



Enabling Practical IT Service Management

White Paper

January 2006

Contents

Understanding ITIL.....	1
ITIL Background	1
ITIL Principles.....	1
ITIL Core Disciplines	2
The ITIL View of Supporting Technology	3
NetIQ's Approach to Practical IT Service Management.....	4
Knowledge-Based Service Assurance.....	4
Building Maturity in IT Service Management	5
Intermediate Maturity in IT Service Management	11
Advanced Maturity in IT Service Management	12
IT Service Management Technology Architecture	14
Elegant Integration.....	14
Openness.....	15
Usability.....	15
Backup and Availability	16
Control and Security	16
Conclusion	16
About NetIQ Corporation ...	17

With the onslaught of expanded regulations and stagnation in IT budgets, IT Service Management (ITSM) best practices are increasingly viewed as a way to meet these challenges. The result is that an explosion of information and opinions related to ITSM best practices has been created by vendors, government agencies and professional organizations. IT professionals who study this content often find good ideas, but struggle with how to practically implement them within their organization.

The challenge for IT organizations is to evolve from the traditional Systems Management practice of administering individual IT elements to managing end-to-end service levels of key business services provided by IT. ITSM promises to meet this challenge by accomplishing the following goals:

- Align IT services with the current and future needs of the business and its customers
- Improve the quality of the IT services delivered
- Reduce the long-term cost of providing IT services

Unfortunately, many attempts at implementing ITSM best practices are fraught with problems that result in less than satisfactory results. Numerous vendors are promoting strict adherence to the IT Infrastructure Library (ITIL[®]), by far the leading ITSM framework. While there is tremendous value in ITIL, adoption is not for the faint-of-heart, due to its scope and the significant disruption that it will introduce to most IT organizations.

This whitepaper describes a practical approach for IT Service Management that will benefit NetIQ customers by demonstrating NetIQ's methodology and solutions to consistently achieve better results.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2006 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

ITIL is a Registered Trade Mark and a Community Trade Mark of the Office of Government Commerce.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, imMarshal, Intergreat, Knowledge Based Service Assurance, Knowledge Scripts, MailMarshal, Marshal, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Security Reporting Center, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebMarshal, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Understanding ITIL

ITIL Background

IT Service Management is a strategy for gaining control of the cost and quality of IT services. The IT Infrastructure Library (ITIL) is the leading framework for implementing IT Service Management¹, providing a broad set of best practices for IT organizations that wish to implement IT Service Management. ITIL began in the late 1980s when the United Kingdom's government began to collect and organize useful approaches to IT management in a set of books. From the beginning, this collection of observations and guidance has been publicly available. Over the years, the collection proved useful to organizations in all sectors and it has ultimately become a worldwide standard for defining objectives and processes for IT organizations.

The library currently consists of seven books (an eighth on Software Asset Management is related, but not included) and is published by the UK's Office of Government Commerce (OGC). Continuing development of ITIL content is now performed by the IT Service Management Forum (itSMF), an international body made up of a hierarchy of country chapters supported by Local Interest Groups. Members of itSMF are IT practitioners and vendors who contribute to content refresh and maintain currency. Additional information can be found at www.it-smf.com.

ITIL Principles

In most cases, the concepts found in ITIL are not new. Instead, ITIL provides a common set of processes that an IT organization could choose to employ. The framers of ITIL understood that day-to-day management and actions would differ from one organization to the next, so ITIL is offered as guidance, not prescription. In fact, the ITIL guidance rarely defines explicit ways to implement or accomplish these best practices.

Because ITIL is intentionally generic, and even avoids prescribing step-by-step instructions for ITSM deployment, most organizations initially adopt the framework as a common language and set about defining the details and processes that address their immediate needs. ITIL defines multiple best practices, including books such as *Service Support*, *Service Delivery*, *Security Management*, *Application Management* and *ICT Infrastructure Management*. Additional books that assist with implementation include *Planning to Implement Service Management* and *The Business Perspective*. It is this broad scope that presents both the value and the challenge of implementation.

In reality, most IT organizations that deploy ITIL focus only on the practices found in two of the seven books, *Service Support* and *Service Delivery*. These are known as the core books and are the only two for which there are currently certifications. There is tremendous value in these two books for their scope of coverage, which includes ten disciplines and one function. However, there are self-admitted limits to the coverage that these two books provide for IT management, such as a quality assurance methodology, a project management methodology and security and compliance management methodologies. Even if an IT organization successfully deployed all ten core disciplines, it would still have gaps in developing and providing IT services to its customers.

¹ Mendel, Thomas. *ITIL's Final Breakthrough: From 'What' to 'How'*. (August, 2004) CIO Magazine Analyst Corner.

For this reason, many consultants assisting in ITIL implementation recommend an integration of ITIL processes with other industry standards, such as Six Sigma, ISO 9000, PMI, CMM, CobiT, ISO 17799, etc. While this may provide a more comprehensive implementation of IT Service Management, it is a daunting scenario for even the largest companies, and resource restrictions will likely prevent such a wide scope of implementation for most companies. A common approach, therefore, is to begin with selective deployment of the disciplines that will provide the largest value to the IT organization, in an iterative fashion where additional complexity is introduced as the organization matures.

ITIL Core Disciplines

For those unfamiliar with ITIL, the following short descriptions are provided for the single function and ten disciplines defined in the core *Service Support* and *Service Delivery* books.

Service Support

Service Desk – The only function described in the core books, the Service Desk(s) serves as the central point of contact for end users in the ITIL framework. The distinction between a Service Desk and a traditional Help Desk is that a Service Desk is integrated with many of the other disciplines to make it more efficient, enabling it to operate more proactively with end-users.

Incident Management – This discipline is responsible for restoring normal service operation as quickly as possible and minimizes the adverse impact of incidents on business operations. In many organizations, the Service Desk performs Incident Management, but this is not required.

Problem Management – This discipline minimizes the business impact of incidents and problems that are caused by errors within the IT infrastructure. It seeks out recurring incidents to resolve the underlying root cause and prevent recurrence.

Configuration Management – This discipline accounts for all IT assets and configurations. It provides accurate information on configurations, including the relationship between configuration items, and verifies configuration records against the infrastructure. The core component of Configuration Management is the Configuration Management Database (CMDB), which retains all of this information for use by the other disciplines. ITIL recommends deploying Configuration Management with Change Management.

Change Management – This discipline ensures that standardized methods and procedures are used for efficient and prompt handling of all Requests for Change (RFCs), in order to minimize the impact of change-related incidents upon service quality – and consequently to improve the day-to-day operations of the organization.

Release Management – This discipline protects the production environment by planning, designing, building, testing and deploying hardware and software to ensure proper operation.

Service Delivery

Service Level Management – This discipline maintains and improves IT service quality through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and instigation of actions to eradicate poor service – in line with business or cost justification. Through these methods, a better relationship between IT and its customers can be developed.

