Spring 2009

Implementing the Information Technology Information Library (Itil) Framework

Lawrence Wade Lowder
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Regis University
School for Professional Studies

Master of Science
In
Computer Information Systems

Implementing the Information Technology Information Library (ITIL) Framework

Lawrence Wade Lowder

June 24, 2009

Change History Tracking

Date	Version	Description	Author
5/7/2009	1.0	Initial Draft	Wade Lowder
5/14/09	1.1	Updated with Peer review suggestions	Wade Lowder
5/28/09	1.2	Updated formatting for better consistency	Wade Lowder
5/30/09	1.3	Added in final process implementation information	Wade Lowder
5/31/09	1.4	Began final summary section	Wade Lowder
6/8/09	1.5	Made overall revisions to content and structure	Wade Lowder
6/9/09	1.6	Added more analysis to chapter 2 and tied in research with the project analysis sections	Wade Lowder
6/10/09	1.7	Update based on advisor comments to chapters 1 and 2.	Wade Lowder
6/13/09	1.8	Update overall content based on advisor comments.	Wade Lowder
6/14/09	1.9	Reviewed content and added updated authorization pages from new Regis template.	Wade Lowder
6/21/09	2.0	Revision based on comments from reviewers	Wade Lowder
6/23/09	2.1	Final revisions based on advisor review comments	Wade Lowder

Acknowledgements

I would like to thank the following people for making this project and this paper possible. My loving family and especially my wife, Christy Lowder, for her help keeping up the day to day of the family with an "absent" husband. I would also like to thank my colleagues and friends including;

- Josh Gilmore
- Peter Hastings
- Monte Whitbeck
- Jag Kalagiri
- Carie Zoellner-Buell

Finally I would like to thank my advisor through this process Fred Lengerich, especially given the volume and time required to read the material and provide great direction and advice.

Abstract

This project proposes the implementation of the Information Technology Infrastructure Library (ITIL) framework for a mid-sized Real Estate Investment Trust (REIT) specializing in commercial warehouses. Due to rapid growth, lack of process and lack of business visibility, the Information Technology (IT) department struggles to provide highly reliable business systems that meet the requirements for the business. The gap in business relationships results in a negative image for the IT department and causes situations where individual business groups contract directly with outsourced IT providers. After developing the IT solution, the business group contacts the internal IT department for involvement with the deployment. The IT department must ensure the outsourced solution will work with internal IT systems or networks regardless of the technology stack or support model. Often, the costs associated with this last minute support are not captured or reported within the overall outsourced IT project.

The IT department consulted with Forrester research and Capgemini to review the overall IT environment and process maturity. After performing the review and analyzing the findings, IT management determined that process improvement was required to improve overall IT services and IT service delivery speed. Rather than focus on what led to the decision to implement ITIL, this project will discuss how ITIL provided the foundation to ensure timely, consistent and reliable delivery of IT Services. ITIL also helped improve the IT departments' image with the business by assisting in higher quality implementations and consistency resulting in less IT downtime and more controlled IT systems. When asked about the benefit of ITIL, Carie Zoellner-Buell, a VP of Global Infrastructure and Operations said, "ITIL has taken the organization to a whole

new level of operation that we were never able to attain in the past. Using ITIL based processes has allowed us to be much more effective in managing IT by adding structure and efficiency".

Table of Contents

Chapter One: Executive Summary

Due to the REITs high rate of growth as mentioned previously, the business tends to invest heavily in growing out new infrastructure to support business needs. As a result, the normal operating method is to keep operating the existing infrastructure as best as possible while implementing new technologies very rapidly. This operating model often results in lack of repeatable process and policy, gaps in overall operations, legacy systems that are never decommissioned and lack of hardware and software standards. The IT department would like to shift the focus on how it operates. As part of the maturity analysis conducted by Forrester and Capgemini, the IT department was rated a level 1 or "utility level" rating. The level 1 utility level rating is a measure of IT maturity. IT departments at level 1 have basic support functions in place, but often lack overall consistency and repeatability in the support and delivery of IT services. One of the goals of this project is to develop and implement ITL processes that allow the IT department to become proficient at the utility level. This will allow the IT department to move up to the level 2 partnership level with the business and reduce gaps in operations and overall IT Service Delivery. ITIL is a set of process standards or framework for managing a technology environment. ITIL was first documented in the late 1980's to address the needs of the British Government to implement consistency in the way it managed and controlled IT systems OGC (2000). As described in an InfoWorld article (Steinberg 2006), "Companies that have initiated ITIL efforts are already seeing higher customer-satisfaction levels and reduced costs and labor. Although not a panacea for all IT challenges, ITIL is a fundamental conceptual change for how IT will be doing business in the 21st century. Its time has come".

The IT department needs to address scalability and efficiency to maintain consistent delivery levels for the business. By leveraging ITIL and the Microsoft Operations Framework (MOF), the IT department would like to more easily deploy new technology, maintain existing technology and provide adequate operational and support processes. The IT department will attempt to improve overall efficiency, consistency and scalability by implementing ITIL using the delivery and planning templates and tools provided by MOF.

Before the start of the project, the IT department conducted surveys among different business leaders within the company. The results of the surveys indicated that the business wants IT to be firmly in level 2 as a partner to the business on the IT/Business demand and supply curve as described below in the IT Demand and Supply curve from Vaughan (2008).

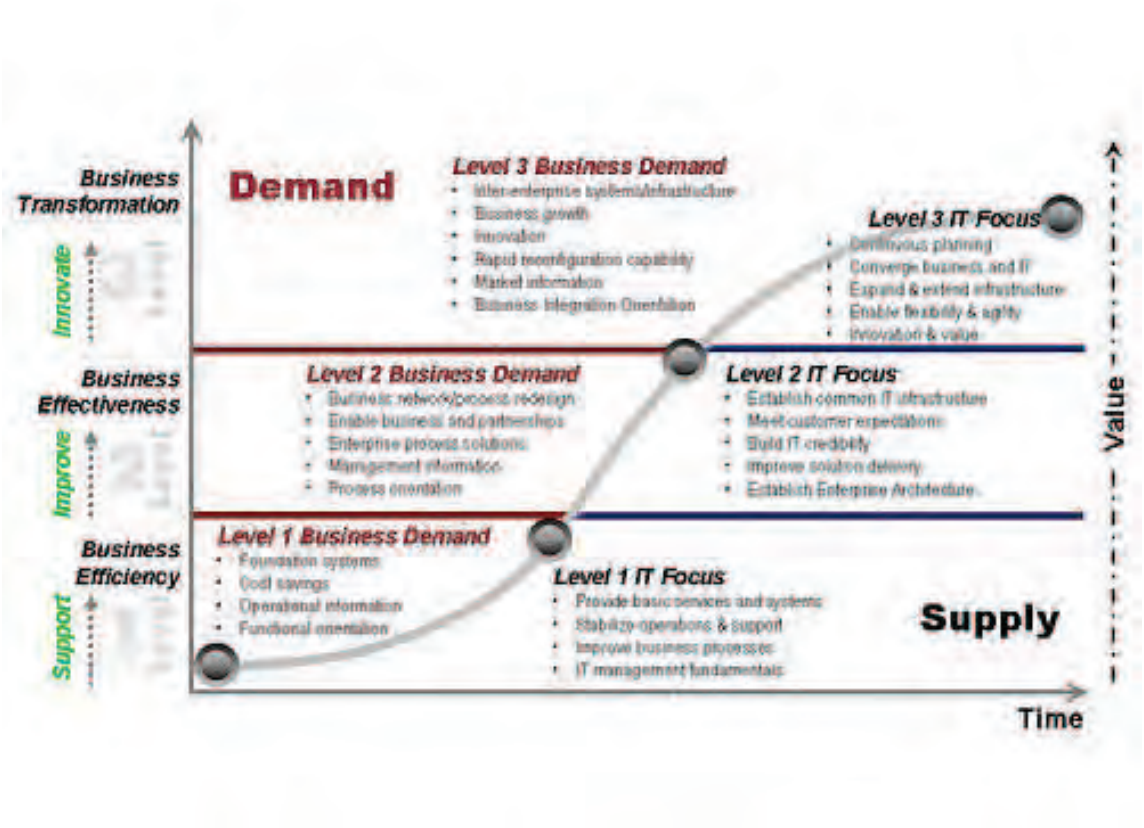


Figure 1: The IT Demand and Supply Curve

The company prioritized level 2 IT goals are:

1. Establish a common IT Infrastructure
2. Meet customer expectations
3. Build IT credibility
4. Improve Solution delivery

From a business perspective, goal one is about consistency in the delivery of hardware and applications. The lack of common hardware and software standards has led to a reduction in overall support which equates to greater service disruptions due to overly complicated and non-standard computing environments. This leads into item two, meet customer expectations. The business expects that service requests and service

issues are resolved within a reasonable and agreed upon timeline. The IT department is not however able to commit to any standard response times or Service Level Agreements (SLA's) due to the variety of hardware and software and lack of process in the environment. The third IT goal from the business is to build IT credibility. The business needs to rely on the IT departments' ability to deliver services and deliver them within agreed upon service levels. The business needs this credibility to ensure that business technology needs are delivered how and when needed to prevent any disruption to the business. The fourth and final goal is to improve solution delivery. This goal is closely related to the previous goals and also includes the expectation that IT solutions are quality working products. This implies increased project, development and testing rigor for IT solution planning and delivery projects. These goals were ranked in this order so that the key business goal can more easily be met. The survey indicated that the fifth goal from the IT Demand and Supply curve, establish an Enterprise Architecture, was not a high priority at the time. The corresponding business goals aligned to these IT goals include:

1. Business network/process redesign
2. Enable business and partnerships
3. Enterprise systems that support business process
4. Process orientation

The first business goal of process redesign is a high priority because of the need for more operational efficiency and agility in meeting new business challenges. As business process are redesigned, the business will rely more on automation and IT systems to handle workflow and business management related tasks and processes. This goal will

offer greater business agility and operational efficiency. The greater reliance of IT systems within business processes, necessitates a more closely integrated IT and business relationship. The second goal is the enablement of business partnerships. IT enables this by providing consistent technologies that enable more automated tasks such as electronic data interchange (EDI), federated identity management, ecommerce, business to business (b2b) processing and automated financial processing and reporting among others. The third business goal is enterprise systems that support business processes. One of the key considerations for this particular implementation is how to map new and more efficient business processes into the legacy Enterprise Resource Planning (ERP) system. During the course of this project, the business determined that the business process redesign would be better aligned by implementing a new ERP system called SAP. The fourth and final business goal is to become process oriented. By fulfilling the goals mentioned above, the business hopes to realize this goal which will allow for better agility in new business processes, better ability to react to changing market conditions and the ability to exceed customer demands and expectations within a cost effective, repeatable model.

The IT department believes it currently operates at the utility level (Level 1) and occasionally operates at Level 2. By implementing ITIL based processes, the IT department will attempt to improve its overall operations and consistently operate at level 2 and meet the above level 2 IT goals. By operating at Level 2, the business will see consistently faster resolution of incidents, better overall communication and more proactive resolution of potential IT service disruptions which will allow for more effective business processes and partnership between the business and IT. Above all,

these improvements will allow the business to more easily meet its level 2 business demand goals.

Since the IT department has already implemented a project methodology called the Microsoft Solutions Framework (MSF), the project team followed the MSF methodology to implement the ITIL framework. The MSF approach consists of 5 project steps. These project steps will be discussed further in the subsequent chapters.

According to a survey conducted by Forrester Research in 2006 of 62 enterprises that have implemented ITIL processes, 70% realized better quality of delivery from IT operations, 52% achieved better process efficiency and 36% saw an increase in productivity in IT Operations. Following the implementation of ITIL processes within the project, the IT department began to see a drop in the number of unplanned outages resulting in significantly improved system uptime and availability in some cases by over 10%, faster incident response and resolution times, more controlled IT changes resulting in fewer failed changes and better overall IT service delivery. The improvements realized by the IT department due to the implementation of ITIL processes were noticeable in IT metrics and business satisfaction that was collected both in surveys and general day-to-day correspondence. The IT department improved overall internal communication by establishing a common terminology and service catalog to align with the business needs. As a result, the IT department consistently attains the IT level 2 maturity goals. The IT department also realized unexpected benefits from the ITIL implementation by using IT service descriptions when cutting operational costs and during restructuring events due to a slow-down in the business during the 2009 recession.

Chapter Two: Review of Research

MOF and ITIL research

When deciding to implement ITIL, companies look for several key areas for improvement according to a phone survey conducted by Forrester research in July of 2007. Of the survey respondents, 71% are looking to improve the reliability of systems and networks, 62% are trying to improve consistency and quality of IT processes and 61% are hoping to improve the overall execution of major projects (Hubbert and O'Donnell 2008). During this project, the team included basic metrics within each process area to determine the effects of new process changes on the overall reliability of the environment, efficiency of processes and the success rates of change. These measurements can then be used to compare the results of the ITIL changes with the improvements that other companies also look for when implementing ITIL.

Companies that implement ITIL are seeing both operational gains and tangible benefits. Proctor & Gamble reported a saving of over $125 million following the implementation of ITIL in 2002 according to a Network World article (Dubie 2002). According to a 2006 InfoWorld article (Steinberg 2006), Caterpillar improved incident response time targets by over 60%. Although some companies are beginning to publish the savings or benefits they are realizing from ITIL, within this project, the team narrowed the metrics to understand the small improvements. This information, such as improvements in change delivery, incident response times, service monitoring improvements and related efficiency has not been summarized to provide an overall cost savings or efficiency improvement dollar amount at the time this project was completed.

When asked about the "negative elements" that were encountered during ITIL implementation in an analysis by Forrester research by Peynot (2006), 52% encountered internal resistance to change, 29% found that business units or internal customers were not prepared to be involved in the new process and 21% indicated they did not encounter any negative elements during the ITIL implementation.

To better understand MOF and ITIL, the author attended the Microsoft course MOF Essentials and also attended three ITIL courses and was certified in each including the ITIL Foundations, ITIL Support and Restore Practitioner as well as the ITIL Release and Control Practitioner.

The ITIL Foundations course provided the basic overview and history of ITIL including an understanding of the interdependencies between all of the related ITIL topic areas. It also provided the basic understanding of ITIL processes and the essential terminology used throughout all of the ITIL processes. This course provided a good overview of all of the major ITIL sections. However it did not necessarily provide real substantive guidance on the actual implementation steps for the ITIL processes. This course did assist in the overall ITIL process relationships so the actual selection and planning of ITIL process areas took into consideration the process interaction points. The MOF Essentials course did provide the process interrelationships as well as the practical how-to methodology for implementing ITIL. The courses should both be taken as they compliment each other with the overall theory as well as the application.

The ITIL Support and Restore course provided an in depth look at both the Incident Management and Problem Management process areas. It also included a close look at the Service Desk functional and process area. The ITIL Release and Control

course provided an in depth look at the Change Management, Release Management and Configuration Management process areas. The ITIL Support and Restore course also provided the in depth analysis around the theory, however the practical application and analysis was lacking. The practical process application was covered in the MOF Essentials, however the Support and Restore and Control and Release material did provide enough detail around the process that it actually helped speed-up the overall analysis and process design using the MOF templates. By understanding the possible process steps and guidance from the ITIL course, the team was able to analyze the MOF templates and determine the most effective process steps for the environment, without omitting any important ITIL process items.

In addition to the ITIL courses and certifications, the author acquired all of the literature available online from Microsoft for the MOF and the ITIL version 2 (Blue Book) as well as the ITIL version 3 book series. This material was used both for project planning as well as reference during the project implementation. Often the process descriptions in the manuals are required to clarify finer details and descriptions for the project team during process analysis. The material was very complete, however at some points the organization of the material is difficult to follow especially when comparing the ITIL version 2 and version 3 material. The material is a reference to use on a per process basis. While it is important to know the process dependencies, as a team develops process, it is easier to focus on one process at a time rather than expecting the entire collection of ITIL guidance to be examined at once. Although the ITIL guidance was quite extensive, the team leveraged the MOF templates to assist in narrowing process focus during the process design phase. The MOF templates are more concise than the

ITIL guidance and allow greater clarity on the design process by providing a starting point that can be tailored to any environment relatively quickly.

Latest Developments in MOF and ITIL

The MOF and ITIL topic areas have evolved substantially over the past 3 years. MOF has expanded to include more operational components as well as more Business/IT alignment, portfolio management and staff management. The latest MOF guidance also provides an overall lifecycle for the various processes. This brings greater clarity around when process steps should occur and what steps should minimally be in place for providing IT Services. IT departments can use this as a foundation for determining overall cost for delivering IT services. Business users can make more informed decisions on what services should be continued, added or removed based on the cost and value the service provides. The latest version of MOF includes better definition and mapping from the MSF development portion into the MOF operational control. This is important as it covers the IT service from the initiation phase to the final service decommission phase in a more complete service lifecycle. Additionally MOF version 4.0 includes a Service Management Function (SMF)[1] that covers the Governance, Risk and Compliance area of IT. This is an improvement because it allows companies to integrate operational processes with governance and control process. The SMF reduces the amount of overhead when proving effectiveness of process for regulatory requirements such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and others. Since the control environment and operational environment are one and the same, IT departments no longer need to add specific regulatory controls to their normal job duties. If the process is designed correctly, the

[1] Each phase of the IT service lifecycle contains service management functions (SMFs) that define the processes, people, and activities required to align IT services to the requirements of the business. Each SMF has its own guide that explains the flow of the SMF and details the processes and activities within it.

regulatory controls are part of the normal day to day control activities such as change management, incident management, problem management and configuration management and others. Regulatory controls were a particularly challenging aspect of the ITIL implementation, due to their disparate nature and general lack of integration with normal daily operational processes. The IT teams were following solid processes however they also had "add-on" steps to document for SOX. If a system was in scope for SOX, the team had to consciously remember to perform the add-on steps. With the new ITIL processes it is more manageable and assists the IT team in making the control framework more a part of normal processes rather than a separate list that the IT team manages to every once in awhile or whenever an auditor asks for information. The new ITIL process is less likely to fail because it removes a decision point based on an external classification (in scope for SOX or out of scope for SOX) instead all production systems are following the same operational process rigor. An additional initiative was started after the ITIL implementation to assist in reducing the number of in scope regulatory controls and integrating the new controls with the ITIL based processes.

Recently the ITIL version 3.0 (v3) guidance has become more prevalent within the IT community due to the release of the ITIL v3 training courses. As more IT professionals are trained in ITIL v3, more companies will begin adopting it and updating existing ITIL process to the new ITIL v3 structure. According to itsmwatch.com, the main differences in ITIL v3 are the realignment of topic areas into five books;

1. Service Strategy
2. Service Design
3. Service Transition

4. Service Operation
5. Continual Service Improvement

The Service Strategy section provides an overview of how to establish a service framework. This is a great addition to the ITIL guidance since this specific and detailed instructions and objectives was missing in v2. It also provides information on how to determine what an organization should implement and why. This helps alleviate some of the issues that companies had by taking a one size fits all approach. The service strategy section provides tools that a company can use to determine what service areas can best align the IT department and IT services with the business and future business goals. The addition of this guidance should assist ITIL implementation teams in including the business sooner in the ITIL implementation process. This should allow IT departments to focus ITIL more closely on the high business value processes and realize faster improvements to IT business services with the greatest impact.

The Service Design section provides the methods an IT department can use to actually design the services and the service management processes. This includes the updates and changes to existing services to improve performance and adapt to changing environments including regulatory changes. This is important as it provides the how-to for taking the business processes and designing and implementing the appropriate IT services. This section was fairly theoretical in the ITIL v2 model. This is one reason the MOF guidance was used by many companies as it aided in the design of processes that the ITIL guidance assumed the implementer already knew how to complete. Although the ITIL v3 includes service design, some companies may continue to use the MOF

templates for time savings and ease of use or simply because the ITIL Service Design book is too much material to read.

The Service Transition section discusses how to develop, improve and apply new or changed service capabilities into production. This section adds value by ensuring service improvements and additions are introduced safely and in a controlled manner. The IT department benefits by implementing this section as it assists in ensuring compliance with SLA's, stability in the environment and good business relationship with customers who are able to continue operations without disruption.

The Service Operation section covers the methods and practices that are used to manage service operations to obtain the best possible effectiveness and efficiency while still maintaining stability. The Service Operation section is the cornerstone of the new ITIL guidance because it provides the detailed guidance around managing the day to day ITIL services as well as the control perspectives for dealing with issues or problems, availability, capacity and scheduling. The operations guidance provides the IT staff with a solid method for using processes to get the best possible operational results. This guidance was a little vague in ITIL v2 and made ITIL process training for process participants more challenging. Many of the questions that the trainees raised were operational in nature and were not always answered by the process. Unfortunately some of these questions were only answered over time once the process was implemented and performance metrics were collected (also called Key Performance Indicators or KPI's) and measured.

The Continual Service Improvement section provides the methods to ensure the IT services and service management processes are providing the best possible business

value over time. This section is based on the Deming quality model plan-do-check-act. This section is important as it provides the roadmap for maintaining the process and services once they are rolled-out. The prior ITIL v2 guidance did not provide a great deal of information on how to maintain processes once they are implemented. As discussed further in this paper, without a solid structure for maintaining processes, it is difficult to keep process in place and effective due to changes in business process, regulations, technology and staff. This section also discusses the strategies for improving services over time, but also managing the process for determining when an IT service has reached the end of its value proposition to the business. The team found this concept interesting as this is not usually "in-scope" when implementing a new IT service for some organizations. This results in a collection of IT services that are maintained over time that may be costing more to sustain than the value they provide to the business.

To summarize, ITIL v3 expanded and added to various topic areas to provide more specific guidance on the process areas as well as the how-to aspects of ITIL implementation. The how-to aspects for implementing ITIL, including the ones listed below, will allow for more thoughtful and planned ITIL implementations by removing some of the guess work that ITIL implementers were faced with creating themselves in ITIL v2. According to itsmwatch.com, these improvements can be grouped into the following general topics,

1. How to develop a business-driven strategy for IT service management.
2. How to design a system to support the chosen strategy.
3. How to transition the newly designed system to the production environment (in terms of people and processes as well as technology).

4. How to support operations in an ongoing fashion.

5. How to continue improving processes and operations.

Contribution of this project to the field

One of the objectives of this project analysis is to provide IT professionals with some insight into the challenges and rewards of implementing an ITIL framework. It should also assist in the planning and implementation of ITIL by expanding on various tools, methods and templates that can be used to speed the delivery and keep documentation consistent. This project should also assist IT professionals in understanding that once ITIL processes have been implemented, there is a great deal of monitoring, auditing and updating that must take place to keep the processes efficient, relevant and part of the normal course of business. IT professionals will also recognize that part of any project includes the ability to prove success to the project sponsor and to the business. This success may not always be as apparent in IT project deliverables as it is with IT process deliverables. Unfortunately, this success is also difficult to prove without a good pre-implementation baseline of the process area and good KPI's to demonstrate improvement in the after-implementation process area.

Chapter Three: Methodology

The Microsoft Solutions Framework

The project methodology for this ITIL implementation followed a modified Microsoft Solutions Framework (MSF) approach. This approach was developed by Microsoft and it was modified to fit the companies' specific working environment. The MSF approach is not limited to the Microsoft Technology stack or suite of products. Even though the methodology is a Microsoft based approach, throughout the course of this project, many of the systems in the IT department involved are Red Hat Linux, HPUX and IBM AIX based systems. The methodology is more about the steps in preparing and delivering the intended results than assisting in guiding specific Microsoft product delivery. This methodology is used for development projects as well as non-development, infrastructure or process related projects and deliverables. Based on the type of project, the project manager will determine what phases and deliverables will have the greatest value to the success of the project and may omit or narrow the focus of some deliverables. The key project phases in the methodology include;

1. Envisioning
2. Planning
3. Developing
4. Stabilizing
5. Deployment

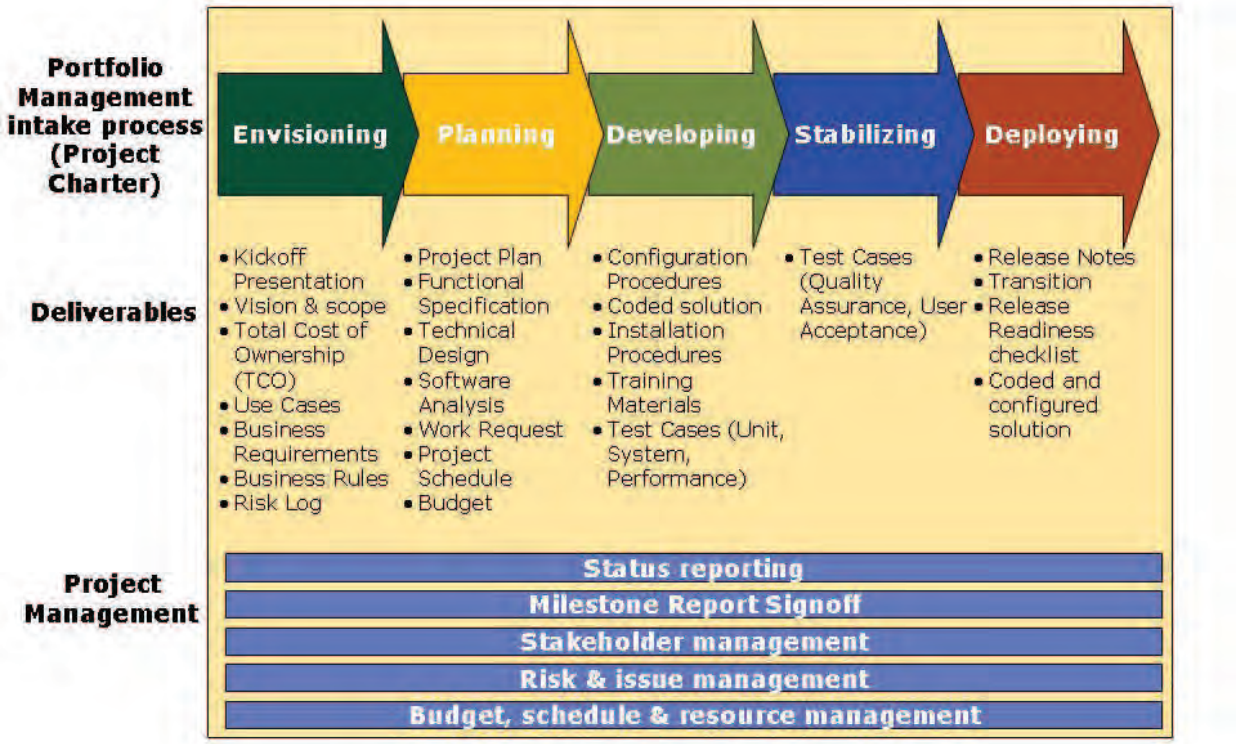


Figure 2: The Solutions Framework Methodology

Each of these project steps includes a set of possible deliverables. Depending on the size, type and complexity of each project, the project manager and project team will eliminate deliverables that add no value or those that are not applicable as mentioned above. Each deliverable has a pre-defined template or specific set of meta-data or information that is required.

