Service Catalogs and Security Processes

Security Processes and Control Frameworks

The overriding mandate of today's corporate regulatory environment—a complex web of legislation such as Sarbanes-Oxley, GLBA, Basel 11 and HIPAA—is not that businesses have "forensic" processes established to identify and document financial malfeasance after the fact, but rather that they have strong, well-documented control processes in place to prevent fraud and abuse from occurring in the first place. The onus for ensuring that these processes exist has evolved upward from business operations to executive suites and boards of directors.

This shift in emphasis—from finding and punishing corporate wrongdoers to ensuring that controls exist to prevent abuse—has led to new interest at the highest business levels in established but continually evolving financial and IT best practices and frameworks such as ITIL®, COBIT, COSO and other overlapping controls and guidelines.

Perhaps the most relevant of these to IT organizations is COBIT, which stands for Control Objectives for Information and related Technology. Created in 1966 by the Information Systems Audit and Control Association (ISACA), COBIT's stated aim is to provide "managers, auditors, and IT users with a set of generally accepted measures, indicators, processes, and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company."[1] The complexity of COBIT has spawned a large library of interpretations and implementation guidelines. It consists of 34 high-level objectives regarding the use of IT assets that cover 215 control objectives categorized in four domains:

• Plan and Organize;

• Acquire and Implement;

• Deliver and Support; and

• Monitor and Evaluate.

The control objectives cover IT applications and systems in these four domains as they are applied to virtually every operational and financial process within an enterprise. The control objectives have three purposes: 1) ensure that IT processes support business objectives; 2) regulate how users access these processes, and; 3) automatically enforce corporate governance policies in how they use them.

COBIT concepts and language are mirrored in ITIL, the Information Technology Infrastructure Library, an authoritative source of IT best practices, notably in operations and service management. COBIT, however, provides a more structured and prescriptive approach to IT controls, rather than ITIL's narrative and descriptive approach; this makes COBIT the preferred foundation for U.S. businesses required to meet Sarbanes-Oxley control and monitoring requirements.[2] Sarbanes-Oxley is, of course, the sweeping measure passed by the U.S. Congress in 2002 as a response (or an overreaction,

[1] ISACA

[2] "Control Framework Misconceptions," George Spafford, Earthweb, JupiterMedia, 11/2004.

according to critics) to Enron, WorldCom and other accounting scandals. Its central intent is to ensure reliable financial information from public companies, requiring an attendant focus on the software that houses financial and operational data. In creating IT controls for compliance, businesses must:

• Assess risk;

• Control relationships and deliverables from outsourcers;

• Integrate security into the development process; and

• Monitor all changes that might impact critical systems.[3]

Security Processes and Service Catalogs

Enterprise IT management systems from vendors such as CA®, HP® and the BMC® Remedy® suite of applications are designed to support COBIT frameworks and ITIL best practices in business process automation and management applications. For example, BMC refers to this as "creating a sustainable compliance capability that is integrated into the day-to-day operations of your IT department. … We call this concept continuous compliance, and it is a result of running IT well." This statement reflects the challenges many IT departments face today—making applications and systems continuously compliant with corporate security processes mandated by senior management and "running IT well"—that is, more cost-effectively and directly supportive of business objectives than ever before.

Both needs intersect in the area of service catalogs, which are now proven to be a boon to "running IT well" but are less obviously helpful in supporting and enforcing corporate security processes.

Service catalogs are becoming the foundation for defining and delivering services, as well as for demonstrating the value of IT, HR, facilities, procurement, sales and marketing, and other service-oriented groups within the business. They offer any enterprise function a way to publish available services over the web, standardize service deliverables, establish service level expectations, and market service offerings to internal and external customers. For IT in particular, several factors are driving their adoption by large organizations. These include the increasing pressure on IT organizations to:

• Document and communicate their value to the business;

• Reduce costs and increase efficiencies;

• Reduce service request backlogs through standardization and automation; and

[3] Software Security Compliance Guide, Ounce Labs, 2006

• Adopt COBIT and ITIL standards in service delivery management, of which service catalogs are a key component.[4]

Service catalogs are "request-centric, forms-driven, and workflow-based."[5] Service catalogs built on top of enterprise IT management software suites allow businesses to manage requests for applications and processes—from employees, customers, suppliers and others—presented through web-based forms. But they also introduce several challenges to security processes and compliance requirements, such as:

• Are service catalogs easy to build and request forms easy to add?

• Is the service catalog portal secure?

• Who has authorized access to specific types of requests?

• How is this access being used?

• Who must approve specific requests, and how is the approval workflow process handled and enforced?

• What is the process for decommissioning accounts and "de-authorizing" users?

• How does the system provide auditability; that is, how are user request authorizations and approval processes monitored, enforced, and shown to be compliant with data and information security requirements?

Building Service Catalogs to Meet Security Needs

Properly implemented, service catalogs provide the capabilities and processes to address these security and compliance issues. Ideally, a service catalog should:

• Enable users without development skills to quickly build and implement actionable service catalogs. This enables functional groups outside of IT, such as facilities and HR, to create catalogs and manage requests utilizing the service process workflows in their enterprise IT management system.

• Enable automatic management and fulfillment of user service requests by enabling requests and approvals to be embedded in email messages.

• Effectively manage service requests by enabling users to track the status of their requests, and helping management to accurately monitor service delivery time and quality.

[4] Kinetic Data White Paper

[5] BMC

In addressing security processes, the service catalog provides centralized capabilities to:

• Give users authorized access to certain types of requests;

• Establish and enforce approval policies;

• Track how requests are handled and approved; and

• Provide an audit trail for every step in the process.