Capacity Management – This discipline ensures that the capacity of the IT infrastructure matches the evolving demands of the business in the most cost-effective and timely manner. It allows for proper planning to meet future capacity needs, resulting in the ability to defer expenditures in some cases and avoid costly panic-buying in others.

Availability Management – This discipline optimizes the capability of the IT infrastructure, services and supporting organization to deliver a cost-effective and sustained level of availability that enables the business to satisfy its business objectives. This is achieved by determining the availability requirements of the business and matching these to the capability of the IT infrastructure and supporting organization.

Financial Management for IT Services (FMITS) – This discipline allows an IT organization to understand whether it is cost-effectively providing services and to accurately budget, account for and potentially charge for those services.

IT Service Continuity Management (ITSCM) – This discipline is concerned with managing an organization’s ability to continue to provide a pre-determined and agreed-upon level of IT services to support the minimum business requirements following an interruption to the business.

The ITIL View of Supporting Technology

ITIL describes three necessary ingredients for a successful ITSM deployment: People, Process and Technology (also referred to as tools). In regards to tool selection, the first question the ITIL guidance suggests that you ask is, “Do I really need software tools?” It goes on to answer this question by saying, “The need for, and the sophistication of, the tools required will depend on the business need for IT services and, to some extent, the size of the organisation.”² Organizations can attempt to implement ITSM manually, but the sheer number of people required for this approach makes processes ineffective and inefficient - contrary to the goals of Service Management. One can find discussions of tool requirements in all of the chapters, and the general guidance is that “all but the smallest organisations” will require the use of Service Management tools, because automated tools allow:

- the centralization of key functions
- the automation of core Service Management functions
- the analysis of raw data
- the identification of trends
- preventive measures to be implemented

ITIL also defines two categories for tools³, which can be described as workflow management and operations management. Workflow management is typically represented as a help desk application that allows the creation and tracking of tickets for certain work activities such as trouble tickets and requests for change. Operations management tools enable operators to work more efficiently by automating the collection, analysis and reporting of data as well as managing entitlements to perform activities required by the processes.

NetIQ, as a provider of systems and security management solutions, is focused on developing effective operations management tools. This paper will demonstrate NetIQ’s best-practice approach to deploying IT Service Management in a practical way, as well as describe specific products that benefit the deployment at each step of maturity. Implementing ITSM using these technology recommendations in concert with effective process development and organizational management of the people involved will provide a foundation for successfully reducing the cost and improving the quality of IT services, and if desired, can lead to ISO20000 certification.

² *ITIL Service Support v.2.0*, Chapter 10, Service Management Software Tools

³ *ITIL Service Support v.2.0*, Chapter 10.1, Types of Tools

NetIQ's Approach to Practical IT Service Management

Knowledge-Based Service Assurance

As a software vendor with a long history of helping customers improve their ability to manage large IT environments, NetIQ is a strong proponent of IT Service Management best practices. NetIQ employs experts in the field with experience in ITSM consulting and is a vendor sponsor of the IT Service Management Forum (itSMF). NetIQ representatives are featured regularly as speakers at itSMF Local Interest Groups and at ITSM related conferences, and many NetIQ employees have achieved Foundation and Manager's certification in IT Service Management.

NetIQ views IT Service Management as one of four fundamental disciplines to assure services. NetIQ calls this approach Knowledge-Based Service Assurance (KBSA), a representation of which can be seen in the diagram below.

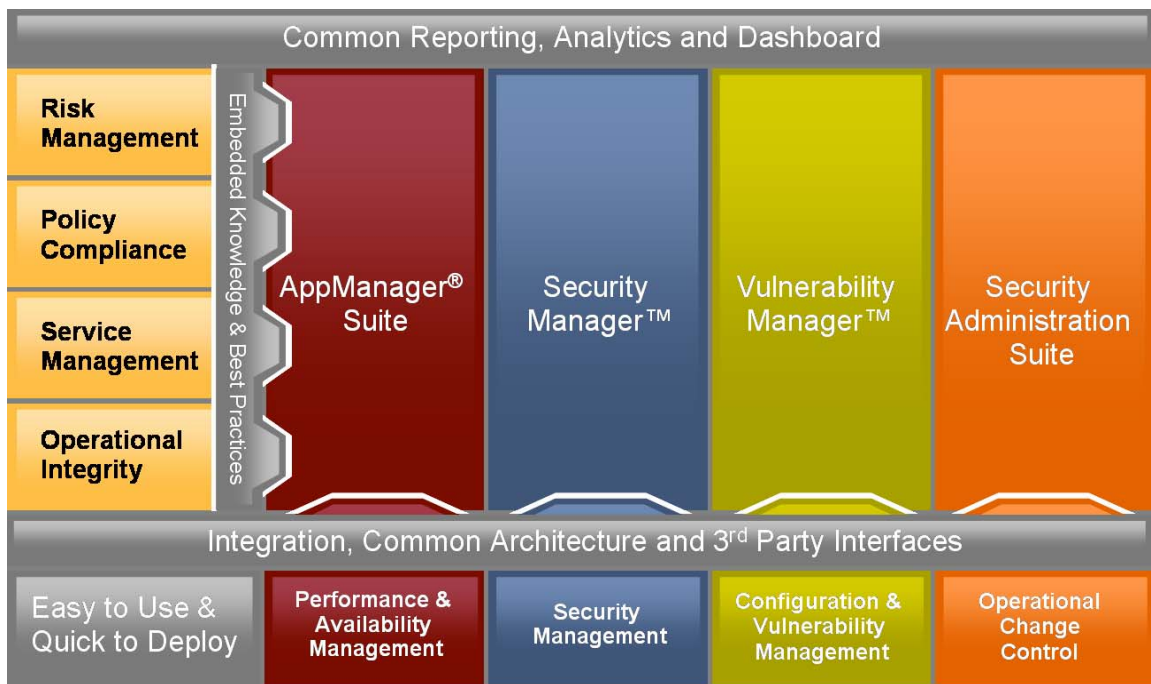


Figure 1: The Knowledge-Based Service Assurance matrix, demonstrating the four disciplines (rows) and four product families (columns) of which it consists.

The products developed by NetIQ form a cohesive set of solutions for practical implementation of Knowledge-Based Service Assurance. A complete description of the KBSA approach can be found in the NetIQ Knowledge-Based Service Assurance Solutions White Paper, which can be found at www.netiq.com. The remainder of this paper will focus on specifics related to IT Service Management, which is principally supported by NetIQ's flagship product, AppManager® Suite, but crosses all product lines, demonstrating support from a wealth of perspectives.

