The Project Manager's Guide to Sarbanes-Oxley

November 2007

EXECUTIVE GUIDE SERIES

Tenron®

EMPOWER YOUR PROJECT WORKFORCE

Occupational fraud and abuse in 2006 will slice 6% (or $600 billion) off corporate revenues.

- A study by the Association of Certified Fraud Examiners (CFE)

Over 80% of fraud involves asset misappropriation — with cash, or its equivalents — being targeted 90% of the time. The average fraud scheme lasts about 18 months before it's detected and over half cost their victims at least $100,000; nearly one in six cause losses of $1 million or more. Those larger losses are often the work of mid- to upper-level management.

- CFE

Why Project Managers Need To Know About Sarbanes-Oxley

The number of project-based organizations/departments continues to increase, and newly formed Project Management Offices (PMOs) are introduced daily. Now, more than ever, Project Managers are forced to build stronger ties to the financial operations within any project-oriented business or department that must adhere to Sarbanes-Oxley and/or its equivalent in countries across the world.

The Sarbanes-Oxley law has made corporate governance a mandatory element of financial reporting, operational control and the daily running of a publicly traded company. Furthermore, institutional investors are creating significant pressure for privately held companies to comply with Sarbanes-Oxley.

After the corporate fraud and scandals of the last several years, shareholders and the government are demanding accountability from all companies and organizations. The Sarbanes-Oxley law states that CEOs must certify the financial reports of the organization. Public organizations that do not comply will face the wrath of their shareholders and creditors, as well as SEC (Security and Exchange Commission) investigations and severe penalties.

Regardless of the type of project, Project Managers and the Project Management office as a whole are responsible for a significant amount of the costs (in the case of internal projects), or revenues (in the case of revenue generating projects), that directly affect the overall financial performance of most organizations.

Forecasting cost and revenue on all projects or project portfolios, analyzing and measuring financial risk, maintaining real-time data about where a project is against budget, having traceability of the data, documenting and standardizing core processes and best practices within the PMO are all examples of how Project Managers help reinforce the decision making of their financial executives and help comply with Sections of Sarbanes-Oxley.

Non-formalized process, methodology, data capture, and reporting, can increase the risk of inaccurate forecasts, budgets, project status, project health and after the fact, untimely reporting. This provides far too much subjectivity in the financial analysis that an organization's CEO and CFO need to have on a monthly and quarterly basis. The penalties for non-compliance under Sarbanes–Oxley are severe and are in the back of the minds of all executives in today's business world.

Sections of Sarbanes-Oxley that Impact Project Managers

The following sections of Sarbanes-Oxley require specific internal changes for any organization that has to comply with this law and have a direct impact on the Project Management community within all organizations that fall under the compliance microscope:

Section 302 - Expanded Representation by Certifying Offices

Section 302 requires CEO and CFO sign-off on the company's quarterly financial reports. The key officers must assert that the company's financial report is accurate, that all material changes have been reported in a timely manner, and that the company has the appropriate internal controls to protect against any fraud or inaccuracy in its reporting.

Section 404 - Effectiveness of Internal Controls

Section 404 relates to the effectiveness of internal controls to intercept and detect any irregular, fraudulent, questionable or unauthorized corporate activity. This section mandates the company to file an annual Internal Control Report (ICR), as well as quarterly reviews and reports of any material changes in internal controls. The annual ICR must communicate:

- Management's responsibility to establish and maintain internal controls over financial reporting
- The criteria used to evaluate the effectiveness of internal controls
- Management's conclusion to the effectiveness of the established internal controls
- An auditor (a chartered public accountant) must attest to and report on management's evaluation

According to the SEC's threshold on internal controls, management is not permitted to conclude that its internal controls are effective if there are one or more material weaknesses. If the company's management asserts that internal controls are effective, then this is also an assertion that there are no material weaknesses in such controls.

© Tenrox, All rights reserved.

The SEC places the ultimate responsibility of financial reporting with the company's certifying officers. Consistent with the description of accounting control laws, certifying officers are responsible for ensuring that all corporate transactions are properly authorized and recorded; they are also responsible for the safeguarding of all company assets against unauthorized and improper use. The company must also comply with rules and regulations directly related to financial statements. However, Sarbanes-Oxley does not encompass effectiveness and efficiency of a company's operations or compliance with other regulations.

