Operations Governance: The New Management Application

Prepared by:
John P. Morency, Managing Director
Transitional Data Services, Inc.
92 South Street
Hopkinton MA 01748

(774)-759-9025 (Voice)
(978)-808-4112 (Mobile)
jmorency@transitionaldata.com (e-mail)

Operations Governance: The New Management Application

Introduction

As a result of both the operations and competitive changes that are occurring, application management products, regardless of whether they are hardware- or software-based, will increasingly be evaluated based upon their ability to make IT more project-focused and support-automated. However, achieving these two objectives must be in addition to, versus instead of, maintaining day-to-day service level quality.

Given the rapidly increasing complexity of today's IT infrastructure, addressing this latter requirement is a formidable undertaking. This is especially true given the increasing number and complexity of infrastructure components required to support end-to-end service delivery. The result has been an increasingly strong need for management systems that can synergistically coordinate and orchestrate component management in order to facilitate a more efficient and effective support organization.

The challenge, however, does not end there. Also to be addressed is the task of ensuring timely support for key business objectives. The specific objectives identified by IT as being the most pressing over the coming year are listed in Figure 1.

Key Business Initiatives
Which business priorities will your IT organization implement or support in 2005?

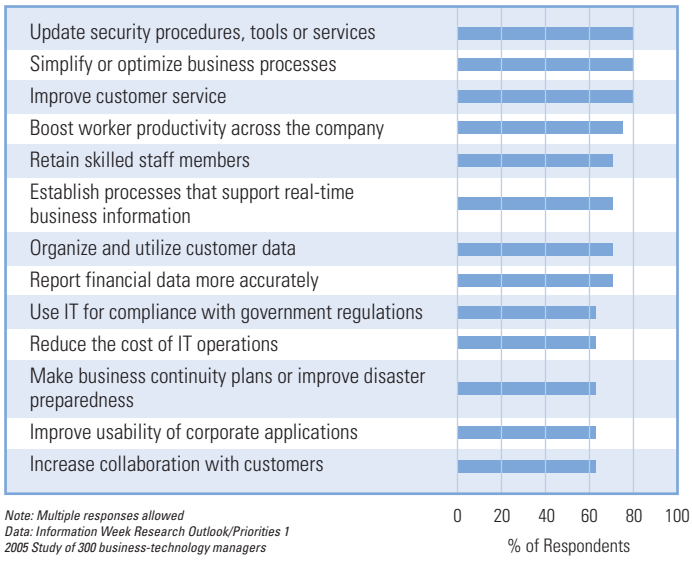


Figure 1 - Key IT Priorities (source: Information Week)

Addressing these challenges still requires the underlying presence of quality configuration, availability and performance management. However, the extent to which management products can more directly address one or more key business priorities is increasingly determining their likelihood of implementation. It's not that the need for the core management functionality has gone away. Rather, the bar has been raised. The new opportunity is the targeted application of technology to support IT Operations Governance management.

IT Governance Management is not entirely new. IT Governance - the art of aligning IT deliverables with business objectives - has been an important organizational priority for at least the past five years. However, up to this point, the primary focus of products that claim to support IT governance have focused on supporting initiative portfolio management, project tracking and investment decision support. In general, these offerings have been far more oriented towards project management and investment governance than toward operations governance, i.e. ensuring that day-to-day IT operations aligns effectively with what the business needs to do day by day as well as with what the business has to do.

This is the aspect of IT governance management that is new. In this paper, we'll discuss the application of governance management to support what many businesses have to do - citing regulatory compliance deficiency remediation as one example - as well as what they need to - effectively address one or more of the business priorities shown in Figure 1. In addition, we'll also discuss how the use of more mainstream availability and performance management technology may be a far better fit for the day-to-day support of operations governance.

Applying Governance Management to Compliance Remediation

One key IT governance application is ensuring organizational compliance with governmental or industry regulations. Currently, the most prominent compliance icon is Sarbanes-Oxley (SoX) 404, which becomes mandatory for every American public company (as well as foreign subsidiaries) by the middle of 2006.

After all the required controls are defined, the next phase of a SoX assurance process is typically control remediation. Remediation is only applied to those required controls that have been determined to be deficient, either because they previously were not in place or lacked required management functionality.

Examples of IT control remediation activities include:

- Updating the development project approval process definition in order to ensure that appropriate levels of business unit approval exist occur prior to beginning new projects;
- Formalizing information pre-requisite requirements specific to production turnover;
- Restricting the extent to which end users can install software on their desktop PCs;
- Adding additional storage to support required financial and/or customer data record retention;
- Formalizing service level management and reporting;
- Documenting and institutionalizing Change Control request, review and approval processes;
- Requiring explicit finance group approval for any application or system change that could impact the integrity of corporate financial data.

