Salesforce.Com: A Viable Platform for Achieving Sarbanes-Oxley Compliance in CRM Applications

Introduction

In the wake of corporate scandals that came to light earlier this decade, Congress passed the Sarbanes-Oxley Act (SOX) in 2002 as a measure to increase transparency and accountability in financial reporting to public company shareholders. At a high level, SOX dictates mandatory certification by corporate officers that the facts they report are accurate and that their companies have instituted strict internal controls to ensure accuracy and transparency.

SOX is a complex piece of legislation, containing 11 Titles, with multiple sections under each Title. The most controversial of these, and the focus of this paper, is Section 404 -- Management Assessment of Internal Control. This section relates to the effectiveness of the financials being reported, and to the processes and controls used to provide the information being reported. The complexity and ambiguity of this section has caused many sleepless nights for executives of public companies, which must comply with SOX. Unfortunately, the Act itself does not specify how to achieve SOX compliance.

SOX "compliance" is therefore a suspect term that has been overused since the passage of the Act. Complying with SOX depends wholly on a company's controls and procedures concerning accounting processes, not on what type of software it uses -- even if that solution claims SOX "compliance" as a feature. For example, the type of questions that are asked by an auditor concern:

- **"What controls and approval procedures are in place to ensure that the financial statements are accurate and there are no misrepresentations?"** and
- **"Is there a clear separation of duties in the lifecycle of an order entry?"**

At heart, SOX seeks to ensure public companies undertake the necessary checks and balances to ensure that financial reporting fraud will not proliferate. It is no defense for a company being audited under SOX to say, "We use software that is SOX compliant." There is no such thing as a "SOX-compliant" solution because, as noted, they are solely dependent on accounting controls and procedures. And accounting software solutions are only as good as the controls implemented and maintained by companies that use them.

Complying with SOX depends wholly on a company's controls and procedures concerning accounting processes, not on what type of software it uses.

There is much confusion and anxiety regarding which systems and platforms are the best choice for a public company to use to help achieve SOX compliance. Salesforce.com, a relatively new, Internet-based technology platform, has raised many questions relating to its ability to build SOX-compliant customer relationship management (CRM) applications.

To begin with, Salesforce.com is a hosted solution. Though the on-demand or Software as a Service (SaaS) software delivery model is becoming more prevalent due to its attractive value proposition, most large enterprises do not yet have much experience with it. These IT managers have legitimate concerns about placing their critical data off in the Internet cloud, out of their immediate control. Finally, since it is new, Salesforce.com's development platform is unfamiliar. So companies evaluating the platform are naturally hesitant to embrace new technologies without first understanding the implications of building SOX-compliant applications.

The objective of this white paper is to demonstrate that Salesforce.com is one platform that companies can use in conjunction with the necessary internal policies and controls to help achieve SOX compliance. But many of the principles discussed here apply to other CRM technology platforms, both on-demand and on-premises. Other CRM vendors, including Microsoft, SAP and Oracle have their approaches to enabling SOX compliance. As with Salesforce.com, these are only as good as the client's internal business processes and controls. The truth is that rigorous application of software development methodologies is required for SOX compliance, no matter which development software is used to build and deliver the application.

The Myth of SOX-in-a-Box

While there are some generally accepted practices and guidance for determining what is effective in promoting SOX compliance, there are no definitive black and whites.

In the Salesforce.com practice area at Cognizant, our enterprise clients often ask, "Is Salesforce.com Sarbanes-Oxley compliant?" In reality, as mentioned in the introduction above, no vendor's system is SOX compliant "out of the box."

Since any computing platform is simply a tool that reflects and manages key corporate processes, a better question would be: "What Salesforce.com features can help my organization quickly implement the controls mandated by SOX?"

While evaluating any software solution, the focus should be on how it can help increase the effectiveness of internal controls; reduce material misrepresentation of risk; increase transparency; and enforce the flow of transactions, ensuring auditability, improving record retention, and restricting unauthorized changes. Much as one might wish it, there is no "SOX-in-a-Box."

When Does SOX Apply?

When evaluating technology platforms that may serve as the foundation for achieving SOX compliance, it is helpful first to determine the types of enterprise data that are subject to SOX. Unfortunately, this is not necessarily a straightforward task. As with many other aspects of the often-murky law, determining whether or not a system is subject to SOX is subject to interpretation. As a general rule, systems that store, affect, and report on "financially significant" transactions are within the SOX purview. However, it is not always easy to determine whether a system affects "financially significant" applications.

