DIGITAL

JULY/AUGUST 2007 EDITION • VOL.26, ISSUE 4

SOFTWARE MAGAZINE

The Software Decision Journal

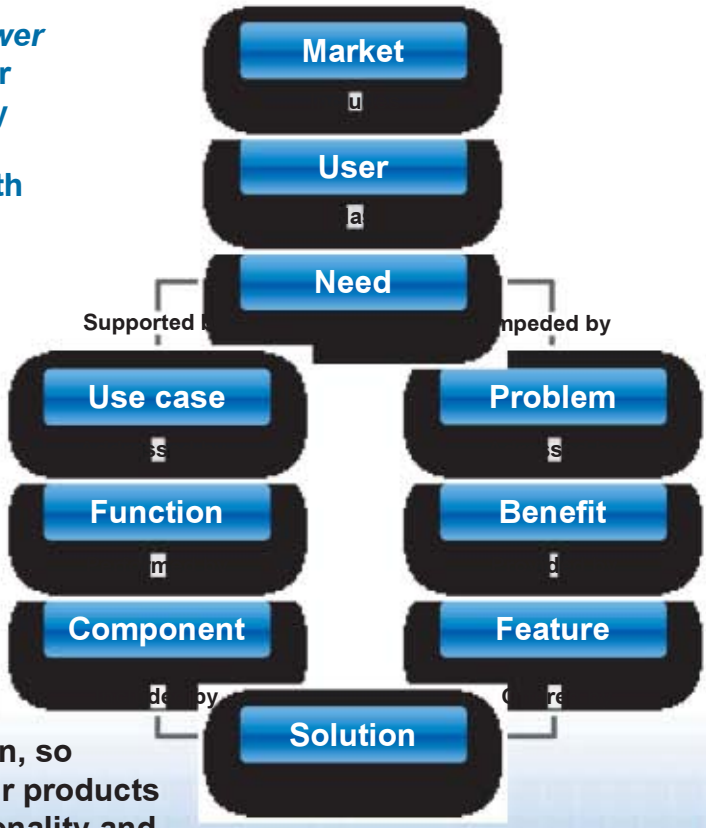
CMDB Aims To Be Single Source Of TRUTH

A KING CONTENT PUBLICATION

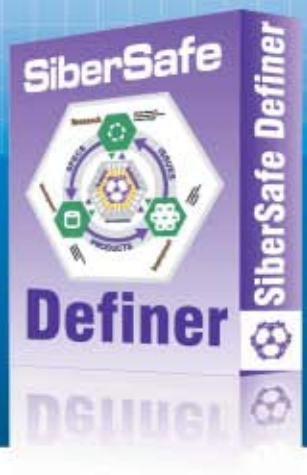
www.softwaremag.com

SiberSafe Definer™

Accelerate **product development,** ***lower*** **operational costs,** ***increase*** **customer satisfaction, and** ***improve*** **traceability by connecting those who define, document, and manage products with those who build, market, and use them – with SiberSafe Definer™, SiberLogic's unique integrated requirements management solution.**



Collaboratively capture your product requirements. Connect market research and business analysis to user needs and product features. Aggregate your product knowledge into specifications, test criteria, user manuals, even marketing collateral – and *keep them all synchronized*. Effortlessly trace changes up and down the chain, so when you upgrade or repurpose your products for a new user base, product functionality and documentation are always in step. It's the ultimate in product quality: from market drivers to customer satisfaction, via SiberSafe Definer.



SiberSafe Definer™

INTEGRATED REQUIREMENTS MANAGEMENT

Visit us online at www.productdefiner.com/swmag for white papers, demos, and more

For more information about how SiberSafe Definer can streamline your organization's product development, contact us at 1-866-SIBER-LG or via sales@siberlogic.com.

SIBERLOGIC®

COVER ILLUSTRTATION BY CHUCK MACKEY

DIGITAL SOFTWARE MAGAZINE
The Software Decision Journal
VOLUME 26, ISSUE 4 • JULY/AUG 2007 EDITION

COVER STORY: IT INFRASTRUCTURE

16 CMDB Aims to Be Single Source of Truth

A CMDB must achieve specific goals to be successful; Advice: prioritize the issues, map IT processes to those issues; Then determine data each person needs to get the job done

By Jasmine Noel

>> DEPARTMENTS

>>FEATURES

APPLICATION PACKAGES

8 Banks Cashing in on Service-Oriented Architecture

As financial organizations become more global, SOA offers a feasible way to make that happen. However, a change of mindset is required

By Lana Gates

SECURITY

21 Security Requirements Engineering: A Road Map

A lack of security requirements leads to insecure software; Proper planning, however, can enhance the security of a software development lifecycle

By Rudolph Araujo

editor's letter

JULY/AUGUST 2007 EDITION

Search For Truth Fuels Configuration Market

The search for the single source of truth about configuration of the IT infrastructure is fueling growth in a software market that analyst Jasmine Noel notes may wrongfully be called configuration management database (CMDB). (See p. 16-20.) Use of the term database for this purpose implies a less than dynamic change among collaborating services, but the term is winning out anyway. CA, IBM Tivoli, HP, EMC, Symantec, and Microsoft all have entries via their own product developments or acquisitions.

The exercise of implementing the CMDB leads the IT organization into the challenging exercise of prioritizing issues, determining which IT processes address those issues and which people are involved, and matching the requirements to what the product suppliers are offering. Thus the CMBD activity is focused where IT meets the business, and it helps to avoid expensive change failures by getting it right the first time more often. Jasmine reports data from the IT Process Institute showing top IT performers implemented five time more changes with a higher success rate than medium performers.

Along the same theme of enabling collaboration, service-oriented architecture is enabling a lower-cost way to integrate across software systems, which is enabling a new wave of functionality in marketing many application packages, including financial packages, as Managing Editor Lana Gates writes about in this issue. (See p. 8-13.) She quotes Sharad Vajpayee of 3i Infotech, an IT services firm, as saying SOA helps release "trapped ROI" from legacy applications—that's a nice business return.

Project and portfolio management also play a more important role as IT manages itself more like a business. Serena Software's purchase of Pacific Edge Software helps to bring application lifecycle and portfolio management under one umbrella, a key assist to IT as it strives to differentiate its businesses via software. A survey by Serena on customer spending patterns showed that 70 percent of the IT budget for application development was going toward custom projects, and 30 percent to packaged applications, according to Nathan Rawlins, senior director of product marketing with Serena. IT organizations are willing to invest to maximize their development investments. As the effort continues, we will be following developments to find the single source of truth about IT configurations.

Regards,

John P. Desmond
Editor

P.S. Software and service suppliers still have time to complete the 25th annual Software 500 survey. Go to www.softwaremag.com to register and complete this year's survey. Results will be published in the September/October digital *Software Magazine* for the first time anywhere.

DIGITAL SOFTWARE MAGAZINE
The Software Decision Journal
www.softwaremag.com
July/August 2007
Software Magazine Vol. 26, Issue 4

KING CONTENT

Software Magazine is a property of King Content Co.

KING CONTENT CO.
P.O. Box 135
E. Walpole, MA 02032
Phone: (508) 668-9928
Fax: (508) 668-0442
www.king-content.com

PRESIDENT
John P. Desmond

For print subscriptions, go to:
www.MySWMag.com

The Software Magazine digital version is delivered in QuVu (patent pending) format, which is licensed from and used by permission of Qiosk.com, INC.

softwaremag.commentary

USABILITY ENGINEERING

By Meryl Enerson

Outsourcing the User Experience

Outsourcing has gotten a bad name for itself recently, in some measure because of the growing popularity of outsourcing to overseas markets in an attempt to reduce costs. ■ But outsourcing the User eXperience (UX) of a software application, website, or Web service is a horse of a different color. Although cost-saving can be a goal, UX work (including user research, analysis, and user-centered design) is much more frequently undertaken as a form of transformational outsourcing—it is used to improve the quality of the application and undertaken to have impact on the bottom line.

The drivers for engaging a UX firm effort may come from business initiatives (new functionality, an upcoming new release), brand and marketing (the need to upgrade an image or an outdated look), or simply feedback from clients, customers and users of an application: customers may be complaining that the application takes too long to complete; it may be hard to find critical information or functionality on a Web-based service; there may be too many calls to Technical Support for your product.

A redesigned user experience can be a critical tool to help companies:

- Improve the quality of an application or suite of applications
- Attract or retain customers or users
- Increase sales
- Improve usability or "findability" of key features or content. (See Fig. 1.)

Meryl Enerson is president and founder of Enervision Media, Inc., a user-centered research and design consultancy. She has assisted numerous organizations in evaluating and improving the user experience of their websites and applications. Contact her at meryl@enervisionmedia.com.

Common Pitfalls

When you decide to engage a UX vendor, you can't help hoping for that perfect "honeymoon" scenario: you hire the outside vendor, they hand you results in a couple of months, you plug in the deliverables, and you sit back and wait for your bottom-line results to mushroom upwards.

But in reality, outsourcing the user experience is more like an internal project than a "black box" purchase of outside labor. It requires focus and participation from you as client to be most successful. You also need to avoid the more common problems and pitfalls that can derail a UX project.

Pitfall #1: Resistance from Existing Team Members

Introducing a new vendor to your existing design, development, or user experience team is bound to ruffle a few feathers. In some cases, there may be a single team member who thinks he or she is being replaced and, as a result, may get a little distressed, angry, or difficult to work with during the process.

Alternatively, your existing (external) development or design group may feel competitive with the UX vendor and will endeavor (consciously or unconsciously) to sabotage your UX project. An example of this is when one or more developers responsible for implementing a new front end wait until the deliverables come in before informing senior management that the design is "simply not doable" in the timeframe.

The Solution Tactics that can successfully minimize resistance from team members include:

Getting people involved. Team members involved in implementation may be invited to requirements-setting sessions, for example, so their voices can be heard.

Establishing clearly defined roles for the key players involved in implementation. Be sure that roles do not overlap too much. This is particularly true where the vendor is concerned.

Defining a clear feedback process. Feedback from you and your team members to the vendor should be funneled through a single point-person (e.g., the project manager for the project). This gives team members a voice,

while ensuring consistent and consolidated communication.

Pitfall #2: Inadequate or Unrealistic Requirements

Put simply, you will not get results from an outside UX effort unless there is a good set of requirements established as the first step in the effort. Without a requirements document of some kind, there is room for miscommunication, misinterpretation, and even finger-pointing at later stages of the project.

Requirements are often made that are vague, poorly worded, or inadequate in scope. This is usually the result of not taking adequate time to complete the "needs analysis process." Conversely, you can have too many requirements, if you leave the vendor to collect requirements from stakeholders separately.

The Solution Ideally, the setting of requirements is a joint effort at the start of a UX engagement, between the internal manager/stakeholders and the UX vendor. I call this work stage the needs analysis step. Make sure your UX vendor includes an adequate amount of resources and time to complete this stage.

During needs analysis, the UX team will collect information from you on subjects including your short- and long-term business goals, your technical constraints, your users or customers, and the scenarios for use.

By the end of this stage, you should have a mutually agreed upon, crisp definition of the requirements for the user experience, including things that must be in the design and what the users must be able to accomplish. Metrics for success can be included as part of the requirements, but they should be appropriate for the timeframe and budget (i.e., don't expect to triple sales on a small five-figure budget or within a one-month timeframe). Be realistic.