There is a significant overlap between internal controls for financial reporting and disclosure controls and procedures. The former are the focus of Section 404, while the latter are addressed in Section 302. Companies need to ensure Section 404 compliance and provide assurances, to certifying officers having to sign for Section 302 certification, that there are no internal control deficiencies. Any internal control that is a subset of disclosure control must also be evaluated on a quarterly basis and any material changes in those controls must be reported on a quarterly basis.

Section 409 - Rapid Reporting

Section 409 requires disclosure of material changes on a "rapid and current basis" (rapid reporting). Rapid reporting implies that the company's internal control systems can report on projects and operations in real-time. The company must be able to assess its current situation instantly and accurately.

Section 802 - Destruction, Alteration, or Falsification of Records

Section 802 links any knowingly falsified or altered documents to provisions of the criminal code. The company must establish strict audit records and a comprehensive document retention policy. A company's executives cannot simply say "documents were destroyed without our knowledge", this section and section 404 mandate the company's executives to ensure that the proper systems are in place to make sure that all documents are preserved in their original state and are protected against willful and malicious alterations.

It is important to note that in the context of the law, documents are not just contracts and agreements one signs with third parties. Examples of what is considered to be a document also include: all emails, project plans, timesheets, expense reports, budgets, invoices, charge backs, risk assessment memos, meeting minutes, scope definitions, project proposal and budget approvals, and project milestone sign-offs.

© Tenrox, All rights reserved.

Section 906 - Corporate Responsibility for Financial Reports

This section links representations made in conjunction with sections 302, 404,409 and 802 by certified signing officers to provisions of the criminal act. Section 906 outlines specific penalties, including imprisonment and multi-million dollar fines, against certifying officers for financial reports that do not comply with Sarbanes-Oxley.

How Project Managers Can Comply With Internal Control Regulations

Project Managers have two options for complying with effective internal controls. The first option is the traditional method of using manual processes to comply with a new law or methodology. The second option is to use the compliance requirement as an opportunity to automate business processes.

Manual Compliance Method. Traditionally, many companies comply with new regulations using the "polling method," as follows:

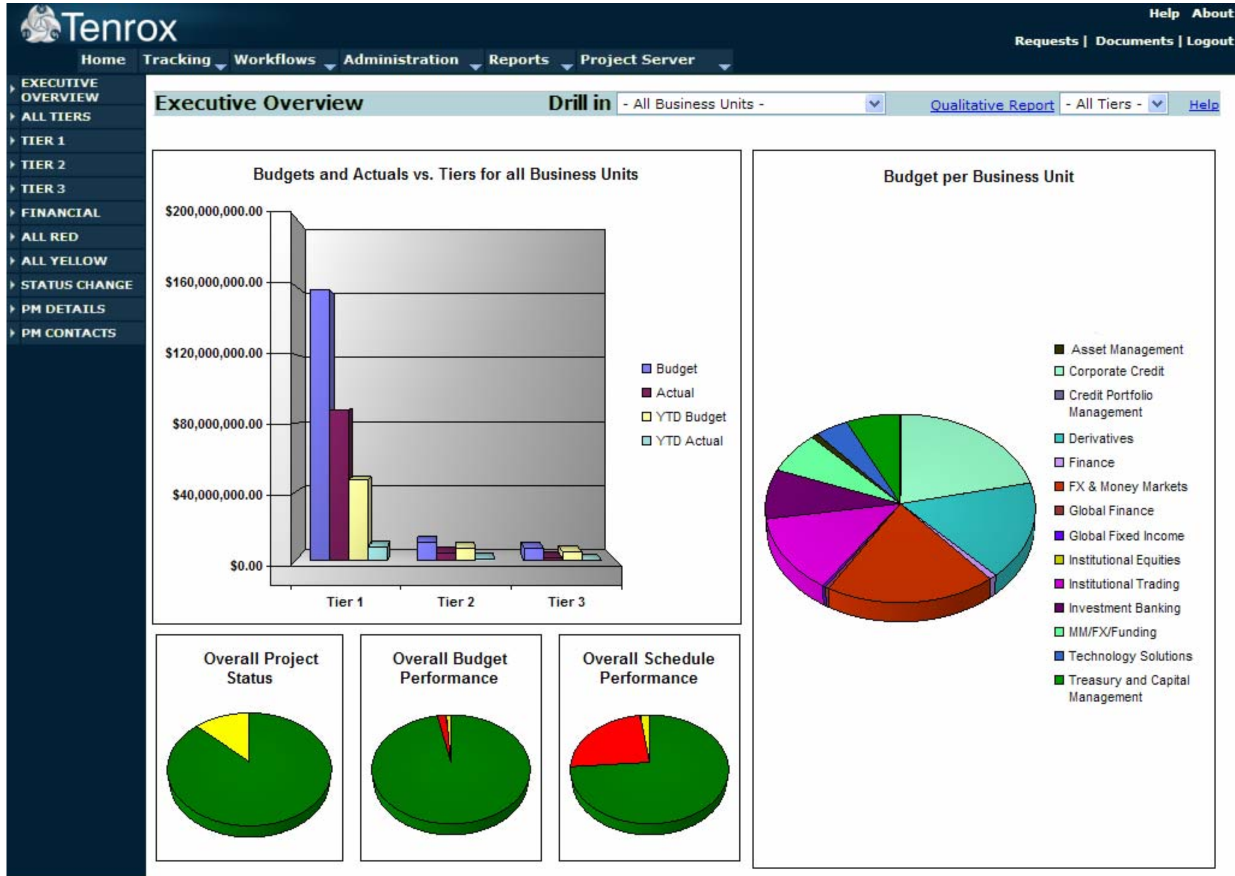
- Hire consultants
- Build spreadsheets, form driven initiatives
- Agree on paper-based sign-off process
- Schedule frequent meetings to evaluate and review compliance