Building Maturity in IT Service Management

As previously discussed, organizations deploying ITIL and other ITSM disciplines often take a selective and iterative approach. This is necessary to minimize the impact that deployment will have on production operations and because realistically, the available resources for implementation will be limited until value is demonstrated. An additional challenge is that the ITIL guidance does not prescribe an implementation starting point, leaving it to the practitioner to decide – a difficult decision even for the experienced. NetIQ understands this reality and recommends the following practical approach to building maturity in IT Service Management.

Step 1: Implement Element Monitoring

This is a step that most organizations either have in place or know they need to have in place. All IT organizations perform some level of Incident Management, because it is impossible to ignore. Thus, the need to monitor elements in an IT environment is obvious, in an effort to gain forewarning of incidents before users begin calling and enable the accelerated completion of the incident life cycle. While many products are on the market for this purpose, NetIQ's AppManager has several key advantages that simplify this step:

- **Leverage Embedded Knowledge:** AppManager contains over 2000 Knowledge Scripts®, which can be leveraged to expertly monitor dozens of operating systems, applications and hardware devices, with little to no customization required.
- **Implement Monitoring:** With auto-discovery of deployment targets and remote agent deployment capabilities, AppManager can be installed and maintained by fewer personnel than bloated framework products require.
- **Aggregate and Respond to Events:** Because of its breadth of cross-platform support, a common interface with the simplicity of drag-and-drop management can be utilized to respond to all events, drastically reducing the incident life cycle time. NetIQ also provides ResponseTime modules to compare the user impact with internal events.

Once Element Monitoring implementation is complete, and a process for maintaining it is established, this level of maturity can be considered achieved.

ActiveDirectoryReplication	ExchangeReceiveMail	NotesCreateSaveMailNote	OracleGLTier2AccountInquiry
ActiveDirectoryResetPassword	ExchangeSendMail	NotesCreateSaveSendAttach	OracleGLTier2JournalEntry
BaanAddItem	FileReceiveShortConnection	NotesCreateSaveSendMailNote	PacketBlasterLongConnection
BaanGenerateMPSMRPBatches	FileSendShortConnection	NotesCreateTextIndexServer	PacketBlasterRevLongConnect
BaanLoadDEM	FTPGet	NotesIndexedDBLookup	PointCastv1InitialUpdate
BaanLoadItemMaster	FTPPut	NotesNonIndexedDBLookup	PointCastv2InitialUpdate
BaanMaintainCustomer	HeadlinerInitialLoad	NotesReceiveEmail	PDP3ReceiveEmail
BaanMaintainEmployeeAdd	HeadlinerSubsequentUpdate	NotesReplicateMail	SAPR3AuthPaymentOnInvoice
BaanMaintainProductBom	HTTPGIFTtransfer	NotesReplicateServer1DB	SAPR3BasicStock
BaanMaintainPurchaseOrder	HTTPSSecureTransaction	NotesReplicateServer50Auto	SAPR3BatchCharacterizeStock
BaanMaintainSalesOrder	HTTPTextTransfer	NotesReplicateServer50Docs	SAPR3CreatePurchaseOrder
BaanMaintainServiceOrder	InquiryShortConnection	NotesReplicateServerCheck	SAPR3CreateSalesOrder
BaanPrintCompaniesListSelect	LDAPDirectoryLookup	NotesSendEmail	SAPR3GoodsReceipt
BackWebSignupAndInfoPakDnld	MicrosoftRDPEExcelStartUp	NTFilePrintPrintaFile	SAPR3GoodsReceiptInspection
BackWebUpdate	MicrosoftRDPIEStartLoadMSN	OracleAPTier1FindInvoice	SAPR3Login
CastanetChannelDownload	MicrosoftRDPOutlookOpenBox	OracleAPTier1InvoiceMultDist	SAPR3MaterialtoMaterialXfer
CastanetInitialRun	MicrosoftRDPTermServerLogon	OracleAPTier2FindInvoice	SAPR3PickingBatchDetermine
ccMail	MicrosoftRDPWordStartUp	OracleAPTier2InvoiceMultDist	SAPR3PostGoods
CitrixCAExcelStartup	MSSQLQuery	OracleARTier1InsertCustomer	SAPR3PrepareanInvoice
CitrixCAIEStartup	NetworkNewsTransferProtocol	OracleARTier1ViewCustomer	SAPR3QMResultsRecording
CitrixCAOutlookOpenFullBox	NotesAttachOpenDB	OracleARTier2InsertCustomer	SAPR3SalesOrderDelivery
CitrixCATerminalServerLogon	NotesAttachOpenInitDB	OracleARTier2ViewCustomer	SMTPsendemail
CitrixCAWordStartUp	NotesAttachServerDetach	OracleEATier1AccountInquiry	Telnet

Figure 2: A few of the thousands of Knowledge Scripts available in AppManager out of the box.

Step 2: Establish Availability Management

Availability Management has not historically been a priority for most ITSM deployments, but service availability is the number one concern of the business for an IT organization and, therefore, should be considered early on in the implementation. As defined by ITIL, this discipline optimizes the capability of the IT infrastructure, services and supporting organization to deliver a cost-effective and sustained level of availability that enables the business to satisfy its objectives. In order to be cost-effective, administrators must understand the availability priorities of the business by service. NetIQ's AppManager Control Center provides the foundation to achieve this level of maturity:

- **Implement Business Service Maps:** Availability of individual elements is less important to the business than availability of the service from an end-user perspective. Grouping elements into a Service Map View, which demonstrates the relationships between elements necessary to provide the service, allows administrators to gain a service perspective and enables impact visibility.
- **Analyze Key Performance Indicators:** Management Groups can be built in AppManager Control Center by service, allowing Key Performance Indicators (metrics) to be established to alert on meaningful threats to availability by service.
- **Prioritize Systems Administration:** There never seems to be enough hours in a day for administrators to both respond to incidents and complete tasks to ensure and improve availability. Once a service perspective is gained, however, the prioritization of events can be established in AppManager to ensure that elements that support the most critical services are receiving appropriate attention.



Figure 3: AppManager Control Center's ability to combine elements into Service Groups can be seen in this top-level view. Drill-down to view the impact on availability is as simple as clicking on the service.

Once Availability Management is implemented as described, and a process for maintaining it is established, this level of maturity can be considered achieved.

Step 3: Institute Service Level Management

To further improve alignment of IT with the business, a process must be established to collect record and report against service levels that the business cares about. NetIQ's AppManager Control Center, AppManager Analysis Center and ResponseTime Modules provide the foundation to achieve this level of maturity:

- **Establish Business Requirements:** A Service Catalog can be established in AppManager Control Center to list the services provided by IT in terms that the business recognizes. Service Map Views can then roll up into the appropriate Service Catalog item. Service Level Requirements are also collected from customers and entered into AppManager Analysis Center.
- **Measure End-User Experience:** NetIQ provides an extensive set of ResponseTime Modules, which emulate end-user behavior such as using email, using web based applications or running desktop applications over a Citrix connection. These modules automatically record data that reveal the service experience that end users encounter.

