3GAMMAINSIGHTS

EMBEDDING COMPLIANCE

How to integrate Sarbanes-Oxley in your projects

Matt Williamson

3GAMMA
GREAT BUSINESS DESERVES GREAT IT

Failing to meet internal control requirements can be extremely costly – not only in direct financial terms, but also from a reputational perspective. In the UK the £1.53 billion fine recently handed to Barclays Bank, including a £284 million fine from the UK's Financial Conduct Authority for failure to control business practices, made headline news across the world.

September 2015

Internal controls are incredibly important to business operations but are often seen as something abstract and separate while they in fact should be part of business as usual and all ongoing development activities. Trying to resolve and remedy a lack of internal controls as a separate, post-event activity is not only risky – it's also expensive. Control and assurance must be based on the business risk, be in line with external rules and regulations and be built in from the start.

In the article "Risky Business!" published in May 2015, 3gamma outlined the effects of the cost associated with treating internal controls as discrete, separate activities. A key takeaway being that it's crucial to integrate the right level of internal control and risk assurance in all ongoing activities, both within the business and the IT organisation.

3gamma was recently engaged in a large, complex programme to streamline financial reporting within a large, multi-national manufacturing organisation. The first phase of this programme was targeted at financial simplification, reduction of complexity in financial processes and the streamlining of General Ledger codes and reporting charts. As a part of this engagement, 3gamma was responsible for ensuring the project had a financial controls plan, which included a plan to ensure compliance with a very specific financial control – the Sarbanes-Oxley Act. The approach taken was to operate the project in a controlled way, not to operate the project and then create evidence of control.

Based on these experiences, 3gamma has compiled a set of key recommendations on how to ensure compliance with Sarbanes-Oxley in a project setting. However, the approaches outlined in this article are not unique or limited to Sarbanes-Oxley, but can be adapted to other external and internal control frameworks as well.

Compliance: Having the right approach

Some might say that projects that fall under a regulatory audit require a large set of additional activities in order to "be compliant", as if having compliance requirements is an additional deliverable in itself. However, your project should already be managed in a controlled framework. In most cases the regulatory aspect is an application of good practice and sensible control. Any project that has a clear assessment of risk and a clear, structured approach to delivery, taking into account those risks, should only see the regulatory aspect as provision of available evidence – not as additional activities in themselves. Understanding the audit requirements and evidence presentation up front means you should be able to operate controls seamlessly, providing the auditors with access to the documents you have already created as part of your delivery. If you're creating one document as part of your project methodology and another to evidence compliance, consider how to merge the two to achieve both objectives.

The Sarbanes-Oxley Act: Ensuring correct financial reporting across companies

The Sarbanes-Oxley (SOX) Act was introduced in 2002 in the wake of several financial scandals. Previously, financial organisations were self-regulating but the Enron and WorldCom affairs in the early 2000s led to shareholder and general public scepticism in the ability of the financial industry to self-regulate, and US congress was forced to take action to improve accountability and clarity of financial practices. SOX compliance is mandatory for any organisation trading on the US stock exchange (defined as a public company) but many other organisations also adopt SOX processes as an internal measure of financial best-practice even if they are not legally required to do so.

SOX is primarily a financial governance and accountability regulation. Most of its clauses are aimed at providing clarity, preventing fraud and securing error avoidance in financial practices. However, since IT in the modern world supports corporate finance in such an integrated way it is not possible to isolate financial activities from their supporting IT systems. This is why IT controls within a SOX context are inevitable.

SOX is not limited to projects though; business as usual-SOX controls affect things such as IT change management, user access and data retention. However, due to the more invasive and revolutionary impact of IT projects, there are often more activities or controls to apply during a project phase. Consequently, project managers need to appraise themselves of SOX to keep business and IT projects on the right side of compliance.

A project's full impact on a company's financial processes must be understood

A project in isolation is not "SOX compliant", but following the guidelines below will ensure it doesn't put the organisation's compliance at risk.

Any organisation impacted by the SOX Act is obliged to be independently audited on a regular basis and the results are submitted to the financial regulator. Therefore most organisations will operate an internal policy to ensure they will be successful in such an audit. Depending on the size of the organisation and the number of SOX-impacted projects taking place, an organisation may choose to bring in an external company or a specific internal function, separate from the external auditors, to fulfil what is known as 2nd line assurance. This is a pre-audit designed to test the controls implemented at 1st line (the project). It points out any risks before the external auditors (3rd line) arrive. This 2nd line assurance is a helpful resource for any project manager.