If product investments are required to support remediation, the most effective ones are generally those that provide far more than a control deficiency band-aid. Their focus is also upon addressing as many of the governance priorities listed in Figure 1, in addition to specific deficiency remediation, through a single investment. In general, this is the approach that will make it far more likely that the benefits that result from the remediation exercise far outweigh the associated product and implementation cost.

Governance Management Case Study

In order to illustrate this principle, we present an example of an actual TDS client for whom operations governance management was long overdue. The key challenge for this client (a financial services company) was the consistent delivery of high availability and responsiveness for a new set of financial portfolio management applications that had been initially developed for independent agents in the US, but was also being extended to agents in both Europe and the Far East.

The operations management software portfolio (made up of nearly 25 individual management products) available to support this partner Extranet was quite extensive. Supported functionality included network, system and application monitoring (both inside and outside the firewall) as well as inventory, configuration, report and SLA management support across several different vendors.

However, despite this rich set of utilities, their collective value was often limited at best when problems affecting extranet service quality arose, especially during nights and weekends. During those times, support coverage was limited and primarily provided by lower cost, lower skilled operations staff. These were the individuals that were the front line of customer support when overseas agents were in the middle of their normal workdays.

The Problem

A very typical problem scenario involved the generation of "Application Unreachable" alerts from geographically distributed, Internet-based synthetic transaction generation agents. Alert support had been configured to forward occurrence notification to a centralized management server. Once alert notification was posted to the management server, a trouble ticket was automatically generated. Trouble ticket creation notification often occurred in tandem with the arrival of problem calls to the Operations Center from disgruntled overseas agents.

Once a trouble ticket was opened, the remainder of the resolution task became manual. The simple fact was that not one of the existing management products was capable by itself of both isolating the cause(s) of the problem and providing actionable information that an operations support person could readily act upon. Lacking this capability, operations were solely dependent upon direct support from the IT staff. And if the "right" IT staff member could not be contacted when outages occurred, problem isolation and resolution ceased until the support staff returned, either on the following morning or at the end of a weekend. The inevitable result was trouble tickets that were open for several hours (and sometimes days), unhappy agents and a negative impact on the company's brand image in an extremely strategic market.

The Impact

Our analysis of trouble ticket processing times specific to the detected response time and availability problems showed that specific occurrences were only 25% of the opened tickets by volume. However, they required nearly 98% of the total ticket resolution time due to the long durations in which tickets were left open by operations until a higher-level support or development resource could be contacted.

The Causes

When we analyzed solution entries for closed tickets, we found that application outages were a frequent result of incorrectly applied application, server or network infrastructure changes. Unfortunately, the operations staff really had no easy way of being able to correlate the occurrence of the "Application Unreachable" outages with the application of faulty changes. Clearly, there was a Change Management process problem. In addition, however, inadequate root cause determination and resolution management support as well as inadequate operations support staff skill sets were also key contributing factors.

Given the scope of the problem, the solution required a combination of improved management process, root cause determination automation and support skill sets. The product-independent elements were directly related to improving governance. In addition, it was clear that the right supporting management products could also address a number of the business priorities listed in Figure 1, in addition to the service management-specific issues. These include:

1. Boosting IT productivity and effectiveness by dramatically reducing the resolution time per ticket;
2. Improving the quality of customer service by becoming more responsive when outages did occur;
3. Reducing the cost of IT operations by being able to deliver higher quality customer service without having to necessarily hire more expensive talent.

This was clearly a governance management problem that required two important solution elements. The first is the select application of industry best practices to improve clearly broken support processes. The second is the upgrading of existing management products or the implementation of new products in order to support best practice processes and deliverables. The next two sections will present specific best practice and product approaches that TDS has found to be very well suited to addressing the service improvement requirements of our case study client as well as operations that have similar needs.

Best Practice Option: COBIT

Few argue the value of IT best practices. The question that is asked far more frequently concerns which of the many best practice standards yield the most effective results. TDS' consistent experience is that the most effective set of best practices for improving data center operations are defined in the Control Objectives for IT (COBIT).

The COBIT standard, first released in 1996 by the IT Auditors Association, defines a control implementation and measurement framework that was specifically designed with IT efficiency, predictability, accountability and auditability in mind. Given these objectives, a frequent application of COBIT is the definition of IT operations controls that help facilitate business compliance with both governmental and industry-specific regulations.