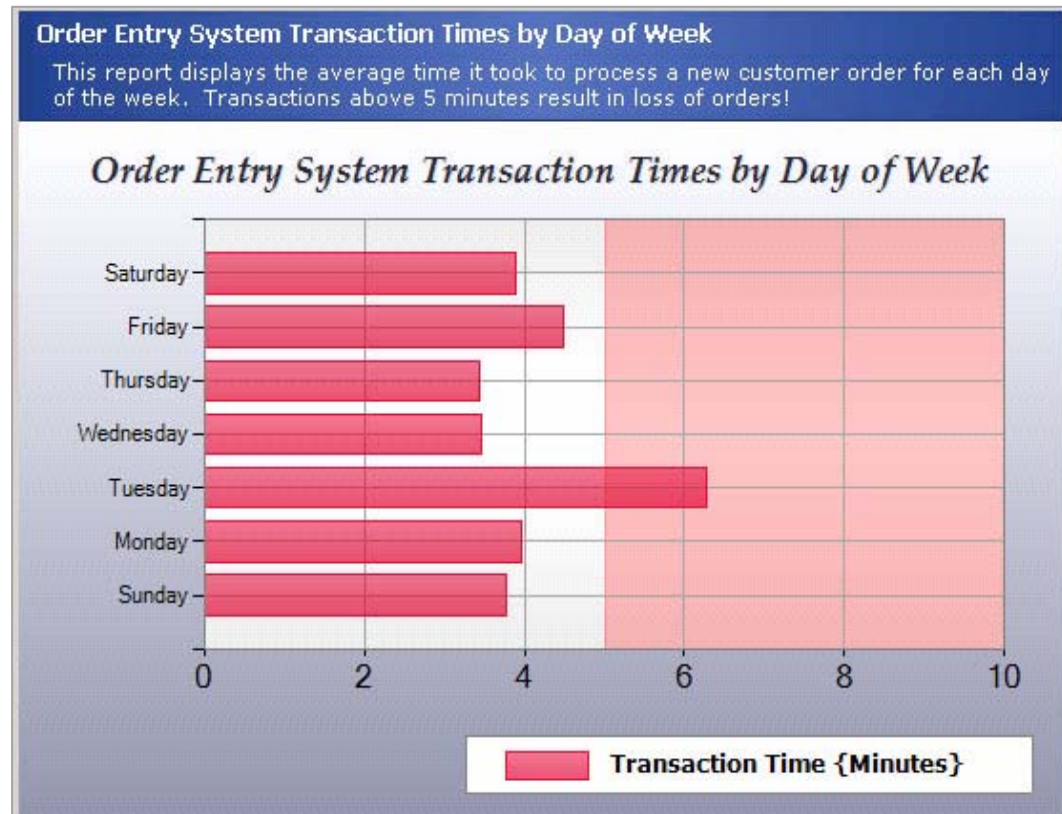


Figure 4: AppManager ResponseTime reporting can readily indicate service level violations.

- Report Service Level Achievement:** Collecting all of this data is worthless unless it can be reported in a way that quickly identifies whether service levels have been achieved. AppManager Analysis Center provides the capability to not only graphically report data but to record minimum Service Level Requirements and compare the two so that service level achievement is instantly discernable.

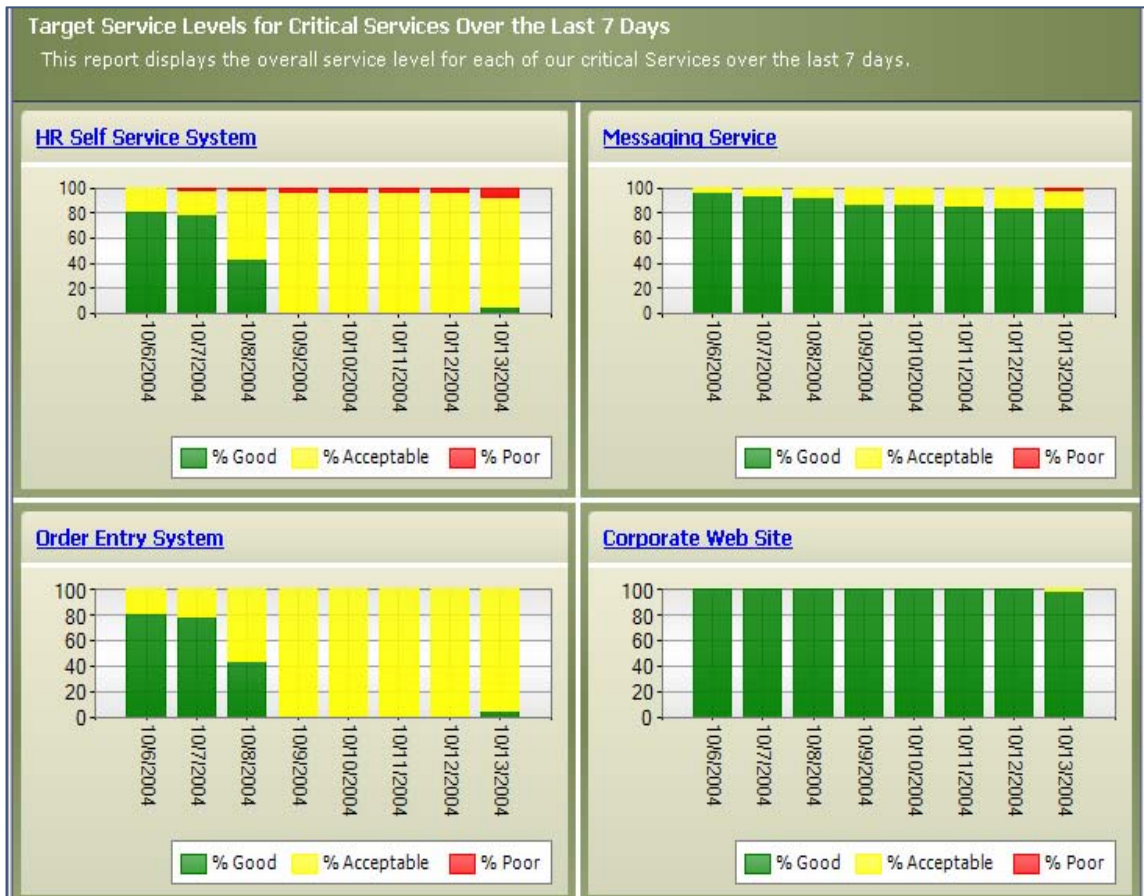


Figure 5: AppManager Analysis Center is an ideal service level achievement reporting tool.

Once Service Level Management is implemented as described, and a process for maintaining it is established, this level of maturity can be considered achieved.