In some cases, this is simple. At Cognizant's Salesforce.com practice, we have built many applications on the Salesforce.com platform that have little to do with financial transactions. For example, at a major insurance company we implemented a customer retention application whose sole purpose was to facilitate the organization of information related to enterprise workflow by proactively calling out at risk customers before their contracts expired. Clearly, this system did not need to comply with SOX mandates.

As with many other aspects of the often-murky law, determining whether or not a system is subject to SOX is subject to interpretation.

In fact, many Salesforce.com applications that are either custom built using the vendor's powerful development platform or installed via its Application Exchange environment are not subject to SOX compliance.

At the other end of the spectrum, full-featured GAAP-compliant accounting applications used for financial reporting would need to be SOX-aware. Oracle's NetSuite.Com is one example.

The Evolving CRM Landscape

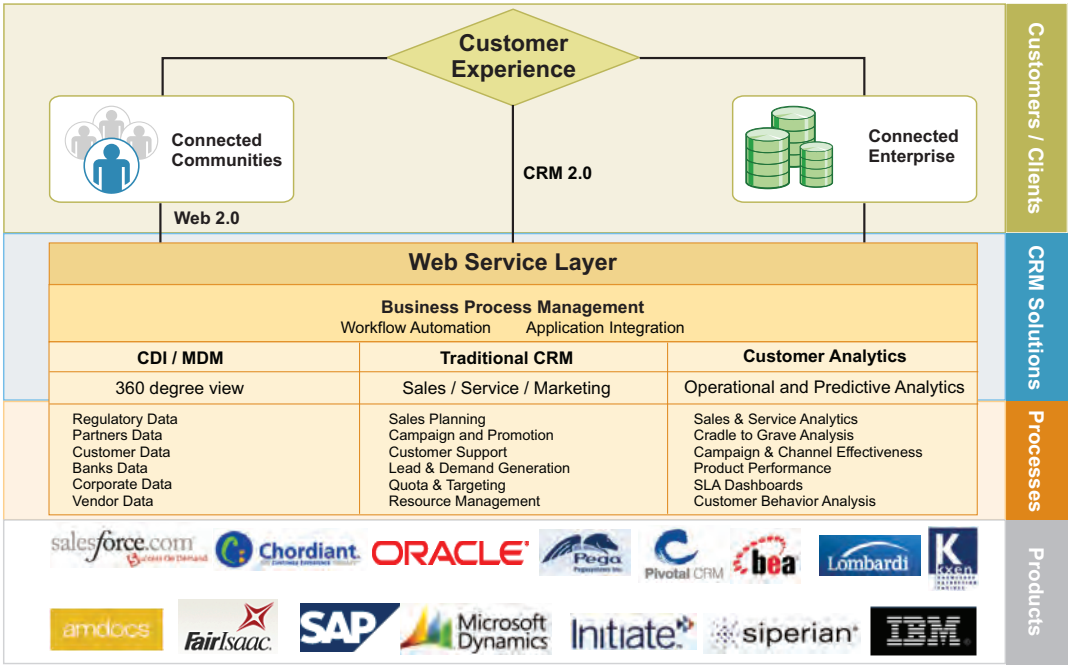

Figure 1

With the recent release of the robust Salesforce.com on-demand development platform, Cognizant expects to see a rapid rise of standalone, pure-play accounting applications deployed on the Salesforce.com platform. These will fall under SOX provisions.

The gray area between these two extremes requires careful analysis. One example: Sales order entry applications that originate as financial data in Salesforce.com but are not the official book of record. This data would include sales compensation applications and asset and inventory tracking applications that are integrated with CRM systems.

Salesforce.com CRM is often used to affect future financial data. Products/price books, contract management, revenue schedules, and line items that ultimately are used for pipeline forecasting are all potentially subject to SOX interpretation, depending on how they are used.

Moreover, as CRM gains visibility and matures, the lines between "financially significant" accounting applications and traditional CRM are blurring rapidly. The official financial data might lie in a back-end "book of record" system and officially be used for financial reporting, but CRM is playing an ever-increasing role in originating, organizing, searching, filtering, and even reporting on financially significant data.

Figure 1 depicts Cognizant's view of the future of CRM. It highlights the need for SOX diligence when designing fully-integrated CRM systems.

