTUALLY PERFORMED**

A useful self-assessment links objectives and risks to named control owners, evidence, frequency and follow-up. Policies alone are not evidence that a control operates.

GOVERNANCE | RISK | CONTROL ACTIVITIES | MONITORING

Includes a five-component control map, design-and-operation matrix, fillable assessment and 90-day remediation plan.

JCONNERPC.COM

CONTROL FRAMEWORK

# Assess the system, not isolated checklists

Internal control is an integrated process. Evaluate whether the organization sets expectations, identifies risk, designs controls, communicates reliable information and monitors whether controls continue to operate.

01

### Define objectives

State the reporting, operational and compliance outcomes the organization needs to achieve.

02

### Identify risk

Describe what could prevent the objective, including fraud, error, override, cyber and third-party risks.

03

### Evaluate control design

Determine whether the control, if performed as designed by a competent person, would prevent or detect the risk timely.

04

### Evaluate operation

Inspect evidence that the control occurred at the required frequency and that exceptions were resolved.

05

### Remediate and monitor

Assign owners, due dates, interim safeguards and follow-up testing for deficiencies.

**A review is not a control unless it is precise**

Document what the reviewer compares, the threshold for investigation, the evidence retained and how exceptions are resolved.

CONTROL ARCHITECTURE

# Translate the five components into operating evidence

The components are drawn from widely used internal-control frameworks; tailor principles and controls to the organization's objectives and risks.

| Component | Management question | Operating evidence | Warning sign |
|---|---|---|---|
| **Control environment** | Are accountability, competence, ethics and oversight expectations clear? | Org chart, role descriptions, policies, conflict process, board materials and performance actions. | Senior override is routine or responsibilities are unclear. |
| **Risk assessment** | Are objectives and material risks identified and updated for change? | Risk assessment, fraud discussion, change analysis and mitigation decisions. | Controls are copied forward without considering new systems or activities. |
| **Control activities** | Are preventive/detective controls designed at the right precision? | Approvals, reconciliations, access reviews, exception reports and evidence of follow-up. | Sign-offs show occurrence but not what was reviewed. |
| **Information / communication** | Does reliable information reach the right people in time? | Report definitions, data ownership, escalation paths and governance reporting. | Key reports are manually altered or source and completeness are unknown. |
| **Monitoring** | Does management identify and correct control failures? | Self-assessments, internal audit, issue logs, retesting and board oversight. | The same audit findings recur or remediation closes without evidence. |
| **Technology / third parties** | Are access, change, interface and outsourced-process risks addressed? | User access, change logs, backups, SOC reports and complementary controls. | Terminated users remain active or vendors are trusted without oversight. |

ASSESSMENT DISCIPLINE

# Design, implementation and operating effective

Use separate conclusions. A well-designed control may not be implemented, and an implemented control may not operate consistently.

### Design

Identify the objective, risk, control owner, frequency, evidence and precision. Determine whether the control could address the risk.

### Implementation

Confirm the control has been placed in operation and the owner understands how and when to perform it.

### Operating effectiveness

Inspect evidence across the relevant period and determine whether the control operated consistently and exceptions were resolved.

### Deficiency evaluation

Consider likelihood, magnitude, compensating controls, aggregation, duration and who relies on the affected process.

### Do not confuse policy with performance

A policy describes an expectation. The control is the specific action performed, evidenced, reviewed and followed up.

Framework references: COSO Internal Control - Integrated Framework; GAO Green Book.

HIGH-VALUE PROCESSES

# Financial close and technology-dependent contr

Focus first on processes where errors can become material, cash can be misappropriated or system access can undermine otherwise strong controls.

### Close and reporting

Evaluate account reconciliations, journal entries, estimates, consolidations, disclosures and final financial statement tie-out.

### Cash and purchasing

Assess bank access, disbursement approval, vendor changes, purchasing authority, receiving and reconciliations.

### Payroll

Assess employee setup, pay changes, time approval, payroll processing, tax filings, reconciliations and terminated-user access.

### IT dependencies

Identify key reports, interfaces, spreadsheets, user access, changes, backups and service organizations supporting financial controls.

### Spreadsheets can be key controls or key risks

Protect formulas, control inputs, identify versions, review hidden cells and links, retain source data and document management review.

The assessment should be scaled to the organization's objectives, complexity and risk.

FILLABLE READINESS CHECK

# Internal control design and operation check

Apply to each key process or control selected for self-assessment.

| | | |
|---|---|---|
| ☐ | The objective and specific financial, operational, compliance or fraud risk are documented. | **OWNER / TARGET DATE** |
| ☐ | A named owner has authority, competence and time to perform the control. | **OWNER / TARGET DATE** |
| ☐ | The control's frequency, threshold, evidence and exception process are defined. | **OWNER / TARGET DATE** |
| ☐ | Information used in the control is complete, accurate and retained. | **OWNER / TARGET DATE** |
| ☐ | Segregation of duties and management-override risk have been considered. | **OWNER / TARGET DATE** |
| ☐ | Evidence shows the control operated throughout the assessment period. | **OWNER / TARGET DATE** |
| ☐ | Exceptions were investigated, resolved and escalated when necessary. | **OWNER / TARGET DATE** |
| ☐ | Deficiencies have owners, due dates, interim safeguards and retesting plans. | **OWNER / TARGET DATE** |

Check an item only when the underlying support has been reviewed, not merely requested.

FILLABLE PLANNING MEMORANDUM

# Key control assessment

Complete one memorandum for each high-risk or key control.

### OBJECTIVE, PROCESS AND RISK ADDRESSED

### CONTROL DESCRIPTION, OWNER AND FREQUENCY

### INFORMATION USED AND COMPLETENESS/ACCURACY CONTROLS

### DESIGN AND IMPLEMENTATION CONCLUSION

### OPERATING EVIDENCE, EXCEPTIONS AND CONCLUSION

### DEFICIENCY, INTERIM SAFEGUARD AND REMEDIATION PLAN

**Completion standard**

Retain the evidence supporting each conclusion and document review of unresolved or judgmental items.

90-DAY ACTION PLAN

# Turn findings into an accountable plan

Use the action plan to move from observations to sustainable controls with clear evidence and ownership.

| Priority action | Owner | Due | Evidence / status |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

### Prioritization lens

Prioritize deficiencies that could permit material reporting error, fraud, unauthorized access, cash loss, regulatory failure or repeated audit findings.

AUTHORITATIVE FOUNDATION

# Sources and technical guidance

COSO and the GAO Green Book provide recognized frameworks for evaluating systems of internal control. Apply the framework appropriate to the organization.

### COSO Internal Control

Official COSO resources for the Internal Control - Integrated Framework.

www.coso.org/internal-control

### GAO Standards for Internal Control in the Federal Government

The 2025 Green Book, effective beginning with fiscal year 2026 and permitted for early implementation.

www.gao.gov/products/gao-25-107721

### AICPA Professional Standards - currently effective SASs

Risk assessment and understanding internal control in a financial statement audit are addressed in the current AU-C standards.

www.aicpa-cima.com/resources/download/aicpa-statements-on-auditing-standards-...

### Use of this publication

This guide provides general information, not a substitute for the applicable standards, laws, contracts, plan documents or professional judgment. Evaluate the complete facts and current requirements for each engagement.