The first step in this customized MSF is the envisioning phase. This phase is used to brainstorm, narrow focus, begin to frame-up the problem or benefit, develop a high level approach and potential value in running a project. This phase is typically performed upon approval from IT management, but before business approval to proceed with the

full project and before a budget has been fully allocated. The possible deliverables for the envisioning phase include:

- The Kickoff Presentation
- Vision & scope document
- Total Cost of Ownership (TCO)
- Use Cases
- Business Requirements
- Business Rules
- Risk Log

These deliverables are used to present the project idea to the decision makers and earmark funding to proceed with the planning and eventual execution of the project.

The next step in the process is the planning phase. During this phase, the project team is fully assembled, roles and responsibilities are determined and a full project plan and basic move-forward plan is created. During this phase the team will meet for a kick-off session and will begin to understand their role in the project. The possible deliverables for the planning phase include:

- Project Plan
- Functional Specification
- Technical Design
- Software Analysis
- Work Request
- Project Schedule
- Budget

The third step is the developing phase. During this phase, actual work is performed based on the project plan, requirements documentation and technical design. This also includes steps for training team members on new technologies and creating training materials for users. Once this phase is completed, it moves into a stabilization phase and may include testing. The deliverables for the developing phase include:

- Configuration Procedures
- Coded solution
- Installation Procedures
- Training Materials
- Test Cases (Unit, System, Performance)

The fourth step is the stabilizing phase. This phase is where the majority of quality assurance and testing is performed. For projects that are process driven such as the implementation of ITIL, this phase is used for peer review of the process documentation as well as testing for a change management process tool or other tools that enable the new processes. The deliverables for the stabilizing phase include documented test cases (Quality Assurance, User Acceptance)

The final step in the methodology is the deploying phase. This phase is where the final project steps are performed. This phase includes the communication to management, support staff and users of the completion of the project, training and a release readiness review with the Change Advisory Board. The deliverables for the deploying phase include:

- Release Notes
- Transition

- Release Readiness checklist
- Coded and configured solution

By using the MSF approach, the project structure and project requirements and delivery flow were very familiar to the project team. The MSF approach also assisted in the communication of the project to the stakeholders. As part of the normal project methodology, regular monthly steering committee sessions were held to review resources constraints, deliverables and schedule. This regular communication and review was very beneficial as it provided needed project direction to the project manager as well as regular status to IT leadership. The IT leadership team was able to show support of the ITIL initiative by providing communication updates to their teams and active subordinate involvement throughout the process delivery.

The MSF approach ensured the overall success of the ITIL implementation by providing a solid foundation for planning and executing the project from start to finish. During the envisioning phase, detailed requirements, schedules and risk management plans were created. Throughout the project, updates and tollgates ensured the project risks were updated as they evolved and appropriate communication and mitigation steps were taken to address any roadblocks.

During the deployment of the ITIL processes, the release readiness steps helped ensure adequate review and approval of all processes by the IT leadership and ITIL steering committee members. This buy-in assisted in the support of the processes by the leadership team during the roll-out and ongoing adherence.

ITIL Processes and Background

The Information Technology Infrastructure Library, or ITIL, is a set of process standards or framework for managing a technology environment. ITIL was first documented in the late 1980's to address the needs of the British Government to implement consistency in the way it managed and controlled IT systems. Since ITIL was first published, it began to gain recognition by private industry as an excellent prescriptive guide to managing technology and overall IT Service Management. ITIL is a non-trivial challenge for many organizations to implement due to the volume of material that is described in the ITIL reference books. The most difficult decision organizations typically face is narrowing the focus of their ITIL adoption to only those areas that truly matter and provide value to the organization and remain realistic with implementation target dates. The current published version for ITIL is version 3.0.

The Microsoft Operations Framework (MOF) is a descriptive methodology for implementing the ITIL framework. The author considers it descriptive since unlike the ITIL books, MOF provides detailed Service Management Functions (SMF's) for implementing each ITIL related function. These SMF's include complete process documents that organizations can use as is or modify to narrow or expand the scope to meet the needs of the current technology environment. Similar to implementing pure ITIL process, organizations must decide what components of MOF to implement based on need and value to the organization. The current published version of MOF is version 4.0.

The decision to implement ITIL version 2 for this project was made in early 2007 and was made after reviewing analysis from Forrester research and Capgemini during an

IT maturity assessment. The assessments highlighted key areas for improvement within the IT department. The assessment highlighted areas for improvement and these areas were eventually used in assisting with the scoping of the ITIL project. The leadership team also determined that the best way to gain quick results was to use the MOF version 3.0 (the most current revision of MOF at that time) process documentation as a guide. Additionally, the organization had already made a significant time investment in rolling out the Microsoft Solutions Framework as a guide to implementing and managing IT related projects and tasks. Since the MSF and MOF are closely aligned, implementing ITIL using the MOF approach was a logical next step in the advancing the overall maturity progression of the IT department.

By implementing the MOF based processes for this ITIL implementation, the project team gains efficiency by quickly reviewing the SMF documentation and adopting the process with modifications to more closely align to the current IT environment and staff size. Additionally, the team is hoping to tightly couple the existing MSF process with the new MOF process to allow for better handoff of projects to assist in stability and consistency in managing new IT services once they are delivered using the MSF process. This approach will also add benefit by leveraging the common terms and processes that have already been addressed by implementing MSF and adopted by members of the IT organization.

Chapter Four: Project History

How the Project Began

In preparation for this project, the IT leadership team organized a 2-day planning event in May 2007 with 18 members of the IT management team and individual contributors across all functional teams within the IT organization. The 2-day event was organized and facilitated by Capgemini in their Advance Solutions Environment in Chicago Illinois. The initial meeting day was used to provide an overview of the main process areas within MOF so that everyone understood the processes and terminology used in MOF. The remainder of the meeting time was dedicated to discussion around current pain points within IT. The teams focused on every possible detail of the existing IT environment and areas of concern around the organization including issues between functional teams and process gaps. By the end of the 2-day event, the team had a list of the MOF process areas in prioritized order, as well as a very high level implementation road-map by process area. Described in figure 3 below, the team agreed that the top areas of improvement for MOF process implementation would be the following:

- Incident Management
- Service Desk
- Service Monitoring and Control for the Email environment
- Configuration Management
- Change Management
- Financial Management
- Service Level Management

The two day planning event allowed the team to quickly assemble the main deliverables in the envisioning phase of the project. Following the 2-day event, the project team took the notes and discussion topics and web based event log complete with pictures of white boarding sessions and completed the final envisioning documentation.

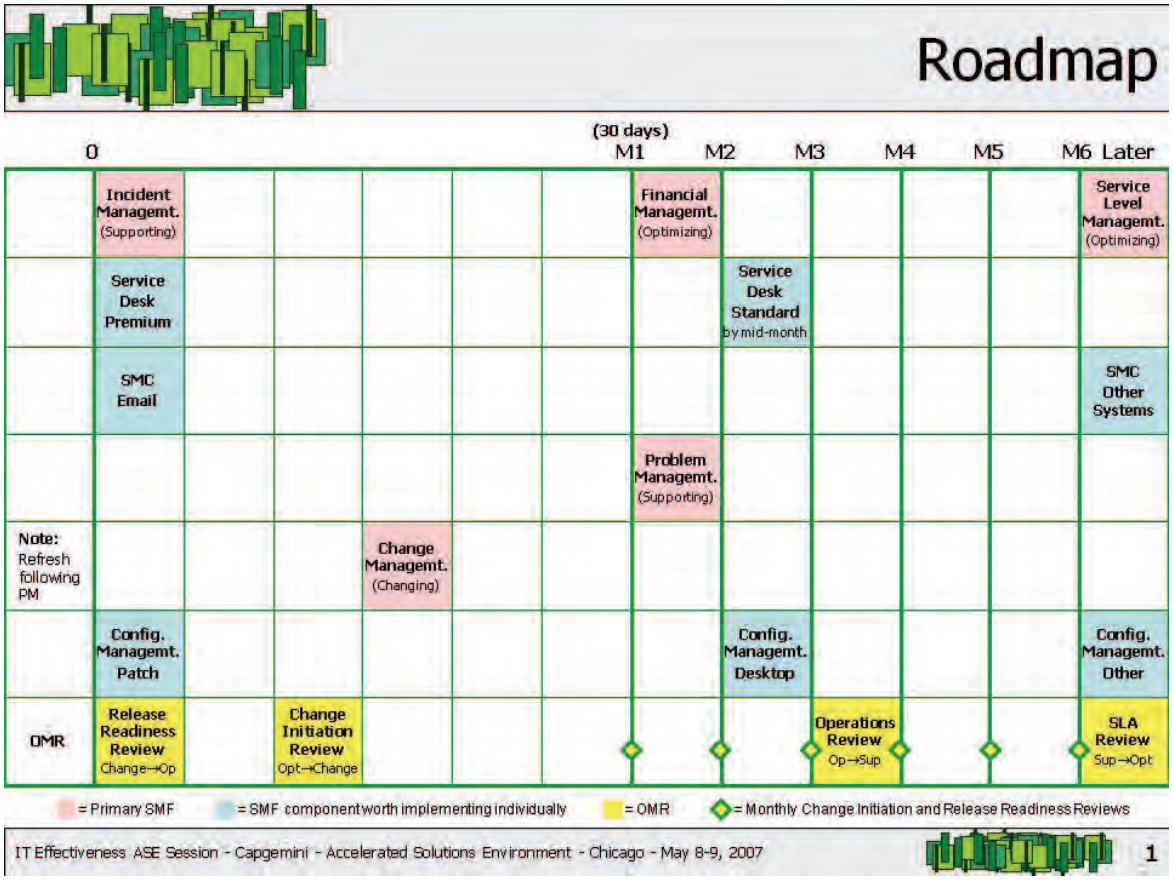


Figure 3: The original project timeline

The original roadmap as seen in figure 3 above was used to assist in creating the detailed project plan. The planning process took approximately 2 months to complete. During this time, the project management office (PMO) was established and along with the project sharepoint sites, the templates for the process deliverables were completed and the initial training for the team was completed.

How the Project was Managed

The PMO took ownership for the initial project coordination and roll-out as well as the longer term process upkeep as described in figure 4 below. The PMO has responsibility for the overall coordination of the ITIL implementation, project managers, timeline and review of project deliverables and budget. The PMO is also responsible for long term management and updates to the ITIL process. This includes maintaining consistency in the process documentation and ensuring appropriate process change management is used when implementing process change. IT management performs the ultimate approval for all of the initial processes as well as future updates, additions and changes.

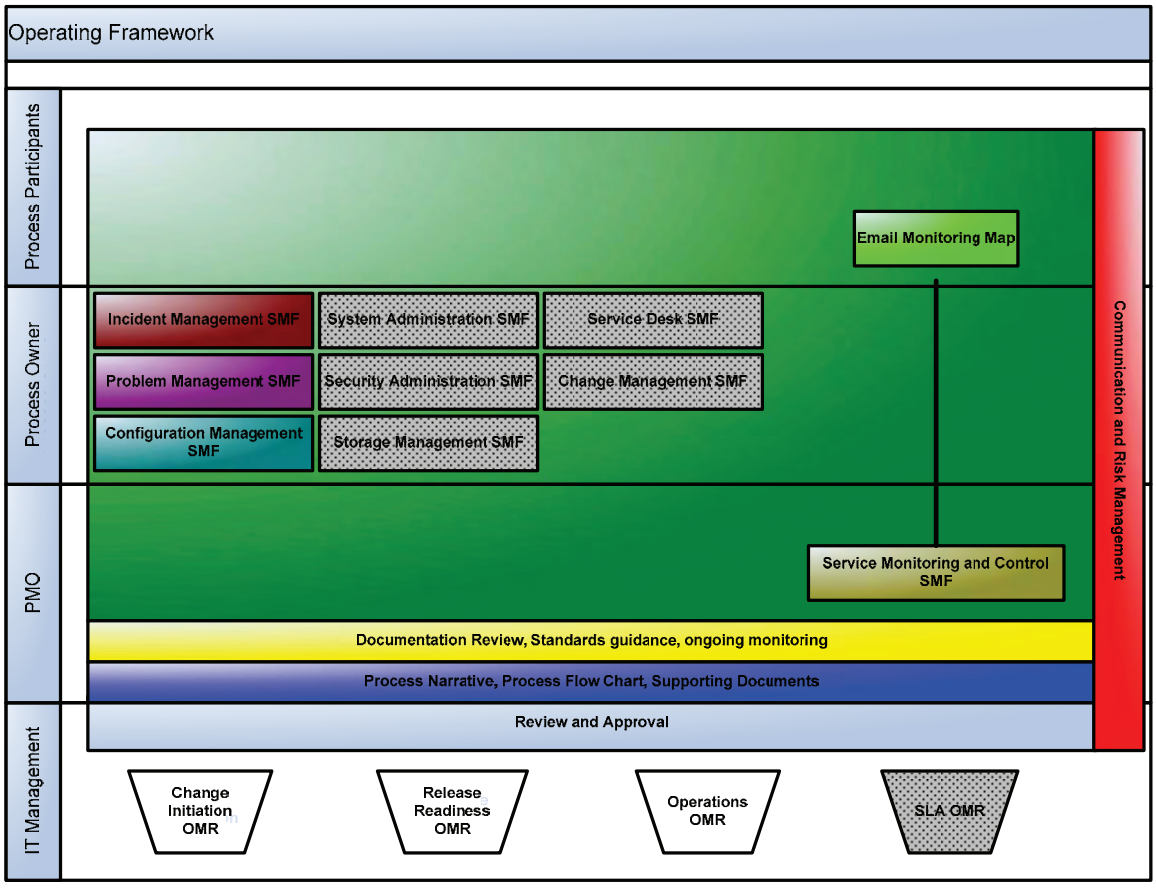


Figure 4: The Process PMO

Project Team structure

In addition to the PMO, the project organizational chart was defined to include the project sponsor (the CIO), as well as a steering committee comprised of the IT Leadership team and all of the support and subject matter experts required as described below in figure 5.

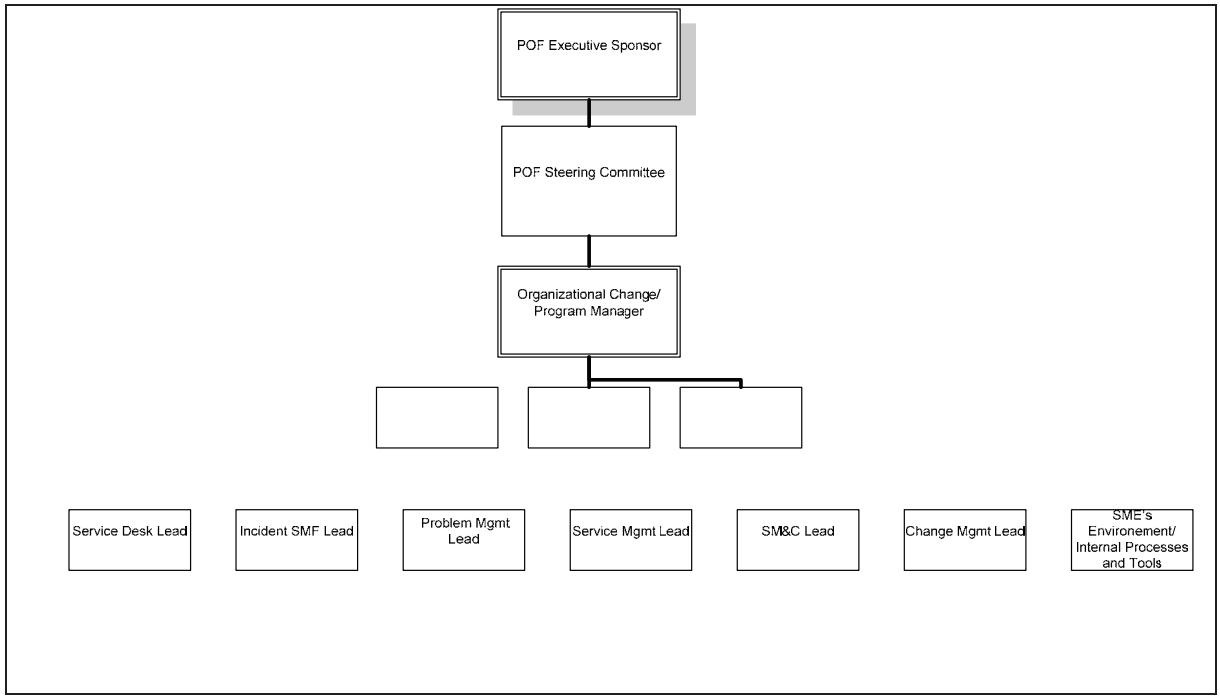


Figure 5: Project Organizational Chart

To assist the project team in understanding the roles required for each of the process areas, the roles and responsibilities were defined in the table 1 below. This table was referenced often throughout the project and within the processes as individual contributors often assumed more than one role in different processes. Larger organizations may not experience this as the key process roles are assigned to dedicated team members as their primary job duties rather than additional duties to existing team members.

Role	Description
Service Manager	- Manage the service portfolio of new and existing services, in alignment with business strategy - Manage service portfolio cost - Manage prioritization and resource allocation for new services and CSI proposals
Continual Service Improvement (CSI) Manager	- Provide ongoing communication and training on POF and CSI - Capture, analyze and report on KPIs across all processes and services - Work with Service and Process owners to identify and deploy CSI projects based on KPI analysis
Service Level Manager	- Document and publicize Service Level Management (SLM) Process - Define, measure and report on SLM KPIs - Provide ongoing training on SLM as needed - Work with CSI Manager to identify and deploy SLM process improvements
Incident Manager	- Document and publicize Incident Process - Define, measure and report on Incident Management KPIs - Provide ongoing training on Incident Management as needed - Work with CSI Manager to identify and deploy Incident Management process improvements
Service Desk Manager	- Document and publicize Service Desk (SD) Process - Define, measure and report on SD Management KPIs - Provide ongoing training on SD Management as needed - Work with CSI Manager to identify and deploy SD Management process improvements
Problem Manager	- Document and publicize Problem Process - Define, measure and report on Problem Management KPIs - Provide ongoing training on Problem Management as needed - Work with CSI Manager to identify and deploy Problem Management process improvements
Change Manager	- Document and publicize Change Process - Define, measure and report on Change Management KPIs - Provide ongoing training on Change Management as needed - Work with CSI Manager to identify and deploy Change Management process improvements
Configuration Manager	- Document and publicize Configuration Process - Define, measure and report on Config Management KPIs - Provide ongoing training on Config Management as needed - Work with CSI Manager to identify and deploy Config Management process improvements
Release Manager	- Document and publicize Release Process - Define, measure and report on Release Management KPIs - Provide ongoing training on Release Management as needed - Work with CSI Manager to identify and deploy Release Management process improvements
Service Monitoring & Control Manager	- Document and publicize SM&C Process - Define, measure and report on SM&C Management KPIs - Provide ongoing training on SM&C Management as needed - Work with CSI Manager to identify and deploy SM&C Management process improvements
Security Manager	- Document and publicize Security Process - Define, measure and report on Security Management KPIs - Provide ongoing training on Security Management as needed - Work with CSI Manager to identify and deploy Security Management process improvements
Financial Manager	- Document and publicize Finance Process - Define, measure and report on Financal Management KPIs - Provide ongoing training on Financal Management as needed - Work with CSI Manager to identify and deploy Financal Management process improvements
Capacity Manager	- Document and publicize Capacity Process - Define, measure and report on Capacity Management KPIs - Provide ongoing training on Capacity Management as needed - Work with CSI Manager to identify and deploy Capacity Management process improvements
Storage Manager	- Document and publicize Storage Process - Define, measure and report on Storage Management KPIs - Provide ongoing training on Storage Management as needed - Work with CSI Manager to identify and deploy Storage Management process improvements

Table 1: Roles and Responsibilities

Once the overall project structure was established, the remaining planning was completed including the full project plan in Microsoft Project format. Additionally, a graphic depiction of the plan was created in a roadmap, see figure 6. This was used to present the overall plan to the project team and management. As described below, the roadmap showed the approximate dates for each of the SMF's for the first year.

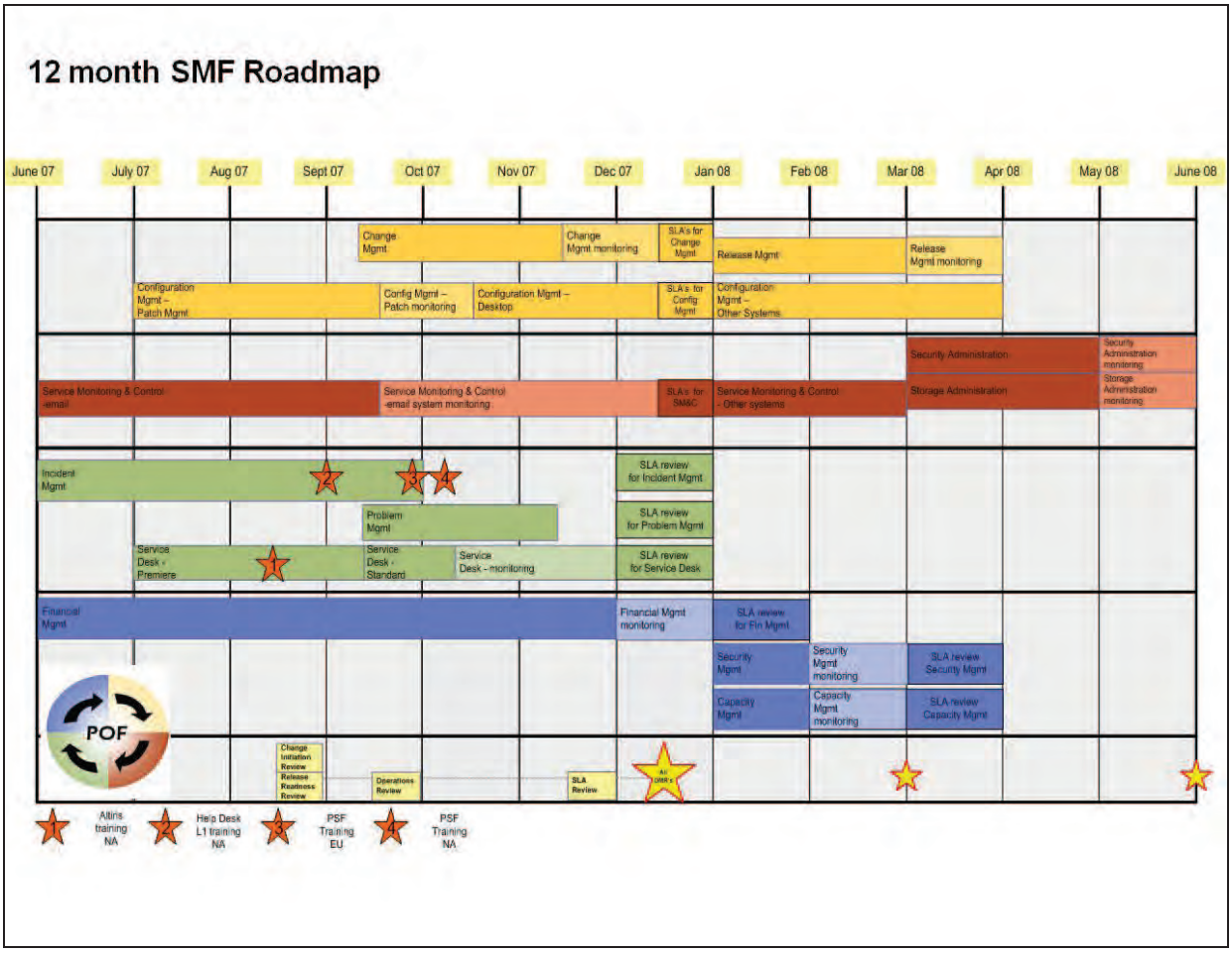


Figure 6: The 12 month roadmap

The roadmap includes several important milestones including training and reviews. These reviews are a component of the MOF process and are called Operational Management Reviews or OMR's. The initial reviews were meant to be a tollgate for major process reviews prior to their implementation and shortly after implementation. In the normal course of a functional MOF environment, the reviews exist to monitor the four primary objective of MOF including Change Initiation Review, Release Readiness Review, Operational Review and Service Level Agreement or SLA Review.