Enterprise customers have complex integration requirements. Many have turned to Cognizant to leverage our proven ability to integrate CRM systems with their back-office accounting applications. Salesforce.com, in many cases, is the de facto user interface into many back-office applications. In that case, the best practice is to assume SOX applies to all of the data.

For example, at a major publishing company, Cognizant built a tightly integrated CRM system that originates and then transmits all order entry-related data to a back-office database used for generating invoices. In this case, the only user interface elements in the back-end database pertain to generating billing calculations and invoices.

Therefore, due to ever-increasing overlap, Cognizant advised that the publisher implement Salesforce.com for all its CRM activities, regardless of whether the individual function was subject to SOX compliance. In any area where it could be subject to SOX compliance, we advocated erring on the conservative side, even if analysis could technically yield a conclusion that the implementation would not require it.

We feel that the controls mandated by SOX are good practices for corporate IT even if various components within this CRM system were not originally considered necessary to being SOX-compliant. Meanwhile, the legislation spells out certain requirements that companies must meet at a minimum in order to be SOX-compliant.

Salesforce.com Features and SOX

Salesforce.com contains features that address these SOX requirements. For example:

- **Protection of physical access to data.**

One of the oft-cited concerns by companies evaluating on-demand services like Salesforce.com is how to ensure the physical security of their data residing outside the firewall. After all, if one cannot assure the protection of relevant data, then it will be impossible to comply with SOX. The lack of security in on-demand is a myth, one that it is being debunked over time. Data is no less secure when hosted on a vendor's servers than it is when accessed from a company's own infrastructure. In fact, the opposite is usually true.

Salesforce.com has built a secure hosted computing platform that far exceeds the controls available at most private enterprises. (See www.salesforce.com/security for more information.) The company has spent tens of millions of dollars in building a redundant, mirrored, totally physically secure infrastructure that for-profit enterprises could not achieve using their own internal IT resources. Since its business model is built on a multi-tenant architecture in which layered servers are shared by thousands of companies, physical security is at the top of Salesforce.com's priority list. A single breach would irreparably damage the company's relationship with its large customer base.

Cognizant encourages all enterprise customers evaluating Salesforce.com to visit one of Salesforce.com's impressive data centers to tour the facilities and get a first-hand view of its comprehensive, robust security provisions.

- **Role-based data access.**

SOX requires that IT organizations take measures to ensure their relevant financial data is not tampered with for malicious purposes. Controls against unauthorized access and use of relevant data should be designed independent of the technical platform. IT organizations need to restrict access to sensitive data to the personnel whose professional roles legitimately require access. Salesforce.com protects relevant data from unauthorized access by using role-based controls.

For example, a salesperson, a customer service representative, an accounting user, and their respective managers can all have different access according to the level of data they need to see.

Salesforce.com can also be set up to restrict data access based on sales territory or different job profiles for different departments.

- **Internal workflow controls to guard against misuse of data by authorized users.**

Robust, configurable workflow rules and approval processes are two of the features that function without the need for code-level customization with Salesforce.com. These are two very powerful features that allow an organization to quickly implement and fine-tune application-level controls to reduce the risk of manipulative or fraudulent data coming into the system.

In addition to its "out of the box" workflow functionality, Salesforce.com also enables users to create custom rules for workflow management with triggers based on any business event or period of time. These workflow rules are easy to modify in response to or in anticipation of changing business needs and market developments.

Salesforce.com users can create multi-step approvals to automate sales or business processes that are distinct to their company, such as discount requests or opportunity close approvals.

In Cognizant's Salesforce.com projects, we implement a "gatekeeper" methodology to ensure that data sent to back-end systems passes through a robust approval process implemented using Salesforce.com approval functionality.

At the previously mentioned publishing company, Cognizant implemented an advanced framework of alerting managers any time financially significant data is changed, as well as a robust approval process for sending any financial data to an external accounting system. Any time a user attempts to enter or edit financial data, an accounting specialist receives an e-mail with a link to a pre-built custom report that summarizes the subject activity. Only upon an explicit approval by the specialist does the system send the data to an integration server to be synced to the "book of record." These controls provide multi-layered protection against fraud.

- **Controls to guard against fraud once the data is committed.**

If financially significant data is needed in the CRM system, as is increasingly the case, it needs to be tightly controlled.