When this is the case, this group will usually attend the project decision board and attest that the project has been delivered in a way that meets the requirements of a SOX audit. In some cases, the 2nd line assurance group may choose to 'operate' or test the controls, which means putting the evidence through the same rigor as an external audit. This can sometimes lead to rework, lessons or additional evidence provision. If the project has applied agreed controls and provided requisite evidence, it should pass easily through this stage.

Understanding the impact: Risk assessment

As a project manager, the first step is to understand whether the project is impacting a financial system or a financial process. Significant thought should be given to this since it's not always obvious if there will be an impact. For example, it's quite obvious that a SAP payroll project will have financial implications, but a new HR system could also have SOX implications since it interfaces with the financial systems. This is also true for a software upgrade if it's for an application that interfaces with financial systems. This impact assessment itself will actually form a key part of your SOX 'control'. One way of doing this is to complete an impact risk assessment or regulatory impact determination (RID) report. This could be a simple set of questions which determine whether your project has a regulatory impact. On the following page, an example is given for SOX.

SOX and financial controls impact

The purpose is to provide guidance to determine the system's impact on data and record integrity in the area of financial reporting.

Questions

No	Question	Check impact	
		Yes	No
1	Is the solution or system used to automate, calculate or approve financial transactions including requisitions, purchase orders, cash disbursement requests, cash collection, approvals of expenditures, invoice processing/ payment, or workflow routing?		
2	Does the solution or system control, record or monitor the acquisition or disposal of assets?		
3	Does the solution or system involve the entering of contracts?		
4	Does the solution or system control, record or monitor donations or other issues that impact taxes?		
5	Does the solution or system collect, maintain or manipulate information for financial close reporting?		
6	Does the solution or system affect sales reporting, including net sales?		
7	Does the solution or system affect cost of sales or inventory?		
8	Will the system or change impact the segregation of duties that are required to ensure prevention of fraud?		
9	Will the system or change affect an existing report/transaction or new report/transaction that is identified as part of a SOX key Control?		
10	Will the system or change impact the configuration of master data (e.g. customers, vendors, products, etc.) or affect the General Ledger?		
11	Will the system or change be evidenced and auditable by external sources (e.g. internal auditors, SOX auditors, external financial auditors)?		
12	Does the system or change interact with a previously identified SOX/FCF application?		

Conclusion:
Please document your result and rationale in the space provided.
Yes = SOX/FCF Impact
No = No SOX/FCF Impact

Result	Rationale
Yes/No	Does the system or change interact with a previously identified SOX/FCF application?

Control and transparency in the project is not enough – it must be supported by documented evidence

SOX is not in itself an activity or a set of tasks. If a project is being delivered in a controlled, transparent and methodical way, then most SOX requirements should be inherently met. The key word is evidence, and it's the collation and provision of this evidence that may require planning and tracking in your project plan. Setting up regular checkpoints to ensure you are building a portfolio of evidence is also wise, as waiting until the end is both a daunting and potentially risky strategy. SOX mandates that you run your project in a compliant way. Going back to create requisite documents after the event is not acceptable to an auditor. Most additional work, compared to a non-SOX project, stems from documenting and collecting evidence to prove that your project was delivered in a controlled manner against SOX principles.

A number of IT controls exist as part of SOX and their relevance depends on the size, type and impact of the project being delivered. These requisite controls should be identified and agreed at the start of the project. Once this identification stage is completed, it is critical to consider what evidence the project will provide so that every control area can be evidenced.

Break down control categories into general controls applied within the project

In a recent 3gamma client project, the following categories of SOX control objectives were considered based on the risk analysis:

- *Project methodology:* Demonstrate that the project has been delivered in a controlled manner using a defined methodology.
- *Impact assessment:* Demonstrate that the project has completed an impact assessment on all affected systems to ensure that any downstream systems are also assessed for SOX impact.
- *Testing:* Demonstrate that the project has been tested and that the testing was signed-off according to a recognised test plan.
- *Data migration:* Demonstrate that any financial data integrity is maintained and controlled through the project lifecycle including how access to financial data is enforced and what processes are in place to prevent unauthorised access or changes to financial data. This applies to production and non-production environments.
- *Implementation and go-live:* Demonstrate that the required and necessary approvals from both business and IT were in place prior to putting the project into the live environment. Also ensure that any business as usual-SOX controls (such as change management) were applied to any system identified as part of the impact assessment.