The MOF is defined in a collection of white papers for each of the main processes and operational review areas. The white papers are available for download on the Microsoft website at http://www.microsoft.com/mof. The Microsoft white paper for the Change Initiation Review describes is as, "…the initial management checkpoint before approving a change to the production environment. The Change Initiation Review is also a key integration point between the project-oriented Microsoft Solutions Framework (MSF) and the operations-oriented MOF since it synchronizes with the Project Plans Approved Milestone in MSF. The Change Initiation Review considers whether to accept the change for deployment and whether to approve plans for operating and supporting the change. It also considers whether to approve the plans required for the readiness of the target production environment to operate and support the deployed change. The Change Initiation Review results in a go/no-go decision about whether to approve the request for change (RFC) and initiate spending on the development of the solution". This is an important step in maintaining stability and control of the production environment. The team also found this to be an excellent communications forum between IT teams.

The Release Readiness Review is also a key component in the MOF process as it helps to establish the criteria for determining the readiness of an IT component for use. The Release Readiness OMR is described in its Microsoft whitepaper as, "…the final management checkpoint and approval step before deploying a release. The Release Readiness Review is a key integration point between MSF and MOF and is a major milestone in MSF. The Release Readiness Review ensures the readiness of the release for deployment and considers the operability and supportability of the release itself, as well as the readiness of the target production environment to support and operate the deployed

release. The Release Readiness Review results in a go/no-go decision about whether to deploy the release". Release readiness was also a difficult component to implement due to the number of steps required from the project to successfully fulfill the review requirements. Once implemented, the release readiness review greatly assisted in communication between IT teams even within the planning process for new projects.

The Operational Review is used as temperature check on how the operating environment is working. The Microsoft whitepaper for the Operational Review describes this review as, "…used to evaluate significant milestones in the operations life cycle. This review can in turn be used to evaluate performance for release-based activities as well as steady state, or daily, operational activities. The Operations Review is primarily concerned with assessing the effectiveness of an organization's internal operating processes. These processes play an essential role within an organization because they provide the foundation for delivery of automated business services". At the time this project was completed, the team did not implement the operational review section.

The SLA Review is the fourth component within the review activities and is the key area that is used to improve overall service delivery for an IT organization. The Microsoft SLA Review whitepaper describes the SLA Review as, "…an opportunity to review performance against SLA objectives and, more importantly, to gather perceptions and opinions from business representatives on any perceived changes in service during the period of the SLA implementation phase. If any service levels are perceived to have been breached but have not been highlighted by the service review or reports, this may indicate that there are issues with the criteria of the SLA and objectives". At the time this project was completed, the team did not implement the SLA review section because the

new baseline of service availability was not available. Once this baseline is determined, the team will begin establishing reasonable SLA targets and obtaining agreement of these targets with the business.

During the initial planning and project timeline creation, the entire team was very optimistic about the amount of process change that could be adopted simultaneously and included these in a very condensed time frame. The initial timeline at one point in the month of October had a total of seven process streams occurring at the same time including Change Management, Configuration Management, Service Level Monitoring, Incident Management, Problem Management, Service Desk and Financial Management. Although the process documentation and deliverables were not overwhelming, the team found that the rate of process change adoption was a challenge since most of these processes involved the same teams. The timeline was eventually stretched to accommodate not only the process design and documentation and also the organization change requirements for the actual implementation of each process.

Requirements to Implementing ITIL

According to the ITIL Service Support book, there are some basic prerequisites to implementing ITIL. One of the core criteria is management commitment to the implementation. During this project, IT management was very committed to the success of the implementation and helped drive this by regularly participating in review sessions, status meetings and project budget reviews. Management also provided support to ensure adequate project planning was completed throughout the life of the project. The blue book also provides a good discussion around why ITIL implementations fail. The more obvious reasons include lack of commitment and understanding, lack of training, loss of a champion, lack of funding, unrealistic implementation schedules and inappropriate scoping when analyzing processes. These also include difficulty when trying to change the company's culture, inadequate controls or project methods when planning and executing the implementation, loss of motivation or quick wins after the initial push and excitement. All of these however can be addressed through training, good project management and risk mitigation throughout the project. During this project regular training was provided, regular project reviews and updates were performed and a risk management plan was developed.

Another area of impact to this ITIL implementation was overall company culture. The blue book narrows the definition of culture down to the beliefs and values of an organization. The project team found that the company culture was open to change, however the rate at making change was not easy to anticipate. To better understand this definition and gather more data points on the perceived importance of culture and what the prerequisites to implementing ITIL are, a brief survey was conducted with 5 IT

professionals that have been involved with ITIL or MOF or are experts in ITIL or MOF implementation. Out of all the survey respondents, everyone felt that training was an important aspect of the ITIL implementation process and scored it a 5, with 5 being the most important and 1 being the least important. Additionally business support of the implementation scored an average of 4.25. The final questions in the survey showed no significant variation in the difference in scores with an average rating close to 3. One question was slightly above the 3 rating for the level of importance in keeping ITIL documentation current with the latest ITIL guidance, for example updating ITIL v2 based documentation to the ITIL v3 standard.

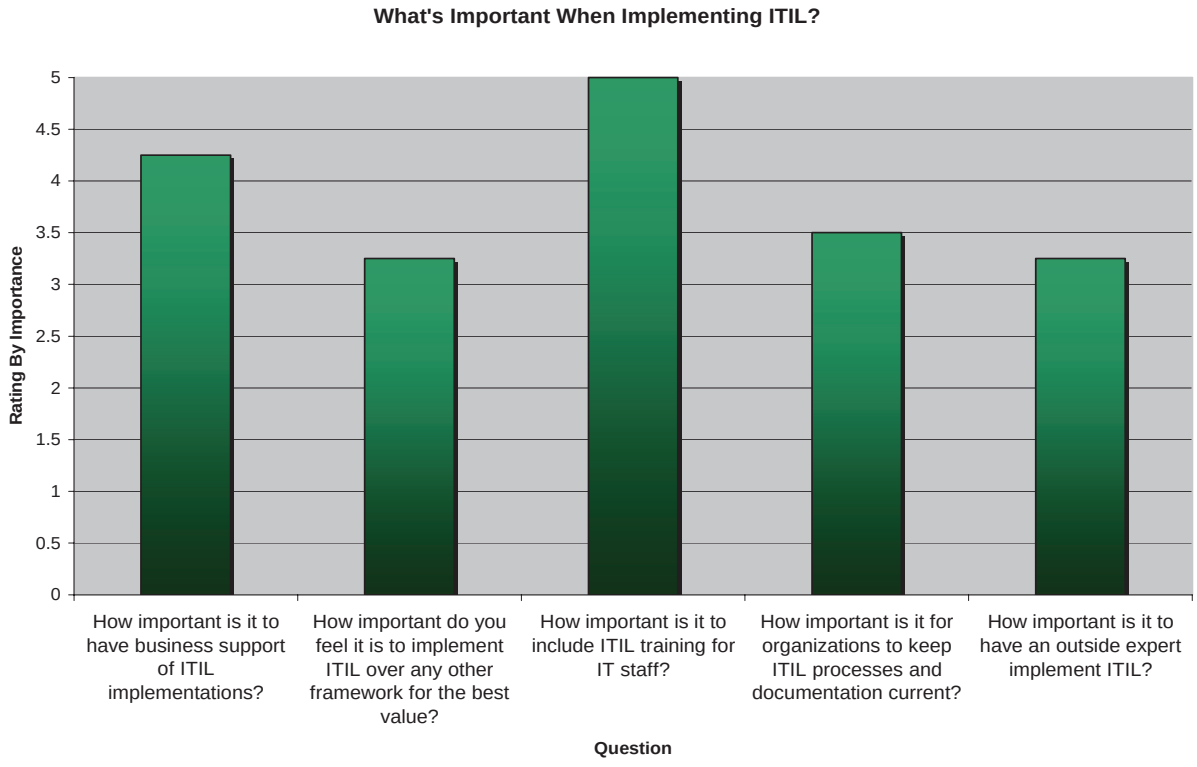


Figure 7: Survey Summary Results- what is important when implementing ITIL

When survey participants were asked to describe the single most important aspect of implementing ITIL, the top answers were good communication, a strong advocate to drive cultural change, buy-in from the business and a baseline to measure success against. Cultural change was mentioned by more than one respondent and one respondent commented that "…it is difficult to achieve true permanent change without changing the culture". When asked what if any pre-requisites exist to implementing ITIL, all respondents felt business sponsorship and or executive support was the most important component. When talking with the participants, the reoccurring theme was around involving the business up front and maintaining that support throughout the project. The next question was, how should an organization plan for implementing ITIL. All respondents felt a project management methodology should be used and one respondent felt that any duration estimates should be over-estimated during the planning process.

Two questions that did not appear related showed some relationship when looking at the results. The first question was what do you consider the biggest value add to a company from ITIL and the second question was how can ITIL hurt a company. The responses to the first question were efficiency, standardization and allowing the business to make better decisions while maintaining a more stable environment. The second question answers were almost the inverse of the first. The answers included adding too much process and bureaucracy, implementing process for the sake of process without knowing why and not understanding the business.

The final question in the survey was, where do you think ITIL is going in the future. All respondents felt that there will be wider adoption of ITIL in the future and that companies will be more selective in which components of ITIL they implement. The

respondents also discussed the complexity of ITIL v3 as a challenge and at least one respondent felt it would improve ITIL if it aligned process areas with job functions. An example would be the job function of a database administrator (DBA) typically performs a specified list of tasks in the ITIL process. One respondent also mentioned that it would be helpful if ITIL was adopted as more of a standard so that companies could be certified in ITIL similar to an ISO[2] certification.

[2] ISO is an abbreviation used by the International Organization for Standardization. The ISO maintains a web presence at http://www.iso.org/iso/home.htm.

The Process Implementation

Service Level Management, according to the ITIL definition, is the process used to ensure that any events that could negatively impact the normal delivery of IT services is kept to a minimum. This is done by managing the SLA's and Operational Level Agreements (OLA's) or contracts (also called underpinning contracts) and ensuring these are met. For this project, a major component of the Service Level Management process was the actual definition of the IT services that the IT organization currently delivers for the business. By documenting this current capability, the IT organization also identified all of the dependencies for each IT service so that when defining SLA's, the appropriate IT components are considered.

One of the more critical portions of the project was the establishment of an IT Service Catalog. The ITIL guide organizes the Service Catalog under the Service Level Management section. The Service Catalog was very beneficial as it provided a key talking point around the tangible scope of the IT department. This was very helpful as the business and IT had many challenges defining what IT "does" and how they should operate. The Service Catalog also played an important role for many different processes including Change Management, Service Monitoring, Incident Management and almost all of the other process areas. The Service Catalog also helped the IT department to establish a more comprehensive dialogue with various business units when discussing service availability, new features as well as dependencies between technologies and processes. When creating the Service Catalog, the project team interviewed contributors in all of the functional IT groups to understand the IT services they support. A core list of these services was documented and the team was careful to assign names and terms to

these areas that are familiar to the end business users. The IT owners for each of the IT Services were identified so that future IT Service definition would be more focused. The resulting IT Service Catalog was documented in a simple table as shown below in Table 2. Similar services were grouped under main categories and a column was added to define the service owner. Each service was named in simple terms that are familiar to the average company business user. This list was also expanded during the Change Management process definition to document a list of know changes that is referenced as a KCTL or Known Change Type List. This KCTL was used to assist in streamlining the change management approval process by documenting low risk commonly executed changes that require less stringent approvals prior to implementation.

Core Services	Service Owner	Service Map	KCTL Defined
Collaboration			
Corporate Calendar		Yes	Yes
Extranet Web Folders		Yes	Yes
File Services		Yes	Yes
Intranet		Yes	Yes
LiveMeeting		Yes	Yes
MOSS Team Sites		Yes	Yes
Print/Fax/Scan		Yes	scheduled
Sharepoint Team Sites		Yes	Yes
SOX Accelerator		Yes	Yes
Communications			
Audio/Visual		Yes	Yes
Modular Messaging		Yes	Yes
Telephony		N/A	Yes
VoIP		Yes	Yes
Corporate Web Presence			
Internet Connectivity		Yes	Yes
External Web Site		Yes	Yes
Property search		Yes	Yes
CRM			
CRM		Yes	Yes
Development			
Circle Developer		N/A	N/A
Comparables		Yes	Yes
Document Management		Yes	Yes
Investor Fund Portal		Yes	Yes
Project Direct - EU		scheduled	scheduled
Project Direct - NA		Yes	Yes
QMS		Yes	Yes
Financial Management			
PeopleSoft Financials - EU		Yes	Yes
PeopleSoft Financials - NA		Yes	Yes
Financial Planning and Analysis			
DynaSight		scheduled	
ProClarity Analytics Server		Yes	Yes
TM1		scheduled	
Fund Management			
Circle Investor		N/A	
Fund Investment Tracker		Yes	Yes
Human Resources			
PeopleSoft HR - EU		Yes	Yes
PeopleSoft HR - NA		Yes	Yes
Marketing			
Interwoven MediaBin		Yes	Yes
Messaging			
Blackberry		Yes	Yes
Corporate Email		Yes	Yes
Windows Mobile		N/A	
Portfolio Management			
Portfolio Management		TBD	
Property Management			
Property Lease		N/A	
Yardi - EU		scheduled	
Yardi - NA		Yes	Yes
Service Desk			
Service Desk		Yes	Yes
Desktop Applications		N/A	N/A
Desktop Support		N/A	N/A
Premier Support		N/A	N/A
Supporting Services	**Service Owner**	**Service Map**	**KCTL Defined**
Active Directory		Yes	Yes
Altiris		Yes	Yes
Backups		Yes	Yes
Citrix		Yes	Yes
DataBase Service		Yes	Yes
DataCenter - NA		Yes	Yes
DataCenter - EU		Yes	Yes
DocAve		Yes	Yes
EDW		Yes	Yes
Enterprise Analytics Cubes		Yes	Yes
Nagios		Yes	Yes
Oracle - EU		Yes	Yes
SAN		Yes	Yes
Tipping Point		scheduled	scheduled
Trend AV		N/A	N/A

Table 2: The IT Service Catalog

The next step in defining the overall IT Service Catalog was to create a graphical depiction of each service. This is called a service map. The service map is important because it defines not only all of the technology that provides a service, it also shows the "who" aspects such as who uses it and who supports various components of the service. To assist the service owners in working through the service map creation process, we created a basic document that describes how to read a service map. This document explains each portion of the service map and what each of the symbols and colors represent (see figure 8). This document was an extremely helpful aid since none of the service owners had ever seen or heard of a service map or participated in the creation of a service map.

How to read a Service Map

The Service Map is a High-level logical representation depicting what it takes to offer a service, who uses the service and how it is used. The service map also indicates ownership of each component of the Service Map.

The service map is a key component to the service-based approach to IT operations that is central to this Operations Framework. Every Service Management Function (SMF) will rely on the service map.

For example:

- Incident Management will use the service map to define all possible points of failure for the service
- Change Management will use the service map to define which components could be changed and the potential impact of those changes
- Service Monitoring and Control will use the service map to determine what components need to be monitored to ensure the health of the service
- Financial Management will use the service maps to understand the components required to offer the service, assisting in cost accounting by service.
- IT Service Continuity Management will use the service maps to determine all dependencies when developing the Business Continuity/Disaster Recovery plan.

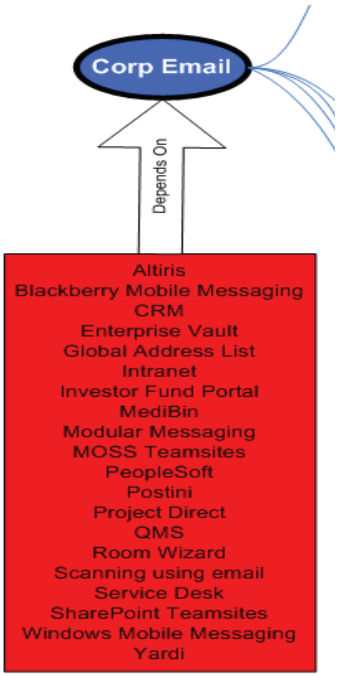
The Service Map Legend

The Service Map Legend indicates, by color, which group owns each component of the Service Map.

Owner	Color Code
System Engineers	Light Green
Network Engineers	Green
SAN	Violet
Operations	Light Orange
Service Desk	Yellow
Security	Brown
Architecture	Grey
Information Management	Pink
Enterprise Apps	Turqoise
Property Management	Bright Green
Customers	Red
Vendors	Black
Line = Hardware or Application Stream	
Ellipse = Service	

Dependencies of Business Functions and other services

The red box indicates which business functions and/or other services that rely on this service



Software

The software indicates all applications, clients, agents, etc. that reside on the production machines used to offer this service.

Note: There may be more than just those applications required to offer the service. For example, if an application on a server fails, it could potentially break the service, even if that application is not used in providing that service, therefore it is included in the service map to assist with Incident Management, Problem Management, Change Management, etc.

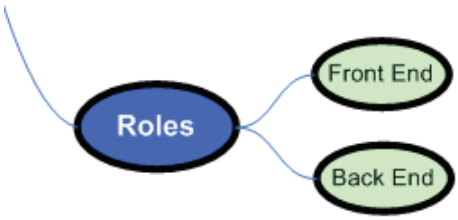
Hardware

This indicates all of the infrastructure hardware used to offer the service.

Note: This does not include client hardware, such as desktops, laptops, etc.

Roles

This indicates differing roles and/or configurations that may be used in the infrastructure that provides this service



Customers

This indicates different groups of users who may potentially use the service in differing ways. This is useful in determining communications plans and potential SLA requirements.

Service Dependencies

This indicates the dependencies of this service. These dependencies could be technical dependencies or organizational dependencies. Organizational dependencies are used to determine potential Operating Level Agreements (OLA's) between different IT groups.

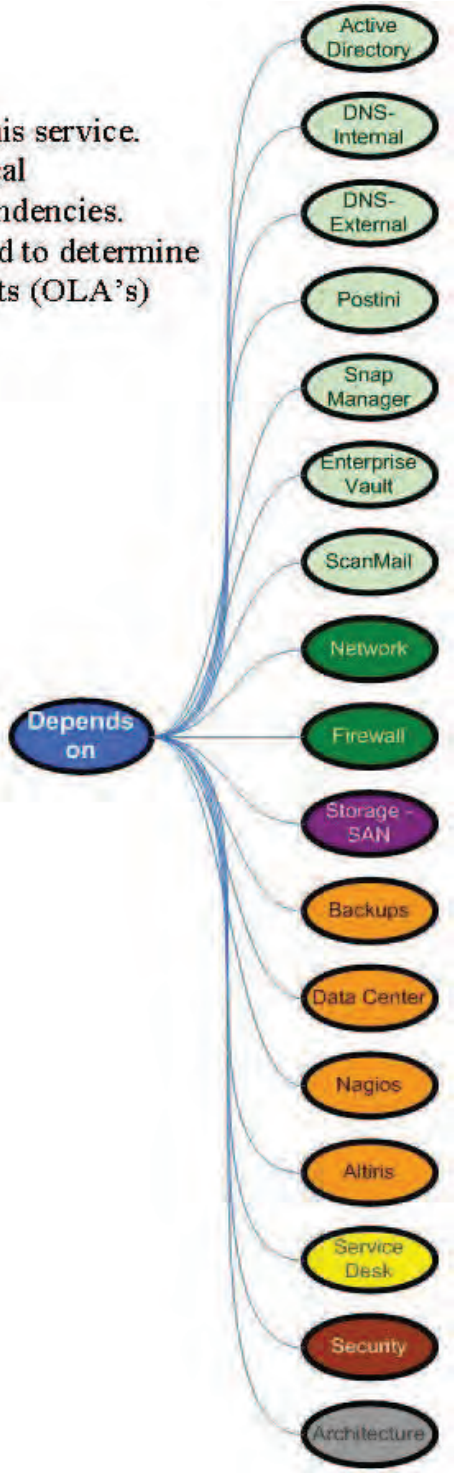


Figure 8: How to Read a Service Map

Once the service maps were completed through iterative interviews and white boarding sessions, they were reviewed by the steering committee, finalized and posted on the project web site. The service maps and Service Catalog were referenced throughout the subsequent process creation and were used to build specific deliverables that organized the processes into a cohesive operating framework regardless of IT functional area, technology or geography. The overall Service Catalog and service maps were the most beneficial deliverables during the implementation because it became the tangible source for the IT department for not only everything that IT provides to the business, but also drove standard terminology and understanding of the dependencies throughout IT. The IT service catalog was also used for non-ITIL purposes. During the recession that began in 2008 through 2009, the IT Service Catalog proved to be a useful tool for analyzing and prioritizing cost reduction initiatives. Rather than using the Service Catalog to negotiate service levels with the business, IT used the Service Catalog to determine what if any services could be eliminated or delivered in a more cost effective manner via virtualization, outsourcing or Software as a Service models. It was also used to reassign responsibilities for service delivery after a major reorganization within the IT department. Companies that do not have an organized Service Catalog can benefit from creating a catalog even without implementing ITIL processes. Additionally, the IT management staff can use the Service Catalog and process reporting to assist with budgeting and capacity planning. This also serves as a driver to more closely align IT services to business needs and business strategy by improving the business' understanding of what IT does and how IT provides IT support.

The final step during project planning was to develop a standard template for the narrative documents. The narrative documents are written steps for each of the ITIL process areas. Templates were also created for the process flow documents, policy documents and training documents. This allowed for a more cohesive set of processes and cleaner overall deliverable set.

The Service Desk Process

The Service Desk process ensures the Service Desk provides consistent and prompt response to incidents and service requests. The Service Desk serves as the face and voice of the IT organization to the business and in some organizations as the representation of the organization to external customers. The Service Desk also serves as a communication focal point for service events, issues and other IT related items that impact IT service delivery to end users.

The organization customized the Service Desk process to better fit the current environment which includes two branches of the Service Desk. The first portion is the Standard Service Desk that all internal users utilize to report incidents and submit requests. The second portion is called the Premier Service Desk and is specifically for the executive team and the executive support staff.

For the Standard Service Desk, the team documented the basic communication flow and process for receiving, documenting and resolving incidents. Based on the ITIL guidance as well as the MOF templates, the final communication flow was narrowed to only a handful of steps. The first step is the communication of the incident or service request by the customer to the Service Desk. From that point forward, the Service Desk analyst documents all actions taken in the ticket including any required escalation. The service desk also handles all subsequent communication with the customer including confirmation that the request or incident has been successfully resolved and the customer is comfortable with closing the ticket.

The next step included documenting the high level steps a service desk analyst would take for resolving incidents. The process was narrowed to the following steps;

1. When a company employee, contractor, or business partner encounters a technical problem, the user contacts the Standard Service Desk by phone or email.
2. The SDA (Service Desk Analyst) creates a ticket in Altiris and documents information gathered about the user and the symptoms that are being reported. The SDA is responsible for end-to-end ownership, tracking, and monitoring the ticket throughout the entire process and is responsible for keeping the customer posted with any progress towards resolution.
3. The SDA then assigns an appropriate priority level to each individual ticket based on its impact and urgency to the company organizations.
4. If possible, the on-duty SDA will attempt to provide an immediate solution by conveying known workarounds, using diagnostic scripts, or based upon their own knowledge and experience. If the solution proposed by the on-duty SDA resolves the problem, then go to step 8.
5. If no answer is found for the problem after research and investigation, the SDA escalates the ticket to the Tier 2 support team. If the solution proposed by the Tier 2 support team resolves the problem, then go to step 7.
6. If the Tier 2 support team is also unable to resolve the incident, the ticket is escalated to the Tier 3 support team. The Tier 3 support team works with the customer until the problem is resolved.
7. Once the Tier 2 or 3 support team has resolved the problem, the ticket is assigned back to the Service Desk for ticket closure.
8. Before the ticket can be closed, the SDA tests and confirms resolution with the customer and obtains his or her verbal or written approval to close the ticket.

9. If the customer agrees and is satisfied with the resolution, the SDA can close the ticket in Altiris. The SDA enters the detailed actions that were carried out to resolve the problem in the knowledge base for future references.

This process was also documented in a process flow using input from ITIL, MOF as well as subject matter experts within the Service Desk as seen in figure 9.

