



KEEP YOUR SOX CLEAN

Why Good Project Managers are a Gift to Senior Management

Victoria Nager, CPA, PMP, CISA
Principal: Good Business Services, LLC
E-mail: vnager@gbscpa.com
Phone: 908.883.0522

What is SOX 404? Why COSO?

Section 404 of the Sarbanes Oxley Act (SOX 404) is a provision that mandates the review and assessment of internal controls over financial reporting for publicly traded companies.

COSO is the accepted framework that is used to comply with SOX 404 requirements.



How do projects impact SOX 404?

SOX risk assessments typically assign higher risk to areas undergoing rapid or significant change.

Projects can affect these assessments because they may be:

- Part of the execution of corporate strategy
- As impactful or more impactful than day to day operations
- Setting the selection criteria for future choices or the direction of the company.
- Disruptive to existing processes and internal controls or fail to deliver on the strategic objectives
- Used to demonstrate the robustness of internal controls within an organization if managed properly

Corporate acquisitions, new plants or IT implementations and clinical studies are examples of projects that can be part of a strategic plan.

What is COSO-Integrated Framework (IF)

COSO is a framework adopted by many organizations to evaluate Executive Management and Board of Directors based on a framework that provides reasonable assurance that corporate objectives will be obtained in areas that include:

- Operations - efficient and effective use of resources
- Reporting - relevant and accurate reporting
- Compliance - comply with relevant laws and regulations

There are quite a few similarities between COSO principles and PMBOK Project Management Process Groups and Knowledge Areas

COSO CATEGORIES

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

Seventeen principles are segregated into these 5 categories

PMBOK PROCESS GROUPS

- Planning
- Executing
- Monitoring & Controlling
- Closing
- Initiating

Nine knowledge areas cross these process groups

COSO – Control Environment

- Management establishes structures, reporting lines and defines roles and responsibilities that support corporate objective. The Board provides oversight of senior management on the assignment of accountability and monitoring of performance of accountable parties.

PMBOK – Planning & Initiating

- The initiating and planning process groups are process groups where roles and responsibilities are defined and objectives are set.

Tools

- Project charter
- Project plan
- Team, stakeholder and steering committee lists
- Sponsorship
- Inputs from experts, stakeholders and sponsors

COSO – Control Environment

- There is a commitment to attract and retain competent individuals with skills that are appropriate to corporate objectives.

PMBOK – Human Resource Mgt. & Planning

- Determining the skill sets, level of resourcing, facilities, and project team structure is critical to the achievement of project objectives.

Tools

- Project plan/Work breakdown structure
- Resource calendar/plan
- Department resource calendar
- Statement of work (SOW)/Contracts
- Resumes or qualification evaluations

COSO – Control Environment

- Individuals are held accountable for performance of their responsibilities in pursuit of corporate objectives through actions that are consistent with alignment to good internal controls.

PMBOK – All Process Groups and Knowledge Areas

A good project manager:

- Identifies responsibility owners
- Monitors task and deliverable quality and execution
- Holds responsibility owners accountable
- Reports performance across the project team and project stakeholders

Tools

- Onboarding/Off-boarding tracker
- Team, stakeholder and steering distribution lists
- Timely team, stakeholder & steering committee reports
- Timely project communications
- Issue/Risk logs
- Quality monitoring tools and personnel

COSO – Risk Assessment

- Objectives are defined in a way that allows the assessment and identification of objectives related risk.

PMBOK – Initiating & Planning

- Developing a project charter provides high level objectives that are then refined through the requirements gathering and project planning process.

Tools

- Project charter with scope, high level project plan/milestones, budget and sponsor input
- Requirements documents
- Functional design documents
- Technical design documents
- Project team input

COSO – Risk Assessment

- Risk mitigation strategies are identified for each risk related to the accomplishment of identified objectives.

PMBOK – Risk Management

- Project changes can be very visible to stakeholders. Project managers who assess, plan and align responses to risks can enhance stakeholder assessment of their performance.

Tools

- SOW/Contracts
- Expert opinions
- Quality monitoring personnel/tools
- Roll back/contingency plans
- Team contact list
- Impact/Risk analysis
- Budget

COSO – Risk Assessment

- The potential for fraud as it relates to the achievement of corporate objectives is assessed.

PMBOK – Procurement Mgt. and Monitoring / Controlling

- Key areas of fraud occur in the areas of procurement and control of schedule, quality and cost.

Tools

- Project plan with stage gates/deliverables
- Quality monitoring tools
- Change order/Project change approvals
- Onboarding/Off-boarding tracker
- P.O. approval, tracking and closure
- Invoice review
- Accounting classification review
- Budget
- Project closure
- Defined SOW/Contracts
- Inventory control

COSO – Risk Assessment

- Management identifies and understands the impact of changes that impact internal control activities and systems.

PMBOK – Initiate, Plan & Close

- The project charter and plan should include an impact assessment of the project on current activities and systems.
- Project close is the handoff that happens as the project moves into the next stage of it's lifecycle. Open items (e.g. continued training, close open P.O.s) can be handled here.

Tools

- Project charter
- Project plan
- Sponsor authorizations
- Change management plan
- Stakeholder/Market/Organization impact assessment input
- Budget
- Purchase requisition/order tracking and closure

COSO – Control Activities

- Control activities are designed to mitigate the risks of achieving objectives to a reasonable level.