This requires constant, almost daily and mechanical effort to establish and maintain compliance. The result is administrative overhead and associated high costs.

Comply & Optimize Method. A much more compelling alternative for compliance is the "real-time method." Companies can automate their business processes using enterprise software known as Project Workforce Management. Project Workforce Management software is integrated with the company's financial system and enables you to:

- Visually design and manage the company's business processes
- Validate and audit all transactions and system activity
- Design reports and executive dashboards to monitor operations and compliance
- Track approvals and digital sign-offs of the company's institutionalized processes

© Tenrox, All rights reserved.



With a PROJECT WORKFORCE MANAGEMENT solution, executives and managers have access to real-time, dynamic, and consolidated reports on their operations. It is a lot easier to analyze and navigate through live audited data on your projects and portfolios (collection of projects), than it is to manually consolidate multiple spreadsheet files to create static, un-audited, and unverifiable data.

PROJECT WORKFORCE MANAGEMENT Software

Project Workforce Management software facilitates compliance by providing:

- Cost accounting and interdepartmental charge back (for proper cost allocation)
- Scope management
- Project cost estimation
- Risk reporting and assessment
- Issue tracking

How can a company's officers certify the financial statements if internal controls are paper and/or spreadsheet based? Or, worse, the organization operates multiple disconnected enterprise software, where administrative staff is asked to manually re-key or manually import/export data between such systems.

© Tenrox, All rights reserved.

Simply, officers cannot and should not depend on such error prone and manual operational systems that can easily cause significant damage to the organization and to their own career. In worst-case scenarios, this type of weak corporate infrastructure may lead to mistakes, errors in judgment, and/or unreported criminal, fraudulent or unauthorized activity.