Additional Commentary on Problem Management

Problem Management, as defined by ITIL, seeks to minimize the adverse business impact of incidents and problems that are caused by errors within the IT Infrastructure, and to prevent recurrence of incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation. The Problem Management process has both reactive and proactive aspects. The reactive aspect is concerned with solving problems in response to one or more incidents. Proactive Problem Management is concerned with identifying and solving problems and known errors before incidents occur in the first place.

The AppManager Suite provides both reactive and proactive Problem Management capabilities. Because of this dual role, the implementation of Reactive Problem Management should be considered during Step 3 and Proactive Problem Management during Step 4. (Further discussion of Proactive Problem Management can be found in Step 4.)

Reactive Problem Management is responsible for providing work-arounds or permanent fixes for known errors to the Incident Management team. To accomplish this, AppManager ships with a Knowledge Base that is linked to AppManager Control Center. If an object in a Control Center Service Map turns yellow or red, the Knowledge Base can be queried right from the object to look for a known error response to the event. This response may be from the included set of known errors, or custom-built work-arounds created by the customer. Also key to Reactive Problem Management is the identification of Configuration Items involved in incidents and the collection of supporting data for Root Cause Analysis. AppManager supports this by providing both an external and internal perspective of incidents through a combination of ResponseTime Modules and AppManager agents, displayed together in Service Map Views in AppManager Control Center. This allows the immediate identification of impact to end users as well as the probable cause of the incident.

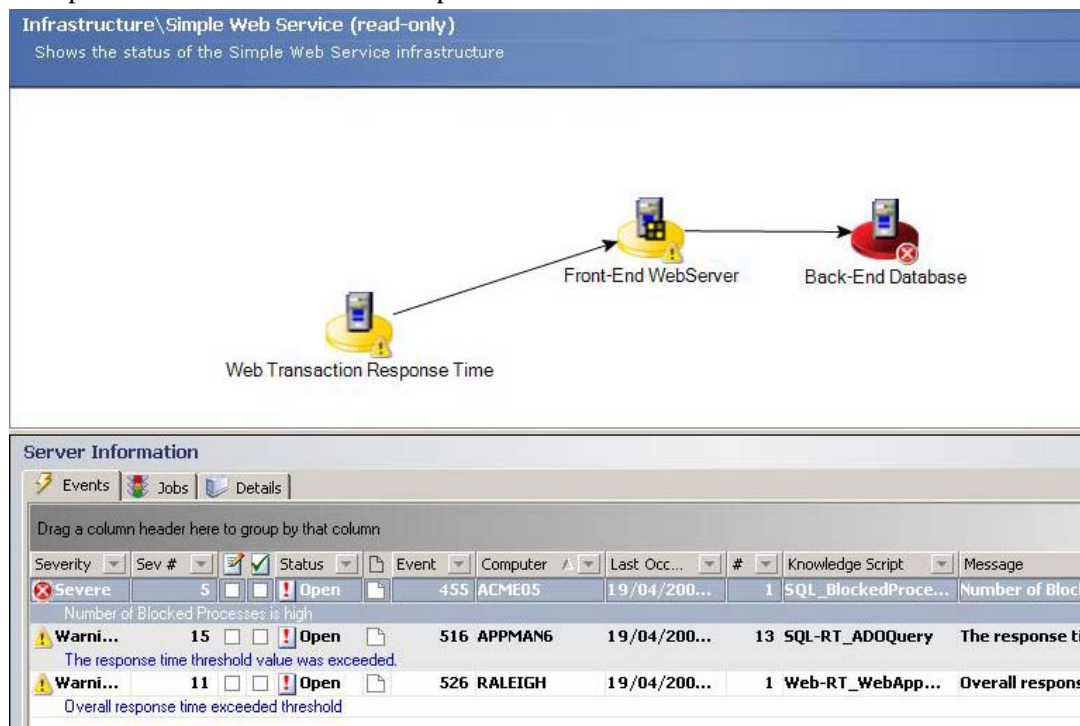


Figure 6: This Service Map View in AppManager Control Center demonstrates how the combination of a Web Transaction, a Database Transaction and the SQL Agent work together to pinpoint a root cause.

Finally, for Reactive Problem Management NetIQ helps preserve and make available data that is critical in the investigation of problems. First, NetIQ Security Manager™ provides the complete consolidation of log files from servers, applications and other services. It makes this data available during the investigation of an incident or the resolution of a problem.

NetIQ Vulnerability Manager™, NetIQ's configuration and vulnerability management solution, similarly makes it easier to investigate a problem (or incident). NetIQ Vulnerability Manager enables customers to quickly gather configuration details of a server, database or service. Delta reports can be performed to highlight changes to configurations that have occurred since the previous assessments (such as known good states or against gold builds).

Step 4: Achieve Predictive Analysis

Every IT manager would like to predict the future and be able to work according to the plan. Unfortunately, the day-to-day firefighting activities that take place in most IT organizations prevent the accomplishment of proactive activities, resulting in a cycle of more incidents. By taking the simple steps described above, however, incidents can be controlled, allowing more time for Predictive Analysis, including activities such as Resource and Service Capacity Management and Proactive Problem Management. Predictive Analysis tools from NetIQ include AppManager Analysis Center and AppManager Performance Profiler, which provide the foundation to achieve this level of maturity:

- **Predict Service Failure:** AppManager Performance Profiler has the unique ability to recognize patterns of events that have led to incidents in the past, and provide Predictive Alerts, including the anticipated time that the failure will occur. Additionally, AppManager Analysis Center identifies the most common recurring events, enabling Proactive Problem Management.
- **Automate Capacity Analysis:** Resource Capacity Analysis can be viewed as tedious work that is more trouble than it is worth. With the improved automation available in AppManager Performance Profiler, however, the most and least utilized resources can be readily identified so that capacity can be most efficiently distributed. Service Capacity Analysis is provided in AppManager Analysis Center by plotting the current trends in service usage to anticipate future needs.