The above list of controls is not exhaustive but provides a sound basis for ensuring compliance. Controls need to be defined based on the company's audit policies, risk analysis and project value. For each control objective a set of controls must be identified.

The list on the next page provides examples with illustrative project actions. None of the these items should be additional tasks or activities if the project is run in a controlled way. However, structuring the project in such a way that evidence is captured consistently, and can be referenced easily, is critical. Spending time thinking about project governance in the context of evidence provision is time well spent, as it will also lead to a better, more traceable delivery of your project. Embedding this in the project setup and delivery will significantly reduce effort needed.

Control objective	Control	Project Action
1. Project methodology	**Key control 1.0:** The project plan is signed off by the project sponsor *This is a key control because the project must ensure that there is an individual who has overall accountability for the plan including the project's impact on the organisation's financial systems and data.*	Obtain sign-off at project governance gate 1. Ensure SharePoint is used as document repository.
	Key control 1.1: The project plan is governed by change control. *This is a key control because unless there is change management over the plan, it cannot be made clear who is accountable and how the financial data will be affected and when.*	SharePoint version tracking is switched on and the weekly programme board reviews the plan. Any changes are captured in the programme board minutes stored on SharePoint at [location].
	General control 1.0: The project plan is stored in an accessible repository (such as SharePoint) *This is a general control and best practice but not strictly governed by SOX.*	Setup clear SharePoint structure for document retention. Ensure that the project team is aware of the need to update version on SharePoint and avoid local versions.

SOX and external regulations can be a daunting prospect but preparation and integration of controls reduces overall effort

Managing SOX compliance can be a daunting prospect for a project manager, but it's a critical dependency for go-live and a key deliverable. Receiving a "no" decision on your project go-live because you cannot provide SOX assurance will be a critical issue in your project at exactly the wrong time.

In 3gamma's experience, when a company is required to remain Sarbanes-Oxley compliance, it is critical to approach SOX as early as possible in the project lifecycle. Every new project should be approached with a SOX perspective and perform the required impact assessment, since it's not always clear when and where SOX is applicable. If it's applicable, ensure that the project operates with a clear methodology and plan for evidence collection and retention upfront.

References

http://eradar.eu/why-is-sox-compliance-important-to-uk-business/
https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act
http://www.express.co.uk/finance/city/578648/Barclays-hit-with-1-53billion-rate-rigging-fine
http://www.3gamma.com/insight/creating-a-solid-foundation-through-cost-effective-risk-management/risky-business/

About the Author

Matt Williamson is a senior IT management consultant at 3gamma, with 14 years of experience from a wide variety of leadership roles in IT programme delivery and IT service management.

3GAMMA INSIGHTS

ABOUT 3GAMMA

3gamma is a leading professional services firm focusing on IT management. As an independent specialist in IT management, 3gamma provides advisory, consulting services and fact-based insights to many of the world's most respected companies. 3gamma operates globally from offices across the Nordics and UK. 3gamma is a knowledge firm that bases its expertise of six core capabilities:

- IT strategy and governance
- IT sourcing lifecycle
- IT legal advisory
- IT risk and assurance
- IT operational excellence
- IT project management and delivery

3gamma Insights brings leading-edge thinking at the intersection of IT and business, illuminating central topics relevant to CIOs and decision makers.

GROUP HEAD OFFICE
3gamma Sweden AB
Drottningtorget 5
SE-411 03 Göteborg
Sweden
Phone: +46 31 309 7910

DENMARK
3gamma ApS
Frederiksborggade 15
DK-1360 Copenhagen K
Phone: +45 53 700 400

UNITED KINGDOM
3gamma UK Ltd
River Court,
3 The Meadows Business Park
Station Approach, Blackwater
Surrey GU17 9ABL
United Kingdom
Phone +44 192 879 6800

STOCKHOLM
3gamma Sweden AB
Centralplan 15
SE-111 20 Stockholm
Sweden
Phone: +46 8 748 0330

MALMÖ
3gamma Sweden AB
WTC Teknikportalen
Skeppsgatan 19
SE-211 19 Malmö
Sweden
Phone : +46 40 627 04 05

UNITED KINGDOM
3gamma Ltd
Manchester Business Park
3000 Aviator Way
Manchester M22 5TG
Phone +44 192 879 6800

FINLAND
3gamma OY
Sentnerikuja 2
FI-00440 Helsinki
Phone +358 50 3 748 371

3GAMMA

GREAT BUSINESS DESERVES GREAT IT