For example, at the publisher, the main focus of the business is to retain existing customers who subscribe to its enterprise content. Therefore, it is critical to not only retain financially related data, but take relevant action to ensure continued customer success, ensure that customers are renewing their contracts, and introduce them to other digital content offerings.

In Cognizant's Salesforce.com projects, we implement a "gatekeeper" methodology to ensure that data sent to back-end systems passes through a robust approval process implemented using Salesforce.com approval functionality.

Therefore, it is critical that the CRM system not only originate financially related data, but also retain it for monitoring. However, from a data-management perspective, existing data can never be manipulated directly; with the publisher, this functionality was implemented using Salesforce.com's trigger-level validations capabilities.

- **Ability to trace financially related data throughout its lifecycle.**

The ability to audit record histories is critically important in achieving SOX compliance. In Salesforce.com, this feature works immediately, without customization, allowing an administrator to set up field-level auditing within minutes. In a system where SOX concerns are relevant, all records affecting finance should be set up as an audit fields.

Cognizant sets up field-level auditing not just on currency-related fields, but prefers to enable field-level auditing on all fields that pertain to a customer order -- from contracts, billing accounts, to order-level details.
Any time a user modifies any of the standard or custom fields whose history is set to be tracked, a new entry is added to the "History" list. All entries include the date, time, nature and originator, of the change.

Moreover, Salesforce.com encourages use of histories in a subtle way: History data does not count against an organization's storage limit. Cognizant's enterprise customers are always concerned about data storage costs of their implementations; with Salesforce.com, field-level auditing is not a concern.

In addition to field-level auditing, Salesforce.com automatically logs all outbound e-mails sent from the platform as permanent records of communication. All tasks and events leave a permanent trail. Although the platforms notes are easily editable, Cognizant implements a special comments function that is append-only; comments are not editable once entered into the system, ensuring yet another level of security on record-level note taking.

One of the most important questions a SOX auditor might ask during an evaluation is "Who touched this record, when, and what did they change?" Therefore, Cognizant advocates robust contract, billing, and revenue-related record retention and auditing controls for the enterprise using Salesforce.com's built-in capabilities.

Finally, we implement extensive integration logging in our Salesforce.com engagements to provide full traceability of data being sent to back-end systems. Our custom electronic data interchange (EDI) application used to integrate Salesforce.com systems with enterprise back-end servers utilizes the Salesforce.com API and provides for robust integration logging.

Choosing an Implementation Partner

As advocated in this paper, SOX principles can and should be applied to any CRM implementation that involves financially

significant applications. Cognizant uses its proprietary On-Demand Software Development Lifecycle to implement this. Throughout the cycle of gathering functional requirements, technical requirements, and designing software specifications, the Cognizant team evaluates specifications for their impact on the data and impact on internal controls, interfaces, and security. Cognizant is ISO 9001 certified, a sign of our serious commitment to quality.

A Solutions Assurance Group should be set up to independently monitor for SOX compliance. At Cognizant, we have personnel that ensure that our designs meet institutionalized best practices surrounding regulatory compliance and requirements traceability.

Though the use of the Salesforce.com platform rapidly decreases total deployment time, technology in and of itself is no substitute for rigorous processes that extend from project planning and solution design through management and implementation. SOX risk is reduced by ensuring that projects are taken through the traditional development cycle, albeit in a more rapid timeframe (see Figure 2).

Conclusion

The purpose of this paper has been to illustrate that the most important step in achieving SOX compliance is to deploy processes and controls in the capture of functional requirements around separation of duties, identifying controls needed, and auditing requirements.

Cognizant advocates robust contract, billing, and revenue-related record retention and auditing controls for the enterprise using the platform's built-in capabilities.

We dispelled the myth that any system, including Salesforce.com, will short cut the real work involved in working toward SOX compliance. If you are evaluating Salesforce.com as a solution, you can be sure that it does have the capability to implement the required controls in a properly designed system.