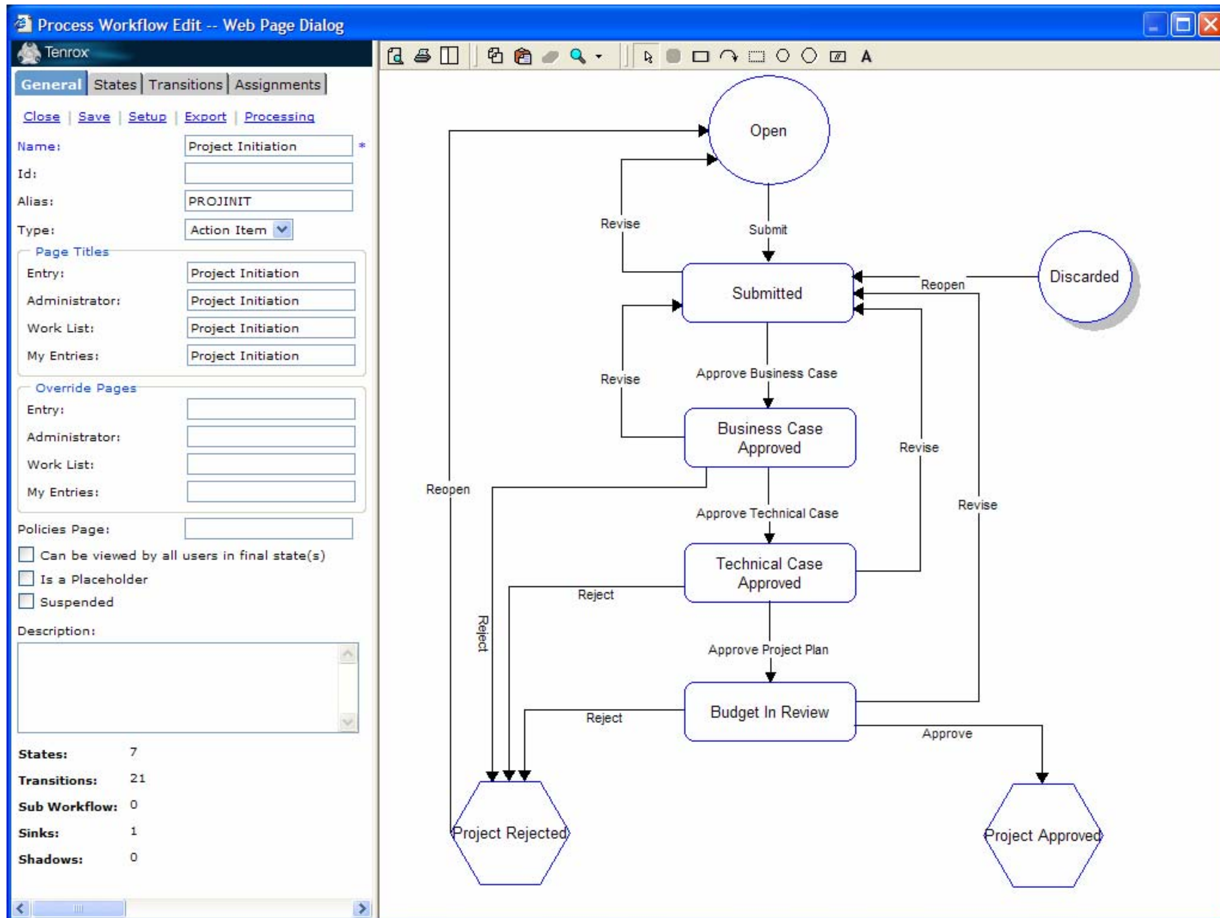
To be able to rapidly report on the company's financials and any material changes, your operational systems must provide real-time business information. This information must be collected in full compliance with all applicable regulations including Sarbanes-Oxley. Project Workforce Management is an integrated solution for operational control, compliance and governance that builds on your existing investments in enterprise software. Project Workforce Management automates operational processes and substantially facilitates compliance by providing executives with an audited and real-time view of their business.

Automating business processes is the key to establishing confidence in your organization. A process-managed enterprise:

- Has simultaneous and instant macro and micro views of its operations
- Can more rapidly correct mistakes
- Incorporates predefined, centralized, institutionalized and self-managed processes and procedures that automatically enforce compliance and governance
- Supports secure role-based and audited information systems
- Has substantially lower operating costs and administrative overhead

Project Workforce Management software enables executives to securely collaborate in real-time with all stakeholders including operational, project and financial managers, and to preemptively identify and manage any potential trouble spots.

© Tenrox, All rights reserved.



As the diagram above shows, Project Workforce Management allows one to visually design, manage, and track all operational processes. Business processes that are automated by Project Workforce Management include timesheet management, expense reporting, project initiation, scope control, issue tracking and incident management, billing, invoicing and interdepartmental charge backs.

Project Workforce Management software ensures that all work and spending is in compliance with Sarbanes-Oxley by providing:

- Executive dashboards and analysis reports provide a consolidated real-time view of the organization’s projects
- Visually designed and managed approval and routing of all work processes
- All user entries are validated at the point of entry; any exceptions are highlighted to facilitate quick detection of any potential issues
- Detailed reporting on all payable, billable, funded, and capitalized projects
- Visibility and transparency of all transactions; the system tracks approvals and changes of all projects, budgets, costs, charges, expenses and revenue
- Full audit trail and reporting of all system activity

© Tenrox, All rights reserved.