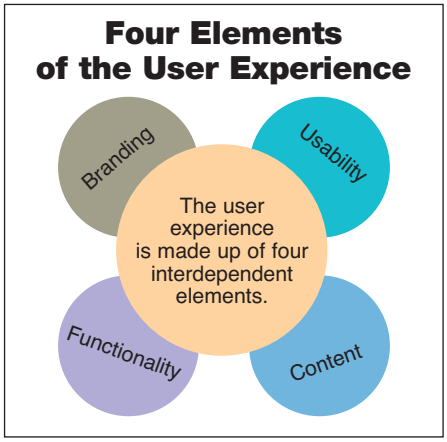


Figure 1

Pitfall # 3: Surprises in the Deliverables

You're not alone if you don't like to be surprised in your deliverables from vendors. You've signed up for "X" and you expect "X" to be delivered.

But UX projects can go awry when clients and vendors don't communicate about the nature of the end product. This can include poor definitions from the vendor about the total number of deliverables, the schedule for deliverables, or the form each deliverable will take.

Some clients expect the vendor to keep redesigning a front end "until it's right," for example, but the vendor may be expecting to do a maximum of two rounds of design reviews, plus a polish.

The Solution Make sure the proposal or contract details (and explains, if necessary) the nature of the UX deliverables, including the expected format(s), and the number of rounds of revisions for each key deliverable. This is particularly important for flat-fee projects. Provisions for additional requests and timeframe extensions should be made as well.

Strategies for Successful UX Outsourcing

It's not just about the vendor. As the client, you need to take a few steps to ensure success in any user experience project:

1) Establish your shared (stakeholder) goals. It's up to you to get the stakeholders in the same room and discuss your reasons for bringing in the vendor. Before you start the engagement, try to define your shared vision for success, and what you ideally want out of the process. It helps enormously to have the stakeholders on the same page.

2) Outsource for discrete deliverables. If you know what you want upfront, you are more likely to get it from your vendor. Examples of some common user experience deliverables include:

- **User research** (including usability testing of an existing application, or interviews with your client base)
- **User-centered requirements** (user scenarios, task analysis, requirements documents)
- **Look & feel deliverables** (key pages or all pages of the application in Photoshop files or production-level graphics)
- **User interface specifications** or wireframes
- **Entire front-end design**

3) Involve team members early and consistently. To avoid resentment and resistance to the outsourcing effort, engage your existing team members in the process, and establish clear roles between them and the outside firm for the duration of the project. This helps eliminate the "us versus them" mentality and the negative feelings that can sabotage an important redesign or UX project.

Eliciting input from team members will also help the outside team create better user experience deliverable(s) for your company. And by involving team members early, you set the stage for ownership of the final design or hand-off of project deliverables, which will help you take your software application further, faster. SW

softwaremag.commentary

BUSINESS PROCESS VIEW

By David Kelly

BPM Vendors Embrace Software as a Service

Services-based software has been around for a while. Back in 1999, during the Internet hype, several companies offered hosted applications for everything from enterprise procurement to sales force automation. After the Internet market crashed, several of these companies managed to survive, primarily because they filled a niche in the market that was economical and effective: enabling departments of large enterprises to utilize an electronic procurement solution, for example, while paying a monthly fee that did not require the IT sign-off or budget approvals that an in-house, enterprise-scale solution would.

As the Internet matured, and the notion of a Service-Oriented Architecture (SOA) and Web 2.0 applications began to emerge, services-based software continued to thrive in pockets, but now had a more-global technology platform to stand upon. Over the past several years, we have seen an uptick in the number and variety of services-based software solutions across enterprise computing. Again, one of the main selling points is budgetary, with a sole department being able to sign off on using the service under the IT radar. Among the services that Upside Research has reviewed in the past year, the average monthly fees range from $500 to $2,000 per month depending on the number of users.

Another selling point is speed of deployment, because many business-focused applications can get bogged down in implementation cycles within the enterprise. With services-based software, many customers can get up and running literally in days or weeks, once they have signed the papers and worked out billing arrangements. In most cases, the solution is hosted at a central location by the solution provider, and for a monthly fee (based on transaction rates or number of end users) the customer has use of the software—and access to any upgrades or improvements that occur—all with minimal or no interruption in service.

This is extremely appealing for efficiency-driven organizations that want to feel the business benefits of a software solution as quickly as possible without the IT burden of having to configure, manage, support, maintain, and upgrade a software application. In many cases, the potential total cost of ownership with a services-based solution is five to 10 times less than for traditional installed software. With companies focused on return on investment more than ever, a services-based approach enables a project to become profitable more quickly, too.

BPM Getting Into the Act

The Business Process Management (BPM) market has become more caught up in the services-based software movement in recent months, with BPM vendor Savvion building a strong offering around Business Process Outsourcing (BPO). Essentially, Savvion has a group of service providers that work with Savvion's customers to extend their key business processes into an outsourced model.

On a similar note, Metastorm, another BPM vendor, has made its BPM platform "BPO-ready," enabling its partners to use Metastorm BPM as the foundation for Software-as-a-Service (SaaS) offerings and outsourced services.

Open-source BPMS vendor Intalio has extended its belief that companies should not have to write code to create business processes. The company's services-based software strategy is focused on letting its partners take the Intalio BPMS and extend the product in some very interesting ways. One partner, Coghead, has used Intalio BPMS to create a complete BPMS natively built for the Web, with zero code design and development, in a hosted model.

Beyond partnering with a service provider to outsource BPM, some vendors are taking a more service-focused approach that targets key business

David Kelly is the founder and president of Upside Research. Formerly senior VP of Analyst Services at Hurwitz Group, David can help companies profit from the diversity of a changing technology landscape.

Buyers Guide: Services-Based Business Process Management Tools

Company	Strategy	Product	Details
Appian	Hosted SaaS	Appian Anywhere	**Appian** has made its entire BPM suite available as a services-based solution. Appian Anywhere is a subscription-based service available to anyone with a Web browser and a Web connection. The goal is to enable customers to quickly build and deploy composite applications.
Intalio	Partnering with ISVs	Intalio BPMS	**Intalio** has enabled its partners to use the zero-code, open-source Intalio BPMS as the foundation for several different flavors of hosted BPM services. The company believes that business processes should be able to be designed and implemented without having to hard-wire code and applications, and thus supports the efforts of its partners to bring native Web-based BPMS solutions to market using the Intalio BPMS server as the foundation.
Integrify	Hosted SaaS	Integrify OnDemand	**Integrify** offers a hosted version of its order requisition management solution to customers who want to quickly add enterprise request management without having to manage the infrastructure. Integrify OnDemand is positioned as an alternative for project teams that want fast process management results without the overhead. The company enables hosted customers to easily move the solution in-house if they desire for maximum flexibility.
Lombardi	Hosted SaaS	Lombardi Blueprint	**Lombardi** Blueprint offers the ability for project teams to work on collaborative process discovery as a means of shortening the typical cycle between expressing interest in and actually launching a BPM project. Blueprint provides collaboration, process discovery, and documentation capabilities and is hosted.
Metastorm	BPO	Metastorm BPM Platform	**Metastorm's** strategy is to make its BPM platform "BPO-ready" so that partners can leverage the Metastorm BPM platform as the foundation for SaaS offerings and outsourced services. Metastorm's positioning is to provide partners with the ability to rapidly develop multiple process-based application offerings, to customize business processes for each customer, and to maintain and change processes/applications more easily.
Savvion	BPO	Savvion Business Manager Platform	**Savvion** partners with outsourcing vendors to enable its customers to gain greater efficiencies with their BPM projects. Typically, a process has already been designed and modeled, often using Savvion Process Modeler, and then the customer works with a service provider to outsource the business process into a hosted environment where BusinessManager is running.

processes that are offered as a service. For example, specific self-contained processes such as order requisition, enterprise procurement, and capital expenditure requests are being offered to enterprises in a services-based model.

Because many of these types of processes are very similar in terms of workflow, they are easy to offer as services. The service provider will offer some templates for a process such as order requisition, and provide graphical tools to end users to modify the workflow to reflect their company's own internal processes. Integrify is one example of a company offering processes such as request management to customers in a services model.

At least one BPM vendor has gone a step further and made its BPMS available in a services-based model. Appian Software launched Appian Anywhere in February, making the entire Appian BPM Suite available to business users through a subscription service. Users have access to portal, collaboration, content management, process and rules capabilities to build and run business processes, often without involving IT.

Another trend is offering part of the BPMS as a service. For example, Lombardi Software recently announced its Lombardi Blueprint product, which offers a hosted process modeling application. Lombardi Blueprint is designed to promote collaborative process discovery, which equates to providing operational-level business managers with a tool to help determine the best place to launch a BPM initiative.

According to Lombardi, the genesis for this product came from the goal to help customers shorten the average three to six months it takes for a business to prioritize its business processes and select one for an inaugural BPM project. Part of the time is spent discovering the business processes and determining which one will be best for BPM. Lombardi Blueprint provides collaboration tools among team members for the discovery process, as well as a repository for users to document their regulatory needs. All of this information is stored in XML, making it easily exportable into any other BPM suite.

The key for vendors that also provide complete BPMS platforms in the traditional licensing and implementation model will be to define for customers where it makes sense to utilize the services-based offerings in conjunction with an enterprise solution. By clearly providing users with scenarios for use of the hosted or services-based BPM solutions, the vendors will be able to encourage growth of this new channel without undercutting their original solutions, and will be able to reach new customers for whom a traditional installed BPM platform is not an option. SW

APPLICATION PACKAGES

BANKS
CASHING IN ON
Service-Oriented Architecture

Financial application software suppliers are exploiting new capabilities made available with Service-Oriented Architecture (SOA), aimed at lowering total cost of ownership, simplifying integration and customization, and enhancing performance. Financial institutions, steeped in legacy systems, are increasingly embracing SOA as a means to access and distribute information locked in those systems—and do it in real time, helping them become truly global organizations. SOA offers a way to organize the services they want and to build connections to the systems they already have.

It used to be that financial institutions—namely banks—only had to worry about internal customers and how to keep them happy. They were able to do that reasonably well with their white rooms of computers. They knew where all their computers were. They had a limited set of applications, a limited set of users, and very limited and strictly monitored interfaces on the outside, if any. But the onset of Internet banking has broadened banks' customer reach significantly. Today, banks have to be online 24x7 on a global basis or they lose customers.

This creates myriad challenges as banks face regulatory and compliance requirements, the necessity for near-real-time, uninterrupted processing support with guaranteed response times, the problems of application overlap caused by mergers and acquisitions, and the need to maintain a complete, 360-degree view of each customer. At the same time,

As financial organizations become more global, SOA offers a feasible way to make that happen. However, a change of mindset is required

BY LANA GATES

banks are experiencing increasing market competition and thus the need to reduce the cost of operations and IT. So, in an effort to retain customers, increase time to market, and better manage a multi-channel environment, financial institutions are viewing services as an approach to agility.