PMBOK – Monitoring & Controlling

“Monitoring and controlling project work is the process of tracking, reviewing and regulating the progress to meet the performance objectives defined in the project management plan.”

P61 PMBOK Fourth Edition

Tools

- Project plan
- SOWs/Contracts
- P.O. approval authority
- Invoice review and approval authority
- Quality monitoring personnel/tools
- Change management approvals
- Milestone/Deliverable/Stage gate approvals
- Clear sponsorship
- Status reporting/Tracking

COSO – Control Activities

- Controls over information technology activities are designed to support corporate objective achievement.

PMBOK – Monitoring & Controlling

- Increased focus on Cyber-Security by corporate boards make this an especially sensitive area that benefits from consistent application of integrated change control and monitoring of risks, schedule and cost.

Tools

- Onboarding and Off-boarding tracker
- Access management tracking
- Access management testing
- Quality control tools/testing/personnel

COSO – Information and Communication

- Sufficient internal communication is provided and received on objectives, risks, responsibilities and performance to support the successful achievement of objectives within the confines of good internal control.

PMBOK – Communications & Controlling

- A good project manager monitors delivery of vendors, internal resources and stakeholders against risks and reports performance to stakeholders and sponsors.

Tools

- Onboarding/Off-boarding tracker
- Team, Steering Committee and Stakeholder Lists
- Timely Progress & Steering Committee Reporting
- Issue/Risk logs
- Budget/Change request/Change order approvals
- Milestone/Deliverable approvals/Project plan

COSO – Information and Communication

- Communication with external parties is sufficient with providers on their responsibilities and expected performance to support the successful achievement of objectives within the confines of good internal control.

PMBOK – Procurement, Communications & Controlling

- A good project manager monitors delivery of vendor supplied goods and services and reports performance to suppliers, stakeholders and sponsors.

Tools

- Onboarding/Off-boarding Tracker
- Team, Stakeholder and Steering Committee Lists
- Periodic Progress and Steering Committee Reports
- Issue/Risk Logs
- SOWs/Contracts
- Change request/change order approvals
- Milestone/Deliverable approvals/Project plan
- Invoice approvals
- Purchase requisition and purchase order tracking/approvals

COSO – Monitoring Activities

- Ongoing assessments are performed in a timely fashion to determine if internal controls are operating effectively.

PMBOK – Monitoring and Controlling

- Quality assurance and Quality monitoring and team management activity reviews are key to determining if the project and related internal controls are operating effectively.

Tools

- Onboarding/Off-boarding Tracker
- Issue/Risk Logs
- Change request/change order approvals
- Milestone/Deliverable/Stage gate approvals/Project plan
- Quality assurance metrics
- Quality monitoring/testing
- Quality monitoring personnel

COSO – Monitoring Activities

- Internal control deficiencies are sufficiently communicated timely to parties responsible for the corrective action. This may include senior management and the board of directors. Corrective actions are assessed to determine if deficiencies have been remediated.

PMBOK – Controlling & Communication

- Reporting performance is key to maintaining the sponsorship necessary to ensure corrective action.
- Key stage gates and remediation plans can support successful execution of corrective action.

Tools

- Sponsorship
- Timely team, stakeholders and steering committee status reports
- Team, Stakeholder and Steering Committee List
- Remediation plan with accountable parties
- Milestone/Deliverable/Stage gate approvals
- SOWs/Contracts

Keep Your SOX Clean Secret Sauce Tools

Keep Your SOX Clean Secret Sauce Tools	
Access management tracking	Project charter
Accounting classification review	Project plan
Budget	Project closure
Change management plan	Project team input
Change management approvals	Quality assurance metrics
Project change approvals	Quality control personnel/tools
Change request/order approvals	Quality control testing
Clear sponsorship	Quality Monitoring Tools and Personnel
Defined SOW and contracts	Remediation plan with accountable parties
Department resource calendar	Requirements documents
Expert opinions	Resource plan/calendar
Functional design documents	Resumes or qualification evaluations
Impact/Risk analysis	Roll back/Contingency plans
Inventory control	Sponsor authorizations
invoice review and approval	Sponsorship
Issue/Risk Logs	Stakeholder/Market/Organization impact assessment/input
Milestone/Deliverable/Stage Gate approvals	Status reporting/tracking
Onboarding and Off-boarding tracker	Steering Committee List
P.O. approval authority	Stakeholder list
P.O. tracking and closure	Technical design documents
Steering Committee Reports (Report to project sponsor)	Well designed easily enforced SOWs / Contracts
Periodic Progress Reports	Work Breakdown Structure

References:

COSO 2013: Implementing the Framework, Institute of Internal Auditors, Altamonte Springs 2013

Project Management Body of Knowledge (PMBOK Guide) 4th Edition, Project Management Institute, Newton Square Pennsylvania 2008

Project Management Body of Knowledge (PMBOK Guide) 5th Edition, Project Management Institute, Newton Square Pennsylvania 2013



Contact Information:

Victoria Nager

Principal

Good Business Services, LLC

E-mail: vnager@gbscpa.com

Phone: 908.883.0522