- Configurable pay and billing rules that validate timesheets, expense reports and invoices (charge backs), and requests at the point of entry
- Policy control and communication
- Automated approval and exception management of employee work, spending and travel
- Organization and work-based document management facility
- Role-based security and data access

Sarbanes-Oxley Law:	How Project Workforce Management Software Facilitates Compliance
Section 302 - Expanded Representation by Certifying Offices	▪ Audited, process-managed and effective internal controls allow the certifying officers to confidently sign the company's financial reports
Section 404 - Effectiveness of Internal Controls	▪ Centralized, tracked, audited, and institutionalized business processes ▪ Work processes are automatically validated for compliance at the point of entry ▪ Leads to verifiable data and effective internal controls that can be depended upon
Section 409 - Rapid Reporting	▪ Centralized and detailed work process information is used to report on and analyze the company's business in real-time ▪ The company is able to quickly report on its financial situation and any material changes on a quarterly or as-needed basis
Section 802 - Destruction, alteration, or falsification of records	▪ All system activity is audited ▪ Any document or transaction changes are recorded and can be reported on; documents to preserve and audit include invoices, timesheets, expense reports and project artifacts such as scope change requests and project risk assessments
Section 906 - Corporate Responsibility for Financial Reports	▪ Helps certifying officers report on the company's financials on a timely basis ▪ Detect questionable transactions and activities, protect company assets and avoid trouble with the law

© Tenrox, All rights reserved.

The Risks of Poor Governance: Three Case Studies

The risks of poor corporate governance have been laid bare in some very high profile fraud cases and corporate governance failures. Sarbanes-Oxley regulations, had they been in place, could have informed investors of impending disaster, helped detect and prevent the fraud in its initial phase, or at least provided investors with some warning signs.

Numerous fraudulent and illegal acts were committed at Enron, WorldCom and Arthur Anderson. The sections below highlight only portions of the criminal activity that pertain to effective internal controls, for the purpose of illustrating the impact of the new law on a company's operations.

Enron

No rapid reporting of material changes: Off balance sheet accounting (violation of section 409): Enron, for a very long time and as a standard business practice, routinely made investments in projects and businesses that had nothing to do with its core business. Many of these investments had implied liability and carried a substantial investment risk. However, Enron's financial statements and public filings did not reveal to its investors the extent of these liabilities and their potential impact on the company's financials and core business. This is a violation of section 409 on Rapid Reporting, which states that a business must report any material changes on a rapid and current basis. The unraveling of those investments and the related liabilities is what started the company's downward spiral.

Poor revenue recognition controls: (violation of section 404): On Feb. 20, 2001, Enron announced that it had entered into a $1.3 billion, 15-year contract with Eli Lilly, the Indianapolis-based pharmaceutical company. Enron was to manage the supply of electricity and natural gas for Lilly facilities in Indiana, as well as perform operations and maintenance on energy assets and related energy infrastructure upgrades that would increase energy efficiency at Lilly facilities. The problem with the deal, however, was that Indiana had not yet deregulated its wholesale electricity market. Enron, therefore, could not yet provide Lilly with electricity. Enron, however, chose to forecast how much it would earn during the projected 10 years of the contract and valued the deal at around $600 million over a 10-year period. The company then began to recognize $60 million each year as realized revenue. Fraudulent and intentionally deceitful revenue recognition policy is, of course, a violation of effective controls (section 404).

© Tenrox, All rights reserved.

WorldCom

Incorrect accounting of expenses and project types: (violation of section 404): In WorldCom's case, the company's revenue from its core business was starting to deteriorate due to competitive pricing pressures and the company's poor performance. To show continued profits, the company's management decided to reclassify certain projects. For example, WorldCom was spending millions every quarter to maintain its telecommunications network. Cost of such maintenance projects should be classified as an operating expense and reported as such in the company's income statement. WorldCom's management team decided to compensate its profit shortfalls every quarter by reclassifying some of these maintenance projects and capitalizing them. The cost of a capitalized appeared as an asset on the company's balance sheet, and only a fraction of the cost appeared as an amortized expense (depreciation) in the company's income statement. As a result, the company was able to substantially improve its profit picture.