Weighing the Benefits

"Adopting SOA can provide definite benefits by allowing companies to rapidly build and deploy reusable business applications, release 'trapped ROI' from legacy applications and mainframe resources, better integrate applications through BPEL (Business Process Execution Language) and workflows, and effectively allow financial services companies to offer new and innovative service models to clients," explains Sharad Vajpayee, vice president of India-based 3i Infotech, a global information technology company with customers in the banking, insurance, manufacturing, contracting, retail and distribution, and government industries.

Percy Barraclough, CTO of SunTec, a global technology company also based in India, concurs. SOA, he says, is a principle of good management, good design, maximum duplication, and maximum reutilization. "The basis," he explains, "is an extension of object-oriented design within applications, bringing forward the concept of open integration across applications. This has significant relevance for financial institutions because of the diverse source of information and its relevance to charging and billing."

Financial institutions, in particular, need systems that are much more agile than the systems they've used in the past. "It's much easier to use SOA to cope with the stream of continuing changing business needs," notes Germany-based Jost Hopperman, research analyst and vice president of Forrester Research, Inc., with headquarters in Cambridge, Mass.

Financial institutions rely heavily on legacy systems and cannot afford to discard them, nor do they want to. At the same time, however, they need to share the critical information and functionality embedded in those systems with other applications, including those of customers and partners, often in real time or near-real time and, increasingly, over the Internet. "SOA can be a great way to encapsulate legacy applications and distribute their functionality across the enterprise and beyond in a standard way," says Michael Guttman, vice president and CTO of The Voyant Group, LLC, a Westchester, Pa.-based consulting company dealing with transitions to SOA, Business Process Management (BPM), and related technologies. "The trick is to do it in a way that meets all the necessary quality-of-service and security requirements, and without disrupting or overloading the legacy systems."

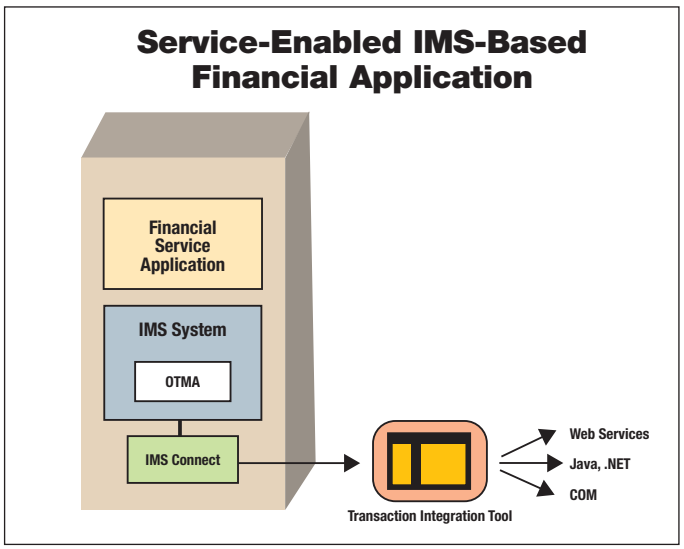


Figure 1 Source: Attachmate

And, SunTec's Barraclough adds, SOA is essential if financial firms are to address new challenges such as new services, new initiatives, innovative models for servicing the market, and increasing competition.

There are many ways to service-enable legacy financial applications. An IMS-based application, for example, can be service-enabled through the use of a transaction integration tool. (See Fig. 1.) A CICS application can be service-enabled using an on-mainframe or off-mainframe approach. (See Fig. 2.) Another option is service-enablement through the terminal screen. (See. Fig. 3.)

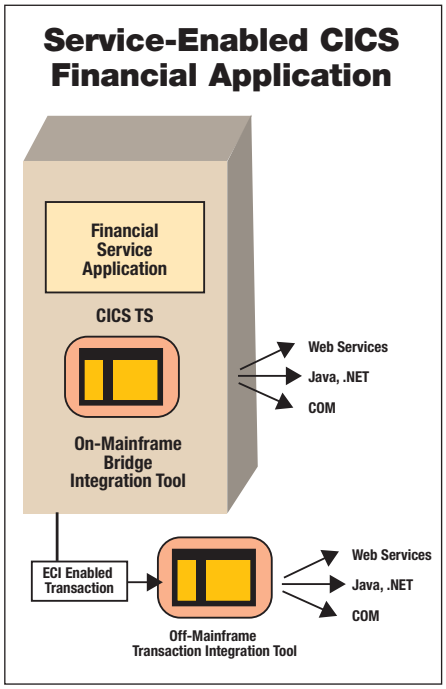


Figure 2 Source: Attachmate

Embracing SOA

Wells Fargo is one organization that is embracing SOA to address new challenges. In fact, the bank led the shift to SOA for financial institutions through its successful launch of Internet banking back in 1995. Today Wells Fargo is in its second generation of SOA technology. "It's our primary way of doing distributed computing," notes Eric Castain, chief architect for Internet services, based in San Francisco, Calif. "It's our way of integrating the various accounting systems to give a customer-centric view of the relationship to Wells Fargo."

The goal of obtaining an integrated view of its relationships with customers is what drove Wells Fargo to SOA in the early 1990s when a customer service agent needed to interact with multiple computer systems to get an overall view of a customer's relationship with Wells

Fargo. "That integrated view in the 1990s became SOA of now," Castain adds. The organization can now provide "anytime, anywhere information for the customer," he continues. "It's a consistent experience that offers the agility to react to business requirements." (See Fig. 4.)

"The key to successful SOA is understanding services," says Mark Tiggas, chief architect for enterprise payment strategies in Wells Fargo's technology information group in Minneapolis. "We believe very strongly in the number of tools that are emerging to help us integrate and leverage the power of services," he adds. Some of those tools include Sun Microsystems' JAX-B (Java Architecture for XML Binding) and JAX-WS (Web Services toolkit), open-source tools such as Apache SOAP, Microsoft Visual Studio for .NET development, and a number of tools to assist in managing and performance monitoring, such as those offered by AmberPoint. In addition, the major Web application and communication servers have introduced some level of Web services integration into their product lines as well.

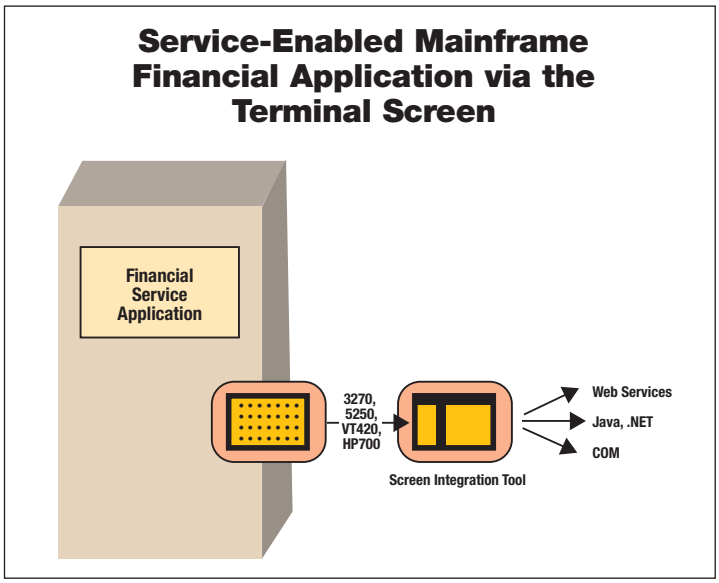


Figure 3

Source: Attachmate

SOA is a standards approach, providing a business-centric view of development and business. Because Wells Fargo has multiple channels and multiple interactions, a business-centric view is vital. Before this, a customer would receive a different answer from a teller than from an ATM about his or her checking account balance, for example. "Because of what we've done [with SOA], the information is fresh everywhere," Tiggas says. "You get the same answer." SOA makes the information more real-time and more consistent.

Cole Taylor Bank is another example of a financial institution embracing SOA. After more than 75 years of service to small and mid-sized businesses in the Chicago area, Cole Taylor Bank realized it had an inflexible data environment with un-optimized customer services. This resulted in management issues as well.

Needing a distributed infrastructure to standardize, connect, and scale IT systems, Cole Taylor Bank turned to Sonic ESB. Using that product, the bank was able to simplify data management, automate account visibility, and expedite customer services.

Sonic ESB helps Cole Taylor Bank deploy new applications and business

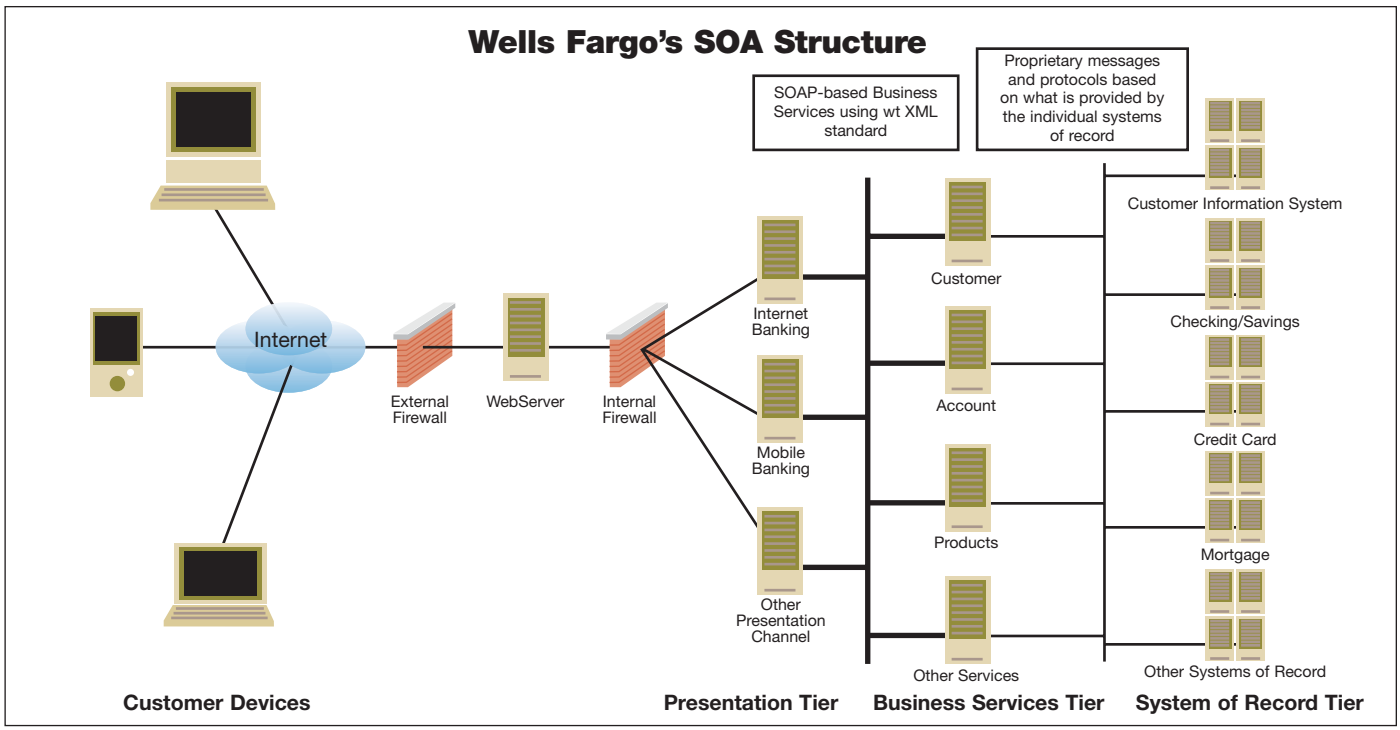


Figure 4

Source: Wells Fargo

New SMP Event in Austin, Texas

SOFTWARE Marketing Perspectives
CONFERENCE & EXPO

One Day Seminar **Tuesday, Oct. 23, 2007**

Hyatt Regency Austin on Town Lake
Austin, Texas

The producers of the Software Marketing Perspectives Conference & Expo – the leading event for software industry product managers and marketers – bring a one-day seminar to the Austin, Texas market, home of the Austin Product Management & Marketing Forum (www.AustinPMMForum.org).