New types of requests and special security processes should be easily added, and service catalog forms should be designed to initialize the security process up front by ensuring that no required fields are left blank.

Service catalogs increase workflow efficiency by eliminating emails and phone calls to requestors for additional information. They ensure that requests don't languish in in-baskets but are instead processed according to approval policies and, through the use of predefined escalation procedures, within specific time frames.

Case Study

A large entertainment conglomerate that operates film studios, theme parks, retail stores and movie theaters hires thousands of employees each year. In a typical example, a manager is hired to oversee theaters in a specific territory. The company uses upwards of 40 different software applications, many of them part of or integrated with its enterprise IT management system, to manage its business at all levels. The newly hired manager needs access to about a dozen of them, including:

• Salesforce.com

• Blackberry enterprise access

• Oracle Financials

• SAP

• BMC Remedy

• RIM US/RIM EMEA

• Windows NT Domain

• Siebel Sales

• Siebel Marketing

• Custom internal applications

Sarbanes-Oxley introduced many new requirements pertaining to application access provision for new employees. Pre-Sarbanes-Oxley, provisioning application access to new hires involved a flurry of phone calls and emails, and processing manual forms

from HR, IT, and other functions. Post-Sarbanes-Oxley, the old process would have been unworkable. There was no way to introduce accountability and auditability into the process without hiring expensive outside consultants and adding a new layer of software on top of the process, which would achieve only cosmetic improvements since much of the underlying human and manual activity would remain untouched.

By implementing a service catalog atop its enterprise IT management system, the company solved all of these challenges with the ease and cost-effectiveness of simply adding another native application to its existing infrastructure. The company now publishes available services over a secure web portal. Authorized managers from HR, IT and other departments can provision the new employee by completing request forms for the software applications required by the new employee. The request forms automatically enforce security process requirements and launch the approval workflow process. The employee can later initiate his or her own requests through the service catalog portal to make changes or obtain access to other applications permitted by his or her authorization level. All activity is tracked and is available in detailed or summary form through pre-configured or customized reports.

The company has essentially “killed two birds with one stone.” The old expensive, manual process for account provisioning is now automated, with accountability and security requirements enforced. The new employee has access to the applications he or she needs to become productive automatically and almost immediately—versus days or even weeks using the old process. The company’s senior directors and board members are now confident that access to important financial and operational systems is fully compliant and auditable to meet new control and reporting requirements.

Specific security features of the service catalog that enable this include:

- The ability to activate/deactivate a request form;
- The ability to configure locale-specific messages for the user in the event of an error (required field missing, survey already submitted, connection problems, etc.);
- The ability to make fields required;
- The ability to allow fields to be conditionally required;
- The ability to hide/show questions and text based on answers or other events;
- The ability to require a user to login before accessing a form;
- The ability to place an expiration date on forms;
- The ability to send notifications to managers based on completed request forms;
- The ability to send notifications based on answer qualifications;

- The ability to audit changes to a user's submission/answers;
- The ability to audit changes of a template;
- The ability to list only the request forms that the user has access to see based on his or her login;
- The ability to assign approvers and backup approvers;
- Multi-level approval support; and
- The ability to determine approver based on categorization of employee/non-employee answers or other criteria.

Conclusion

For many enterprises, service catalogs can be a double-edged sword. They allow you to automate and publish, via the web, access to a vast library of applications and corporate information to both internal and external constituencies. Yet access to and use of those applications and corporate information must be more tightly controlled and auditable than ever before. Increased access with increased control isn't a paradox for organizations that build service catalogs tightly integrated with their existing enterprise IT management system, but rather an easily solved challenge. A properly implemented service catalog can:

- Manage thousands of employee, customer, supplier and partner requests;
- Automate processing of those requests;
- Segment access and duties according to Sarbanes-Oxley requirements;
- Leverage COBIT standards;
- Enforce security processes for access and authorization; and
- Demonstrate that corporate processes are in "control" through automatic tracking and auditability.

Meeting these needs can be an expensive proposition for organizations that choose either to develop a service catalog application internally or implement an application that requires an extensive integration effort with existing enterprise systems. But by utilizing an application designed to work within its existing enterprise IT management framework, an organization can implement a service catalog application as easily as installing and switching on another native IT package.

About the author

John Sundberg, founder and president of Kinetic Data, is an entrepreneur who has demonstrated effective leadership by creating a team culture that has spearheaded the company's consistent growth. During his 15 years of designing and managing successful, innovative information system implementations, he has been a lead architect, developer, or project manager of over 100 projects for medium and large enterprises, with extensive work in large systems, distributed systems, systems management and consulting.

Prior to founding Kinetic Data, Sundberg applied his technical and management expertise at 3M; Programming Alternatives, Inc.; Wilson Learning; and as an independent consultant. At 3M, he was a liaison between IT and several development groups, where he discovered why projects succeeded or failed, leading him to build his company around a team concept, as he found the groups that worked well together produced successful projects.

John is president of the Minnesota Chapter of AFSMI (Association for Services Management International).

About Kinetic Data, Inc.

Kinetic Data is one of the largest and most experienced third-party BMC Remedy software companies in the world. As the only company exclusively focused on developing business service management (BSM) and service delivery management (SDM) software tools specifically for BMC Remedy, Kinetic Data offers the most extensive portfolio of third-party, "built on BMC Remedy" packaged BSM applications available. A BMC Remedy Technology Alliance Partner since 1999, Kinetic Data has helped nearly 100 Fortune 500 and government customers—including General Mills, Avon, Intel, 3M, and the U.S. Department of Transportation—implement BMC Remedy products aligned with ITIL best practices. The company serves customers out of its headquarters in St. Paul, Minn., and offices in Sydney, Australia. For more information, go to www.kineticdata.com.