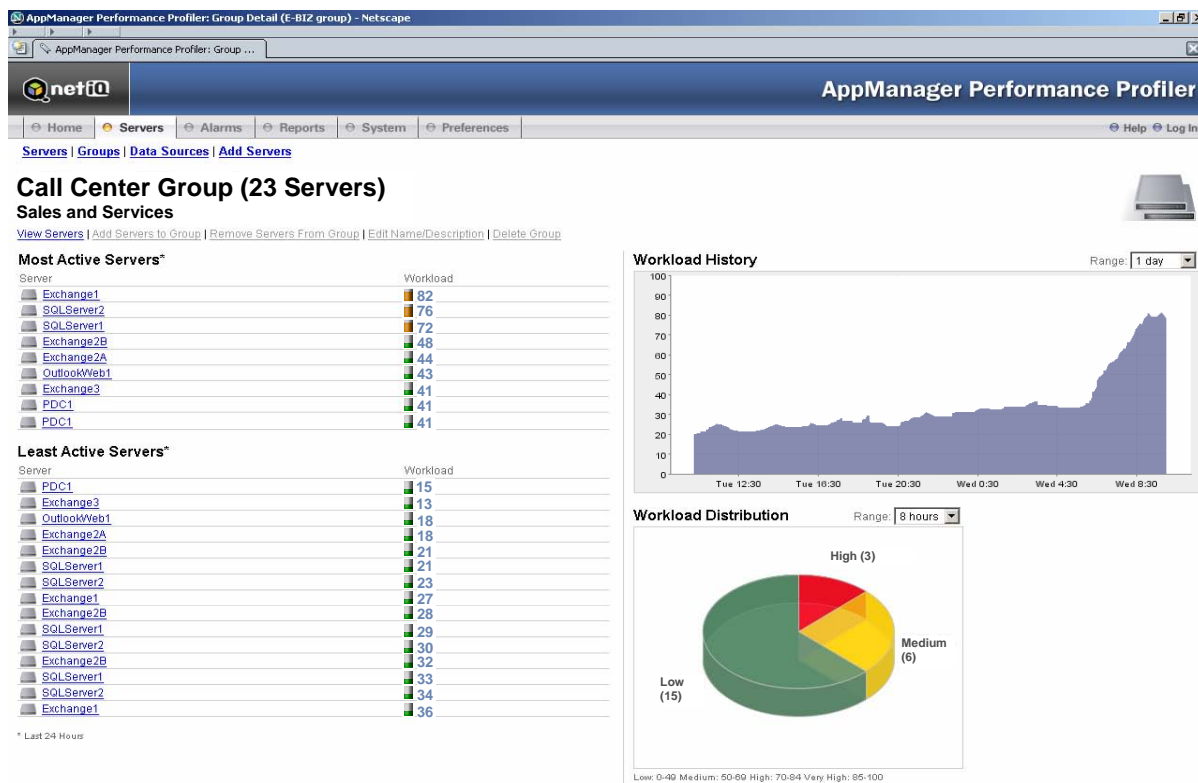


Figure 7: AppManager Performance Profiler readily identifies under- and over-utilized resources.

- **Ensure Efficient Utilization:** If there is excess capacity identified, it can be redeployed to meet areas of greater need, allowing deferred expenditures.

Once Predictive Analysis is implemented as described, and a process for maintaining it is established, this level of maturity can be considered achieved.

Intermediate Maturity in IT Service Management

The steps listed in the section above are less threatening than those described in this section. Introducing IT Service Management into an IT organization will meet resistance to change, because IT operations groups are typically not used to adhering to process. Many administrators view information as power; sharing that information through process and technology can be perceived as a threat. Completion of the steps listed above will build a record of success and improve the ability to implement the more disruptive changes described below.

There is a significant temptation to implement Change Management and its partner Configuration Management early on (even first) in the ITSM deployment schedule. Anyone with experience in IT operations understands that the majority of incidents are caused by poorly implemented changes. For this reason, most large companies already have some form of Change Management in place, even if it does not adhere to ITIL guidance. Additionally, Configuration Management is usually taking place through islands of databases and spreadsheets, maintained to varying standards by finance departments or administrators who manage the systems, with little or no interaction with Change Management.

Because IT organizations are getting by with these ad-hoc processes and because of the impact that implementation of Change and Configuration Management will have, NetIQ recommends implementation of the ITIL standards for these processes and the enabling technology as an intermediate step in the ITSM deployment schedule. The biggest impact of implementing Change Management will likely be felt (ironically) in significant resistance to change from within the IT organization, due to the perception that it impedes getting work done. The biggest impact of implementing Configuration Management will likely be felt in the cost of time and technology to accurately capture Configuration Items, understand their relationships and maintain and share this information. NetIQ has solutions to address the concerns of implementing both of these disciplines.

Change Management

There is tremendous focus in Change Management on implementing a system for recording and tracking Requests for Change (RFCs). This can be accomplished through something as simple as a web-based form tied to a database, or through the use of common help desk ticketing applications. The bigger challenge, though, is in identifying unmanaged and high-risk change that should be brought under control of the process and the Change Advisory Board (CAB). NetIQ refers to this aspect of Change Management as Operational Change Control (OCC).

NetIQ has recently developed new OCC technologies, such as Change Guardian, which provide the ability to alert and report on change activities and entitlement, as well as delegate access controls to make changes. These technologies provide the CAB with the assurance that the process is not being circumvented, and will give administrators the right level of access to accomplish their work while limiting their exposure to internal policy and regulatory compliance violations.

Another important benefit of Operational Change Control is the ability to differentiate between high-risk and insignificant change. ITIL recognizes that there must be a cost-effective lower limit to the scope that Change Management will govern. To accomplish this, it describes the concept of Standard Changes, which are common tasks that can be documented and authorized in advance, freeing the Change Management process, and the CAB in particular, from drowning in minutiae. OCC tools from NetIQ support this concept by differentiating between Managed Changes, Unmanaged Changes and High-Profile Changes, enabling logging, reporting and alerting on change type depending upon policy.

Configuration Management

Best practice guidance in ITIL calls for Change Management to be implemented in conjunction with Configuration Management. This is primarily to allow RFCs to be cross referenced to Configuration Items (CIs) for the purpose of reporting changes by CI and to assess the potential impact that a change will have on other CIs that are related in providing a service. This is accomplished through the implementation of a Configuration Management Database (CMDB) that is integrated with the Change Management tool.

CMDB is a leading topic of discussion among ITIL practitioners, because of its central role in supporting other disciplines and the level of difficulty that it introduces into an ITIL/ITSM deployment. The current ITIL guidance seems to be more applicable to a mainframe environment, where Configuration Management is more centralized and therefore more easily accomplished. In large distributed environments, the challenge of building and maintaining an accurate CMDB becomes exponentially more difficult.

An emerging answer to this challenge is the concept of a “Federated” or virtual CMDB, which leverages the numerous databases that already exist in most IT organizations, collecting metadata on which CIs the databases contain, but does not retain the detailed data specific to individual CIs. Examples of the types of databases that could be leveraged include asset or financial management systems, network administration tools or systems management tools such as the base AppManager QDB.

NetIQ also provides Configuration and Vulnerability Management tools, which support additional ITIL requirements for Configuration Management. NetIQ Vulnerability Manager enables organizations to define service-oriented baselines and measure compliance to those baselines as described in the Configuration Management chapter in the *ITIL Service Support* book (section 7.3.6). Service-oriented baselines are configuration standards that are unique to a given business or technical service. Adherence to these baselines is needed to ensure services operate as intended. Using these baselines, the product enables Configuration Management to quickly identify exceptions that are likely to cause performance problems or introduce security-related risks.