The program will feature speakers – of the caliber of the annual event – beginning in the morning, at lunch and in the afternoon. We will end the day with a reception in the Exhibit Area, which will feature tabletop and booth exhibits from our sponsors.

If you are a product manager, the SMP conference program speakers will help you stay current in your field, and take away practical ideas and suggestions you can apply in your job immediately. The program features experienced VPs and directors of product management, who will speak from experience on the most topical subjects. The conference program operates in a spin-free zone; no sales pitches.

If you are a software or services company that sells to other software companies, the SMP event provides a net-working venue where you can make valuable professional contacts. Russell Foy, director of sales for FeaturePlan, said, "This is the first conference we have gone to where we actually closed deals within days based on contacts we made at the event."

2007 SMP Event Program Topics Included:

A Product Managers Guide to Being Successful in an Agile Environment

The 7 Habits of Highly Effective Product Managers

Assessing and Managing Risks of Product Portfolios

Maintaining Product Marketing in the Midst of a Merger

Integrating the Agile Development Process with the Pragmatic Marketing Framework©

Companies Attending Included:

Aladdin
Alcatel-Lucent
Altiris
Amdocs
Autodesk
Bank of America
Bit Defender
Datatel
Fidelity
Hewlett-Packard Co.
Kronos
Microsoft
Nokia
Oracle Corp.
Performix
RR Donnelly
Sun Microsystems

For more information and to register, go to: www.smpevent.com.

For information on exhibit sales, contact National Sales Manager Carol Samost at csamost@softwaremag.com.

KING CONTENT DIGITAL SOFTWARE MAGAZINE

The SMP event is brought to you by King Content, publisher of Software Magazine.

"In order to realize the full benefit and value of SOA, companies often need a systemic change in architecture and process, which is easy to underestimate."

processes faster, as well as to make portfolio changes directly via a website. In addition, the bank was able to cut time spent on exporting information from a data system into a spreadsheet from eight to 10 hours a month down to 45 minutes, according to a case study entitled "Cole Taylor Bank Deposits the Benefits of Service-Oriented Architecture." As a result, the bank's call center can answer customer inquiries quicker through a centralized view of customer accounts across service applications and servers.

New Mindset Required

While some banks are realizing the benefits of SOA, arriving at actual results is not a quick or easy process, and there are still many challenges to overcome. "In order to realize the full benefit and value of SOA, companies often need a systemic change in architecture and process, which is easy to underestimate," notes 3i Infotech's Vajpayee.

Jerry Silva, research director for the Tower Group, agrees. "The biggest challenge most banks face in deploying SOA comes from the architecture's inherent advantage of breaking down the walls between businesses in the organization, which, therefore, requires a new organizational model and governance policy," Silva wrote in a September 2006 report entitled "The SOA Challenge: New People, New Models, New Ways of Thinking."

That is exactly the challenge most banks are facing. Wells Fargo had to overcome that problem as well. Successful use of SOA "takes a shift in the way you think about how to design systems focusing on business processes," Castain explains. It's an approach more focused on business functionality than technology, he adds.

Wells Fargo has succeeded in changing its thought processes as an organization. "It's so ingrained here now that we don't think of it as anything other than what you normally do," Castain says. He encourages other organizations to view it that way as well. His colleague Tiggas agrees: "It really is about defining the right services and moving forward with services as the center of your thought process." Castain adds, "If you approach it from the business service point of view, then I think you're much more likely to succeed and have an easier time of SOA. Partnering with business is the key step in that process."

The transition process to SOA involves four key maturity levels, according to The Voyant Group's Guttman. Reaching the first level involves acquiring, installing, and becoming proficient in the infrastructure and tools necessary to design, develop, and deploy services. Reaching the second level is more challenging. It involves making SOA the predominant paradigm

7 Lessons Learned Based on SunGard's Adoption of SOA

#1 Governance is more important than technology.
The bottom line: Ensure that every corner of the institution has representation and is governed. Moreover, create processes to ensure that the natural checks and balances are in place to keep the process whole.

#2 Engage key stakeholders from each domain.
The bottom line: Identify, incent and measure participation of key stakeholders in order to help ensure that the SOA meets the needs of the business and that the effort is sustained long-term.

#3 Measure and report on key metrics.
The bottom line: Measurement is needed in order to continually increase the value of an SOA initiative, help ensure participation by team members and garner support from executive management. As such, organizations must define areas that can and should be measured and put processes in place for regularly doing so.

#4 Inventory all assets in a directory or catalog.
The bottom line: The right registry and processes for ongoing expansion and maintenance are critical.

#5 Adoption requires a maturity model.
The bottom line: A maturity model will help organizations properly classify each component and align it with the appropriate standards.

#6 Build integrity into the process and technology architecture.
The bottom line: Without integrity and quality assurance, key stakeholders will no longer have trust in the process and the SOA project will be in jeopardy.

#7 Harvest the low-hanging fruit first.
The bottom line: SOA initiatives will benefit greatly from early successes and the initial projects should have a short time-to-value.

Source: SunGard

for all inter-application communication and distributed computing across the enterprise. "Unfortunately, without proper planning, pushing an organization too rapidly into level two can lead to a glut of one-off services," Guttman notes.

To avoid that, organizations should move quickly to level three, where the organization begins the shift from simply building new services on an ad hoc, as-needed basis to reusing and improving existing ones instead. "To get to that third level, you have to have an overall model and roadmap for your entire enterprise portfolio of services," he explains. "This is the area that even most advanced SOA organizations are struggling with now," he adds.

A level-three roadmap is also essential for organizations that expect to eventually expose their services to outside parties. Those organizations will become increasingly interested in the fourth level of SOA maturity: industry standardization. Most organizations starting into level three, Guttman says, will probably prefer to follow international standards for modeling sets of services aimed at their particular industry—financial, telecom, etc. According to Guttman, few such standards exist for SOA yet, and this, he says, is a good indication of SOA's current overall maturity level: "Most organizations are still at level one or two, while even the most mature organizations are struggling to get from level two to three."

Future Looking Bright

Guttman notes: "It will be another few years at least before enough organizations are far enough into level three that they create a demand for level-four SOA standards." At that point, he adds, SOA will really take off, as businesses rush to integrate their SOA services with those of their customers and partners.

As SOA evolves, so will the way we view and pay for the services it provides. Forrester's Hopperman believes that over time there will be a very strong change in planning approaches in application landscapes in general. "If you have to buy applications, hopefully you will only have to pay for the services you need," he notes. "It will be about planning functionality at the services level instead of the application level."

Don Free, research director in banking for Gartner, headquartered in Stamford, Conn., agrees. Real service-oriented businesses are going to have to do some understanding of whom they're serving, he says, adding, "As organizations become more service-oriented, we're going to see this turn into more of a utility so they pay for levels of volume of usage versus the number of services they have." Free anticipates that scenario is still five to 10 years in the future. But it is definitely coming. As he explains, "the rip-and-replace option is not a very feasible one in the banking environment." SW

Buyers Guide: Financial Application Packages & Services

Company	Focus Area(s)	Products	Services
3i Infotech	BPO, INV, WS	x	x
Advent Software, Inc.	BNK, INV	x	x
Alogent Corp.	EBP	x	
AmberPoint	WS	x	
AXS-One, Inc.	ACC, BPM, BUD, WS	x	
Blackbaud, Inc.	ACC, WS	x	x
Bottomline Technologies	ACC, BNK, EBP	x	x
Cartesis, a Business Objects company	BPM, BUD, RSK	x	x
CheckFree Corp.	ACC, BPM, EBP, RSK	x	x
CODA plc	ACC, BNK, INS, INV	x	
Convergys Corp.	ACC, HRS, LND		x
Cougar Mountain	ACC	x	
DST Systems	ACC, BPM, BPO, INS, INV	x	x
Emerging Information Systems, Inc.	BUD, INS	x	x
Envision Financial Systems, Inc.	BPM, INV	x	
Fair Isaac Corp.	BNK, INV, RSK	x	x
Fiserv, Inc.	BNK, BPO, EBP, INV, LND	x	x
FlexiInternational Software, Inc.	ACC, BNK	x	x
I-many, Inc.	ACC, BPM	x	x
Intuit, Inc.	ACC, BNK, EBP	x	x
Jack Henry & Associates, Inc.	BNK, BPO, INS	x	x
Kingland Systems	ACC, BPO, SEC	x	x
Misys plc	BNK	x	x
Movaris, Inc.	RSK	x	x
Oracle	BNK, INS, LND, RSK, WS	x	x
Progress Sonic	BPM, WS	x	x
RDM Corp.	EBP	x	
S1 Corp.	BNK, EBP, LND	x	x
The Sage Group plc	ACC, BPM, HRS	x	
Stockgroup Information Systems	BNK	x	
Sun Microsystems	BNK, INS, TRD	x	x
SunGard Data Systems, Inc.	BNK, INS, INV, RSK, SEC	x	x
SunTec Business Solutions	BNK, INS	x	
Systems Union Group plc (Infor)	ACC, BUD, RSK	x	x
Technology Concepts & Design	BPM		x
True Automation	INV	x	x
WowTools, Inc.	LND	x	
XRT	EBP	x	

Key to Focus Areas

ACC	Accounting
BNK	Banking
BPM	Business Process Management
BPO	Business Process Outsourcing
BUD	Budgeting
EBP	Electronic Billing & Payments
HRS	Human Resource Services
INS	Insurance
INV	Investment Services
LND	Lending Services
RSK	Risk Management
SEC	Securities
TRD	Trading
WS	Web Services

Wells Fargo Foothill

Technology Finance

Let **Wells Fargo Foothill** find the solutions for your company's needs.

Call or visit us online to learn more.

WELLS FARGO

The Next Stage®

At **Wells Fargo Foothill**, our **Technology Finance** team is dedicated to providing flexible, innovative senior secured financing solutions to the software and technology sectors. From $10 million to $1 billion and more, our credit facilities can be tailored to address the unique needs of a range of business models, including:

- **Perpetual license**
- **SAAS (software-as-a-service)**
- **Hosted solutions**

And as part of Wells Fargo & Company, we also offer our customers direct access to a wide range of additional financial products and services.

(877) 770-1222

wffoothill.com

Developing **RELATIONSHIPS.** Providing **SOLUTIONS.®**

IT INFRASTRUCTURE

CMDB Aims To Be Single Source Of TRUTH

Every week, IT inboxes fill up with announcements, articles, webcast invitations, and case studies related to configuration management databases (CMDBs). Yes, it's a barrage, but it is fueled by some very real needs. IT organizations are desperately trying to improve collaboration between silos of technology expertise, bridge the gap between business performance demands and IT support activities, and improve the relationships among development, testing and operations groups.