WorldCom was engaged in fraudulent project accounting, expense reporting, and asset identification, and lacked audited and verifiable interdepartmental charge back controls; a violation of section 404, effective internal controls. Furthermore, the company was not reporting on its deteriorating profit picture (violation of section 409, rapid reporting), a material change in its business prospects.

Arthur Anderson

Arthur Anderson auditors committed several blatantly fraudulent acts. However, what led to their ultimate downfall and the reason the United States government decided to shutdown the company was the company's management team's intentional destruction of audit documents, emails and memos related to the Enron file; a violation of section 802, **destroying, altering and/or falsifying documents**. Proper computer systems, document retention policies and safeguarding procedures at Arthur Anderson would have prevented or at least detected the intentional destruction of documents that could have been used as evidence of fraud at Enron.

Furthermore, Arthur Anderson, as the auditor of Enron, did not comment on that company's poor internal controls, the abuse of Enron's assets, lack of transparent transactions and the fraudulent activity it had been a witness to. This is, of course, a violation of section 404, where the company's auditor must attest to the effective internal controls of the company being audited.

© Tenrox, All rights reserved.

How Poor Governance Happens: Look For These Weaknesses

▪ The average project exceeds its planned budget by 90% and its schedule by 120%.

▪ Only 16.2% of projects will be completed on time and on budget.

- Standish Group Survey of 8,000 software projects

Operational executives (such as the CTO, CIO, COO and the director of PMO) and Project Managers need to know about the potential threats that can cause poor governance. These executives must evaluate whether their company is suffering from these material weaknesses.

To better understand how you can ensure that your projects are governed and compliant — and for a more detailed explanation of these threats — please ask a Tenrox representative for a copy of the "Executive Guide to Project Governance and Compliance".

"Executive Guide to Project Governance and Compliance" explores the symptoms, cause and solution for the following project and portfolio threats. The guide discusses what steps executives and Project Managers need to take to effectively address these threats.

- Financial threat: ineffective budget, cost and revenue tracking, and lack of charge backs and cost allocations to business units
- Process threat: loosely defined inconsistent business processes for project control
- Governance threat: material weaknesses of internal controls that results in internal or external governance audit failure
- Compliance threat: violation of various industry and government regulations such as employment wage laws, fair labor laws, and generally accepted accounting principles (GAAP)

© Tenrox, All rights reserved.

Summary

Sarbanes-Oxley is a law that affects more than the company's CFO and CEO. The company's CIO, operational executives and Project Managers also directly share the responsibility. The company is mandated to have effective internal controls, which imply:

- Accurate and verifiable financial reports
- Transparent, audited and authorized transactions
- Ensure safeguarding and proper use of all corporate assets
- Timely reporting of any material changes

Compliance is possible without automation; however, companies can use Sarbanes-Oxley as a driving force to change for the better. Companies can achieve compliance and at the same time optimize their operations using Project Workforce Management software.

Leverage this compliance initiative to also reduce costs and administrative overhead, improve project delivery, and enhance the confidence of all stakeholders including your investors, employees and customers. Implementing software does not guarantee compliance but it helps you comply faster and reduces costs. Automation also leads to more predictable revenue, increased visibility and transparency, projects that are delivered on time, lower operational costs and far less administrative overhead.

There are many governance matters that were not covered in this paper such as:

- Document management, access rights, document recovery
- Document retention policy (including emails and other forms communication)
- Processes and procedures to facilitate reporting of fraudulent activity

Document management and putting in place a process that facilitates reporting of any potential governance-related problems are important aspects of compliance. The reader is encouraged to seek out more information on this matter.

Tenrox offers unique software designed to address the business challenges of streamlining operations, effective internal controls, rapid reporting and compliance with regulations including the Sarbanes-Oxley Act. Please call us to discuss how we can help you meet Sarbanes-Oxley's requirements, achieve and maintain compliance, while leveraging your existing enterprise software investments.

For more information, please call us directly at 1.877.4TENROX or visit: http://www.tenrox.com.

© Tenrox, All rights reserved.

Notes

© Tenrox, All rights reserved.

Tenron®

EMPOWER YOUR PROJECT WORKFORCE

www.tenrox.com