This is precisely the reason why the IT Governance Institute (http://www.itgi.org/) utilized the COBIT definitions as the foundation for SoX IT controls in the definitive document IT Control Objectives for Sarbanes-Oxley (downloadable from the ITGI website). The result is that COBIT offers users a two for one proposition for implementing both SoX compliance as well as service delivery improvement in other IT supports categories.

Today's reality, however, is that most operations are far less concerned about the implementation of best practices than they are with the implementation of the "good enough" practices that best fit their operations style, conformance, service improvement, and business alignment objectives.

Implementing "Good Enough" Practices

Determining the right set of "good enough" practices that are most appropriate for a specific operation is especially well suited to the way in which COBIT is defined. One key strength is that its implementation is not an "all or nothing" proposition. Instead, it defines a very modular set of control and measurement options that users can deploy as needed in order to best fit the needs of their specific operation. No process is dependent upon the implementation or success metrics of any other, providing users with a very flexible set of process implementation and improvement measurement options.

This modular set of processes and success metrics differentiate COBIT from other best practice definitions (e.g. ITIL). Not only are management practices defined in 34 separate categories (including Application Availability and Performance Management), but the standards also include specific criteria and metrics that can readily be used to support a continuous improvement initiative for service delivery.

Improvement criteria, success factors and support metrics are all process-specific. For example, the process-specific Critical Success Factors (CSFs) and success metrics (i.e. the Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs)) for Availability (COBIT Process DS10) and Performance (COBIT Process DS3) management are shown in Figures 2 and 3 respectively.

Figure 2 - COBIT Availability Management - Critical Success Factors and supporting metrics

CRITICAL SUCCESS FACTORS (CSFs)

- There is a clear integration of problem management with availability and change management.
- Accessibility to configuration data, as well as the ability to keep track of problems for each configuration component, is provided.
- An accurate means of communicating problem incidents, symptoms, diagnosis and solutions to the proper support personnel is in place.
- Accurate means exist to communicate to users and IT the exceptional events and symptoms that need to be reported to problem management.
- Training is provided to support personnel in problem solution techniques.
- Up-to-date roles and responsibilities charts are available to support incident management.
- There is vendor involvement during problem investigation and resolution.
- Post-facto analysis of problem handling procedures is applied.

KEY GOAL INDICATORS (KGIs)

- A measured reduction of the impact of problems and incidents on IT resources
- A measured reduction in the elapsed time from initial symptom report to problem solution
- A measured reduction in unresolved problems and incidents
- A measured increase in the number of problems avoided
- Reduction in lag between identification and escalation of high-risk problems and incidents

KEY PERFORMANCE INDICATORS (KPIs)

- Elapsed time from initial symptom recognition
- Elapsed time between problem recording and resolution or escalation
- Elapsed time between evaluation and application of vendor patches
- Percent of reported problems
- Frequency of coordination meetings
- Frequency of component problem analysis reporting
- Reduced number of problems

These include the process-specific Critical Success Factors (CSFs) that can be used to define continuous improvement targets as well as assessment metrics (Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs) that can be used to quantitatively measure progress towards one or more service improvement goals.

Figure 3 - COBIT Performance Management - Critical Success Factors and Supporting Metrics

CRITICAL SUCCESS FACTORS (CSFs)

- The performance and capacity implications of IT service requirements for all critical business processes are clearly understood.
- Performance requirements are included in all IT development and maintenance projects.
- Capacity and performance issues are dealt with at all appropriate stages in the system acquisition and deployment methodology.
- The technology infrastructure is regularly reviewed to take advantage of cost/performance ratios and enable the acquisition of resources providing maximum performance capability at the lowest price.
- Skills and tools are available to analyze current and forecasted capacity.
- Current and projected capacity and usage information is made available to users and IT management in an understandable and usable form.

KEY GOAL INDICATORS (KGIs)

- Number of end-business processes suffering interruptions or outages caused by inadequate IT capacity and performance.
- Number of critical business processes not covered by a defined service availability plan.
- Percent of critical IT resources with adequate capacity and performance capability, taking account of peak loads.

KEY PERFORMANCE INDICATORS (KPIs)

- Number of down-time incidents caused by insufficient capacity or processing performance.
- Percent of capacity remaining at the normal and peak loads.
- Time taken to resolve capacity problems.
- Percent of unplanned upgrades compared with the total number of upgrades.
- Frequency of capacity adjustments to meet changing demands.

Management Service Maturity

In addition to process-specific sets of measurable success metrics, COBIT also defines additional criteria that are highly relevant to benchmarking the value and relevance of alternative technologies, products and vendors relative to one or more process improvement initiatives. These are the management process-specific Service Maturity Models (SMMs).