Many of these problems exist because infrastructure management information is not accessible beyond a specific management application. Service desks, software provisioning tools, networking tools, server management products, and so on all store configuration information separately, in different formats. This makes it extremely difficult to audit, correlate, and analyze information across different technologies to answer a specific question, whether it is something as simple as, "How many servers do we have?" or something more complex, such as, "What services will this database change affect?"

While information access and sharing does not heal all wounds, it does go a long way toward bridging the communication gaps that have been part of IT organizations for much too long. Hence the seductive appeal of a solution that can be a "single source of truth" for all of the configuration and dependency information about technologies and business services. It can serve as an automation catalyst for any number of collaborative processes and tasks, because IT and business staff can access the subsets of information they need to perform tasks or make decisions.

Information Technology Infrastructure Library (ITIL) represents this "single source of truth" as a repository and, as ITIL's popularity has skyrocketed, so has its naming convention—the CMDB. (See "What's In the Name?" p. 18.) Needless to say, vendors have been working hard to deliver products to meet the growing demand. BMC Software was first out of the gate with a solution capable of federating information from multiple existing management tools, and it is now promoting the ROI of early adopters. CA and IBM Tivoli released their solutions last year. HP, EMC and Symantec have made several key acquisitions, and Microsoft is launching SystemCenter. Much of this vendor activity has focused on providing the technology as well as the process templates and scenario planners that will help customers and prospects make the

A CMDB must achieve specific goals to be successful; Advice: prioritize the issues, map IT processes to those issues; Then determine data each person needs to get the job done

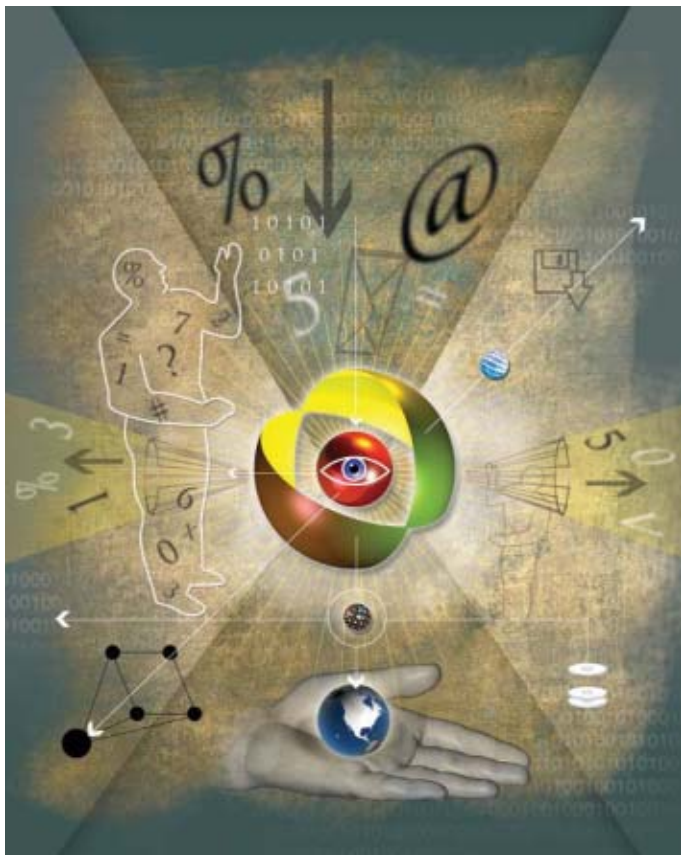
BY JASMINE NOEL

journey from the idealized concept of a CMDB to a workable implementation.

Yet for many enterprises this is still an exhausting journey. It is easy to get bogged down with any number of questions. Does a CMDB replace asset management or service desk solutions? Who owns the CMDB and the data it contains? What is the underlying data model, and how extensible should it be? Amid all of these important questions, one thing is clear—if it is to be successful, a CMDB must be implemented in the context of achieving specific goals. Enterprises have no patience for grandiose integration projects; too many of these have sunk to the bottom because planners only focused on the tip of the iceberg.

To melt the iceberg into manageable ice cubes, many IT organizations are paying more attention to the planning process by doing the following:

- Prioritizing CMDB issues according to business impact
- Determining which IT processes address the issues and which people are involved in those processes
- Determining the type and currency of data each person needs to complete his or her part of the process
- Matching requirements to vendor capabilities.



Prioritize CMDB Issues

This first step is important for three reasons. First, it is crucial to get executive buy-in and leadership for any project that spans different organizational groups. By starting with the issue that is most visible and important to key executives, IT can garner the level of interest and support it needs to keep the CMDB project on track. Second, this prioritization helps secure IT's position as a business enabler, because by doing so it aligns its efforts with specific business goals. IT organizations that are viewed solely as maintenance groups are more likely to find themselves under budget and outsourcing pressure. Finally, by understanding the business impact, IT can determine the metrics it needs to document to gauge the success of the CMDB project.

There are many potential starting points: problem resolution, for example, is a favorite for many enterprises. The evidence is mounting that many service outages are self-inflicted by ad hoc configuration changes. A 2005 survey of 227 J2EE application managers listed configuration and tuning problems and changes to applications as two of the top three causes of application failures. Services are delivered by a wide range of distributed, heterogeneous, interacting technologies: therefore, seemingly innocuous changes to a server configuration can have far-reaching service performance and availability implications. Finding that single problematic configuration change within a complex maze of technology is extremely difficult without the ability to map all the resources associated with the service and quickly compare "before and after" configurations of those resources. Anywhere from 60 to 80 percent of mean time to repair is spent trying to determine the source of the problem and what has changed.

This is where a CMDB comes in handy. It can be designed to contain models that describe how resources interact with each other to deliver a service, configuration details about each resource, and historical information about the relationships and configurations. Access to this type of information allows support teams to find and fix problems faster, thereby minimizing the financial risks to the business.

Policy and regulatory compliance is another hot issue that focuses a lot of attention on configuration and change management. Many governmental regulations require some means of documenting that an enterprise has active control over the ways in which its infrastructure changes. Similarly, enterprises are looking to minimize their security risks with active configuration and change controls. CMDBs are at the heart of configuration and change management processes. The idea is to represent various configuration states (actual, ideal, and planned) so that IT can both perform and document the comparisons needed to determine infrastructure compliance with authorized policies. The goal here is to improve the level of compliance as well as to reduce the cost of audit reporting.

While much of the focus for CMDB deployments centers around cost reduction, some enterprises are more concerned with business agility. The rate of deployment of new applications continues to increase; more companies are moving new applications into production on a weekly and monthly basis. I worked on benchmarking studies with CA Wily in

which we found that in 2005, over a period of less than two months, 47 percent of J2EE application managers reported new application deployment cycles, compared with 33 percent in 2003. Add to that Forrester's report that the average failed change requires 25 hours of IT staff remediation effort, and you will see that IT simply cannot support that level of application change without solid controls in place to get the deployments right the first time. A study of 98 companies performed by the IT Process Institute (www.itpi.org) showed that top IT performers were able to implement five times more changes—with a 12 percent better success rate of infrastructure changes—than the group of medium performers.

In this case, the CMDB becomes the repository holding answers to such risk assessment questions as, "What other assets are dependent on the targets of the proposed change?" or, "What business services are affected by the change?" This type of information dramatically simplifies the risk assessment process. As one ITPI interviewee put it, "It is not that we don't make mistakes anymore but that we have become more scientific in our approach to mistakes. Mistakes are seen more as learning experiences, and the mistakes have become fewer and farther between."

What's in the Name?

It is my opinion that the term "CMDB" is probably the worst possible name for such a solution. The "DB" implies a physical database product that one can potentially buy off-the-shelf and populate with information so that users can start running reports against it. This is impossible because IT's information is too changeable. Information copied into a database on Monday would be inaccurate by Tuesday. Although the name is likely here to stay, my hope is that enterprise CMDB projects will be designed not as static data marts, but as steps toward a dynamic information system that supports collaboration. (Unfortunately, DISTSC is a horrible acronym. If you have a better version, let me know at jnoel@ptaknoelassociates.com.)

—Jasmine Noel

Processes and People

Regardless of the starting point chosen, understanding the processes and people involved is critical, because ultimately the project is about improving and streamlining collaboration. Collaboration among diverse groups with different agendas does not happen naturally. While CMDBs can be implemented as physical technology, actual adoption and use of CMDBs is a highly political process. This is true for both large and small IT organizations. Each group or individual must experience the benefits of the CMDB implementation; otherwise, expect adoption to stall.

For example, an enterprise can map out a problem management process that starts with identifying a specific infrastructure event and continues with assessment of the business impact, assigning responsibility, and so on. Yet the map should also include the individuals involved and the lists of benefits each would receive should a CMDB be implemented. (See Fig. 1.)

There are many process templates from vendors and consulting organizations that can help IT start this mapping activity. We adapted BMC's workflow diagrams for the examples in this article. IBM Tivoli Unified Process (ITUP) is a free downloadable tool that provides detailed documentation of processes and role responsibilities based on industry best practices. CA has process maps, demos, educational services and acceleration programs. Best-practices templates and kits are available from organizations such as Pink Elephant and the IT Process Institute.

The process determination step is also important for limiting the inevitable scope-creeping tendencies. Since a CMDB is the foundation on which every IT process rests, early projects are particularly prone to scope creep. Once the planning is started, it is easy for folks to keep adding new issues, considerations and requirements. These add-ons can be difficult to rein in if the processes and constituents are not identified early.

Measuring Success

To gauge CMDB success for problem resolution projects, look at business-oriented metrics such as tracking reduction in Service Level Agreement (SLA) penalties or revenue loss, and IT process metrics such as reduction in time involved with technical assistance calls or number of personnel involved per troubleshooting incident.

To gauge CMDB success for compliance-related projects, look at metrics such as the number of unauthorized changes, or the number of hours of staff time needed to manage audit reporting.

To gauge CMDB success for agility projects, look at metrics such as the cycle time for change management process, the rate of change failures, the rate of software and update deployments, and the size of staff needed to support the changes.

—Jasmine Noel

Information Needs and Sources

Once the processes and people involved are determined, the focus shifts to understanding the actual details of the information itself.

What are the actual information needs of the people and processes involved? This requires understanding the type of information involved, the level of detail needed, how current and secure the data must be, and what types of collaboration are needed to perform various decisions and tasks. In the problem resolution workflow example, operations staff require access to service-infrastructure dependencies to assess the impact of the event, but not detailed configuration details about each device. However, the currency of the dependency information may vary. For example, enterprises with virtualized server infrastructure may require real-time dependency information for accurate impact analysis. These considerations make each enterprise CMDB implementation unique.

Where is the information stored? The data sources question is very interesting, because almost every management

tool has an internal database that stores some level of information about the infrastructure it is managing. Therefore, implementing a CMDB will require an approach to:

Data reconciliation, for resolving conflicting data resident in different information sources about the same configuration item. Reconciliation is usually implemented as policies that designate specific tools as the trusted source for specific types of information.