A trusted partner like Cognizant can assist by bringing best practices and an implementation methodology that includes a collaborative approach to requirements capture. Cognizant also has implementation project management tools that facilitate collaboration between the

Project Management Roadmap

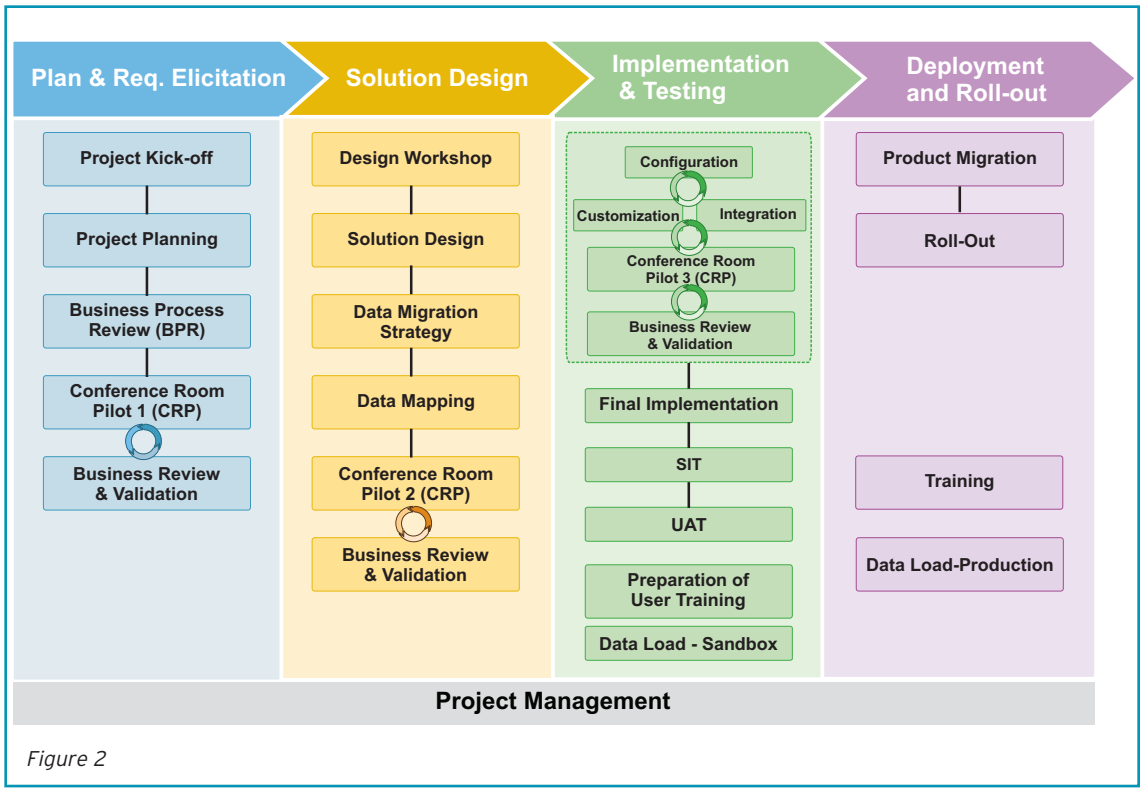

Figure 2

customer and our onsite and offshore project teams to ensure that all design elements are jointly built and approved as the system is developed. A trusted consulting partner that has captured leading practices used in the client's industry can speed the process of identifying the controls needed. We use steering committees for the purpose of bringing forth these practices, and multiple conference room pilots throughout the implementation cycle to ensure that representatives of the user community are engaged early and often.

For more information:

Salesforce.com
www.salesforce.com

The Sarbanes-Oxley Act
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

PCAOB Auditing Standard No. 5
http://www.pcaob.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf

SEC Interpretive Guide
http://www.sec.gov/rules/interp/2007/33-8810.pdf

This white paper was written by Mehmet Ergun, a senior manager in Cognizant's Salesforce.com consulting practice, who has engaged in leading SaaS implementations across Fortune 1,000 enterprises. Mehmet has been building enterprise-scale business applications since 1992 and has led customers through multiple software design/build/deploy paradigm shifts, from the desktop to client/server to the internet and now finally to the next frontier in business applications -- software development within the SaaS architecture. He can be reached at Mehmet.Ergun@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With more than 40 global delivery centers and 59,000 employees as of June 30, 2008, we combine a unique onsite/offshore delivery model infused by a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's Info Tech 100, Hot Growth and Top 50 Performers listings.

Start Today

For more information on how to maximize your customer relationship solutions with Cognizant, contact us at inquiry@cognizant.com or visit our website at: www.cognizant.com.

Cognizant
Passion for building stronger businesses

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
Haymarket House
28-29 Haymarket
London SW1Y 4SP UK
Phone: +44 (0) 20 7321 4888
Fax: +44 (0) 20 7321 4890
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com