The use of maturity models to both assess and improve process performance was first done by the Software Engineering Institute (SEI) at Carnegie-Mellon University (CMU). The CMU approach (called the Capability Maturity Model (CMM) measures the performance of a software engineering organization in the delivery of high quality, error-free code. The capability level of a specific organization is measured on a scale from zero to five. Each numerical measurement is associated with specifically defined competencies in the automated design, construction, testing and delivery of high quality software. A score of five goes to the most process mature organizations and a score of zero are given to those that are the least capable.

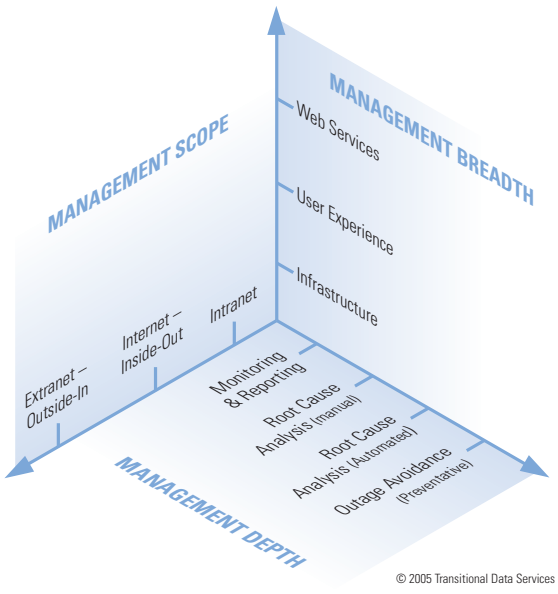
More recently, maturity models are being used to benchmark organizations in competency areas other than software development. Measuring service delivery maturity and business continuity readiness is two of the most recent applications that are more directly related to improving IT operations quality. COBIT is somewhat unique in its support for management process-specific maturity models, whose rankings range from Non-Existent (meaning that the process is not supported at all) to fully Optimized (the management process is fully automated and well aligned with business objectives).

In the remainder of this paper, we'll discuss how the NetScout *nGenius* Performance Manager can be applied to supporting COBIT-based best practice implementation as well as improving IT operations governance management.

Applying NetScout *nGenius* to Improve Operations Governance

At the beginning of this paper, we briefly discussed the perceived commoditization of applications availability and performance management products. However, it should be emphasized that this is only a perception and not necessarily a given. The values shown in each of the three dimensions below (Figure 4) constitute a more useful perspective on management product capability that is complementary to the application availability and performance management Optimizing criteria that were earlier presented.

Figure 4 - Operations Management Value Graph



In fact, if one considers this three dimensional representation of management product capability relative to breadth (the range of managed entities), scope (the range of private and public network support) and depth (the degree of supported management automation), one quickly concludes that there is no one single vendor that is equally optimal in all three dimensions, thereby resulting in lots of opportunity for future differentiation. Despite that fact that no one-vendor product family is fully functional across all three axes, we believe that NetScout is one vendor that comes fairly close.

A key foundation for satisfying both the Value Graph and Optimized that is unique to NetScout is the breadth and scope of supported management data through the Common Data Model (CDM) in *nGenius* Performance Manager (PM). The broad application network entity support provided by CDM adds substantial value to the root cause analysis and outage avoidance automation. This functionality is especially relevant to addressing the SoX Change management remediation requirements discussed earlier as well as implementing a sustained service improvement program that is generally independent of the levels of vendor, technology and product complexity within the underlying delivery infrastructure.

In addition, the utility of *nGenius* Performance Manager is evidenced in the support that it can provide for continuous support service improvement initiatives measured by the KPIs and KGIs presented in Figures 3 and 4. Figures 5 and 6 show examples of the specific KPI and KGI metrics that can be supported by specific *nGenius* Performance Manager application availability and performance management functionality along with a brief description of the specific support that would best an associated improvement initiative.