Data federation, for communicating with these existing management tools. One federation approach is to replicate and store in a central place reconciled, core information about configuration items and pointers to more detailed data in specific management tools. (See Fig. 2.) The details of the scope of that core information can be driven by the needs of a specific common task. Another federation approach eschews data replication and instead depends on policies to reconcile and coordinate information dynamically accessed from existing management tools. Both approaches can be used to implement various management processes, and the choice could be driven by performance and scalability of the specific solution being considered.

How should the information be maintained? Data maintenance has delivered the killing stroke to countless attempts at implementing shared configuration data in the past. Every administrator can attest to having seen inventory lists become useless within days or weeks of initial creation. True, automated discovery and reconciliation of inventory, configuration, and relationship information have significantly improved over the last five years, and thus successful collection of accurate CMDB information directly from the infrastructure itself is a more realistic proposition. Yet integrating this automatically collected information into the CMDB raises several issues. The CMDB must have the ability to represent different configuration states, such as the actual configurations of technologies in the production environment (which may include ad hoc or unapproved changes) and the ideal or approved configuration of technologies in the production environment (which is consistent with approved change processes and compliance policies). The data management processes that synchronize and resolve these different datasets must be explicitly understood for the CMDB to retain its use as the various processes and people adapt and change infrastructure information over time.

Organizations that take the time to understand their actual data sharing needs will get a good understanding of the type of CMDB implementation that will be successful.

Buyers Guide: Configuration Management Database Tools & Services

Company	Focus Area(s)	Products	Services
AixpertSoft GmbH	CIM, CF, ITSM, NM, PC, SIA, SP	x	
AlterPoint	AD, CIM, CF, CS, DF, DIR, DSL, DDM, NM, RTCT, RT, SEC	x	x
BladeLogic	ADM, AD, CIM, CF, CS, DF, DIR, DSL, DDM, IT, ITSM, PC, RTCT, RT, SEC, SCC, SIA	x	
Blazent	AD, DIR, ITSM	x	x
BMC Software	ADM, AD, CIM, CF, DF, DIR, DSL, DDM, IT, ITSM, PC, SIA	x	x
BPMspace	AD, CIM, CF, CS, DF,ITSM, PC, SEC, SIA	x	x
CA	ADM, AD, CIM, CF, CS, DF, DIR, DSL, DDM, IT, ITSM, NM, PC, RTCT, RT, SEC, SCC, SIA, SM, SP	x	x
Caimit	ADM, CIM, CF, DF, DDM, PC, SEC, SIA	x	
easyCMDB	ADM, CIM, CF, DF, DIR, ITSM, NM, PC, SEC, SIA	x	
Ecora	AD, CIM, CF, ITSM, SP	x	
EMC*	ADM, AD, CIM, CF, DDM, ITSM, NM, RTCT, RT, SM	x	
Emu Software	CIM, CF, CS, PC, SEC, SCC	x	x
Escape-K	CF, SEC, SP	x	
GridApp	CF, SEC	x	
HP	ADM, AD, CIM, CF, CS, DF, DIR, DSL, IT, SIA	x	x
IBM	ADM, AD, CIM, CF, CS, DF, DIR, IT, ITSM, NM, PC, SCC, SIA, SM, SP	x	x
Infra Corporation	AD, CIM, CF, CS, DF, ITSM, NM, SCC, SIA	x	x
Interlink Software	ADM, AD, CIM, CF, DF, DIR, DDM, IT, NM, PC, RTCT, RT, SCC, SIA, SP	x	
Managed Objects	ADM, AD, CIM, CF, DF, DIR, IT, ITSM, NM, RTCT, SCC, SIA, SP	x	
mValent	CIM, CF, DF, DIR, ITSM,SIA	x	
N(i)^2	ADM, AD, CIM, CF, CS, DF, DIR, DDM, IT, ITSM, PC, RTCT, SIA	x	x
OneCMDB	ADM, AD, CF, DIR	x	
Opalis	AD, CF, DIR	x	
Opsware	ADM, AD, CF, DF, DIR, IT, ITSM, NM, PC, RTCT, SEC, SCC, SM	x	
Oracle	ADM, AD, CIM, CF, CS, IT, ITSM, NM, SEC, SCC, SIA, SP	x	x
OutSystems	APPDEV, AD, ITSM, NM, RT	x	
Planet Associates	CIM, CF, DF, DIR, DSL, DDM, IT, PC, SIA	x	
ProcessWorx	ADM, AD, CF, DIR, ITSM, PC	x	
RealOps	AD, CS, ITSM, NM, SIA	x	x
Service-now.com	ADM, AD, CIM, CF, DIR, IT, ITSM, NM, SIA, SM	x	
Symantec (Altiris)	ADM, AD, CF, DIR, ITSM, SCC, SP	x	x
Tideway Systems	ADM, CF, CS, DIR, IT, SIA	x	x
Tripwire	AD, CIM, CS, CF, ITSM, PC	x	x
Voyence	CIM, CF, DF, DSL, NM, PC, SEC, SIA	x	x
Zenoss	ADM, AD, CF, CS, IT, ITSM, NM, SCC	x	x

Key to Focus Areas

ADM	Application Dependency Mapping
APPDEV	Application Development
AD	Automated Discovery
CIM	Change Impact Management
CF	Configuration
CS	Consulting
DF	Data Federation
DIR	Data Integration & Reconciliation
DSL	Definitive Software Library
DDM	Dynamic Dependency Mapping
IT	Infrastructure Topology
ITSM	IT Services Management
NM	Network Management
PC	Process Centric CMDB
RTCT	Real Time Change Tracking
RT	Real Time CMDB
SEC	Security
SCC	Server Consistency Check
SIA	Service Impact Analysis
SM	Storage Management
SP	Systems Performance

• sponsor

Vendor Matching

Once you understand your own needs, plan and vision, then you can start the search to find a vendor—not a simple task, for several reasons. It can be hard to keep from rolling your eyes at the nearly identical marketing blurbs on every vendor's website. Yet an important part of the selection process is understanding the vendor's vision or design concept.

A design concept is made up of the assumptions and ideas behind a product's development and implementation. For instance, what problem is the vendor intent on solving? What are the vendor's assumptions about the environment in which the problem exists? How does it see the evolution of IT's operational processes as the solution is adopted? These seemingly fuzzy questions are important, because the vendor must be an active partner in the success of the CMDB project. These are not throw-away projects that can be readily scrapped and restarted. Instead, they are the foundations upon which IT can continuously improve the performance of its business in the future. The success of the initial implementation and long-term enterprise-vendor partnership is often tied to how well vendor answers overlap with enterprise answers to these types of questions and will be the topic of our upcoming research reports.

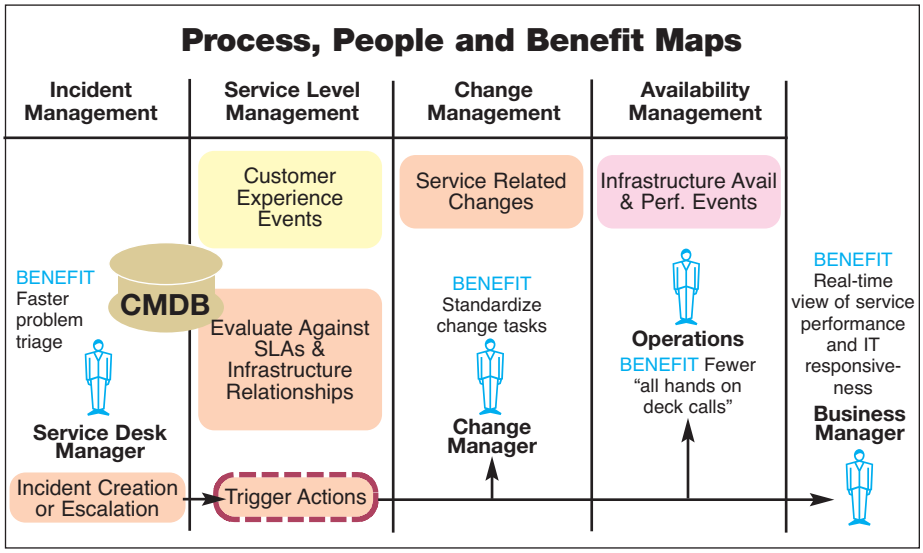


Figure 1

Another problem is the tendency to zero in on features the vendor believes are differentiating regardless of their applicability to the particular enterprise situation. The goal is to remain focused on your needs for:

- Visualizing the available information
- Representing various information needs in terms of type, level of detail, currency, and so on
- Reconciling conflicting information
- Federating and integrating information with existing solutions
- Managing different states of configuration

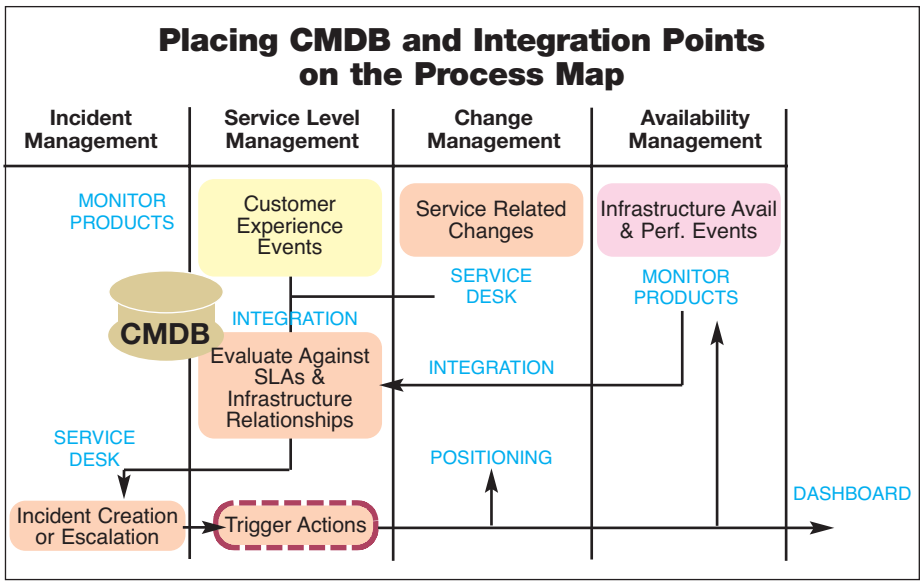


Figure 2

and dependency information—current, approved, pre-production, and so on.

Is That All?

Of course not! There is always something to consider—the CMDB standards that the vendors are working on, process automation technologies, auditing capabilities, SOA-based data integration—the list goes on forever. However, the planning process is complicated enough as it is. The key is staying focused on what is important—business goals, processes, and people and their information needs. Only then does it make sense to start talking about the technology needed to support them.

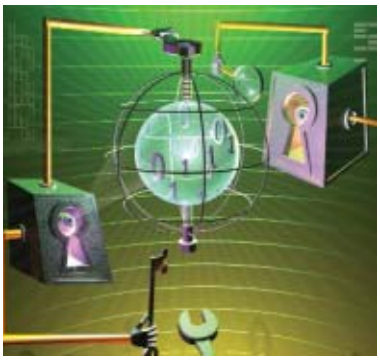
The software vendors are increasingly aware that this is not just a technology feature race—the evidence is in their process-related offerings, their brand simplification, and their sales-force retooling. Yet the competition will be intense. CMDB solutions are fundamental and, if initially successful, can open up any number of other projects for both IT and its vendor partner. This is why CMDB evaluations must be entirely driven by actual IT needs and realistic business goals. SW

Jasmine Noel, of Ptak, Noel & Associates, focuses on converging IT trends and how to leverage them. The company follows trends in ways that help IT directors translate executive strategies into action blueprints. Visit: www.ptaknoelassociates.com.