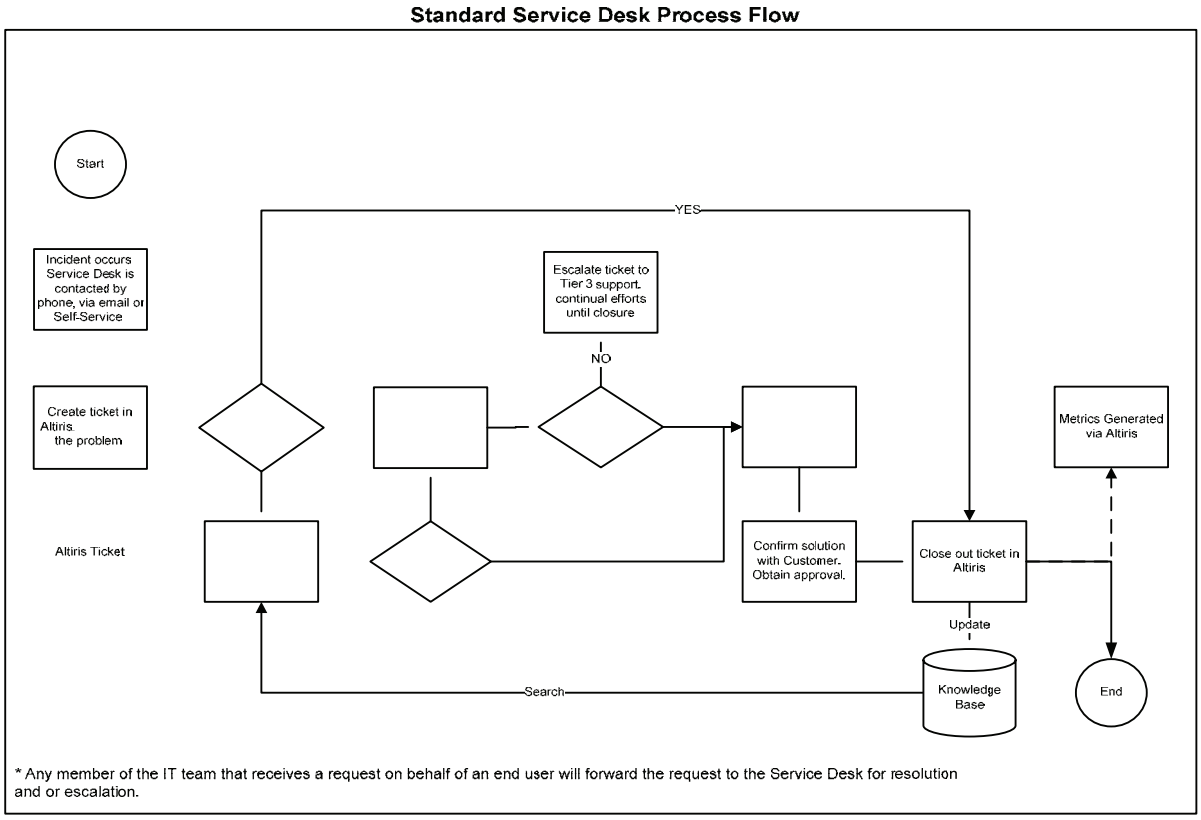


Figure 9: Standard Service Desk Process Flow

One of the key responsibilities in the process is the flow of communication to the customer. The SDA provides ongoing updates during incident resolution process as well as confirmation of the customers' agreement that the incident or request has been completed before the ticket is closed. Another important step is the capture of resolution steps that may be used in future incidents. This information can be captured and made

available to other service desk staff via a knowledge base. The knowledge base can assist in the quicker resolution of incident by making resolution steps or a work around available almost instantly.

The premier service desk process is identical however communication is handled via the premier service desk analysts. Any issues that are escalated are monitored and coordinated with the premier service desk analyst. Similarly to the SDA in the standard process, the premier service desk analyst will capture any resolution steps that may be helpful in the knowledge base.

The results of the Service Desk process

The results of the service desk process were not immediate. The team found that it took some time for team members to adopt the new process and regular reminders to continue using the process. To assist in the overall management of the service desk process, regular auditing of tickets and a dashboard was implemented. The dashboard assists in tracking open tickets, ticket times, ticket resolution and overall responsiveness of the team. In the future the team will coordinate a customer satisfaction survey to understand how the end users perceive the more rigorous process methodology.

The Incident Management Process

The Incident Management process allows for the quick documentation, classification and resolution of issues that impact or may impact the normal level of operations of IT services. Incident Management is an important process for the Service Desk function in resolving and escalating service impacting issues.

This particular process was relevant due to the high number of incidents, lost productivity and associated high frequency of ad hoc troubleshooting to respond to simple incidents. To better manage the incident lifecycle and reduce the overall time to respond, the team identified several deliverables that are believed to be applicable to the environment. This included an incident management policy that outlined the specifics around what incident management is, who and what it applies to and how the department will categorize and track incidents. In addition, the standard process flow and narrative document was created.

The two most beneficial deliverables from the incident management process was the incident priority matrix and the escalation matrix. Before this process was implemented, incidents were often assigned priority based on what the service desk analyst felt was appropriate. Often this resulted in high priority ticket assignments based on job title or how upset a customer was rather than a clear objective priority based on overall impact and urgency. Within the Incident Management policy the team defined impact as a measure of the business criticality of an incident or problem. Urgency was defined as the necessary speed required in solving an Incident of a certain impact. This combination was placed in the matrix below (Table 3) to provide a quick reference to prioritize incidents by IT staff.

Priority Matrix		Impact		
		High	**Medium**	**Low**
Urgency	**Urgent**	Urgent		
	High	1 - High	1 - High	2 - Medium
	Medium	1 - High	2 - Medium	3 - Low
	Low	2 - Medium	3 - Low	3 - Low

Table 3: The Incident Priority Matrix

This matrix was then used to establish target contact and resolution times for incidents. This allowed for consistent prioritization and tracking followed by regular reporting for KPI's and the ability to establish achievable SLA's with the business.

Another challenging aspect of this process was the adherence and coordination to the process by all of the IT teams outside of the Service Desk. One of the concerns during the development of this process by the service desk team was the resolution times may be difficult to achieve if proper escalations were not performed in a timely manner. To assist with the escalation process, the team took the service catalog listing and defined the tier 1, 2 and 3 support teams for each service. This was also defined by region to take into account services that were managed in North America, China, Japan and Europe or across multiple regions. An example of this would be the tier 1 service desk in Japan, escalating to the tier 2 Infrastructure team in North America.

Another aspect of the Incident Management ITIL process is the ability to classify and document the incident as described above and also quickly identify known errors. The ITIL Service Support manual describes a knowledge base or log of known issues as a tool that IT departments should use to quickly resolve known errors with very little effort using documented workarounds or fixes that were used previously to resolve the error.

During this implementation, the team did not have a readily available tool to implement a knowledge base, however the knowledge base was included in the process in anticipation of adding this capability in a later project phase as seen below in the process map in figure 10.

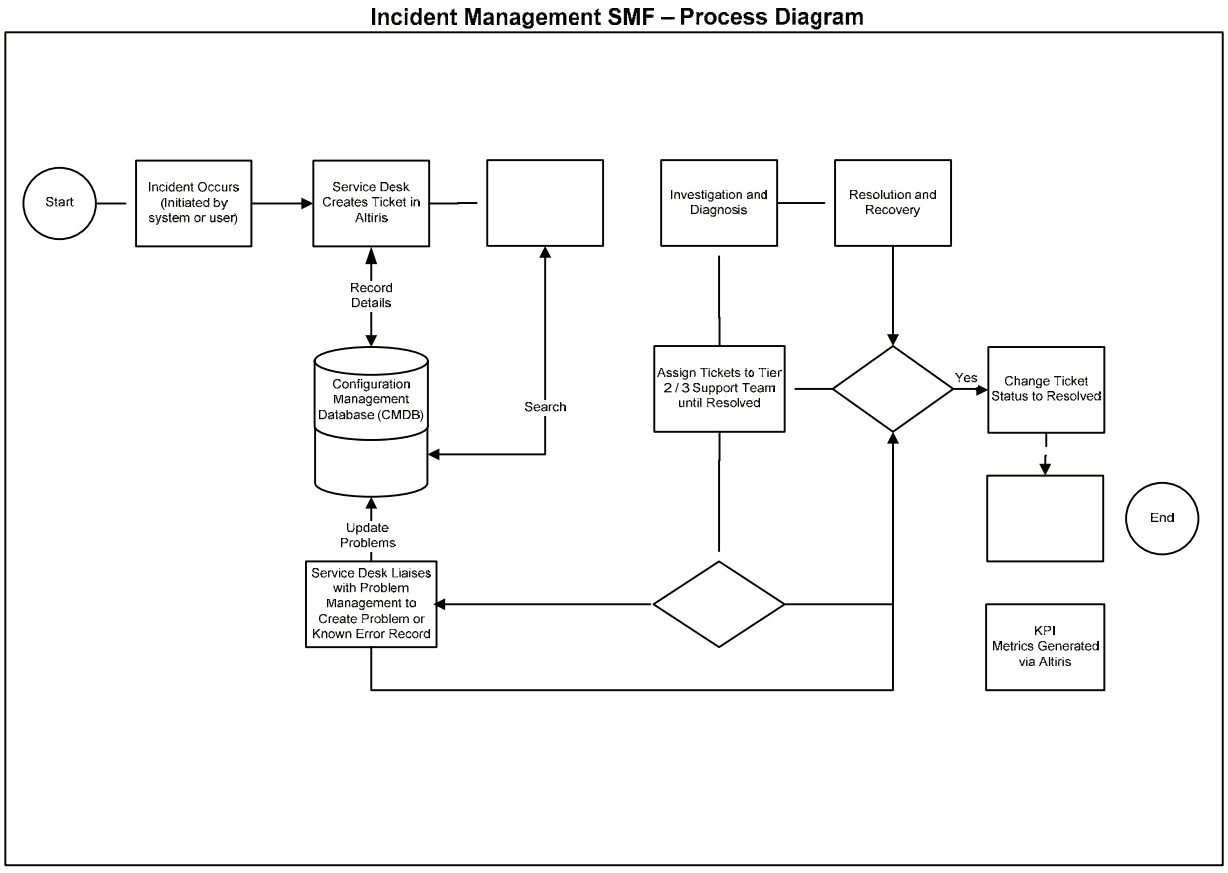


Figure 10: The incident management process map

The results of the incident management process

After the implementation of the Incident Management process, the team took random incident tickets and reviewed them for process adherence. This process continues on a less frequent schedule to ensure process adherence or identify IT members that may require training. Any process gaps are corrected and communicated to the team to prevent the same issues from occurring. A dashboard was also implemented using a

tool called Active Metrics. The dashboard pulls data from a SQL database that serves the Altiris ticketing system. The dashboard allows IT managers to visually see the status of incidents in progress by their team and individual team members. Managers can use this information to proactively monitor and assist if incidents do not meet standard resolution targets.

The Service Monitoring and Control Process

The Service Monitoring and Control process is a MOF based process that establishes requirements for the monitoring, alerting and response to service disruptions that may cause a breach of the SLA or OLA's for that IT service. During the Service Monitoring and Control process work, we identified the IT services that were to be monitored, what conditions to monitor and what audience receives what type of communication via either automated alerts, or manual updates and communication on the status of the IT service. After review, email monitoring was selected as the most critical service for service monitoring. Email was selected due to its criticality in most of the high level business processes and its general lack of monitoring capabilities at the time.

A subset of engineers were called together to identify all of the potential components that should or could be monitored to ensure the availability of email services. To better identify the communication flow when a component suffered a disruption, the table below was created. This also allowed senior management to comment on and approve the level of communication that would occur within the process. Areas identified as an "alert" are automated alerts from monitoring tools. Areas identified as "notify" are coordinated via manually sent email, phone or SMS text messages from process participants.

Email Monitoring Matrix

			Key Stakeholders							
System Level	Function	Tool Used	Infrastructure	Operations	Networking	Service Desk	IT Management	Cross Function Teams	Executive Team	End Users
Exchange Application	Email Uptime	Nagios (ping check)	Alert	Alert			Notify	Notify	Notify	Notify
	Inbound Que	Spot Light on Exchange	Alert	Alert			Notify	Notify		
	Outbound Que	Spot Light on Exchange	Alert	Alert			Notify	Notify		
	Information Store Available	Spot Light on Exchange	Alert	Alert						
	Services Availability	Nagios	Alert	Alert						
	OWA Connection Availability	Nagios	Alert	Alert						
	MAPI Connection Availability	NOT NEEDED	Alert	Alert						
	SAN Disk Availability	Nagios	Alert	Alert						
Infrastructure layer	Local Disk Usage (RAID Health)		Alert	Alert						
	SAN Disk Usage	Nagios	Alert	Alert						
	Memory	Nagios	Alert	Alert						
	Processor	Nagios	Alert	Alert						
	Network (Shared Resources)	Nagios	Alert	Alert	Alert	Alert				
	Outage Event		Alert	Alert	Alert	Alert	Notify	Notify	Notify	Notify
Events	Degraded Services		Alert	Alert	Alert	Alert	Notify	Notify	Notify	Notify

Outage Event: Any event that causes inbound or outbound email services to stop

Degraded Services: Any event that causes a delay in inbound or outbound email processing.

Alert action: A system generated alert via email, SMS, etc.

Notify action: A manual notification via email, SMS, etc.

Notifications should be sent if there is an issue with sending/receiving or Email, in the users perspective, is either not available or experiencing performance issues. The details or components of the failure (matrix items above) are not important but rather the system availability as a whole when working with anyone outside of IT.

Table 4: Monitoring Matrix

The monitoring process itself was kept very simple so that team members could easily remember the process during an outage or event. The basic process is listed below.

Alert Response and Health Checks

The company IT Operations and Infrastructure teams observe and research system health conditions when they occur. System Engineers perform a system health check and determine if alert notifications are "false alarms" based on collected data and information provided by Nagios and Spotlight on Exchange. The health check is an assessment that defines the tolerances and service levels for normal operations. The health check also specifies what conditions require additional monitoring attention and provides guidance on how the system engineer or administrator should respond to out-of-tolerance conditions.

If the system does not pass the health check, the System Engineer opens an Altiris ticket and contacts the Service Desk to provide instructions for responding to end user calls that may be related to the service disruption. The Altiris ticket will trigger any necessary Incident Management analysis and begin the Incident Management process. In addition to working diligently to restore email services, System Engineers must determine when to send service disruption notifications and who should receive notifications from the Email Monitoring Matrix (see above). Systems Engineers and Infrastructure Management will create notifications when required and make sure the notification are distributed by the Service Desk. All actions taken during this process is documented in the associated Altiris ticket.

The Systems Engineer will troubleshoot and attempt to restore email services. If service cannot be restored, Microsoft Support will be contacted and the appropriate Incident Management escalation process will be followed until service has been restored.

Once service has been restored the Systems Engineer will contact the Service Desk to close the Altiris ticket and send any required follow-up notifications. Additionally, the Service Desk will update the Incident description and resolution in the Knowledge Base. Nagios and Spotlight on Exchange continue to perform automated monitoring of the e-mail services and associated IT infrastructure to ensure optimal performance.

This basic overview was put into the standard process flow as seen below in figure 11. This process flow is referred to on a regular basis by the process participants.

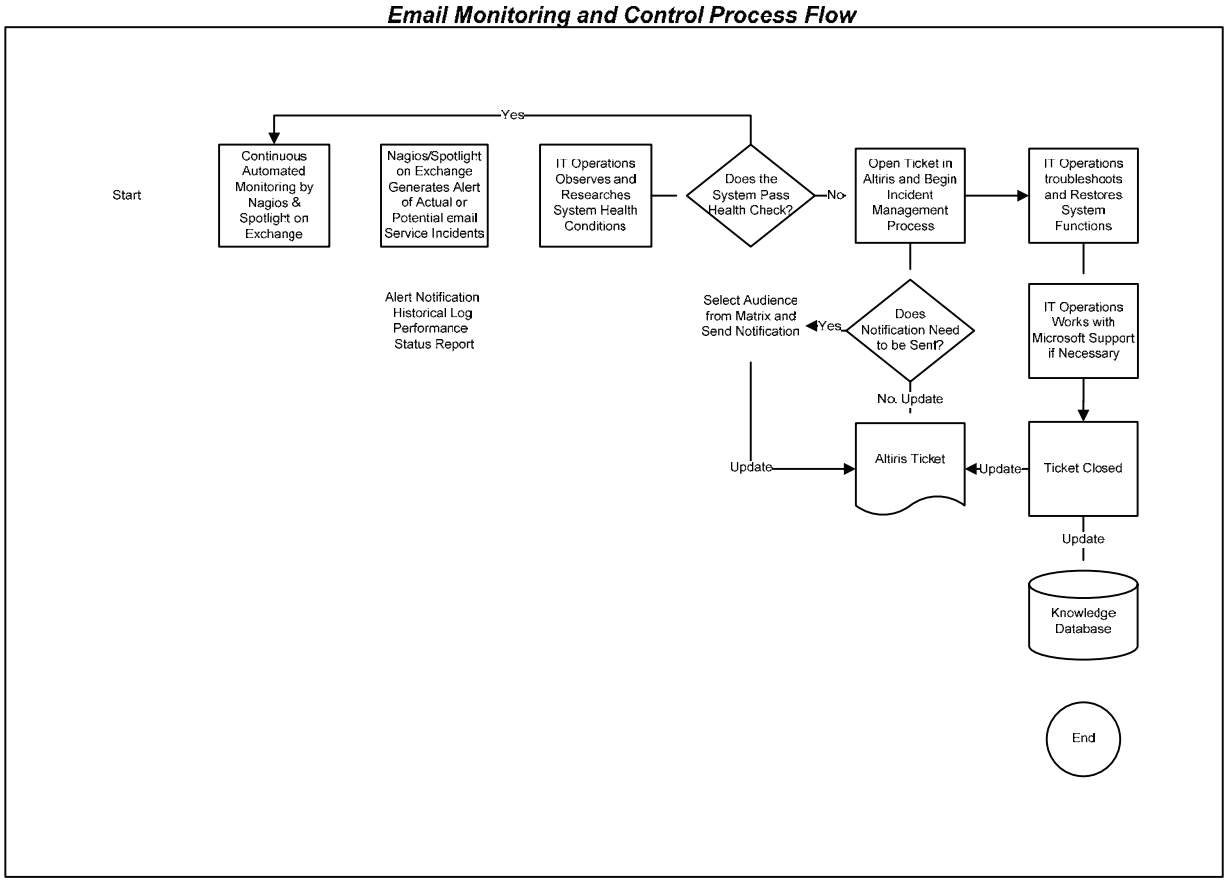


Figure 11: Service Monitoring Process Flow

The Results of the Service Monitoring and Control Process

After implementing the Service Monitoring and Control Process, a noticeable email outage did occur. During the course of the outage, the Service Monitoring and

Control Process provided the appropriate alerts and communication structure to address the issue rapidly and keep all of the critical process participants informed. To illustrate the effectiveness of the new process, a post mortem was completed and the process improvements were shared with the company. The two biggest improvements were time to identify a disruption which improved from hours to immediate identification and response time which went from and average of 3-5 hours to less than 25 minutes.

A monthly operations report was implemented to begin reporting on service disruptions. The Service Monitoring and Control Process is used to track service disruptions (via incidents in Altiris) and it is also used in the generation of the monthly report for email uptime. Identified service disruptions are reviewed and process or technology improvements are identified and implemented using the change management process.

The Change Management Process

The purpose of the Change Management process is to improve the overall service level by minimizing the impact of changes to the overall quality of IT delivery. The Change Management process is important to ensure ongoing IT Service availability by limiting the risk introduced by changes to the service. The Change Management process is closely related with several ITIL processes including configuration management. Accurate information about the IT service is maintained via configuration management and greatly assists in understanding what components are affected by change or may be affected by change. During the roll-out of the Change Management process, the project team initiated a Change Advisory Board, or CAB, with representation from all functional IT groups to assist in the review and approval of changes and the communication of scheduled changes.

During the development of the change management process the team also took Sarbanes-Oxley (SOX) requirements into consideration. The change management process is a critical control used in managing changes to the financial systems that are used for financial reporting. The SOX audit validates that adequate planning, approvals, testing and post implementation reviews are completed with the purpose of identifying potential changes that were not controlled or that may cause problems with financial reporting. The result of the review and process design was a better more controlled flow for documenting, reviewing and accepting changes to the environment. The process was used to automate the steps within a workflow in the Altiris tool. The following paragraph provides an abbreviated overview of the change process that was developed.

The change management process will be followed for every change made within the IT organization. The main goal is to provide a disciplined process for introducing required changes into the IT environment with minimal disruption to operations. As soon as a request for change (RFC) has been entered into Altiris, an evaluation of the risk is performed. According to the level of risk identified (low, medium, high or urgent), the change will follow different development and implementation paths and go through increasing levels of scrutiny and approval. The change may be pre-approved for immediate implementation, or require approval from the service manager, or require additional approval from the Change Advisory Board (CAB). After the change has been implemented in production, a post implementation review may be performed by the service manager or the CAB. All steps are controlled through a workflow in Altiris as seen in Figure 12 below.

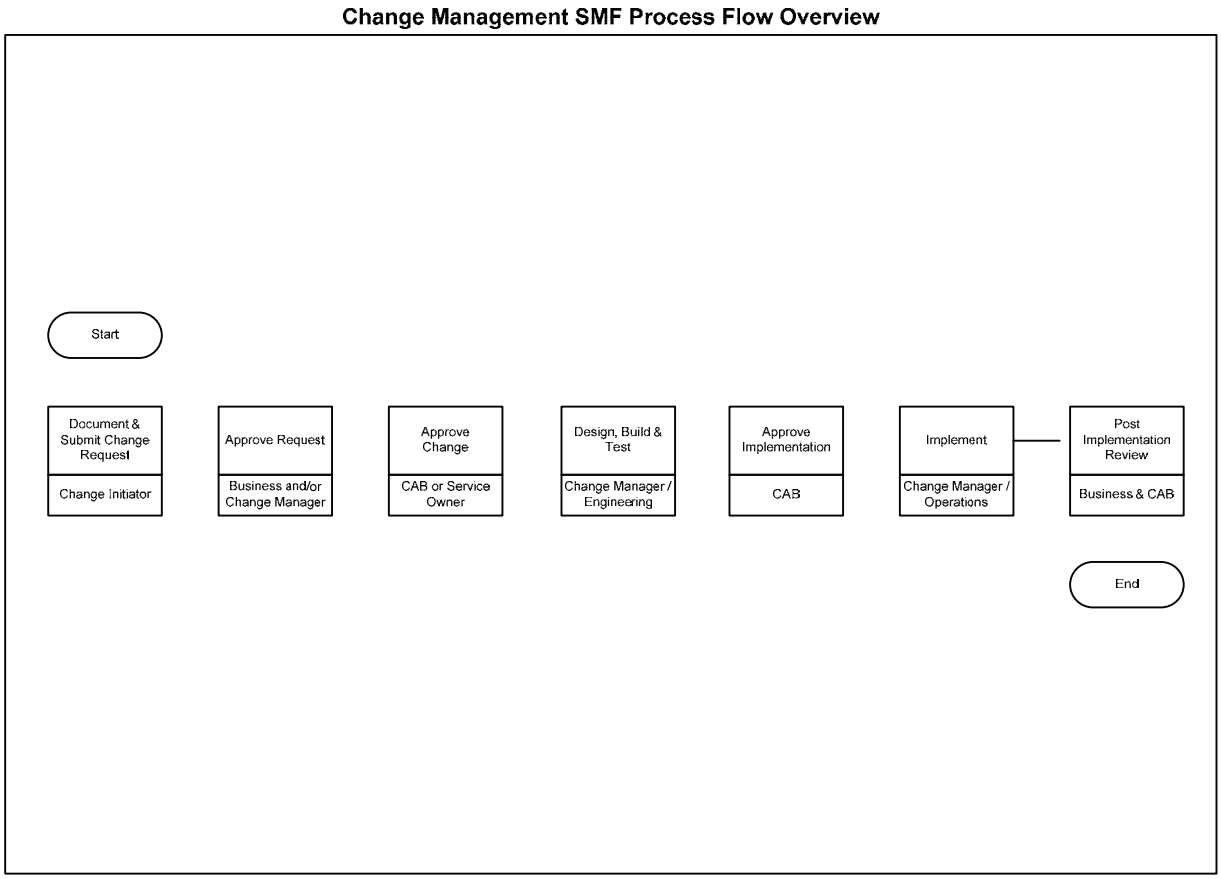


Figure 12: High level Change Management process

The project team created the following standard guidelines for the change management process. The Change Management Process covers new hardware and software installation, configurations, upgrades and patches to communications devices, operating systems, applications, reports, databases and SAN storage devices.

The process and activities for change management are intended to ensure,

- Alignment with IT Management expectations
- Minimal disruption to operations and business-critical services
- Segregation of and coordination of duties while planning and implementing change
- Adherence to departmental process, procedures, policies and standards
- Adequate communication and coordination within IT and with the business before, during and after changes are implemented

Document the analysis of critical aspects of the change including:

- Business or technical purpose

- Impact on systems and processes
- Urgency
- Conflicts and/or configurations issues
- Back-out procedures
- Security
- SOX and Regulatory compliance
- Post implementation effectiveness review
- Cost and benefit of the change
- Alternatives to the change and/or define risk of not performing the change

Manage other change considerations including:

- Budget
- Timeline
- Quality
- Training
- Roll-out plan
- Disaster recovery impact

Manage resources including:

- Identify and involve all resources (systems or people) affected by the change.
- Formalize and capture documentation
- Record and track approval(s) of the change
- Gather reports & analyze key metrics as part of continuous service improvement

Depending on the type of change, the change requester may be required to perform more or less steps in the process. For development related changes, the requester may be required to provide project related documentation related to the MSF process. These steps can be seen in figure 13 below. High risk changes or urgent changes may be required to go through a post implementation review. This review is designed to identify mitigating steps or processes that will improve future changes or assist in preventing unplanned changes.