Figure 5 - *nGenius* Performance Manager KPI & KGI Metric Support - Availability Management

COBIT KGI or KPI	Supporting *nGenius* PM Functionality
A measured reduction of the impact of problems and incidents on IT resources	Tracking application and end-user mis-use of the infrastructure (e.g. streaming video, interactive gaming) in order to reduce the number of preceived service outages
Elapsed time from initial symptom recognition to entry in the problem management system	Threshold alarming on application utilization or on response time/availability - minimizing the time lag from symptom occurence to sympton recognition
Elapsed time between problem recording and resolution or escalation	Settable time over threshold alarming on segments for evidence of users consuming excessive bandwidth or capacity
A measured reduction in inresolved problems and incidents	Behavior visibility of all applications, shrink-wrapped or custom, facilitating strategic decision making on whether increased bandwidth may be the right choice, or some other approach such as re-configuring the network with QoS, or moving a business process to a non-peak time of the day, which ultimately reduces the probability of unresolved service degradations, bottlenecks and outages
A measured increase in the number of problems avoided through preemptive fixes	*nGenius* NewsPapers that contain days to capacity threshold information to order additional capacity for circuits or infrastructure upgrades in order to avoid unplanned outages or service bottlenecks

Currently, KGI and KPI metric values would have to be tracked manually as part of any initiative implementation. Over time, however, it's likely that the tracking of these and similar metrics could be more directly supported by increasingly sophisticated analytics, thereby reducing the manual effort required to implement the improvements even further.

Figure 6 - *nGenius* Performance Manager KPI & KGI Metric Support - Performance Management

COBIT KGI or KPI	Supporting *nGenius* PM Functionality
Number of business processes suffering interruptions or outages caused by inadequate IT capacity and performance	Required capacity measured for all applications, both shrink-wrapped and custom, to determine if infrastructure capacity needs to be adjusted and validates why it needs to be adjusted
Number of critical business processes not covered by a defined service availibility plan	Monitoring of applications with associated QoS levels to evaluate if traffic priority services are being delivered in the proper class
Number of down-time incidents caused by insufficient capacity or processing performance	*nGenius* Newspapers provides capacity planning reports that show actual capacity against standard baselines and 90% baselines
Percent of critical IT resources with adequate capacity and performance capability, taking account of peak loads	Measures all applications, both business and non-business to determine if capacity needs to be adjusted and validates why it needs to be adjusted
Percent of critical IT resources with adequate capacity and performance capability, taking account of peak loads	Response time analysis with alarming capability to address degradation and unavailability of strategic business servers/applications

Summary

TDS' implementation and management experience with both SoX 404 assurance projects and clients whose needs are similar to the one discussed in our case study example have convinced us that supporting effective Operations Governance requires a different functional scope than what has been addressed by more traditional operations management products, which were purely focused on IT infrastructure management, or even the new generation of governance management products, which are very project focused.

Given the list of key IT priorities referenced earlier, along with additional requirements for continuous operations improvement and increased service delivery efficiency, it's clear that support automation with underlying measurement analytics can and must play a more significant role in taking IT in the direction of becoming a more predictable, measurable and accountable service delivery organization. In general, this functionality can be supported much more easily as a natural extension of the current generation of network application availability and performance management products, of which NetScout's *nGenius* Performance Manager is one prominent example.

For the reasons presented, as well as constituting a very viable solution for our case study client, TDS has determined that the NetScout *nGenius* products, supplemented by automated analytics provided with the recent acquisition of Quantiva, support a very sound foundation for effective operations governance management. Consistent with what some users have experienced with SoX 404 remediation, the realized operations benefit in proportion to the implementation cost may also be quite favorable.

nGenius®

The *nGenius*® Solution is comprised of *nGenius*® Performance Manager, *nGenius*® Probes and for specialized situations, additional appliances including *nGenius*® Flow Collector and *nGenius*® Flow Recorder.

nGenius Performance Manager is a software application that analyzes the information collected by *nGenius* Probes as well as other network devices, and delivers the features and functions of multiple performance management disciplines in a single product.

nGenius Probes are hardware monitoring devices that are the industry's most advanced sources for identifying, collecting and analyzing application-level traffic data across the enterprise.

nGenius Flow Collectors are dedicated hardware devices optimized for collecting application conversation data via NetFlow records produced by leading network infrastructure devices.

nGenius Flow Recorder is an appliance that couples storage for large packet trace captures and graphics-based data mining software. It continuously records all traffic and produces a network audit trail for post-event forensics requiring full packet payload details.

CC-0207-05 Rev A

NetScout

NetScout Systems, Inc.
Corporate Headquarters
310 Littleton Road
Westford, MA 01886 USA
Telephone (978) 614-4000
Fax (978) 614-4004
Web: www.netscout.com

Europe
Regus House
268 Bath Road
Slough, Berkshire, SL1 4DX UK
Phone: +44 1753 725561
Fax: +44 1753 725562

Asia/Pacific
Room 105, 17F/B, No. 167
Tun Hua N. Road
Taipei, Taiwan
Telephone +886 2 2717 1999
Fax +886 2 2547 7010