SECURITY

SECURITY REQUIREMENTS Engineering: A Road Map

Developers are often blamed for software security mishaps and punished through losses in wages or embarrassed on walls of shame.[1] At Foundstone, we believe developers, for the most part, don't write insecure code intentionally or because they are negligent; they do so because they haven't been taught any better and don't receive adequate help and guidance from other stakeholders.



Essentially, when dealing with software security, it is a common failure to focus too much on the development phase of the software development lifecycle and not enough on the others. This article, therefore, focuses on security requirements engineering, one of three key support activities that can help tremendously in improving the security of projects churned out by your development teams. The other two areas—security acceptance testing and security knowledge management—will be covered in a future article.

The security community and industry has evolved tremendously since the late '80s, when the first "security attack" was perpetrated in the form of the Morris Worm. This led to the creation of the Computer Emergency Response Team, or CERT, as it is popularly known. For the next decade or so, the industry focused on securing the network and, to a lesser extent, on securing the host. As a result of this, the major security technologies of that era were the devices and software we almost take for granted today—firewalls, intrusion detection systems, and virus scanners.

However, as the Internet exploded and the World Wide Web went from being an academic network of computers to a platform upon which business was done, the threats also evolved. Now the attackers began to attack not just the network and the host, but the applications that sat on top of them as well. In many ways, these applications represented the crown jewels—the confidential data, the precious intel-

A lack of security requirements leads to insecure software; proper planning, however, can enhance the security of a software development lifecycle

BY RUDOLPH ARAUJO

Security requirements engineering can help tremendously in improving the security of projects churned out by your development teams.

lectual property and business intelligence that organizations and indeed consumers did not want to lose.

Increasingly, organizations succeeded in getting their "ducks in a row" on the network and host side, as tried and tested solutions became available. At the same time, however, development teams were struggling with securing the application. Enter new methods of attack such as buffer overflow, SQL injection, and cross-site scripting; the list could go on.

So how have we dealt with this problem over the last few years? As one would expect, the first attempt was a variation on not dealing with them at all: developers released software, hoped for the best, and then fixed issues as they were publicly reported. Next came the phase of penetration testing a few weeks or days before going into production. This, again, provided little time to effectively fix the issues discovered. As an industry, we continued to evolve, and the next phase was to go hunting through code for the common classes of vulnerabilities that were in the news—whether these were buffer overflows in the '90s, or common Web application vulnerabilities more recently.

The more strategic of the organizations at this point invested in software security training and building policies, such as language-specific coding standards to aid their developers in dealing with the problem and to prevent the introduction of future vulnerabilities.

The focus from the beginning has been on developers and the development phase, for the most part; and only rarely has it touched on the secure design elements. As a consequence of this focus, it has become almost instinctive to blame developers and hold them responsible for vulnerabilities in the application. If something goes wrong, it must be the developer's fault—especially now that we have a firewall and a secure coding standard!

Holistic Software Security

Unfortunately, it appears that as a community we, the software security folks, have not learned as much as we should have from the decades of research into software engineering. If you treat a security vulnerability as a bug first and a security issue second, you can quickly adapt many of the lessons that have been learned with regard to improving the security of software applications.

Software security must be viewed holistically. It is achieved through a combination of effective people, processes and technology, with none of these three capable of fully replacing the other two. This also means that, as with software quality in general, software security requires that we focus on it throughout the application's lifecycle—or from cradle to grave, as some like to say. Unfortunately, thus far most of the effort has focused on activities such as application penetration testing, security code reviews and, to a lesser extent, on threat modeling.

While all of the aforementioned activities are critical to improving the security of your applications, they are by no means the only ones. Unfortunately, as both a community at large and individuals looking to tackle the software security problem in our development teams, we have tended to ignore the non-developer-focused activities. In this article we present one of these activities.

Before we get too far, it helps to define a common frame of reference to view software security problems and solutions. Our Foundstone Security Frame[2] helps us better prepare for going into a software development project as well as to perform better root-cause analysis when faced with vulnerabilities. (See Table 1.) In the context of this article, we will use it to help us be more efficient, effective, and thorough.

Security Requirements Are Key

One of the most ignored parts of a security-enhanced software development lifecycle is the security requirements engineering process, and one of the prime reasons for this oversight is that security is assumed to be a technical issue and therefore best handled during architecture and design or, better still, during implementation. Since software requirements are often written by non-technical business analysts, this is a common conclusion.

The problem with this approach, as any experienced software professional will tell you, is that software that does not have its requirements elicited, enumerated, and well-documented will most likely be lacking in quality. This is because its developers do not have a specific target with regard to building security into its design and implementation. Further, quality assurance folks have no benchmark to validate the software against, and traceability—a key software engineering attribute—is unachievable. In fact, it is hard even to build a good threat model without a clear idea of the security requirements.

This is a well-understood concept in the general field of software engineering. A lot of research[3] has been performed on how to effectively elicit, validate, and document software requirements. Further, most modern System Development Life Cycle (SDLC) support tools already provide some mechanism for documenting requirements.[4] Hence, it should not be too difficult to extend these systems and the process itself to include security requirements.

The challenge, however, as mentioned above, is that most organizations we work with are used to thinking solely about functional requirements—requirements that the system and business analysts writing them can put their arms around. (For instance: Should the application have this particular widget, or that one? And how should it respond to the click of a button in the top right corner?) The non-functional requirements, on the other hand, are often marked as "N/A." Our findings have been that this is not necessarily because they are considered unimportant, but rather because they are assumed to be de facto requirements—"the developers should know better than to build a slow or insecure or unreliable system." The assumption always seems to be that these requirements are obvious and hence don't need to be documented.

On examining this problem a little bit further, we discovered that to a large extent the difficulties lay in the lack of awareness and knowledge of the people writing the requirements. The non-functional requirements can be very technical—consider the specification of the encryption algorithm, cipher mode, key lengths and rotation parameters. Defining requirements around all of those would typically require a detailed understanding of the mechanisms around cryptography—not something that is typically found in the job description of a business analyst.

As a solution to this issue, we present a template-driven approach designed specifically to help the non-technical stakeholder define very technical security requirements. Although creating the templates does involve some effort, we have found it to be tremendously effective in ensuring that security requirements are documented (and not just with "N/A"!) as well as implemented and tested.

The first step on this path is for an organization or team (depending on the size and variety of applications involved) to identify all the drivers for security requirements that would, could, and should influence development. In our experience, most often you will see a lot of commonality among the various applications developed within the organization or team, and hence we attempt to leverage that commonality and thus gain efficiencies across multiple projects.

In our experience it is best to think about these drivers along the following categories. As mentioned above, most of them will influence many, if not all, of the applications churned out within an organization.

Regulatory Compliance:[5] This involves specific requirements that would be mandated by various governmental agencies. Depending on the application's scope as well as the legal environment within which the organization operates, a number of regulations may be relevant. Some of these include:

- Sarbanes-Oxley, Section 404
- Health Insurance Portability and Accountability Act
- Payment Card Industry Data Security Standard
- Gramm-Leach-Bliley Act
- SB 1386 and other state notification laws
- Basel II
- Federal Information Security Management Act
- EU Data Protection Directive
- Children's Online Privacy Protection Act
- Local key escrow laws

Industry regulations and standards: These include standards that are specific to an industry: financial services, for instance. This category in our classifica-

Security Frame of Reference

Configuration Management: As part of this category, we consider all issues surrounding the security of configuration information and deployment—for instance, any authentication and/or authorization rules embedded in configuration files, or how the framework and application deal with error messages.

Data Protection in Storage & Transit: Here we consider the handling of sensitive information such as social security numbers, user credentials or credit card information. This category also covers the quality of cryptographic primitives being used, required/minimum key lengths, entropy and usage vis-à-vis industry standards and best practices.

Authentication: Of concern here is the usage of strong protocols to validate the identity of a user or component. Issues such as the possibility or potential for authentication attacks such as brute-force or dictionary-based guessing attacks also fall under this category.

Authorization: This would cover problems of finding appropriate mechanisms to enforce access control on protected resources in the system. Authorization flaws can result in either horizontal or vertical privilege escalation.

User & Session Management: The quality of session identifiers and the mechanism for maintaining sessions are some of the considerations here. Similarly, user management issues such as user provisioning and de-provisioning as well as password management and policies are covered as part of this category.

Data Validation: This is the category responsible for battling the most well-known bugs and flaws including buffer overflows, SQL injection and cross-site scripting. Length, range, format and type checking for inputs and outputs are considerations here.

Error Handling & Exception Management: Here we ensure that all failure conditions—errors and exceptions, for instance—are dealt with in a secure manner. The issues covered range from detailed error messages, which lead to information disclosure, to questions of how user-friendly security error messages are.

Auditing and Logging: This category is concerned with how information is logged for debugging and auditing purposes. The security of the logging mechanism itself, the need and presence of an audit trail and information disclosure through log files are all important aspects.

Table 1 Source: Rudolph Araujo of Foundstone

In some cases, it is best to work with the legal department and internal auditing to arrive at a list of regulations relevant to a given application.

tion is also set up to include standards bodies such as ISO and the norms they define. Examples include:

- ISO 17799
- FFIEC Information Technology Examination Handbook[6]
- SCADA security[7]
- OWASP standards[8]
- OASIS[9]

Company policies: Most organizations that we work with have a slew of internal policies that should and could affect the development of an application. Among the most common are the following:

- Privacy policies
- Coding standards
- Patching policies
- Data classification policies
- Information security policies
- Acceptable use policies
- Export control
- Open source usage
- Results from previous security audits

Security features: Most applications will have some form of security feature: for instance, authentication and authorization models that replicate real-world, role-based access control, or administrative interfaces that will be used for user management, including provisioning and de-provisioning.

In some cases, it is best to work with the legal department and internal auditing to arrive at a list of regulations relevant to a given application. Once that list has been defined, the next step is to examine each of these regulations from a legal viewpoint, as well as the viewpoint of a software development expert. The aim is to convert the list of legal requirements to a set of core technical requirements.

The Foundstone Security Frame can come in extremely handy here. For each of the relevant drivers, consider the various categories in the Security Frame and how they might be impacted. For instance, if your organization is regulated by the Gramm-Leach-Bliley Act (GLBA), privacy of personally identifiable information (PII) is absolutely critical. This in turn can have implications across multiple Security Frame categories, not the least of which is Data Protection in Storage & Transit. The outcome of this step should essentially be a set of specific requirements along the various Security Frame categories that would satisfy each of the applicable drivers defined above. It is also vital at this stage to study the requirements above in order to avoid having to meet overlapping or redundant requirements.