NetIQ Vulnerability Manager will also provide a check against the accuracy of the CMDB by scanning for new CIs and reporting changes to existing CIs. It can inventory applications installed, services running, user accounts, files and directories, service packs and patches, policy settings and other configuration-oriented attributes of a server. This is useful information for other ITIL disciplines such as Change Management, where it can enable confirmation of the currency of Requests for Change (RFCs).

Advanced Maturity in IT Service Management

Most IT organizations reserve the remaining disciplines, Release Management, FMITS (Financial Management for IT Services) and ITSCM (IT Service Continuity Management) for follow-on phases of ITSM deployment. This can be attributed to the fact that application development teams often shoulder a portion of the Release Management activities, that FMITS is supported by accounting teams and often is focused primarily on budgeting, and that ITSCM is either outsourced or ignored. The immediate value of these disciplines to the IT organization, therefore, is less than that of the disciplines previously discussed. NetIQ has not yet developed technologies in purposeful support of these disciplines, due to the lack of market interest in them. This decision is regularly revisited and, when appropriate, will change.

Security Management: The Forgotten Discipline in ITSM

As mentioned previously, there is an entire book on the topic of Security Management in the ITIL library. It is seldom referred to and is largely regarded as less valuable than other

leading standards in security such as ISO 17799⁴. Still, the fact that there is an entire volume dedicated to the subject indicates its importance to the framers of ITIL, and with the continual addition of new government regulations to comply with, most of which contain IT security standards, security can no longer be viewed as an independent domain.

Historically, there has been friction between Security Management practitioners and the IT operations team. In light of the need to meet new compliance mandates, however, this barrier must be lowered. According to Ernst & Young, 70% of surveyed companies reported SOX Section 404 related compliance costs were 50% greater than original estimates in the 2004 - 2005 timeframe⁵. Important steps in reducing these costs include operationalizing compliance activities by embedding them in day-to-day processes and leveraging automation that supports both Service and Security Management reporting requirements.

NetIQ is pioneering thought leadership in the convergence of Security and Service Management disciplines by providing the technology that enables the controlled flow of information between them. For example, NetIQ's security incident management solution, NetIQ Security Manager, can be integrated with AppManager through a standard connector, enabling correlation of incidents that affect both the security posture of the organization, as well as the availability of services. This functionality meets a requirement, specifically described in the Availability Management chapter of the ITIL *Service Delivery* book, which states, "The importance of Availability [is] recognised as one third of the security 'CIA' tenet: Confidentiality, Integrity and Availability." This capability drives efficiency, as multiple teams do not have to duplicate efforts in responding to incidents that are the responsibility of another group, and incidents are not "lost" in the transfer between them.

Another bridge between Security and Service Management is in the Change Management process. Ensuring that controls are in place to provide reasonable assurance that system changes are authorized is a key requirement of most security-related regulations and standards. While a process for approval of changes is necessary, the technology to audit, report and control compliance must also be in place. NetIQ's Operational Change Control products provide a solution for this requirement that benefits both the Security and Service Management disciplines.

A final example of NetIQ technology driving convergence is related to Configuration Management. Security-related regulations dictate that controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes and assist in the verification and recording of the current configuration. NetIQ's Vulnerability Manager provides this level of protection by monitoring and reporting on access to the configurations of high-value systems.

⁴ "Aligning CobiT, ITIL and ISO 17799 for Business Benefit" by the IT Governance Institute and OGC

⁵ Ernst & Young, *Emerging Trends in Internal Controls*

IT Service Management Technology Architecture

Elegant Integration

IT organizations implementing ITSM are pursuing one of two options for tool selection. Frameworks, where one or two vendors with broad product suites meet most of the requirements, and Strategic Architectures, which are a collection of best-in-class technologies, integrated to form a cohesive unit. Unfortunately, the most common approach for tool selection seen among IT organizations implementing ITSM is actually neither of the above, with tool silos selected by various groups with little regard for integration. This approach is rejected as incompatible with IT Service Management best practices.

The Framework approach has the obvious benefit of a reduced number of vendors to manage, but there are inherent risks to this strategy as well, including:

- Most framework products were built through acquisition, so integration may be a bigger challenge than expected
- Once in place, the vendor may act like a monopoly
- If the vendor sunsets a product you rely on, it will be more difficult to replace
- Deployment costs typically skyrocket due to complexity and requirements for specialized consultants
- Finding and retaining qualified employees to manage a framework can be challenging, due to relatively few implementations

The Strategic Architecture approach has two risks to consider:

- Integration points must be designed early on to avoid silos
- Product resource conflicts may exist on some systems

But the benefits to Strategic Architecture can be substantial:

- Flexibility to choose the best tool to meet a given requirement
- Freedom to selectively replace a tool as desired
- Shorter and lower cost implementations, phased as required
- Easier to train support staff on point products
- Competition among vendors breeds efficiency
- Feature overlap, if it exists, can provide mission-critical redundancy

Clearly, the Strategic Architecture approach has greater benefits with fewer risks, but there are some guidelines to follow to avoid “silo syndrome”. First, consider vendors that support data sharing, or “Elegant Integration,” to ease the integration design. Look for multiple connection methods and open data sources. Second, gather requirements and buy-in from all interested groups because silos arise as much from personality conflict as tool incompatibility. Selection should also be made based on alignment with a broad set of requirements such as ITIL, CobiT, Six Sigma, etc.

Critical to supporting ITIL is the integration of management tools, because the processes are so integrated. NetIQ’s AppManager offers out-of-the-box connectors to many other management applications, such as Remedy, Tivoli Enterprise Console, HP OpenView, Micromuse NetCool, Microsoft MOM and several others. Connectors also exist for many industry standard alerting solutions such as Hiplink and Telalert.

The diagram below demonstrates how NetIQ technology can be leveraged to support the workflow of IT Service Management through an Incident Lifecycle.