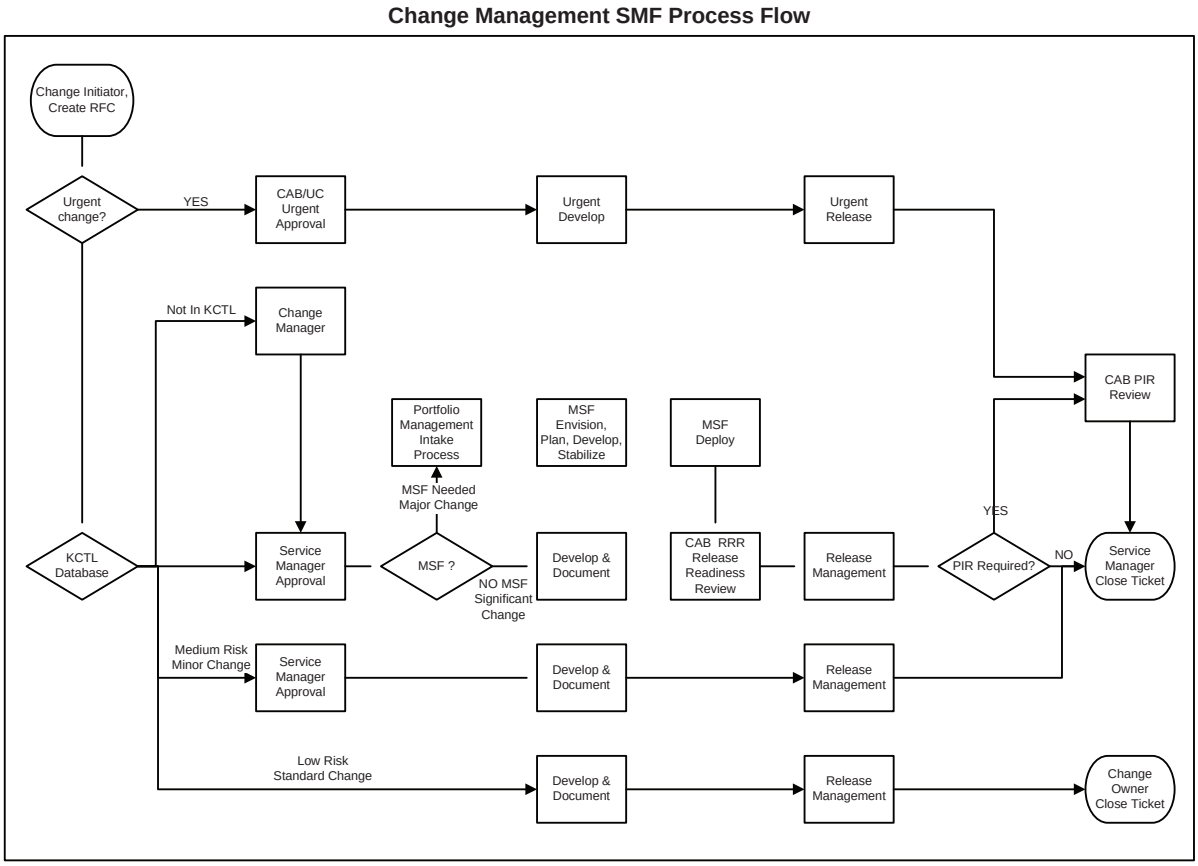


Figure 13: The Detailed Change Management process

The Change Advisory Board (CAB)

According to the ITIL Blue Book, the CAB is a key component that a company uses to assess and prioritize changes and provide change approvals. The key to a successful CAB is to ensure the participating CAB members have a good understanding of not only the business and users but also the technology and related support. This understanding assists the CAB in determining what the associated risk of a change may be and also what impact a change may have on the business and the end users. When organizing members of a CAB, it is important to have a change manager that is responsible for coordinating the CAB agenda, ensuring appropriate attendance by CAB

participants and maintaining detailed notes of the decisions made by the CAB. ITIL guidance is fairly wide in its description of the appropriate membership for the CAB. The team found that for the first phase of the CAB, a representative from each of the IT teams including development, infrastructure, operations, security and the service desk worked well. The team is also considering inviting business sponsors to the CAB sessions in the future as participants. This will allow for greater participation and coordination between the business and IT and also better visibility between business units that may require the same IT resources for IT services and requests that require change management to implement.

ITIL guidance also suggests that a minimum set of requirements are fulfilled by the CAB. The first of these requirements is that the CAB will ensure appropriate representation from the stakeholders depending on the type of change being considered. This could mean very different CAB participation depending on the types of changes under review. The ITIL guidance also recommends involving suppliers (or vendors), users and or customers and problem managers, service level manager, and customer relations staff. Depending on the size of the organization, the same employees may assume more than one of these duties. Our team decided to create a standing series of meetings and participants and let the change manager invite special guests that should attend for specific changes. In this way, the CAB is maintained as a regular repeatable event with the same set of participants and one off participants are still included when required.

Results of the Change Management Process

During the change management process implementation, the IT team noticed an immediate benefit of increased communication and coordination between the different IT teams. There was also a better understanding and ownership of changes due to the mapping of service owners into the change management approval process. Service owners were more informed and better prepared to speak to the business about changes. The team also implemented a standard monthly maintenance window to implement changes. This assisted in reducing the amount of downtime for the business and provided fewer IT outage or maintenance communications. The maintenance windows are coordinated around important business dates such as board meetings and SEC filing deadlines. This also reduced conflicts that may have been caused by IT trying to implement a change during a critical business event or deadline.

The Release Management Process

The Release Management process is used to control the introduction of new IT components to the production environment. The ITIL definition of Release Management includes IT components such as hardware, software and new documentation as items that can be managed under the Release Management process. The Release Management process should include both the technical as well as the non-technical aspects according to the Blue Book. Our project team used the concept of Release Management to create a process control point between the MSF process and the handoff to operations of new IT components. The ITIL guidance provides a good list of goals that are met with the release management process. These goals include,

- plan and oversee the successful rollout of software and relate hardware
- design and implement efficient procedures for the distribution and installation of Change to IT systems
- ensure that hardware and software being changed is traceable, secure and that only correct, authorized and tested versions are installed
- communicate and manage expectations of the Customer during the planning and rollout of new Releases
- agree the exact content and rollout plan for the Release, through liaison with Change Management
- implement new software Releases or hardware into the operational environment using the controlling processes of Configuration Management and Change Management- a Release should be under Change Management and may consist of any combination of hardware, software, firmware and document configuration items
- ensure that master copies of all software are secure in the Definitive Software Library (DSL) and that the Configuration Management Database is updated
- ensure that all hardware being rolled out or changes is secure and traceable, using the services of Configuration Management

The team integrated the Release Readiness process into both the MSF process as well as the Change Management process. As a release is nearing completion within the MSF process, the release coordinator will submit a Request for Change (RFC). The RFC is reviewed by the CAB and this includes a review of the Release Readiness checklist to

ensure all of the major release tasks have been completed. As seen in table 5 below, the release readiness checklist includes all of the functions within IT as well as vendors and the business representation where needed. This checklist is also an important step to ensure the appropriate support structure and training is in place before the release is placed into a live production environment.

Project Name:	<project name>
Release Sponsor:	<release sponsor>
Release Date:	<target release date>
Approval Date:	<omr approval date>
Response	Development
	Has the release undergone peer review?
	Has the release been checked into a source control library?
	Has the release undergone a Security "best practice" review
	Is updated user documentation provided?
	Is updated design documentation provided?
	Has the completed integration test been uploaded to the PSF project site?
	Have unit tests been completed?
	Has user acceptance testing been completed?
	Planning & Architecture
	Has an architectural review been completed?
	Have KPIs been identified and steps taken to enable measurement?
	Have service maps been created / updated?
	Have dependence and data flow diagrams been completed?
	PSF Large Documentation
	Have all mandatory PSF documents been completed and accepted?
	Is all project documentation stored in one central location (i.e. - Sharepoint Site)?
	Release / Cutover Team
	Is a back out plan in place, and if possible, has it been tested?
	Infrastructure Team
	Has a network diagram been completed
	Has a network traffic volume analysis been completed?
	Have port and protocol requirements been completed?
	Have source and destination networks/hosts been identified?
	Has a network design review been completed?
	Has a storage volume analysis been completed?
	Support Team
	Have Service Desk training requirements been met?
	Has a business approval chain been identified for delegating privileges/roles to users?
	Does Service Desk know who uses the system, what they do with it, where they do it, and the business process/business cycle context?

	Has a communication plan been formulated to notify end users and Service Desk of release?
	Has the knowledgebase been updated to enable tier 1 troubleshooting?
	Has the Service Desk received and accepted the FAQs?
	Has the Service Desk received and accepted the escalation path?
	Does Service Desk have appropriate privileges to execute their assigned support functions, and has Service Desk tested these privileges?
	Has Altiris been updated to support proper identification of the new release?
	Operations Team
	Has a contact been identified to approve maintenance activities?
	Have manpower issues been addressed?
	Has a runbook/playbook been completed and accepted by Operations?
	Have SLA's been agreed, and have steps been implemented to measure them?
	Is an Operations health check model in place which states what needs to be monitored, and who is responsible for monitoring the service?
	Are all administrative tools in place?
	Are all administrative documents in place?
	Have security roles & responsibilities been cleaned up when project ends?
	Has the change control process been followed?
	Partner / Vendor representative
	as needed - -
	End User / Business representative
	Has user training been completed?
	Has a Pilot / Beta test been executed?
	Has a User Manual been created?
	Has a User Manual been distributed?
	Has a Communication Message / Plan been designed
	Have all Stakeholders been informed of the Project's Status and Delivery Date?
	Has there been an Announcement for the New Application / Project?
	Has there been an Announcement for the New Application / Project training?
	Security Team
	Has the application passed examination by the automatic security exploitation tools?
	Has the security team reviewed and accepted the system design?
	Has the security accepted the system configuration?
	Has production data used for testing been scrubbed to remove sensitive information?

Table 5: The Release Readiness checklist

Results of the Release Management process

Following the introduction of the Release Management process, the team provided a communication to the IT department as well as updated training on the overall

MSF process. One of the final deliverables for the MSF process was the release readiness checklist. At the time this project was completed, no major releases were completed that were reviewed using the release process. However, in the future the team is hopeful that the process will result in more coordination and better overall delivery planning and execution of releases. This should provide the consistency, stability and overall control of the environment that will assist the business in running day to day operations without interruption.

Process maintenance

One of the final process components that the team included was a process maintenance routine. Unfortunately the ITIL v2 guidance did not include a step by step method for ongoing process maintenance. The team created a quarterly review of process adherence within each of the implemented process areas. The PMO is also responsible for a yearly process review for each of the ITIL process areas. Any needed updates or changes are submitted via the change management process by the process owner for review and acceptance. The process owner will submit the approved changes to the PMO and coordinate any required training or communication.

Summary of Results

At the time this project was completed, none of the major process areas were reviewed as they did not reached the annual review cycle. The team did update the service catalog on several occasions to capture changes to service owners, changes to services (enhancements) and new services that were implemented. The service owners initiated all of these updates and provided the required documentation without requiring management or PMO involvement to begin the update.

The ongoing review of process adherence has not been fully implemented due to recent turn-over and staff reductions. This has made it necessary to reassign process owners, service owners and management teams. Additionally, IT staff has taken on additional duties limiting the amount of process review time they have available to perform.

Additionally, as determined during the survey mentioned above, the maintenance and upkeep of the process documentation to the new ITIL v3 standards is an important

activity to maintain the applicability and evolution of process maturity. The PMO will be reviewing the process maintenance procedure to ensure alignment with the ITIL v3 guidance in the future.

Chapter Five: Lessons Learned

Lessons Learned from the Project

During the initial planning phase of this project the project team and the author took a very complicated implementation and partitioned it into multiple projects. The end result was a very coordinated and methodical roll-out of ITIL. The team however underestimated the level of ongoing effort for each of the process areas. Once the training is completed, ongoing monitoring, auditing and process reinforcement is required to keep the processes in place. Without this constant reinforcement and auditing, IT contributors begin performing tasks using out dated, familiar processes. The author would build more process maintenance time into the planning efforts and establish more frequent process audits and reviews. The overall ongoing adherence to processes should be coupled with individual staff objectives and performance measures to ensure IT staff understand the importance of process.

During the course of this project, the team concluded that you can not always anticipate business climate change. The team saw two major department reorganization efforts, the departure of the CIO and a complete change in the way the business operated due to the recession. The ITIL processes however, were based on sound principles that provide efficiency, control and organization. These three factors assisted in many unanticipated conversations including downsizing, budget planning and realignment of operational duties.

The team also learned that overall support and momentum for the project was assisted by attaining small wins and publicizing these within the department and occasionally with the business. As more wins were publicized, more IT staff began to

realize the positive impact the ITIL process was causing and also helped to inspire the identification of new wins that could easily be achieved within their own areas.

The Next Phase of the Project

The next stage in the project will include a review of the current process documentation and determine what if anything should be updated given the current IT environment with a reduced IT staff. The PMO should also map out an update strategy to the ITIL v3 approach using limited resources and with minimal impact to the environment. The team will also review the need for the implementation of the Problem Management and Capacity Management process areas.

Further metrics and reporting will be developed to provide more clarity around the performance of the IT environment to established operating targets and SLA's. The SLA's will be further refined and agreed upon with the business. This conversation should also tie into budget planning discussions between the IT department and the business. The final next step is to integrate the regulatory controls into the ITIL operational processes. At the time this project completed, budget approval was granted to review the controls and begin work on integrating these into the ITIL process environment.

Conclusion

The primary goal of the IT implementation was to bring the IT department to a level 2 maturity. The first goal to assist in elevating the IT department to a level 2 maturity is developing and implementing a common IT Infrastructure. Throughout the project, a common IT infrastructure was made possible by analyzing and documenting the existing environment and associated IT services. The primary deliverable that made

this goal successful was the IT Service Catalog. The Service Catalog and associated IT Service Maps, provided the detailed IT service listing and infrastructure in an easy to communicate format. This allowed the IT department to establish a common terminology and support foundation for all IT services. Additionally a standard hardware and software listing was created that aligned with the IT strategy and the common IT infrastructure. The goal of implementing a common IT infrastructure was met by analyzing and documenting the existing environment, establishing a baseline of standard hardware and software and using this information to create future IT services and IT direction in alignment with business goals and objectives.

The second goal to reach IT maturity level 2 is to meet customer expectations. The implementation of the Service Desk and Incident Management processes and the ability to monitor and improve performance of the tasks related to both processes made this goal successful. Within the Service Desk and Incident Management processes, standard response time and resolution targets can be monitored and consistently met by ensuring consistent documentation, prioritization, escalation, tracking and communication. By ensuring Service Desk requests and incidents are met with in established targets, business users (customers) have noticed an improvement of IT service delivery and response and this has assisted in building IT credibility.

The third goal of building IT credibility has been achieved as mentioned above by the implementation and execution of the Service Desk and Incident Management processes. IT credibility has also been achieved through the implementation of the IT Service Catalog, Change Management, Release Readiness, and the Service Monitoring and Control Processes. By implementing each of these processes, the IT environment has

evolved and realized more stability, reliability and control. The Change Management and Release Readiness processes have resulted in better cross team communication, coordination and management. This is evidenced by fewer instances of unplanned downtime as a result of improperly tested or implemented changes. Better communication around changes via the CAB and the regular monthly maintenance window is also improving overall operational uptime. Monthly uptime reports have only dropped below 99.9% uptime once in the past 6 months. The one missed target was due to a severe network provider issue and not due to missed internal response targets.

The fourth and final goal is to improve solution delivery. This goal is also successful as a result of the above mentioned processes and also the overall IT departments' greater awareness around service and system dependencies and their impact to business processing. With the greater awareness around how IT systems interrelate, IT teams are taking more time in analyzing, planning and controlling new releases and changes to the environment. Additionally, as part of the Change Management process, post mortem reviews are conducted on any urgent, high risk or failed changes. This analysis is used to improve the change steps used in building change as well as prevent future issues that may result in downtime from process gaps. Project teams have also began to hold pre-implementation briefings with the Service Desk staff and provide training and service guides to assist Service Desk staff in resolving any new incidents that may arise as a result of a change or addition to the IT service delivery environment.

Following the implementation of ITIL processes within the project, the IT department began to see:

- A drop in the number of unplanned outages. The team measured an average of 5-6 unplanned outages per month prior to the implementation of ITIL processes and has improved to 0-2 unplanned outages per month for the last 6 months.
- Significantly improved system uptime and availability including an average uptime rating of 99.9% for IT Infrastructure services for the first 5 months in 2009.
- Incident response and resolution times have improved from 2 days prior to ITIL to an average of 30 minutes or less per incident.
- More controlled IT changes resulting in fewer failed changes. Prior to consistent Change Management, an average of 4-5 changes per quarter experienced significant issues. During quarter 1 of 2009, only 1 change experience significant issues.

The drop in unplanned outages is attributed to the improvements brought by the more rigorous ITIL based Change and Release processes as well as better monitoring of the environment and Incident Management process to correct issues before they cause downtime. All of these processes also led to better ongoing stability and uptime since the environment and any change to the environment is more closely controlled, tested and communicated.

Summary

Following the implementation of ITIL processes, the IT department began to see a drop in the number of unplanned outages, faster incident resolution times, more controlled IT changes and better overall IT service delivery. The improvements achieved by the IT department due to the implementation of ITIL processes were noticeable in IT

metrics and business satisfaction that was collected both in surveys and general day-to-day correspondence. The IT department improved overall internal communication by establishing a common terminology and service catalog to align with the business needs. As a result, the IT department consistently attains the IT level 2 maturity goals. The IT department also realized unexpected benefits from the ITIL implementation by using IT service descriptions when cutting operational costs and during restructuring events due to a slow-down in the business during the 2009 recession.

Companies that implement ITIL are seeing both operational gains and tangible benefits. As discussed in this project, as a result of implementing ITIL, substantial improvements in overall incident response times, resolution times, quality and operational efficiency were achieved. The next step for this project and other organizations that have implemented ITIL is to take the process and efficiency improvements and calculate overall cost savings or other intangible benefits and publish the results within the IT department and with the business.

When asked about the "negative elements" that were encountered during ITIL implementation in an analysis by Forrester research by Peynot (2006), 52% encountered internal resistance to change, 29% found that business units or internal customers were not prepared to be involved in the new process and 21% indicated they did not encounter any negative elements during the ITIL implementation. Throughout this ITIL implementation the only negative element noted was the changing business environment and the difficulties seen from changes in organizational structure and business climate. The use of ITIL assisted the department through these changes and actually helped to show the value of the organization and efficiency that ITIL brings to the department.

An InfoWorld article (Steinberg 2006) provides the following thoughts on ITIL, "Any IT shop servicing a company that is undergoing major changes and/or servicing that company's customers, will benefit from ITIL. For instance, a small shop facing recurrent network outages will find benefits in employing ITIL's Problem Management process to predict and minimize future incidents. A midsize company with a complex IT infrastructure may find that the ITIL Configuration Management solution provides a blueprint for streamlining impact assessments for changes and new applications. A large organization undergoing a major acquisition or consolidation effort will discover that the consistent, repeatable processes outlined in ITIL make those efforts occur much faster and at less cost".

Bibliography

Kapp, J. (2006). *Implementation of Operational Framework in the NLP.* Denver, Co: Regis University School for Professional Studies.

Microsoft Corp, 2004. *1737B Microsoft Operations Framework Essentials.* USA: Microsoft.

Office of Government Commerce, 2000. *Best Practice for Service Support*. United Kingdom: TSO (The Stationary Office).

Office of Government Commerce, 2007. *Continual Service Improvement.* United Kingdom: TSO (The Stationary Office).

Office of Government Commerce, 2007. *Service Design*. United Kingdom: TSO (The Stationary Office).

Office of Government Commerce, 2007. *Service Operation*. United Kingdom: TSO (The Stationary Office).

Office of Government Commerce, 2007. *Service Strategy*. United Kingdom: TSO (The Stationary Office).

Office of Government Commerce, 2007. *Service Transition*. United Kingdom: TSO (The Stationary Office).

Online References

Dubie, Dennis (2002) Proctor & Gamble touts IT services model, saves $500 million. Retrieved June 16, 2009 from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=74762

Hubbert, Evelyn and O'Donnell, Glenn (2008) Inquiry Spotlight: ITIL, Q4 2008. Retrieved June 17, 2009 from www.forrester.com

Lemmex, Don (2008) MOFv4 vs. MOFv3 (top 5 value props). Retrieved May 7, 2009 from http://social.technet.microsoft.com/forums/en/MOF4/thread/3ae14c82-295c-48e2-b5da-988c7d83545e/

Merlyn, Vaughan (2008) Business-IT Maturity and Change in Organizational Mission. Retrieved February 21, 2009 from http://vaughanmerlyn.com/2008/01/07/business-it-maturity-and-change-in-organizational-mission/

Microsoft Corp (2009) Cross Reference ITIL V3 and MOF 4.0. Retrieved May 7, 2009 from http://go.microsoft.com/fwlink/?LinkId=151991

Peynot, Richard (2006) Firms Must Take ITIL Beyond IT Operational Goals. Retrieved June 16, 2009 from www.forrester.com

Steinberg, Randy (2006) Getting a head start on ITIL. Retrieved June 17, 2009 from http://www.infoworld.com/print/25458

Tainter, Mike and Likier, Martin (2007). Key Differences Between ITIL v2 and v3. Retrieved April 18, 2009, from http://www.itsmwatch.com/itil/article.php/3707341

Appendix A: Service Desk Standard Process Narrative

Standard Service Desk SMF
SMF Process Narrative
SMF Implementation Date 12/14/07

Revision History:

Version No.	Revision Date	Performed By	Revision Description
1	10/10/2007	Isaac Wong	Initial SMF Roll-Out Documentation
2	12/03/2007	Isaac Wong	Revision with Neville's comments
2.1	5/5/2008	Wade Lowder	Added Communications Model

Process Owner:
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

Control Process Owners and Other Contacts:
Josh Gilmore, Senior Manager, Global IT Service Delivery

Documentation Authors and SMEs:
Wade Lowder, Senior Manager, North American Operations

SMF Process Overview:

The Standard Service Desk is a company global service organization and the single, vital day-to-day contact point for handling communications and delivering quick, precise, and responsive resolutions to all Company employees, contractors, and business partners. The Standard Service Desk is an interface channel for users to other Service Management Functions (SMF). Its primary objectives are to effectively manage the call center operations and properly handle incident duties such as, classification, logging, assignment, initial diagnosis and escalation.

Company users can submit their requests by phone or via emails and/or Self-Service to the Standard Service Desk. A ticket is opened by a Service Desk Analyst (SDA) for each request and an appropriate priority level is assigned to each individual ticket based on its impact and urgency to the company organizations. Dedicated Service Desk Analysts represent the company tier 1 support team and are available 24 hours a day and 7 days a week to handle all circumstances, coordinate change requests across business, technology, and process boundaries, raise alerts about problems and trends proactively, compile data on service goals and achievements, provide communication, information, and resolutions needed to resolve any IT issues, and monitor customer satisfaction.

IT Systems:

System/Application	Process Supported
PeopleSoft HR	New hire set up and configuration
Sharepoint	Creation of Sharepoint sites
Altiris	Support of Altiris jobs
Blackberry	Blackberry set up and support
T-mobile, Verizon, AT&T, Nextel and others	Cell phone support
Basic CRM support	Basic CRM support
Tape backups	Operations support
Company and IT Notification hub	Notification delivery to business as needed.
Yardi	Yardi Support
PeopleSoft	PeopleSoft support
Cisco Systems VPN Client	VPN support
Account Management in Active Directory	Password reset and unlock
VOIP Support	Phone
Modular Messaging Support	Voice Mail and Phone
Microsoft Office Suite	Microsoft Office Suite Support
Microsoft Outlook	Email support
LCD, Plasma, and video conference	Audio/Visual support

Key Spreadsheets or other End-User Tools:

Type	Name	Filename and Location	Purpose
N/A			

Supplemental Documentation, Reference Material and Reports:

Name
Argus Installation
CRM Installation
Creation of User Accounts
Creating SharePoint Sites
Creating VOIP Phone Extensions
Internet Explorer – Restoring Defaults, Clearing Cache
Modular Messaging Installation and Support
NARF Process
Notification Process
Outlook – Granting Permissions
PeopleSoft Password Reset
Personal Folder Management
PLD Support

Priority Description and Response Requirements
Software License Management
Termination Process
VPN Login Procedure
Webmail Login Procedure

Optional, if applicable to the process
Third-Party Interfaces:

Interface Name & Purpose	Vendor Name
N/A	

Process Narrative:

When an incident occurs to any company employee, contractor, or business partner, the Service Desk Analyst takes the following general steps to resolve an incident. Please see the process flow chart for graphical representation located here.

1. When a company employee, contractor, or business partner encounters a technical problem, the user contacts the Standard Service Desk by phone or email.
2. The SDA creates a ticket in Altiris and documents information gathered about the user and the symptoms that are being reported. The SDA is responsible for end-to-end ownership, tracking, and monitoring the ticket throughout the entire process and is responsible for keeping the customer posted with any progress towards resolutions.
3. The SDA then assigns an appropriate priority level to each individual ticket based on its impact and urgency to the company organizations.
4. If possible, the on-duty SDA will attempt to provide an immediate solution by conveying known workarounds, using diagnostic scripts, or based upon their own knowledge and experience. If the solution proposed by the on-duty SDA resolves the problem, then go to step 8.
5. If no answer is found for the problem after research and investigation, the SDA escalates the ticket to the Tier 2 support team. If the solution proposed by the Tier 2 support team resolves the problem, then go to step 7.
6. If the Tier 2 support team is also unable to resolve the incident, the ticket is escalated to the Tier 3 support team. The Tier 3 support team works with the customer until the problem is resolved.
7. Once the Tier 2 or 3 support team has resolved the problem, the ticket is assigned back to the Service Desk for ticket closure.
8. Before the ticket can be closed, the SDA tests and confirms resolution with the customer and obtains his or her verbal or written approval to close the ticket.
9. If the customer agrees and is satisfied with the resolution, the SDA can close the ticket in Altiris. The SDA enters the detailed actions that were carried out to resolve the problem in the knowledge base for future references.