A parallel step in this requirements process is to classify the applications in terms of how they are impacted by the drivers. This is best done by creating a large matrix, with the drivers forming the columns and the application set forming the rows. Classification then is the task of checking the appropriate boxes depending on whether, based on legal and other opinions, an application is affected by a specific driver.

As a result of the two parallel steps mentioned above, the team should now have a specific set of technical requirements for each application based on its requirement drivers. All of this effort is intended to be performed only once and then revisited periodically. In our experience, it is very rare that these drivers change with each application release, or even particularly frequently. This is primarily because applications tend to evolve very slowly with regard to the drivers mentioned above. Further, as mentioned above, there is much opportunity to leverage commonality across applications, since it is not atypical for many of the applications to be operating within a similar driver environment.

Having now defined this universal set of requirements a priori, as each application release is defined, the specific set of requirements for that release can be drawn out of this set. As part of the process, the data classification and privacy policy can help to identify which data elements handled by the application are affected by the drivers. It is also important to consider features that might be added in this release, and whether they will be affected as well. Based on these pieces of input and the universal set of requirements, a subset of those requirements will be obtained that are relevant for this specific release of this specific application.

The person formulating these requirements now does not need to be an expert in security or in any of the Security Frame categories; he or she can simply check the appropriate boxes to obtain a set of requirements. In fact, this last application step can be easily automated through a template or lightweight application that references all the relevant policies as well as the universal set of requirements, considers the data elements in use, and provides a set of technical requirements that may leverage encryption and access control and other security mechanisms. These can then literally be copy-pasted into the master requirements list.

To wrap up, let us consider an illustrative example. Take, for instance, an online loan processing application. Such an application will obviously make extensive use of personally identifiable information and is determined to be affected by the GLBA driver. This in turn defines specific requirements around confidentiality, integrity, availability, and access to data as well as audit trails that monitor and report on such access.

Now, consider that a new feature is being added that e-mails the result of

Buyers Guide: Secure Application Development Tools & Services

Company	Focus Area(s)	Products	Services
ActivCard Corporation	CA, SM, TR	x	
Aladdin Knowledge Systems Ltd.	CA, SM	x	
Altiris	AS, PM, SA	x	x
Application Security, Inc.	AS, PM, SA	x	x
Aspect Security	CR, PI, SA, TR		x
Beyond Security	AS, CR, SA	x	x
Black Lab Security Systems (BLSS)	AF, AS, CA, SA	x	x
BMC	AS, PI, PM, SA	x	
Breach Security	AF	x	
Check Point Technologies	AF	x	
Cigital	PI, SA		x
Cisco	AF	x	
Citrix	AF, AS, SA	x	
Compuware Corp.	CR	x	
Crosscheck Networks*	AS, SA	x	
Devon IT	MSS		x
Entrust	AS, CA	x	x
F5 Networks	AS, CA, SA	x	x
Fiberlink Communications Corp.	AF, CA, PM	x	x
Fortify Software	CR, PI, SA, TR	x	x
Foundstone, a McAfee Company	CR, PI, TR		x
GemPlus	SA, SM	x	x
IBM	AF, AS, CA, MSS, PI, SA	x	x
Imperva	AF	x	
Integrigy Corporation	AS, PM, SA	x	x
Internet Security Systems	AF, AS, MSS, PM, SA, TR	x	x
Juniper Networks	AF	x	
Klocwork	AS, CR	x	
Layer7	AF	x	
Logic Library	AS, CR	x	
McAfee, Inc.	AS, PM	x	x
Microsoft	TR		x

Company	Focus Area(s)	Products	Services
NetContinuum	AF	x	
NGS (Next Generation Security) Software	SA, TR	x	x
Ounce Labs	AS, CR, PI, SA	x	
Panda	AF, MSS	x	
Parasoft	CR	x	
Patchlink	PM, TR	x	x
PortWise, Inc.	AS, CA, SA	x	
PreEmptive Solutions	CR, PM	x	x
Proginet Corporation	SA	x	
Protegrity	AF, AS	x	
Radware	MSS, SA, TR	x	
RSA Security	CA, SM	x	x
SafeBoot	SA	x	x
SafeNet, Inc.	CA, SA, SM	x	
Secure Software	CR	x	x
Secured Dimensions	CR	x	
SPI Dynamics	AS, SA	x	x
St. Bernard	AS, PM	x	
Sun Microsystems	SM	x	
SurfControl Plc	AS	x	
Symantec	AF	x	
Symark Software	CA, SA	x	
Teamstudio	CR, PI, SA	x	x
Thawte	CA	x	
Trend Micro	AS	x	
Tumbleweed Communications	AF, CA	x	
Vericept Corporation	AS, SA, TR	x	x
Verisign	CA, MSS	x	x
Watchfire	AF, AS, SA	x	x
WatchGuard Technologies	AF, MSS, SA	x	
Websense, Inc.	TR	x	

• source

Key to Focus Areas

AF	Application Firewalls	**MSS**	Managed Security Service	**SA**	Security Audits
AS	Automated Scanning	**PM**	Patch Management	**SM**	Smart Cards
CA	Certification Authority	**PI**	Process Improvement	**TR**	Training
CR	Code Review				

the loan decision to the customer. When a business analyst is defining the requirements around this new feature, he or she would need to consider all of the different data elements that would be part of this e-mail, the transport mechanism used by the e-mail, and the authentication around it. Based on business need and security, it can then be decided to avoid certain data elements, or perhaps use a secure e-mail solution.

We believe security requirements engineering should exist as part of a security-enhanced software development lifecycle if it is to be successful in improving the security of your applications. This is non-traditional, in the sense that it does not merely go after the development phase of the lifecycle. However, in our experience, having helped a number of large organizations implement a secure development lifecycle, we believe that without getting this part of the puzzle correct, your team will not achieve the best possible results from any investment into software security. SW

Rudolph Araujo serves as a principal software security consultant and trainer at Foundstone Professional Services, a division of McAfee. He is responsible for creating and delivering the threat modeling, security code review, and secure software engineering service lines, as well as for content creation and training delivery for Foundstone's Building Secure Software and Writing Secure Code - ASP.NET and C++ classes.

1 http://news.zdnet.co.uk/software/developer/0,39020387,39228663,00.htm
2 http://www.codesecurely.org/wiki/
3 http://en.wikipedia.org/wiki/Requirements_analysis
4 http://msdn2.microsoft.com/en-us/teamsystem/default.aspx
5 http://msdn2.microsoft.com/en-us/library/aa480484.aspx
6 http://www.ffiec.gov/ffiecinfobase/index.html
7 http://www.sandia.gov/scada/standards_and_outreach.htm
8 http://www.owasp.org/index.php/Category:OWASP_Guide_Project
9 http://www.oasis-open.org/

softwaremag.commentary

INDUSTRY INSIDER'S VIEW

By Cindy Lafrance

Filet Mignon or Peanut Butter?

What do you want for dinner: filet mignon, or peanut butter and jelly (PBJ) sandwiches? Seems like a no-brainer to me—how about you? Who would ever take PBJ over filet mignon? But we do it all the time when we build applications and systems. ■ A colleague and I recently found ourselves in a heated discussion regarding a dilemma that is more common than imagined.

I was pressing for an application to contain a specific set of functions while Mike, my colleague, was reiterating the cold, hard budget realities that would absolutely limit our team's ability to deliver all the functions the market wants.

At one point we recognized the real issue. Were we leading by market requirements or by budget? Would we deliver filet mignon or PBJ sandwiches? It's a derivation of the age-old chicken-or-egg debate: What comes first, the mission or the budget? And the answer, of course, is (drum roll, please) the budget. But when do you acknowledge the power of the budget over the mission? Before you order the filet mignon? Or later, when you're washing the dishes to pay the bill?

Imagine this—your objective is to replace an existing business application and computing platform with the latest and greatest technology. There's only one small problem: The budget for your application was set in concrete before the requirements were defined. Not only has the objective been defined, but so has the budget for accomplishing the objective.

Sound familiar? Have you ever been responsible for delivering a solution without the requisite staff, tools or technology? Have you been a member of this team? It happens more often than not. The conflict between mission objectives and budget realities is one that plays out in every organization.

In the requirements evaluation work that we typically do, it is rare to consider the budget impact until after we collect and prioritize the requirements. By then, it is too late. Potential users and team members are intoxicated with what they want. Invariably we have sown the seeds of user and employee dissatisfaction. "This isn't what I wanted," they will cry. Developers will remember the really cool features they wanted to build, and the seeds of "While I'm in the code, I might as well change this too" will create features that the QA staff cannot test.

Think you can resolve this situation with phased implementations, milestone releases, or an Agile development process? Not unless you find a way to elicit requirements without promising specific implementations. Not unless you find a way to institutionalize the concept of minimum essential design and solve problems in a manner that satisfies the filet mignon appetite within the PBJ budget.

How can you do this? First, hold open a space for creative possibilities. Perhaps the greatest gift you can give your project team is to acknowledge the budget realities at the same time you receive the application requirements. Acknowledge the reality without passing judgment and allow your team to discover what they can do. It's very likely your team can surprise you.

As for Mike and I, we agreed that holding open a space for creative possibilities requires new language between the two of us as key leaders on the project. We talk about what we *can* do—not what we cannot do. And we constantly ask, "Is there a better way to meet this requirement that supports both our vision and cost constraints?" Funny, but when we ask this question, our application users and staff come up with new answers.

And maybe that's the secret to the chicken-and-egg question. Not "Which came first?" but "How can we have both?" With new questions come new results. And that is our creative possibility. Never underestimate the power of your questions. SW

Cindy Lafrance is the founder of Lafrance International, an Austin-based strategic marketing firm focused on enabling high-tech firms to understand what their prospects want. She can be reached at cindy@cindylafrance.com.

www.softwaremag.com

Advertising Sales

National Sales Director
Carol Samost

csamost@softwaremag.com
PHONE: 617-962-4725
FAX: 508-668-0442

MAILING ADDRESS:
Software Magazine
P.O. Box 135
E. Walpole, MA 02032

Contact Sales Director for information on:

- Advertising packages
- SoftwareGram E-mail newsletter sponsorships
- Reprints

ADVERTISER INDEX

DIGITAL SOFTWARE MAGAZINE
The Software Decision Journal

SOFTWARE Marketing Perspectives

CONFERENCE & EXPO

4th annual

Software Marketing Perspectives Conference & Expo

May 7-9, 2008

Santa Clara Convention Center
Santa Clara, Calif.

The fourth annual Software Marketing Perspectives Conference & Expo – the leading event for software industry product managers and marketers — is taking shape for May 7-9, 2008, in Santa Clara, Calif. We plan to build on our success from the first event there in June 2006. We'll run four tracks of speakers over two days, open the event with a Welcome Reception and hold a Networking Reception in the Exhibit Hall on Thursday evening, May 8.

Value Proposition for Conference Attendees:

- Stay current in your field
- Take away practical ideas and suggestions
- Network with your peers in product management

Value Proposition for Exhibitors:

- Make valuable professional contacts
- Capture leads that result in sales
- Network with other firms who sell to software companies

For information on exhibit sales, contact National Sales Manager Carol Samost at csamost@softwaremag.com.

KING CONTENT COMPANY

DIGITAL SOFTWARE MAGAZINE The Software Decision Journal

The SMP event is brought to you by King Content, publisher of Software Magazine.