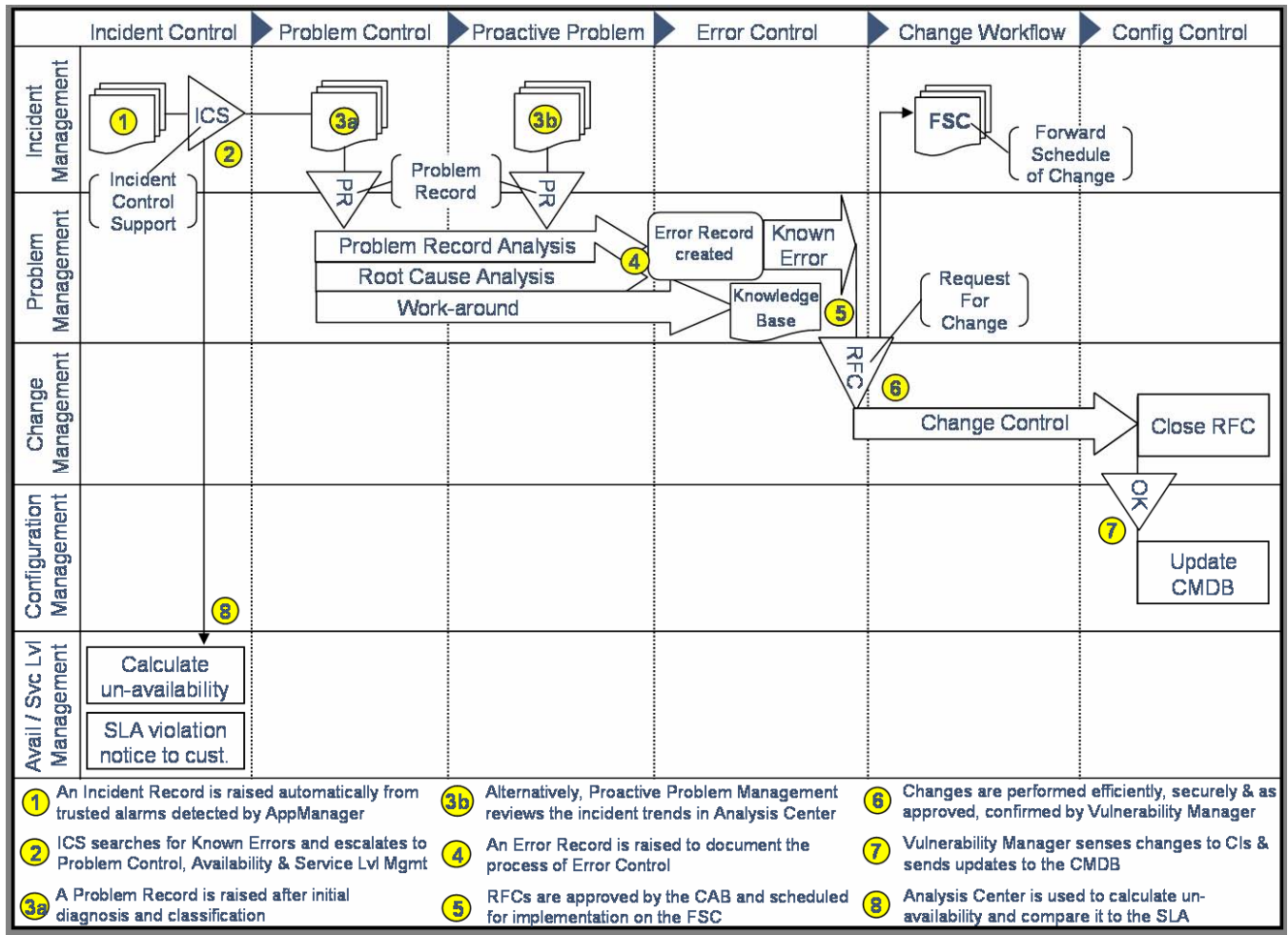


Figure 8: Service Management workflow demonstrating Elegant Integration with NetIQ tools.

Openness

NetIQ's AppManager is known as one of the most open enterprise management solutions available today. With an open database schema and standard scripting language support, AppManager has realized an explosive growth in 3rd party extensions. Multiple platform support, usage of industry standards such as ODBC compliant relational databases and XML, and use of standard VB and PERL scripting languages are a few examples of the open standards that AppManager meets. These characteristics heavily determine the ease of migration and integration and enable future growth.

Usability

NetIQ's AppManager boasts one of the most user-friendly interfaces available in the market today. Using simple "drag and drop" actions and utilizing any number of the over 2000 scripts that ship standard with AppManager, administrators and Systems Engineers can quickly get up to speed and begin using the product within hours and days as opposed to weeks and months. There is no need to learn complex scripting languages or archaic interfaces.

Backup and Availability

NetIQ's AppManager utilizes a Microsoft SQL Server database as its central repository. All configuration information and event\data streams are stored there. Microsoft SQL Server is easily backed up and recovered using most commercially available backup solutions. In addition, SQL Server can be run in a "High Availability" environment by utilizing clustering or log shipping.

Control and Security

NetIQ's AppManager includes a built-in security model, which ensures that the proper personnel have rights to carry out their job functions. New security groups can be created utilizing the included security management tool. Over 100 points exist in AppManager where security functions can be clearly defined. From the ability to update comments associated with events to the ability to launch new monitoring jobs or change monitoring profiles, all functions can be controlled with a significant level of granularity if required. In addition, AppManager can be coupled tightly to Microsoft SQL and Active Directory security groups enabling a simple "role-based" security module that adapts easily to changes in organizational structure.

Conclusion

Initiating an ITSM deployment should be viewed similarly to the implementation of a large ERP system. It will affect the entire IT organization as well as users of the services that IT provides. This is why a well-planned deployment roadmap, with associated objectives, designated resources and the full support of upper management, is critical to success.

The approach described in this paper is designed to leverage the process that is most likely already in place to some degree (Incident Management), elevate it to Availability Management, demonstrate commitment to the business with Service Level Management, and drive efficiency with Capacity and Problem Management. Implementation of these disciplines first will be less disruptive and can be accomplished at a lower cost than the other disciplines, allowing a record of success to produce momentum for the challenge of implementing Change and Configuration Management.

As the IT organization builds its maturity in IT Service Management, special attention is necessary for embedding Security Management best practices and policies in the processes that are developed. This operationalization of security standards will result in greater efficiency, easier audits and better compliance with internal and external policy. Ultimately, the effective combination of Service and Security Management enables the business to take more precisely calculated risks in pursuit of business growth.

NetIQ technology is uniquely capable of enabling this path to effective IT Service Management with tools that support each of these disciplines. This realistic and practical approach can minimize the risk of implementation failure and is cost-effective in comparison with a framework or CMDB-first approach. Enable your IT Service Management implementation with NetIQ's practical approach and proven technologies.

About NetIQ Corporation

A World Leader in Systems and Security Management

NetIQ is a leading provider of integrated systems and security management solutions that empower IT organizations with the knowledge and ability necessary to assure IT service. NetIQ's Knowledge-Based Service Assurance products and solutions include embedded knowledge and tools to implement industry best practices and to better ensure operational integrity, manage service levels and risk, and ensure policy compliance.

NetIQ's modular, best-of-breed solutions for Performance & Availability Management, Security Management, Configuration & Vulnerability Management, and Operational Change Control integrate through an open, service-oriented architecture allowing for common reporting, analytics and dashboards.

NetIQ counts more than 4,000 of the world's leading enterprises as key customers. In addition, our partnerships with industry leaders, such as Microsoft, IBM, HP and Dell, give NetIQ a unique advantage in the global marketplace. With customer-proven solutions and strong relationships, NetIQ delivers the tools you need to reduce your risk and deliver value from day one.

To learn more about NetIQ, visit us online at www.NetIQ.com.