Standard Service Desk Communications Model

Ticket Priority	Communication Target	Escalation Communication Target
High	Requestor Only	Requester, Infrastructure Management and Exec IT Management
Medium	Requestor Only	Requester and Infrastructure Management
Low	Requestor Only	Requester and Infrastructure Management

Key Performance Indicators:

Category	Key Performance Index
Call Statistics	▪ Abandonment Rate ▪ Average Time to Answer ▪ Distribution of Incoming Calls
Ticket Statistics	▪ Open Ticket Count within Time Frame ▪ Closed Ticket Count within Time Frame ▪ Overall outstanding open tickets ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Ticket Activity by Department ▪ Ticket by Priority ▪ First Level Resolution
Service Level Agreement Compliance	▪ Network Availability ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Customer Satisfaction Rating ▪ Percent of SLA Commitments that are met ▪ Spam Statistics

Appendix A SMF Roles and Responsibilities:

Standard Service Desk		
	Position	**Responsibility**
Role 1	SDA – Service Desk Analyst	SDA is responsible for supporting the general customer base of company in all areas of technology. SDA acts the point of contact between the customer and the discipline working the issue and represents the service desk to deliver effective and efficient communications by phone or via email.
Role 2	PSTA – Premier Senior Technical Analyst	The prime responsibility of PSTAs is to support the 5% exception of executives / predetermined premier users. PSTAs are experienced analysts with advanced technical knowledge and customer service skills to provide proper coaching and mentoring to Service Desk Analysts (SDA). The PSTA also supports Tier 1 Service Desk analysts when not supporting Premier calls.
Role 3	Audio / Visual Technician	Audio / Visual Technician maintains, manages company Audio and Visual equipment and provides support and assistance such as, training, documentation and configuration, to company customers for meetings and events.
Role 4	SDS – Service Desk Supervisor	SDS will work with GSDM (See Role 5) to manage regional Service Desk analysts.
Role 5	GSDM – Global Service Delivery Manager	GSDM is responsible for overview of all North American Service Desk analysts. Responsibilities of a GSDM include, but are not limited to, customer satisfaction survey review and rapid response, quarterly meetings with executive assistants of the Premier group, monthly / quarterly status reporting to the OMR operation lead, and Global Service Desk and IT Governance management.

Appendix B Glossary:

Term	Definition
Altiris	Altiris is helpdesk solution software and a tool to help ensure IT infrastructure availability and raise service levels while reducing costs.
GSDM	Global Service Delivery Manager
KPI	Key Performance Indicator
PSTA	Premier Senior Technical Analyst
SDA	Service Desk Analysts
SDS	Service Desk Supervisor
SLA	Service Level Agreement
SME	Subject Matter Expert
SMF	Service Management Function
VOIP	Voice Over Internet Protocol. Individuals inside and outside organizations can contact each other using VOIP.
VPN	Virtual Private Network. VPN is a form of communication over networks that are public in ownership, but emulate a private network in terms of security.
Yardi	Asset and property management software

Appendix B: Premier Service Desk Process Narrative

Premier Service Desk SMF
SMF Process Narrative
SMF Implementation Date 12/14/07

Revision History:

Version No.	Revision Date	Performed By	Revision Description
1	10/08/2007	Isaac Wong	Initial SMF Roll-Out Documentation
2	12/03/2007	Isaac Wong	Revision with Neville's comments
2.1	5/5/08	Wade Lowder	Added Communication Section

Process Owner:
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

Control Process Owners and Other Contacts:
Josh Gilmore, Senior Manager, Global IT Service Delivery

Documentation Authors and SMEs:
Wade Lowder, Senior Manager, North American Operations

SMF Process Overview:

The Premier Service Desk is a company global service organization and the single, vital day-to-day contact point for handling communications and delivering quick, precise, and responsive resolutions with top experienced human resources. Its premier service is served exclusively to the qualified chief officers and executives of the company. The Premier Service Desk is designed to provide the best customer service and restore normal service operations always in high priority fashion.

A ticket is opened by a Premier Senior Technical Analyst (PSTA) for each call, email, or any forms of request to the Premier Service Desk. A high priority level is assigned to each individual ticket. Dedicated PSTAs with advanced technical and customer service skills are available 24 hours a day and 7 days a week to handle all circumstances, coordinate change requests across business, technology, and process boundaries, raise alerts about problems and trends proactively, compile data on service goals and achievements, provide communication, information, and resolutions needed to resolve any IT issues, and monitor customer satisfaction.

IT Systems:

System/Application	Process Supported
PeopleSoft HR	New hire set up and configuration
Sharepoint	Creation of Sharepoint sites
Altiris	Support of Altiris jobs
Blackberry	Blackberry set up and support
T-mobile, Verizon, AT&T, Nextel and others	Cell phone support
Basic CRM support	Basic CRM support
Tape backups	Operations support
Company and IT Notification hub	Notification delivery to business as needed
Yardi	Yardi Support
PeopleSoft	PeopleSoft support
Cisco Systems VPN Client	VPN support
Account Management in Active Directory	Password reset and unlock
VOIP Support	Phone
Modular Messaging Support	Voice Mail and Phone
Microsoft Office Suite	Microsoft Office Suite Support
Microsoft Outlook	Email support
LCD, Plasma, and video conference	Audio/Visual support

Key Spreadsheets or other End-User Tools:

Type	Name	Filename and Location	Purpose
N/A			

Supplemental Documentation, Reference Material and Reports:

Name
Argus Installation
CRM Installation
Creation of User Accounts
Creating Sharepoint Sites
Creating VOIP Phone Extensions
Internet Explorer – Restoring Defaults, Clearing Cache
Modular Messaging Installation and Support
NARF Process
Notification Process
Outlook – Granting Permissions
PeopleSoft Password Reset
Personal Folder Management
PLD Support
Priority Description and Response Requirements
Software License Management
Termination Process
VPN Login Procedure

Webmail Login Procedure

Optional, if applicable to the process
Third-Party Interfaces:

Interface Name & Purpose	Vendor Name
N/A	

Process Narrative:

When an incident occurs to the qualified company chief officers and executives, the Premier Technical Senior Analyst takes the following general steps to resolve an incident. Please see the process flow chart for graphical representation located here.

1. When a qualified company chief officer and executive encounters a technical problem, the chief officer or executive contacts the Premier Service Desk by phone, via email or walk-in.
2. A dedicated PSTA with advanced technical background and excellent customer service skills creates a ticket in Altiris and documents information gathered about the chief officer or executive and the symptoms that are being reported. The PSTA is responsible for end-to-end ownership, tracking, and monitoring of the ticket throughout the entire process and is responsible for keeping the customer posted with any progress towards resolution.
3. The PSTA will work with tickets to the Premier Service Desk received from any office in all domestic or international locations. A high priority level is assigned to all tickets to the Premier Service Desk.
4. If possible, the on-duty PSTA will attempt to provide an immediate solution by conveying known workarounds, using diagnostic scripts, or based upon their own knowledge and experience.
5. If no answer is found in the knowledge base or after research and investigation for the problem, the PSTA can escalate the Premier Service Desk ticket directly to the appropriate Tier 2 or Tier 3 support team for immediate attention.
6. The PSTA determines if procurement is required. If yes, the PSTA engages the procurement office for assistance.
7. Once the problem is resolved, the PSTA tests and confirms the resolution with the chief officer or executive and obtains his or her verbal or written approval to close the ticket.
8. If the customer agrees and is satisfied with the resolution, the PSTA can close the ticket in Altiris. The PSTA then enters the detailed actions that were carried out to resolve the problem in the knowledge base for future references.

Premiere Service Desk Communications Model

Ticket Priority	Communication Target	Escalation Communication Target
VIP	Requestor and IT Executive Management	Requester, Infrastructure Management and Exec IT Management
High	Requestor Only	Requester, Infrastructure Management and Exec IT Management
Medium	Requestor Only	Requester and Infrastructure Management
Low	Requestor Only	Requester and Infrastructure Management

Key Performance Indicators:

Category	Key Performance Index
Call Statistics	▪ Abandonment Rate ▪ Average Time to Answer ▪ Distribution of Incoming Calls
Ticket Statistics	▪ Open Ticket Count within Time Frame ▪ Closed Ticket Count within Time Frame ▪ Overall outstanding open tickets ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Ticket Activity by Department ▪ Ticket by Priority ▪ First Level Resolution
Service Level Agreement Compliance	▪ Network Availability ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Customer Satisfaction Rating ▪ Percent of SLA Commitments that are met ▪ Spam Statistics

Appendix A SMF Roles and Responsibilities:

Premier Service Desk		
	Position	**Responsibility**
Role 1	PSTA – Premier Senior Technical Analyst	The prime responsibility of PSTAs is to support the 5% exception of executives / predetermined premier users. PSTAs are experienced analysts with advanced technical knowledge and customer service skills to provide proper coaching and mentoring to Service Desk Analysts (SDA). The PSTA also supports Tier 1 Service Desk analysts when not supporting Premier calls.
Role 2	SDS – Service Desk Supervisor	SDS will work with GSDM (See Role 3) to manage regional Service Desk analysts.
Role 3	GSDM – Global Service Delivery Manager	GSDM is responsible for overview of all North American Service Desk analysts. Responsibilities of a GSDM include, but are not limited to, customer satisfaction survey review and rapid response, quarterly meetings with executive assistants of the Premier group, monthly / quarterly status reporting to the OMR operation lead, and Global Service Desk and IT Governance management.

Appendix B Glossary:

Term	Definition
Altiris	Altiris is helpdesk solution software and a tool to help ensure IT infrastructure availability and raise service levels while reducing costs.
GSDM	Global Service Delivery Manager
KPI	Key Performance Indicator
PSTA	Premier Senior Technical Analyst
SDA	Service Desk Analysts
SDS	Service Desk Supervisor
SLA	Service Level Agreement
SME	Subject Matter Expert
SMF	Service Management Function
VOIP	Voice Over Internet Protocol. Individuals inside and outside organizations can contact each other using VOIP.
VPN	Virtual Private Network. VPN is a form of communication over networks that are public in ownership, but emulate a private network in terms of security.
Yardi	Asset and property management software

Appendix C: Incident Management Policy

Incident Management Policy

Version
1.01

Effective Date
09/01/2008

Prepared by
Company IT Operations

1. Process and Document Information

PROCESS OWNER
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

CONTROL PROCESS OWNER
Josh Gilmore, Senior Manager, Global IT Service Delivery

DOCUMENT OWNER
Wade Lowder, Senior Manager North American Operations

DOCUMENT HISORY
All revisions made to this document are listed here in chronological order.

VERSION #	REVISION DATE	PERFORMED BY	REVISION DESCRIPTION
1.0	09/01/2008	Wade Lowder	Initial Policy Release
1.01	4/20/09	Wade Lowder	Minor wording clarifications

REFERENCED MATERIAL
Refer to the following documents for further information:
Incident Management SMF Narrative
Incident Management Workflow Diagram

2. Introduction

PURPOSE

The purpose of this policy is to provide standards and definitions relating to company incident management process and outline the different responsibilities of the company Information Technology department with regards to reacting and responding to various types of operation, network and information security incidents that may occur within the company IT department.

This document presents general incident response policies that are independent of particular hardware, platforms, operating systems, and applications. Specifically, it requires establishment of an effective incident response program and best practices to detect, analyze, prioritize, and handle incidents.

SCOPE

This policy applies to all electronic information, computer equipment, network equipment, telephone equipment, operating systems, and application software that are owned, operated, managed, hosted, rented, or leased by company or any of its subsidiary divisions.

This policy addresses only adverse events that are IT System and or security related and excludes adverse events caused by sources such as natural disasters and power failures.

AUDIENCE

This document applies to all personnel with an assigned role in supporting IT products and/or services for company or any of its subsidiary divisions.

3. Incident Management Overview

OVERVIEW

Incident Management is the process used to identify an issue and work towards its resolution as quickly as possible. Such a process is a key control in resolving outages that impact critical applications or revenue-impacting projects, and has a direct impact on a company's "bottom line."

Company Incident Management process is focused on both day-to-day management of common technology service issues and major production outages, and is meant as a common framework for all company locations to follow to ensure standardization and compliance with company Incident Management methodology.

DEFINITION

EVENT

Any observable occurrence or action in a system or network. Events can include but are not limited to a user connecting to a file share, a server receiving a request for a Web page, a user sending e-mail, and a firewall blocking a connection attempt.

ADVERSE EVENTS

Events with negative consequences, including but not limited to system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page, any execution of malicious code that destroys data.

INCIDENT

Event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction or degradation in the quality of that service or existing technology that impacts the ability of company staff to perform job functions.

IT SECURITY INCIDENT

Violation or imminent threat of violation of IT security policies, acceptable use policies, or standard security practices.

SEVERITY ASSESSMENT

IMPACT

There are three impact levels used to assist with accurately determining the correct impact level of an IT incident. Impact is a measure of the business criticality of an Incident or Problem.

	Impact	Determination
1	High	High regulatory, financial or operational risk
2	Medium	Moderate regulatory, financial or operational risk
3	Low	No regulatory, financial or operational risk

URGENCY

Urgency is the necessary speed required in solving an Incident of a certain impact. High impact Incidents do not by default need to be solved immediately.

	Urgency	Determination
0	Urgent	Immediate response is required, above and beyond that given to any other incident. It typically require cross-company coordination, management escalation, mobilization of additional resources, and increased communications to resolve major incident such as loss of core system, connectivity or power.
1	High	Prompt response is necessary due to volatility of data and/or the compromise of highly sensitive data.
2	Medium	Moderate need for a timely response and/or possible compromise of sensitive data.
3	Low	No involvement of sensitive data and workaround(s) exists for the customer

PRIORITY

Priority is defined as expected effort to resolve an Incident. The priority code determination is simply a function of the impact taken in conjunction with the urgency as depicted in the matrix below:

Priority Matrix		**Impact**		
		High	**Medium**	**Low**
Urgency	**Urgent**	Urgent		
	High	1 - High	1 - High	2 - Medium
	Medium	1 - High	2 - Medium	3 - Low
	Low	2 - Medium	3 - Low	3 - Low

TARGET CONTACT AND RESOLUTION TIME

The IT organization will strive to resolve each incident within certain limits of time defined by priority code. This commitment is a critical component of the company Incident Management OLA.

The table below provides initial contact and resolution time by priority code.

Priority code	**Description**	**Initial Contact time ***	**Target resolution time ***
0 **	Urgent **	15 Minutes	4 hours (24X7)
1	High	30 Minutes	2 Business Days
2	Medium	2 Hours	3 Business Days
3	Low	4 Hours	5 Business Days

* Time frames listed above for initial contact and resolution reflect normal business hours.

** Urgent incident status indicates working with the customer until the incident is resolved regardless of normal operation hours.

4. Incident Management Policy

POLICY STATEMENTS

- Incident Identification and communication will follow the procedures defined in the Incident Management SMF Narrative Document and Process Flow.
- Company will respond to IT incidents as required by law and applicable operating agreements.
- All incidents are generally reported via either event monitoring systems or user notification via phone or email. In order to avoid delay in management decisions and actions, qualified company executives can choose to walk-in and report critical incidents they experience to the Service Desk.
- All incidents will be logged with and tracked through the company Service Desk.
- A member of the company Service Desk team will be designated to handle IT incidents with low, medium or high priority during normal operating hours.
- A member of the company Service Desk team will be designated to handle IT incidents with urgent priority during normal business hours as well as outside normal operating hours.
- All incidents will be investigated and resolved using the processes defined in the Incident Management SMF Narrative Document and Process Flow.
- Company will form IT incident response team(s) based upon needs as directed by IT Operations, to investigate and resolve IT incidents.
- Company IT incident response teams will test the incident response program at least once annually with simple walk-throughs to ensure all appropriate staff members are fully aware of all procedures and responsibilities in the event of an IT incident.
- IT Operations will be responsible for maintaining and reviewing the incident response program annually, as well as after IT incidents and during post-incident meetings, with new procedures, team members and contact information. Updates to the process will be made as necessary.
- Appropriate training will be held to ensure staff members understand the IT incident response procedures. Training will occur at least once annually.
- Individual IT groups are responsible for providing supporting materials detailing operational procedures necessary to handle IT incidents.

VIOLATION OF POLICY

It is the duty and obligation of every company employee, contractor and third-party vendor to report any activity that violates this policy to the process or control process owner or the Chief Information Officer (CIO). Any exceptions to this policy must be approved in advance by the process or control process owner and the Chief Information Officer.

ENFORCEMENT

Company management is responsible for communicating these requirements to all appropriate personnel. (At a minimum, this policy should be communicated to all appropriate personnel in the "audience" section of this document.) In addition, IT management, Security, Auditing, and Compliance personnel will periodically survey this activity to ensure that policy objectives are being met.

EXCEPTIONS

Requests for exception to any portion of this policy must be submitted in writing to company IT Infrastructure and Operations Management. Before any actions can be taken, approval from all members of company IT Infrastructure and Operations management must be obtained.

EFFECTIVE DATE

All changes to this policy take effect immediately.

Appendix D: Incident Management Escalation Matrix

ESCALATION MATRIX BY • SERVICE • ORIGIN • INCIDENT TYPE • TIER LEVEL (1,2,3)		ESCALATION TEAM ASSIGNED BY INCIDENT ORIGIN																	
		NORTH AMERICA							EUROPE					CN		AS	
		NA-Service Desk	NA-Operations	NA-Engineering	NA-Network Engineering	NA-PeopleSoft	NA-Yardi	NA-Information Management	EU-Service Desk	EU-Engineering	EU-PeopleSoft	EU-Yardi	Escalation to North America	CN-Service Desk	Escalation to North America	AS-Service Desk	Escalation to North America
		NA	NA	NA	NA	NA	NA	NA	EU	EU	EU	EU	NA	CN	NA	AS	NA
Collaboration	**Owner**																
Corporate Calendar		1						2,3	1				2,3	1	2,3	1	2,3
Extranet Web Folders		1						2,3	1				2,3	1	2,3	1	2,3
File Services		1	2	3					1	2,3				1	2,3	1	2,3
Intranet		1						2,3	1				2,3	1	2,3	1	2,3
LiveMeeting		1,2	3						1,2	3				1	2,3	1	2,3
MOSS 2007		1						2,3	1				2,3	1	2,3	1	2,3
Print/Fax/Scan		1	2	3					1,2	3				1	2,3	1	2,3
SharePoint 2003		1						2,3	1				2,3	1	2,3	1	2,3
SOX Accelerator		1						2,3	1				2,3	1	2,3	1	2,3
Communications																	
Audio Visual		1	2		3				1	2,3				1	2,3	1	2,3
Modular Messaging		1	2	3					1	2,4				1	2,3	1	2,3
Telephony		1	2	3					1	2,5				1	2,3	1	2,3
VoIP		1	2	3					1	2,6				1	2,3	1	2,3
Corporate Web Presence																	
Internet Connectivity		1	2		3				1	2,3				1	2,3	1	2,3
Extenal Web site		1						2,3	1				2,3	1	2,3	1	2,3
Property search		1						2,3	1				2,3	1	2,3	1	2,3
CRM																	
CRM		1						2,3	1				2,3	1	2,3	1	2,3
Development																	
Circle Developer		1		need 2,3					1	2,3				1	2,3	1	2,3
Comparables		1						2,3	1				2,3	1	2,3	1	2,3
Document Management		1						2,3	1				2,3	1	2,3	1	2,3
Investor Fund Portal		1						2,3	1				2,3	1	2,3	1	2,3
Project Direct - NA		1						2,3						1	2,3	1	2,3
Project Direct - EU									1				2,3				
QMS		1						2,3	1				2,3	1	2,3	1	2,3
Financial Management									1								
PeopleSoft Financials - NA		1				2,3								1	2,3	1	2,3
PeopleSoft Financials - EU									1		2,3						
Transcentive		1					2,3										
Financial Planning and Analysis																	
DynaSight		1		need 2,3					1	need 2,3				1	2,3	1	2,3
ProClarity Analytics Server		1						2,3	1				2,3	1	2,3	1	2,3
TM1		1		2,3					1	need 2,3				1	2,3	1	2,3
Fund Management																	
Circle Investor		1		need 2,3					1					1	2,3	1	2,3
Fund Investment Tracker		1						2,3	1				2,3	1	2,3	1	2,3
Human Resources																	
PeopleSoft HR - NA		1				2,3								1	2,3	1	2,3
PeopleSoft HR - EU									1		2,3						
Marketing																	
Interwoven MediaBin		1					2,3										
Messaging																	
Blackberry		1	2	3					1	2,3				1	2,3	1	2,3
Corporate Email		1	2	3					1	2,3				1	2,3	1	2,3
Windows Mobile		1	2	3					1	2,3				1	2,3	1	2,3
Property Management																	
ProLease		1						2,3	1				2,3	1	2,3	1	2,3
Yardi - NA		1					2,3							1	2,3	1	2,3
Yardi - EU									1			2,3					
Service Desk																	
Desktop Applications		1	2	3					1	2,3				1	2,3	1	2,3
Desktop Support		1	2	3					1	2,3				1	2,3	1	2,3
Premier Support		1	2	3													
Supporting Services																	
Active Directory		1	2	3					1	2,3				1	2,3	1	2,3
Altiris		1	2	3					1	2,3				1	2,3	1	2,3
Backups		1	2	3					1	2,3				1	2,3	1	2,3
Citrix		1					2,3							1	2,3	1	2,3
Oracle-NA		1				2,3								1	2,3	1	2,3
Oracle-EU									1		2,3						
DataCenter, NA			1,2	3										1	2,3	1	2,3
DataCenter, EU										1,2,3							
DocAve		1						2,3	1				2,3	1	2,3	1	2,3
EDW		1						2,3	1				2,3	1	2,3	1	2,3
Enterprise Analytics Cubes		1						2,3	1				2,3	1	2,3	1	2,3
Nagios		1	2	3					1	2			3	1	2,3	1	2,3
SAN		1	2	3					1	2,3				1	2,3	1	2,3
Tipping Point		1		need 2,3					1,2	3				1	2,3	1	2,3

Appendix E: Incident Management Process Narrative

Incident Management
SMF
SMF Process Narrative
SMF Implementation Date 09/01/08

Revision History:

Version No.	Revision Date	Performed By	Revision Description
1.0	09/01/08	Wade Lowder	Initial Document Release

Process Owner:
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

Control Process Owners and Other Contacts:
Josh Gilmore Senior Manager, Global IT Service Delivery

Documentation Authors and SMEs:
Josh Gilmore, Senior Manager, Global IT Service Delivery
Wade Lowder, Senior Manager, North American IT Operations

SMF Process Overview:
The Incident Management SMF enables the company IT organization to promptly direct and allocate IT resources to resolve incidents that adversely affect IT services or infrastructure based on urgency and the impact on the business. It allows the Service Desk to quickly and effectively react and respond to user-reported incidents as well as responding proactively to alerts from the event management systems. This critical process ensures that service request information is accurately recorded, incident status is closely tracked throughout the entire process, and incident escalation to internal or external groups is properly prioritized and routed to the correct support resources. New problems are checked against known errors and problems so that any previously identified workarounds can be quickly located. Incident management then provides a structure by which problems can be investigated, diagnosed, resolved, and then closed. The process ensures that the incidents are owned, tracked, and monitored throughout their life cycle. There may be occasions when major incidents occur that require an elevated level of technical expertise. Incident management includes a process for handling these major incidents, including management and functional escalations, effective communications, formal rollback plans, and interfaces with the Problem Management SMF for further review and analysis to proactively prevent incidents from reoccurring.

IT Systems: System/Application	Process Supported
Altiris	Incident documentation, escalation and resolution documentation, reporting.
Monitoring tools (Nagios, HPSIM, Cacti, Spotlight, etc)	Incident identification and reporting. Incident resolution confirmation.
Communication tools (Phone, email, SMS, Altiris)	Entry point for customer to initiate the Incident Management process. Resolution and escalation coordination.
Active Metrics	Reporting and trending of incident response times

Key Spreadsheets or other End-User Tools:

Type	Name	Filename and Location	Purpose
NA			

Supplemental Documentation, Reference Material and Reports:

Name
Incident Management Policy
Escalation Matrix
Incident Management Process Flow

Optional, if applicable to the process
Third-Party Interfaces:

Interface Name & Purpose	Vendor Name
NetApp Monitoring	Network Appliance
IBM Monitoring	IBM

Process Narrative

The Incident Management SMF follows the general steps below for handling service requests from users and all alerts generated from the event management system.

1. Company departments experience new incidents that either impact or threaten to impact the normal operation of the business.
2. New incidents are reported by any company associate by contacting the Service Desk by telephone, or e-mail. Incidents are also generated by system monitoring alerts.
3. Regardless of the source, all incidents are recorded in Altiris as a ticket by the Service Desk so that the problem can be tracked, monitored, and updated throughout its life cycle. This information is later utilized for problem management reporting, process optimization, and planning. While creating a ticket, the Service Desk verifies user configuration and technical details, such as software version, previous incidents relating to equipment, etc.
4. Once the ticket is created, the incident is classified and assigned a Priority. Priority is based on impact and urgency. Tickets assigned with an "urgent" priority indicate major incidents requiring increased coordination, escalation, communication, and resources.
   See the Incident Management Policy for company definition of incident Urgency, Impact, Priority and Target Resolution Time.
5. The Service Desk processes all requests against known errors, existing problems, and previous incidents in the Knowledge Base in order to identify documented workarounds.
6. The investigation and diagnosis process attempts to fully understand the incident, collect diagnostic data, analyze data trends, identify incident root cause, and suggest appropriate approaches to execute resolutions and rectify the issue in order to help recover to normal operation as quickly as possible.
7. The resolution and recovery process covers the steps anticipated and required to resolve the incident, often by interfacing with the change management process to implement remedial action. Once a solution or workaround is identified, tested, and confirmed, this process notifies the Service Desk of the solution details, interfaces with the change management process to implement changes, confirms resolution actions and carries out recovery actions.
8. Requests requiring a specific technical skill set beyond that of the Service Desk are escalated to the appropriate Tier 2 or 3 groups for resolution. Escalated tickets should be thoroughly investigated, and the findings or issues documented in the ticket prior to escalation. Escalation shall be initiated as quickly as possible by assigning the ticket to the next Tier. Tier 2 or 3 Support teams are responsible for taking ownership, working with the Service Desk (who works with the customer), and updating the ticket until the incident is resolved. As soon as the issue has been corrected, Tier 2 or 3 should change the status to "Resolved" and re-assign the ticket to the Service Desk for closure and confirmation with the requestor. Incident are escalated based on the Incident Management escalation matrix

The Service Desk liaises with the Problem Management SMF to create, categorize and analyze any new problems identified during the process. The focus of Problem Management is to resolve the root cause of errors and to find permanent solutions. Any new information acquired from the incident is added to the Knowledge Base for future reference.

9. Tier 2 and Tier 3 groups are required to accurately document all tickets assigned to them. This includes: capture incident details, confirmation of resolution with Service Desk (who confirms with the end user), and categorization of incident closure type, change of ticket status to "Resolved" and re-assignment of ticket to the Service Desk team for closure.
10. When the issue is resolved and any new information is updated to the Knowledge Base, the Service Desk closes the Altiris ticket upon verification of the accuracy with the customer.

Key Performance Indicators

The following Key Performance Indicators (KPIs) provide a measurement of this SMF effectiveness.

Category	Key Performance Indicators (KPI)
Call Statistics	▪ Abandonment Rate ▪ Average Time to Answer ▪ Distribution of Incoming Calls ▪ On hold time ▪ Total call volume
Ticket Statistics	▪ Open Ticket Count within Time Frame ▪ Closed Ticket Count within Time Frame ▪ Overall outstanding open tickets ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Ticket Activity by Department ▪ Ticket by Priority ▪ First Level Resolution ▪ Number of open tickets by support groups ▪ Number of tickets transiting through tier 2 and tier 3 ▪ Average ticket duration by support group. ▪ Service Matrix – incidents type by support group ▪ Ticket time at tier 1 to resolution. ▪ Time to escalate and resolve at tier 2 and 3.
Service Level Agreement Compliance	▪ Network Availability ▪ Average Time Spent on Ticket by Status, Activity, Analyst, Priority and Department ▪ Customer Satisfaction Rating ▪ Percent of SLA Commitments that are met ▪ Spam Statistics

Summary of Roles and Responsibilities

Incident Management Roles		
Role	**Position**	**Responsibilities**
Role 1	Incident Manager	Responsible for the Incident Management Process and reporting. Manages the work of support staff within the Incident Management Process. Makes recommendations for process improvement. Develops and maintains the systems involved in supporting the Incident Management process (e.g. Altiris, Active Metrics, etc.).
Role 2	SDA – Service Desk Analyst (Tier 1 Support)	The SDA is responsible for supporting the Company customer base in all areas of technology. The SDA acts as the point of contact between the customer and the discipline working the issue and represent the Service Desk to deliver effective and efficient communications by phone or via email and includes updates and information in Altiris.
Role 3	PSTA – Premier Senior Technical Analyst	The prime responsibility of the PSTAs is to support the 5% exception of executives / predetermined premier users. PSTAs are experienced analysts with advanced technical knowledge and customer service skills to provide proper coaching and mentoring to Service Desk Analysts (SDA). The PTSA also supports Tier 1 Service Desk analysts when not supporting Premier calls.
Role 4	Audio / Visual Specialist	The Audio / Visual Specialist maintains & manages Company Audio and Visual equipment and provides support and assistance such as, training, documentation and configuration, to Company customers for meetings and events.
Role 5	SDS – Service Desk Supervisor	The SDS will work with GSDM (See Role 5) to manage regional Service Desk analysts.

Role 6	GSDM – Global Service Delivery Manager	GSDM is responsible for overview of all North American Service Desk analysts. Responsibilities of a GSDM include, but are not limited to, customer satisfaction survey review and rapid response, quarterly meetings with executive assistants of the Premier group, monthly / quarterly status reporting to the OMR operation lead, and Global Service Desk and IT Governance management.
Tier 2	Tier 2 Support	Tier 2 support is responsible for investigation, resolution and documentation of incidents (within Altiris and related documentation) escalated by the Service Desk. Issues may relate to operating system, servers, networks, enterprise applications and technologies from multiple locations. Responsibility also includes the identification of problems or trends, the design of work-arounds, initiation of "Requests For Change" or escalation to Tier 3.
Tier 3	Tier 3 - Support	Tier 3 support is responsible for investigation, resolution and documentation of incidents or problems (within Altiris and related documentation) escalated by the Tier 2 groups. Issues will involve complex infrastructure, systems, applications or network issues. Their work often leads to "Requests For Change" which they may be responsible to design, test and implement in production.

Appendix B: Key Words Definition

Term	Definition
Altiris	Altiris is the Service Desk solution software and a tool to help ensure IT infrastructure availability and raise service levels while reducing costs.
CI (Configuration Items)	Key IT components or assets. The information captured and tracked will depend upon the specific CI, but will often include a description of the CI, the version, constituent components, relationships to other CIs, location/assignment, and current status. The items that should be included as CIs include hardware, system software, application software, documentation, people, and so forth.
CMDB (Configuration Management Database)	Configuration Management Database. The single logical data repository for CI information. Whenever possible this database should be self-maintaining, with automated updates to CIs.
GSDM	Global Service Delivery Manager. See SMF Roles and Responsibilities
Incident Classification	Recording the incident and accurately allocating the correct degree of resources required for resolution.
Incident Investigation	Researching to determine if the incident is unique or has been experienced before.
Incident Support	Providing support throughout the entire life cycle of the incident in order to resolve the incident as quickly as possible and with the least impact to business processes. During initial support the incident is matched against existing incidents and known errors.
Incident Resolution	Resolving the incident as quickly as possible through the effective use of all appropriate tools, processes, and resources available including appropriate updates in Altiris.
Incident Recovery	Returning the effected environment to stability once the incident has been resolved.
Incident Closure	Effecting proper closure of the incident, ensuring that all pertinent data surrounding the life cycle of the incident is properly discovered and recorded.
Incident Information Management	Properly recording and categorizing incident-related information for future use by all levels and organizations within the enterprise.
KPI	Key Performance Indicator
Known Error	An incident or problem for which the root cause is known and a temporary workaround or a permanent alternative has been identified. If a business case exists, an RFC will be raised, but—in any event—it remains a known error unless it is permanently fixed by a change.

Urgent Incident	An incident with a high impact, or potentially high impact, which requires a response that is above and beyond that given to normal incidents. Typically, these incidents require cross-company coordination, management escalation, the mobilization of additional resources, and increased communications.
Normal Service Operation	Normal service operation is defined as a service operation within service level agreement (SLA) limits.
PTSA	Premier Senior Technical Analyst. See SMF Roles and Responsibilities.
RFC (Request for Change)	This is the formal change request including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.
SDA	Service Desk Analysts. See SMF Roles and Responsibilities.
SDS	Service Desk Supervisor. See SMF Roles and Responsibilities.
Service Desk	A function that provides the vital day-to-day contact point between customers, users, IT services, and third-party organizations. The Service Desk not only coordinates the incident management process, but also provides an interface into many other IT processes.
SLA	Service Level Agreement
SME	Subject Matter Expert
SMF	Service Management Function
VOIP	Voice Over Internet Protocol. Individuals inside and outside organizations can contact each other using VOIP.
VPN	Virtual Private Network. VPN is a form of communication over networks that are public in ownership, but emulate a private network in terms of security.
Yardi	Asset and property management software

Appendix F: Service Monitoring and Control for Email Process Narrative

E-Mail Monitoring and Control SMF
SMF Process Narrative
SMF Implementation Date 2/1/08

Revision History:

Version No.	Revision Date	Performed By	Revision Description
1.0	2/1/2008	Wade Lowder	Initial SMF Roll-Out Documentation
1.1	12/18/08	Wade Lowder	Minor formatting updates

Process Owner:
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

Control Process Owners and Other Contacts:
Luis Jurado, System Engineer
Don Dawson, Sr Systems Engineer
Niels Kinderdijk, Sr Infrastructure Analyst

Documentation Authors and SMEs:
Wade Lowder, Senior Manager, North American Operations

SMF Process Overview:

The E-mail Monitoring and Control (SMC) SMF enables the company IT Infrastructure staff with the ability to perform real-time observation, generate alerts of health conditions in an IT computing environment, identify root causes, correct any service exceptions with automated tools wherever appropriate, and initiate remedial actions to be proactive in dealing with system events and effective resolving service incidents in a timely manner to minimize possible adverse impacts. In addition, the E-mail Monitoring and Control SMF also gathers data that can be used by other SMF's to improve IT service delivery.

The E-mail Monitoring and Control SMF are typically responsible for e-mail monitoring process heartbeat, job status, queue status, server resource loads, response times, and transaction status and availability. The E-mail Monitoring and Control function has both reactive and proactive aspects. The reactive aspects deal with incidents as and when they occur. The proactive aspects deal with potential service outages before they arise. Same or similar incidents that occur frequently and are not detected by existing monitoring tools might indicate a need of system health check to determine if the current monitoring method is effective and if company needs to acquire new monitoring tools or improve existing monitoring tools. As a result of a successful implementation of the E-mail Monitoring and Control SMF, company IT Operations can expect to reduce or prevent some service incidents from happening, minimize response time for service incidents, and improve overall availability of services and user satisfaction.

IT Systems:

System/Application	Process Supported
Microsoft Exchange Server	Email uptime, inbound and outbound queue, Exchange services
Nagios	Service, OWA connection, and SAN Disk availability
SpotLight on Exchange	Uptime and Processes Monitoring
MessageStats from Quest	Reporting on Mailbox activities

Key Spreadsheets or other End-User Tools:

Type	Name	Filename and Location	Purpose
None			

Supplemental Documentation, Reference Material and Reports:

Name	Filename and Location
Exchange Environment Architecture Diagram	Company Exchange 2003 Design- http://na-portal/sites/IT/infrastructure/Shared%20Documents/Architecture/Company%20Exchange%202003%20Design.vsd
Exchange Dependencies List	Exchange Dependencies- http://na-portal/sites/IT/infrastructure/Shared%20Documents/Architecture/Exchange%20Dependencies.xls

Optional, if applicable to the process
Third-Party Interfaces:

Interface Name & Purpose	Vendor Name
None	

Process Narrative:

The Service Monitoring Control SMF follows the general steps below. Please see the process flow chart for graphical representation located here.

Identification of Monitoring Requirements
The Company IT Operations and Infrastructure teams are responsible for identifying the most efficient and cost-effective method to monitor the mission-critical email communication services and the associated IT infrastructure by first determining if there is an existing monitoring tool(s) available.
Nagios and Spotlight on Exchange are automated service monitoring tools that are currently in place and configured to continuously monitor the email services and associated IT infrastructure in the company IT environment. Automated monitoring functions of Nagios and Spotlight on Exchange help reduce human errors, increase responsiveness, and allow resources to be assigned to other duties.

Monitoring and Alerting
Nagios and Spotlight on Exchange generate alert notifications to the company IT Operations and Infrastructure teams in case of actual or potential service outage / interruption, dismount, memory shortage, queue issues and etc. (Reference Appendix B)
The company Operations and Infrastructure teams can access and pull details on alert notifications, historical logs, performance and status reports when necessary.

Alert Response and Health Checks
The company IT Operations and Infrastructure teams observe and research system health conditions when they occur.
System Engineers perform a system health check and determine if alert notifications are "false alarms" based on collected data and information provided by Nagios and Spotlight on Exchange. The health check is an assessment that defines the tolerances and service levels for normal operations. The health check also specifies what conditions require additional monitoring attention and provides guidance on how the system engineer or administrator should respond to out-of-tolerance conditions.
If the system does not pass the health check, the System Engineer opens an Altiris ticket and contacts the Service Desk to provide instructions for responding to end user calls that may be related to the service disruption. The Altiris ticket will trigger any necessary Incident Management analysis and begin the Incident Management process.
In addition to working diligently to restore email services, System Engineers must determine when to send service disruption notifications and who should receive notifications from the Email Monitoring Matrix (Appendix B). Systems Engineers and Infrastructure Management will create notifications when required and make sure the notification are distributed by the Service Desk. All actions taken during this process is documented in the associated Altiris ticket.
The Systems Engineer will troubleshoot and attempt to restore email services. If service cannot be restored, Microsoft Support will be contact and the appropriate Incident Management escalation process will be followed until service has been restored.

Once service has been restored the Systems Engineer will contact the Service Desk to close the Altiris ticket and send any required follow-up notifications. Additionally, the Service Desk will update the Incident description and resolution in the Knowledge Base. Nagios and Spotlight on Exchange continue to perform automated monitoring of the e-mail services and associated IT infrastructure to ensure optimal performance.

Key Performance Indicators:

Key Performance Indicator (KPI)	Description
Exchange Uptime Percentage	The uptime of Microsoft Exchange, and this number should be kept as close to 100% as possible most of the time. If the goal is 99% availability per month, it translates to around 7 hours of actual loss of email service per month based on a 24/7 M-S SLA. **Measurement and Reporting of this KPI:**
Mean Time to Repair	This statistic is typically used in capacity and availability management; however, SMC should analyze problems that were corrected using SMC's Control. This metric measures the effectiveness of the automated response from this process. This value should decrease as more situations are handled by SMC automation. **Measurement and Reporting of this KPI:**
Alert to Ticket Ratio	This is a key statistic that indicates the quality of SMC alerts. The goal is to achieve a 1:1 ratio between alerts and tickets. This indicates that each alert is valid and has a well-defined and well-documented problem set associated with it. **Measurement and Reporting of this KPI:**
Mean Time to Detection	This statistic should dramatically improve with the implementation of effective SMC tools. Alert latency is the measurement of the delay from when a condition occurs to when an alert is raised. Ideally, this value is as low as possible. **Measurement and Reporting of this KPI:**
Number of Tickets with No Alerts	A high count of tickets with no alerts is an indication that monitoring missed critical events. This statistic can be used as a starting point for improving instrumentation and rules. **Measurement and Reporting of this KPI:**
Number of Events per Alert	As rules and correlation improve, this count should increase. Often, multiple events are triggered; however, there is typically only one true source of issue. A High Events per Alert count may also indicate opportunities for reducing the number of exposed events. **Measurement and Reporting of this KPI:**
Number of Invalid Alerts	Alerts that are generated with incorrect fault determination should be carefully reviewed and corrected. The number of invalid alerts may increase during the initial deployment of new infrastructure components and services; however, it should drastically decrease with better rules and event filtering. **Measurement and Reporting of this KPI:**

Appendix A SMF Roles and Responsibilities:

Service Monitoring and Control SMF		
	Position	**Responsibility**
Role 1	SMC Requirements Initiator	The SMC Requirements Initiator role can be carried out by anyone within the organization who needs to use the service monitoring and control SMF (i.e. other SMF owners, business, customer, or third parties). The SMC Requirements Initiator follows the documented process for submitting requirements, reviews and agrees on service monitoring and control requirements with the monitoring manager, and revises and resubmits rejected service monitoring and control requirements.
Role 2	Global Service Delivery Manager (GSDM)	GSDM is the process owner with end-to-end responsibility for the service monitoring and control process. GSDM identifies, collects, and manages requirements from SMC and other SMC requirements initiators. GSDM also works with Release Management to deploy the SMC technical solution, reviews the SMC process, reports on and maintains the SMC process, provides regular feedback on operational performance, both in general and against specific service levels, and manages monitoring operators.
Role 3	SMC Monitoring Operator	The Monitoring Operator is responsible for the day-to-day execution of the service monitoring and control process and applies automated incident-detection tools wherever possible.
Role 4	SMC Engineer / Architect	The Engineer / Architect role is responsible for providing higher-level support for the relevant daily execution of the SMC process and applies automation and tools wherever possible. The Engineer / Architect designs the service monitoring and control technical solution, develops the SMC technical solution, configures automated monitoring of system components, ensures that detection of alerts from all infrastructure components within the area of responsibility and system resources are in good working order, configures the SMC tools according to SLR and system-specific events to be monitored, and monitor backup, restore, and verification procedures.

Role 5	SMC Developer and Tester	These roles are responsible for extending and integrating components of SMC tools and technologies. The SMC developer develops integration and extends the SMC tool, extends tool capabilities using API and frameworks, creates scripts and status probes used in the SMC process flow activities, and participates in discussions with application and software development teams. While the SMC tester tests the internally developed capabilities and extensions.
Role 6	SMC Steering Committee	The SMC Steering Committee is responsible for creating, establishing and approving high-level general process guideline, policies and procedures.

Appendix B Email Monitoring Matrix:

				Key Stakeholders							
System Level	Function	Tool Used	Infrastructure	Operations	Networking	Service Desk	IT Management	Cross Function Teams	Executive Team	End Users
Exchange Application	Email Uptime	Nagios (ping check)	Alert	Alert			Notify	Notify	Notify	Notify
	Inbound Queue	Spot Light on Exchange	Alert	Alert			Notify	Notify		
	Outbound Queue	Spot Light on Exchange	Alert	Alert			Notify	Notify		
	Information Store Available	Spot Light on Exchange	Alert	Alert						
	Services Availability	Nagios	Alert	Alert						
	OWA Connection Availability	Nagios	Alert	Alert						
	MAPI Connection Availability	NOT NEEDED	Alert	Alert						
	SAN Disk Availability	Nagios	Alert	Alert						
Infrastructure layer	Local Disk Usage (RAID Health)		Alert	Alert						
	SAN Disk Usage	Nagios	Alert	Alert						
	Memory	Nagios	Alert	Alert						
	Processor	Nagios	Alert	Alert						
	Network (Shared Resources)	Nagios	Alert	Alert	Alert	Alert				
	Outage Event		Alert	Alert	Alert	Alert	Notify	Notify	Notify	Notify
Events	Degraded Services		Alert	Alert	Alert	Alert	Notify	Notify	Notify	Notify

Outage Event: Any event that causes inbound or outbound email services to stop

Degraded Services: Any event that causes a delay in inbound or outbound email processing.

Alert action: A system generated alert via email, SMS, etc.

Notify action: A manual notification via email, SMS, etc.

Notifications should be sent if there is an issue with sending/receiving or Email, in the user's perspective, is either not available or experiencing performance issues. The details or components of the failure (matrix items above) are not important but rather the system availability as a whole when working with anyone outside of IT.

Appendix C Glossary:

Term	Definition
Altiris	Altiris is helpdesk solution software and a tool to help ensure IT infrastructure availability and raise service levels while reducing costs.
GSDM	Global Service Delivery Manager
KPI	Key Performance Indicator
Messaging Application Programming Interface (MAPI)	Messaging Application Programming Interface is a messaging architecture and Component Object Model based API for Microsoft Windows. MAPI allows client programs to become (e-mail) messaging-servers. MAPI is closely related to MAPI/RPC, the proprietary protocol that Microsoft Outlook uses to communicate with Microsoft Exchange.
Microsoft Exchange Server	Microsoft Exchange Server is a messaging and collaborative software product developed by Microsoft. It is part of the Microsoft Servers line of server products and is widely used by enterprises using Microsoft infrastructure solutions. Exchange's major features consist of electronic mail, calendaring, contacts and tasks, and support for the mobile and web-based access to information, as well as supporting data storage.
Nagios	Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do. It has been designed to run under the Linux operating system, but works fine under most *NIX variants as well. The monitoring daemon runs intermittent checks on hosts and services you specify using external "plugins" which return status information to Nagios. When problems are encountered, the daemon can send notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.). Current status information, historical logs, and reports can all be accessed via a web browser.
Outlook Web Access (OWA)	Outlook Web Access is a webmail service of Microsoft Exchange Server 5.0 and later, originally called Exchange Web Connect (EWC). The web interface of Outlook Web Access resembles the interface in Microsoft Outlook. Outlook Web Access comes as a part of Microsoft Exchange Server 2007 and previous versions of Exchange. This feature is currently available via the following links; • https://webmail.company.com/exchange (North

	American users) • https://webmail.company.com.cn/exchange (China users) • https://webmail.company.nl/exchange (European users) • https://webmail.company.co.jp/exchange (Japan and Korean users)
Redundant Array of Inexpensive Disks (RAID)	Also known as Redundant Array of Inexpensive Drives. RAID is an umbrella term for computer data storage schemes that divide and/or replicate data among multiple hard drives. RAID can be designed to provide increased data reliability and/or increased I/O (Input/Output) performance.
Short Message Service (SMS)	The Short Message Service (SMS), often called text messaging, is a means of sending short messages to and from mobile phones. Messages must be no longer than 160 alpha-numeric characters and contain no images or graphics.
Storage Area Network (SAN)	A Storage Area Network is architecture to attach remote computer storage devices such as disk arrays, tape libraries and optical jukeboxes, to servers in such a way that, to the operating system, the device appear as locally attached. Although cost and complexity is dropping, as of 2007, SANs are still uncommon outside larger enterprises.

Appendix G: Change Advisory Board Meeting Agenda Template

Change Advisory Board Meeting Agenda

Date/Time/Location

Date:
Time:
Location:

Participants

List participants here

Objective

Specific Item(s)

-

Weekly review of IT Changes

- CIR (Change Information Review)
- RRR (Release Readiness Review)
- PIR (Post Implementation Review)
- Process Improvement.

Agenda

[Please provide an estimated duration for each agenda item]

Specific Agenda Item(s)

-

Standard Agenda Items

- CIR (Change Initiation Review)

Enter here any specific information about the change that is not already documented in the RFC itself, or to call attention to specific issues, such as urgency, impact, technical

- RRR (Release Readiness Review)

Enter here any specific information about the change that is not already documented in the RRR itself, or to call attention to specific issues, such as urgency, impact, technical difficulty…..

- PIR (Post Implementation Review)

Enter here any specific information about the change implementation that is not already documented in the PIR itself. Provide an outline of lesson learned and suggested action or process change to be discussed

- Known Changes Types List Review

Enter here any suggestion to the update the “Know Changes Type List”

- Process Performance Metrics

Review the following KPI graphs:

- Process Performance Metrics

Review the following KPI graphs:

  - # of RFCs submitted (weekly trend)
  - # of RFCs by Category/Model (weekly trend)

- # of RFCs by Service (weekly trend)
- # of RFCs by CI (weekly trend)
- # of RFCs completed successfully (weekly trend)
- # of RFCs unsuccessful (weekly trend)
- # of Incidents traced to Changes (weekly trend, detailed list)
- # of FSC references (weekly trend)

- Process Improvement Opportunity

Enter here any process Improvement suggestion

Meeting Notes

Appendix H: Change Management Process Narrative

Change Management SMF
SMF Process Narrative
SMF Implementation Date 02/01/09

Revision History

Date	Version	Description	Author
2/1/2009	1.0	Initial Draft	Wade Lowder

Process Owner:
Carie Zoellner, Vice President, Global IT Infrastructure and Operations

Control Process Owners and Other Contacts:
Wade Lowder, Senior Manager, Operations and Security

Documentation Authors and SMEs:
Wade Lowder, Senior Manager, Operations and Security
Josh Gilmore, Senior Manager, Global IT Service Delivery

SMF Process Overview:

The change management process will be followed for every change made within the IT organization. The main goal is to provide a disciplined process for introducing required changes into the IT environment with minimal disruption to operations. As soon as a request for change (RFC) has been entered in Altiris, an evaluation of the risk is performed. According to the level of risk identified: low, medium, high or urgent the change will follow different development and implementation paths and go through increasing levels of scrutiny and approval. The change may be pre-approved for immediate implementation, or require approval from the service manager, or require additional approval from the Change Advisory Board (CAB). After the change has been implemented in production, a post implementation review may be performed by the service manager or the CAB. All steps are controlled through a workflow in Altiris.

IT Systems:

System/Application	Process Supported
Altiris Workflow	RFC Entry, approval and tracking
Request For Change (RFC)	Altiris form for submitting a change request

Key Spreadsheets or other End-User Tools:

Type	Name	Filename and Location	Purpose
None			

Supplemental Documentation, Reference Material and Reports:

Name	Filename and Location
Change Management Process Flow	Change Management-Process Flow.doc - SharePoint/Change Management/Working docs
Change Management – CAB FAQs	Change Management-CAB FAQ.doc - SharePoint/Change Management/Working docs

Optional, if applicable to the process
Third-Party Interfaces:

Interface Name & Purpose	Vendor Name
None	

Process Narrative:
Change Management

Goal & Objective
The purpose of this document is to define the procedure to be followed for all Requests For Change (RFC) to IT components. The goal of the change management process is to ensure standardized methods and procedures are used for efficient and prompt handling of all changes and minimize the impact of change related incidents on service quality. This process exists to improve operational stability and therefore it applies to all Company locations and environments.

The Change Management Process covers new hardware and software installation, configurations, upgrades and patches to communications devices, operating systems, applications, reports, databases and SAN storage devices.

The process and activities for change management are intended to:
Ensure
- Alignment with IT Management expectations.
- Minimize disruption to operations and business-critical services.
- Segregation of and coordination of duties while planning and implementing change.
- Adherence to departmental process, procedures, policies and standards.
- Adequate communication and coordination within IT and with the business before, during and after changes are implemented.

Document the analysis of critical aspects of the change including
- Business or technical purpose
- Impact on systems and processes
- Urgency
- Conflicts and/or configurations issues
- Back-out procedures
- Security
- SOX and Regulatory compliance
- Post implementation effectiveness review
- Cost and benefit of the change
- Alternatives to the change and/or define risk of not performing the change

Manage other change considerations including
- Budget
- Timeline
- Quality
- Training
- Roll-out plan
- Disaster recovery impact
- Identify and involve all resources (systems or people) affected by the change.
- Formalize and capture documentation.
- Record and track approval(s) of the change.
- Gather reports & analyze key metrics as part of continuous service improvement.
- Scope

The change management process shall be followed for each change made to the production IT environment with an identified direct or indirect impact on any technical, business operations or regulatory IT environment.

Change Management Process Owner
The VP of Infrastructure and Operations is the owner of the change management process. All requests to modify this process must be submitted to the VP of Infrastructure and Operations. All requested modifications to this process shall be reviewed by the Change Advisory Board and if approved will result in a new version of this document. History of process updates and process deviations approvals shall be kept on file by the IT department.

Segregation of Duties
The review and approval of changes by consensus of the CAB, composed of individuals from multiple functional teams creates the appropriate management oversight to enforce appropriate segregation of duties in all changes.
Change Management Tracking System
The Company Altiris System will be used to track and support the change management process. Altiris provides information and documentation capture and retention along with workflow capabilities.

Roles and Responsibilities
Specific roles have been defined within the Change Management process. These roles align with the Company Operations Model and represent at a high level the functions that must be performed in the Company IT environment for successful Change Management. The three significant roles defined for the change management process are:

1. Change initiator- IT staff submitting the RFC
2. Change manager- IT Owner of the Change Management Process
3. Change builder- IT staff implementing the actual change

Two committees have management responsibilities for the change management process. These two committees are;
Change Advisory Board (CAB) is responsible for the following;

- Assesses and approves changes to the production environment.
- Reviews the status of a change throughout the change process.
- Assesses progress with respect to the approved schedule.
- Determines how to correct any identified problems.
- Communicate findings to appropriate managers and stakeholders, including business stakeholders and the IT executive committee that they represent.

CAB Urgent Committee (CAB/UC) is responsible for the following;

- Assesses and approves urgent changes to the production environment.
- Reviews the status of an urgent change throughout the change process.
- Updates the CAB on urgent change status.

Request For Change (RFC) Process Flow Summary

Each approved Request For Change (RFC) shall be assigned a point person (service manager) responsible for the change implementation and control.

The Change Management process is organized into six steps;

1. Request For Change (RFC)
2. Assessment/Classification
3. Change Initiation Review (CIR) and approval
4. Design, Development and Testing
5. Release readiness review (RRR) and approval
6. Change Implementation
7. Post Implementation Review (PIR)

Request for Change (RFC) Initiation
A Request For Change (RFC) can be initiated by anyone in IT using the IT Request For Change Form available via Altiris. A Change Control Number is automatically created and assigned as the Ticket number. The RFC becomes the point of reference for all activities associated with the change.

The RFC must answer the who, what, when, where, why and how questions of the proposed change. It must describe the change, the effort it will take to implement the change and by whom, the method of implementation, and the configuration items involved. It also includes supporting information about the purpose of the change, its impact on the organization, the back out plan in case of failure, the cost of the change, the budget approval sign-off if necessary, and the urgency of the proposed change. It should contain sufficient information to allow the service manager to quickly and accurately assess the change at the initial screening stage and again at its official review stages for approval or rejection.

The change initiator also needs to provide supporting documentation, such as the business case, cost-benefit analysis, proposed implementation plan to the service manager and others involved in the change approval process (including business users) for those changes requiring a PSF.

RFC Classification
RFC Urgency
The service manager shall analyze all aspects of the request in detail to prepare for a successful change. This analysis will result in a classification which will allow the request to take the appropriate path and require the appropriate levels of approval.

Urgent: Change that is required to correct a loss of or severe degradation of service or to prevent the loss of service or degredation. Meetings of the CAB/UC may need to be convened with little advance notice. Resources may need to be immediately allocated to deploy such authorized changes.
NOTE: An urgent change will immediately follow the urgent change path for authorization by the CAB/UC as described later in this procedure.

High: A High risk change is defined as a change requiring more than 40 hours of work, affecting more than 25% of an application or users and may involve multiple teams, applications or systems to implement and may impact financial reporting capabilities or data.

Medium: A Medium risk change is defined as a change that has a lower chance of affection any user or application and has a low potential to impact financial reporting capabilities or data.

Low: A Low risk change has almost no chance of affecting clients, customers applications or financial reporting capabilities or data. Low risk changes can be done

during the normal course of business. This includes moves, adds and changes, printer configuration, changing end user systems with the user or user data restores.

RFC Risk Assessment
A risk analysis of the change shall be performed considering the impact and likelihood of service interruption due to the change by reviewing the following criteria:

IMPACT
- Scope
- Number of regions, locations, processes, functional areas, users
- Regulatory or legal impact
- Complexity
- Systems and technologies involved
- Difficulty of implementation
- Number of machines, time, technicians involved
- Strength of roll back options
- Down time generated
- User training and support required
- Business consequences if implementation fails

LIKELIHOOD
Likelihood of occurring

The result is a risk assessment level, high, medium, Low on users, the business, or the IT infrastructure.

RFC Change Category: Standard, Minor, Significant, Major
Based on the risk assessment performed, each change will be assigned a change category. This category will drive the type and level of approval required.

Standard change: A change rated at low risk level. This type of change is very well known, simple and repetitive and affect the smallest percentage of users. IMPORTANT: Standard changes do not require any approval.
Example: profile update, password reset

Minor Change: A change rated at medium risk level. This type of change is well known, controlled, affect a limited number of user but may create issues if not properly scheduled, communicated or executed.
Examples: standard hardware, software, or database maintenance and other “nice to have” changes.

Significant change: A change rated at high risk level: This type of change affects a high percentage of users and the impact of a failure would deteriorate the service level. These changes are typically nonstandard, technically complex and may involve downtime of the network or a service.

Examples: configuration changes; hardware or network changes; restores; or any change that requires extra analysis and control.
Major Change: A change rated at high risk level requiring a significant amount of work and the use of the PSF process. This type of change is business-critical system, large in scope and/or impact the highest number of users or regions.
Example: changes to an operating system or major subsystem, application upgrades, implementation of a new application or technology
Other items to review during risk assessment and/or development

Scope: systems and processes involved
Used to determine the scope and feasibility of the Request For Change (RFC).
Asset Name or Description – The unique name of the IT asset, database, server, etc. or a complete description of the IT resource that will be affected by the proposed changed.
Objects Affected – The objects (SQR, Shell Script, Panel, etc.) affected by the proposed change.

Dependencies & Prerequisites – IT resources and/or processes dependent on the devices and/or objects that will be affected by the proposed change. IT resources and/or processes changed prior to implementation of proposed change.

- Install Requirements – Considers the overall amount of time it takes to prepare the change, implement the change, and recover from a failed change.
- Detailed Instructions / Steps Required – Applies to both development and implementation of the proposed change.
- Security issue(s)
- Analyze the impact of the change on the security of the production environment
- SOX and regulatory Compliance Issue(s)
- Analyze the impact of the change on SOX compliance related controls
- Communication & Training Needs
- Determines which users and IT staff need to be notified and trained and support
- Rollback Procedures
- Procedures that return the IT resources and/or procedures to the same state prior to the change. Determines if the proposed change could significantly impact system availability
- Scheduled Job add/change/delete
- Determine if change will create, delete or modify an IT scheduled job.
- Documentation Requirements
- Assesses the degree to which procedures must be amended to adequately describe what has changed.
- System Boot Required – Yes or No
- Timeline Estimate
- IT provides a Completion Date Estimate.
- Known Change Type List
- For efficiency and automation purpose, a list of possible changes by service type is maintained and referred to as the Known Change Type List (KCTL).
- KCTL Content
- This list contains the following information

- Service name and service components
- Individual changes names
- Risk assessment by change
- Service Owner Name
- Change Builder Name
- KCTL Approval Process
- The KCTL is owned and maintained by the change manager.
- Each change shall be approved by the CAB before it is included in the KCTL.
- RFC Approval Summary
- Based on the risk identified, a change category is assigned (Standard, Minor, Significant, Major or Urgent). Each change category follows a specific process and requires certain approval(s).
- Standard Change: Pre-approved

Minor Change: One approval by the Change Manager
This single approval authorizes both development and deployment in production
Significant Change: Approvals by Change Manager & CAB
The approval comprises of 2 approvals: a first approval by the service manager to authorize development, and a second approval by the CAB to authorize deployment in production (Release Readiness Review)

Major Change: Approval by Change Manager, CAB and other PSF Steps
The approval comprises of 3 approvals: a first approval by the service manager to authorizes development, and a second approval by the CAB to authorize deployment in production (Release Readiness Review) and a third approval of the Post Implementation Review (PIR) In addition, this change follows the PSF methodology and other built-in approval steps

These approvals are summarized in the table below

Approval Required by Change Category						
	KCTL Pre-Approved	Service Manager	Portfolio Management	CAB RRR	CAB PIR	CAB/EC
Standard	X					
Minor		X				
Significant		X		X	Optional	
Major		X	X	X	X	
Urgent					X	X

RFC Development Approval

Each and every change shall be approved prior to development, either by default through the pre-approved KCTL or through a formal approval by a service manager or.

For the RFC routed to the service manager, upon submission of the RFC in Altiris, it is routed automatically by a workflow to the appropriate Service Manager:
If the information is insufficient, additional information is requested
If the change if not technically feasible or not in line with technology or management expectations, the requestor is informed of request rejection
If the change is feasible, a due date for providing a complete assessment is entered in Altiris and communicated to the requestor and IT management for resource planning.

The type of approval required is determined by the change category associated with the change in the KCTL. Standard and urgent changes shall be documented and receive the same level of approval, but urgent changes are typically reviewed and approved after the change has actually been completed by the CAB/EC. The documentation may not be completed until after the change.

Standard Change: Pre-approved by the CAB
These well-defined changes with low risk have been presented to the CAB, approved and documented as "standard" in the KCTL (Known Change Type List). They are pre-approved and can be deployed immediately. They are not reviewed by the service owner nor the CAB

Minor, Significant and Major Changes: Initial approval by Service Manager
Any minor change (assessed as medium risk) shall be initially approved by the Service Manager, who has the option to present the RFC to the CAB as necessary.
High & Medium Impact: Approval by CAB (Change Advisory Board)
Any change assessed with either a high risk or a high impact shall be approved by the CAB. The CAB has a broad membership that possesses enough cumulative knowledge to fully understand the implications of the change. Additionally, the CAB may invite SME's to further discuss and understand the proposed change
RFC Deployment Approval
Certain RFCs require approval prior to deployment

Standard and Minor Changes Deployment: No approval necessary
Deployment has already been approved. The change builder identified in the RFC is responsible for successful implementation in production.
Major & Significant Change Deployment: Approval by the CAB (RRR)
Any change assessed with either a high risk or a high impact shall be approved by the CAB through a Release readiness Review. The CAB has a broad membership that possesses enough cumulative knowledge to fully understand the implications of the change. Additionally, the CAB may invite SME's to further discuss and understand the proposed change

RFC Post Implementation Approval

Certain RFCs require a post implementation approval by the CAB. Follow up actions may be assigned and tracked by the CAB
Standard & Minor Change: No review required
Significant Change: Review by the CAB is optional, if requested in the RFC.
Review by the Service manager is required
Major Change: Review by the CAB is required
Urgent Change: Review by the CAB/Urgent is required
See Urgent Changes Implementation Approval section below.
Implementation Failure or problem: Review by the CAB is required
If Company is not satisfied with the change or unexpected problems are encountered during implementation, IT may decide to rollback the change to conduct further development and testing. A post implementation review is required to minimize similar problems in the future.

Design, Development and Testing Guidelines:
Level of effort and control.
Based on the final impact assessment of the RFC (Standard, Minor, Significant, and Major), the level of analysis, documentation and management shall be increased appropriately.
Standard change: Changes are well known, a pre-defined process exist, analysis and documentation shall be thorough, to the point and be captured in the RFC

Minor Change: The RFC document may be sufficient to capture most or all the information necessary to execute the change. Analysis and testing shall be focused on the "efficient delivery" of the Request. Critical information and approvals and testing results shall be captured
Significant Change: The RFC will capture the request, assessment, guideline for level of documentation expected and approvals. The following documentation may be created as deemed beneficial to the process: user requirement document, system requirement document, test plan, implementation plan, communication plan, training plan & back out plan.

Major Change: Analysis and documentation shall be extended to discover, investigate and resolve issues and will typically follow the PSF process. Standard user requirement document, system requirement document, test plan and implementation plan documents should be used to help with methodology, guidance on activities. Certain sections may be deliberately omitted for efficiency – In such case, the section shall not be deleted but marked N/A. A user acceptance test shall preferably be performed to conclude the test phase

Development Version Control
Development should capture version, preferably using versioning control software such as SourceSafe when appropriate

Testing Environment

Testing should preferably be performed in a test environment. Where such environment does not exist, a specific testing procedure shall be developed with appropriate standards. Such tests shall preferably be done during off-hours or during system scheduled downtime, then backed out.

Testing Responsibility
Standard and Minor changes may be tested by the developer or the change owner. Medium risk or Impact changes shall be tested by other individuals than the developer or the service manager

High risk and/or high impact changes shall be ultimately tested by users
IT Tests: Unit, Integration, Validation and System
As appropriate, the assigned developers may create detailed Unit, Integration, Validation and System Test Plans to document testing. A summary of the test shall be documented and approved

The assigned IT developers may use all or part of the Company IT Developer Testing Document to document the test type, procedures applied, test data, expected results, and results of testing. Test execution and responsibility shall be assigned by the project manager taking into consideration operational, resources and segregation of duties issues. Deviations during testing shall be documented, corrected and retested or satisfactorily explained by the developers. A summary and conclusion of the test shall be documented In the Company IT Developer Testing Document. The document shall be reviewed and signed as delineated in the RFC, and preferably include Service Manager where the change is implemented.

User Acceptance Test
As appropriate, a User Acceptance Test Plan may be created, and documented.
The users performing the test may use part or all of the Company IT User Acceptance Testing Document to document the test procedures, test data, expected results, and results of testing. Test execution and responsibility shall be assigned by the business unit manager. Deviations during testing shall be documented, corrected and retested or satisfactorily explained by the developer(s). A summary and conclusion of the User Acceptance test shall be captured in the Company IT User Acceptance Testing Document. The document shall be reviewed and signed as delineated in the ITCRF, and preferably include the Business Manager where the change is implemented.

Back Out Test Plan
As appropriate, a back out test plan may be created and documented. The test execution and responsibility shall be assigned by the service manager. The individuals performing the test shall document the test procedures and test results. Deviations during testing shall be documented, corrected and retested. Release Readiness Review (RRR) Approval:

Urgent Change

The urgent change process enables Company to continue normal operations or restore them as quickly as possible, in an accelerated process that follows the normal change process to the extent that time constraints permit a quick implementation.
Typically, urgent changes only allow for a limited testing and often require that normal processes and controls be bypassed.

CAB/UC Mission
Urgent changes cannot be authorized by a single individual and must be approved through a change advisory board urgent committee (CAB/UC).
The CAB/UC has the same purpose and performs the same functions as the regular CAB. The differences are that the CAB/UC membership is smaller than the regular CAB, and the CAB/UC is able to meet and make decisions at short notice. The CAB/UC must be empowered to make quick decisions without having to refer to the CAB and must have the full authority to approve or deny urgent changes.

CAB/EC Membership
The Change Management Owner, (VP of Global Infrastructure and Operations), is the permanent chairman of the CAB/EC.
The Chairman of the CAB/EC will be contacted every time an urgent change is requested and will create the CAB/EC team based on the specific requirements of the change. This group should best represent the team(s) most impacted by the urgent change.
The Senior Manager of North American Operations will be copied in any Urgent change requested to support the CAB/EC chairman.
It is the responsibility of the Chairman to plan for delegation of authority when necessary, such as absence due to travel, training and vacation.

CAB/EC 3 main responsibilities
Risk Evaluation
Approval/denial of Urgent Implementation
Provide support and control during the development and implementation

Technical support
Resource allocation, internal or external
Communication to Management
Communication to End Users

Urgent Change: Service Level Objective
Response Timeframe: 1 Hour (acknowledgement of issue & responsibility)
Approval/Denial Timeframe: 4 Hours
Urgent RFC Assessment and Possible Outcome
Urgent changes may be approved or denied based on their assessment of the situation
Denial: The change is justified and necessary, but can wait until the next scheduled CAB. Resources are allocated accordingly.
Approval with delayed implementation: Event causing severe impact but is not mission critical and rectification of the incident can slightly be deferred to allow for a higher level of planning without waiting for the next CAB. Resources are allocated accordingly.

Approval for immediate implementation: Event severely affecting users and/or degrading the service. Approval is given for immediate implementation, mainly driven by time constraint. The event is given the highest priority for change building, testing, and implementation resources.

Capturing Events & Actions in the Urgent RFC
Each urgent change shall be captured in Altiris through an urgent RFC. The RFC shall be the primary repository for capturing event information, analysis and actions taken. If and when necessary, other Altiris tickets may be created and linked with that RFC. When possible, management approvals or comments should be captured in that RFC. This RFC will also serve as a communication tool for other viewers/managers.

Development and Test
Development and test of the urgent change proposed should preferably be conducted in a test environment. Testing may be bypassed if authorized by the CAB/UC

Roll-Back and/or Backup
Appropriate roll-back procedure shall be determined prior to implementation of the urgent change. If specific Roll-Back procedure cannot be created, the availability of a prior full system and data back-up shall be checked and a full system and data backup of the current state shall also be performed.

Immediate Testing
Immediately after the implementation of the change, a thorough testing shall be conducted by IT members and a selected group of users to confirm the effectiveness of the change and identify any negative impact or side effect. Results shall be documented in Altiris ticket linked to the RFC

Urgent RFC Implementation Failure
If the urgent change fails, or if subsequent testing identifies any problem, the issue shall be documented and appropriate corrective action(s) shall be initiated which may include, roll-back, supplemental development, work around….. and follow the standard change management process steps as permitted by the situation.

Post Implementation Review
After implementation of the Urgent Change in production, a PIR (Post Implementation Review) should be completed by the CAB EC in charge or the Service Manager. Findings should be documented and saved in the RFC ticket. As part of this effort, Company IT should make its best effort to retroactively complete the various steps involved in the Standard Change Management process. All urgent changes PIRs should be reviewed by the CAB

Urgent RFC Closure
Urgent RFC shall be closed by the service manager, after review by the CAB

Monitoring: Key Process Indicators

On a periodic basis (Frequency To be Determined), the CAB shall review the overall change management process effectiveness though review of the following metrics:

Primary Indicators

- # of RFCs submitted (weekly trend)
- # of RFCs by Category/Model (weekly trend)
- # of RFCs by Service (weekly trend)
- # of RFCs by CI (weekly trend)
- # of RFCs completed successfully (weekly trend)
- # of RFCs unsuccessful (weekly trend)
- # of Incidents traced to Changes (weekly trend, detailed list)
- # of FSC references (weekly trend)
- Additional Indicators
- # of RFCs (and any trends in origination)
- # of Changes implemented in the period,
- Total
- By Configuration Item
- By configuration type
- By service, etc
- By reason for Change (User requests, enhancements, business requirements, service call/Incident/Problem fixes, procedures/training improvement, etc)
- # of RFCs rejected
- # of changes in backlog, broken down by CI and by stage in the Change Management process.
- # of Changes that were not successful
- Total
- Broken down by CI
- Broken down by reasons (e.g. incorrect assessment, bad build)
- CI with high # of RFCs/PRs, and reasons (e.g. volatile User requirement, fragile component, bad build)
- Figures from previous periods (last period, last year) for comparison

Appendix

Appendix A: Change Management Process Flow Overview

See Change Management Flowchart document on the network located at http://aursps01/sites/IT/POF/CGMSMF/Change%20Management%20Working%20Docs/Change%20Management%20Overview.vsd

Appendix B: Summary of Roles and Responsibilities

Roles	Responsibilities
Change initiator	Initiates the change. Follows processes for submitting an RFC. Assists the change manager in updating the RFC. Provides input in the post-implementation review.
Change Manager	Owns the change management process Initiate, develop and obtain approval for improvements in the change management process Provide tools, documentation and training to support the process Propose CAB members and facilitates CAB meetings. Prepares CAB meeting agendas and provides all necessary review information to the CAB members prior to board meetings. Assigns teams to conduct RFC impact analyses and risk assessments. Escalates RFCs that the CAB cannot decide to the IT executive committee. Analyzes, prioritizes, classifies, and schedules RFCs. Approves minor changes unless they are also urgent changes. Provides change notification to change initiator and other affected parties. Monitors the successful completion of all RFCs to ensure that the processes used follow the change schedule. Reviews and evaluates the change process.
Change Owner	Receives approved changes from the CAB. Follows the change schedule that the CAB approves. Coordinates the phases of the change development project (as applicable). Provides project status feedback to the change manager and CAB. Identifies any problems as they arise. Works with the change initiator to ensure that the change meets the change initiator's requirements. Reports status and presents findings to the CAB. Prepares for and leads the post-implementation review. Note: this role is carried out by the service manager or the project manager assigned to a PSF
Change Builder	Develop the technical aspects of a change Test the change Document technical aspects of the change Build the change to release in production Implement the code or configuration in production or deliver the code to the organization responsible for implementing in production. Note: Typically this is a developer role

Roles	Responsibilities
Change advisory board (CAB)	Assesses and approves changes to the production environment. Reviews the status of a change throughout the change process. Assesses progress with respect to the approved schedule. Determines how to correct any identified problems. Communicates findings to appropriate managers and stakeholders, including the IT executive committee that they represent.
CAB urgent committee	Assesses and approves urgent changes to the production environment. Reviews the status of an urgent change throughout the change process. Updates the CAB on urgent change status.
IT executive committee	Approves major changes to the IT environment when the CAB cannot reach a final conclusion. Performs the same tasks of analysis and authorization that the CAB conducts. Has the requisite authority to veto RFCs (if the committee deems it necessary) that the CAB has approved.
Service Manager	IT Service Owner Provision and monitor an IT service on a daily basis. Provides SLA compliance measures Analyze, validate, then approve/reject change requests Drive short term and long term service improvements

Appendix C: Roles & Responsibilities Definitions

1. Change Initiator

The change initiator initiates changes by submitting an RFC to the change manager. Everyone in the organization should be authorized to initiate an RFC. Below the manager level, however, it is recommended that employees submit RFCs to their managers who review them to ensure that the change requested is in keeping with business strategy and the vision for that area before passing them to the change manager. The change initiator is responsible for completely filling out the RFC form, which includes the reason for the RFC, the requested implementation date, and the systems and personnel affected by the change. This person is notified whether the change was approved and is kept up-to-date on the status of the RFC throughout the change process. The change initiator assists the change manager and CAB in determining the RFC priority and, at the conclusion of the change, participates in the post-implementation review.

2. Change Manager

The change manager is responsible for managing the activities of the change management process for the IT organization. This individual focuses on the process as a whole more than on any individual change. However, the change manager is involved in every step of the process—from receipt of an RFC to the implementation of the change in the IT environment—and is ultimately responsible for the successful implementation of any change to the IT environment. The change manager's responsibilities include:
Receiving RFCs and ensuring that they are properly recorded in the change log.
Selecting CAB members and facilitating CAB meetings.
Preparing CAB meeting agendas and providing all necessary review information to the CAB members prior to the meetings.
If necessary, assigning teams to conduct RFC impact analyses and risk assessments.
Analyzing and prioritizing RFCs.
Categorizing, assigning change owners, and scheduling RFCs, subject to approval by the CAB.
Approving requests for minor changes.
Providing change notification to change initiator and other affected parties.
Monitoring the successful completion of all RFCs, including the change development project phases and ensuring that these processes follow the change schedule.
Reviewing and evaluating the change process.

3. Change Owner

The change manager assigns (with the CAB's approval) an individual to be the change owner for a particular change. The change owner is responsible for planning and implementing a change in the IT environment. The change owner assumes responsibility upon receiving an approved RFC from the change manager or the CAB. The change owner is required to follow the change schedule approved by the CAB. For changes that are significant enough to require following a change development model—for instance, the MSF Process Model for application development—this individual is responsible for coordinating the project phases of the assigned change.

For standard changes, the service desk is typically the change owner. For major, significant, and minor changes, the change owner may also serve as the release manager. The change owner should routinely provide project status feedback to the change manager and identify any problems as they arise. The change owner presents all formal updates and proposals to the CAB after the CAB approves the RFC for passage through the various MSF phases.

The change owner must work with the change initiator to ensure that the change meets the change initiator's requirements and that it successfully corrects any problems or provides the correct system enhancements intended by the RFC.
After implementing the change, the change owner assists the change manager in evaluating the change process as it applies to the particular change. The change owner also coordinates and presents the post-implementation review analysis to the CAB.

6. Change Advisory Board (CAB)
The Change Advisory Board (CAB) is a decision-making body for the IT organization and evaluates and votes to approve or reject RFCs

7. CAB Membership
The CAB is made up of individuals with stakeholder interest in the production environment. Since RFCs can affect any part of IT and any organizational group, the makeup of the CAB should reflect the focus of the particular RFC being reviewed. However, a core group of individuals from IT operations is permanently assigned to the CAB. This group may include representatives from the MOF service management functions (Release Management, Capacity Management, Configuration Management, Availability Management, Security Management, or Service Desk) and should contain at least one member from each of the seven role clusters in the MOF Team Model.
The remaining members of the board may vary depending on the expertise required to effectively evaluate each RFC and the areas directly affected by the change, as determined by obtaining information from configuration management about the impacts of the change. The change manager is responsible for selecting the CAB members for each change. For large hardware and/or software changes, the change manager may decide to appoint an OEM vendor representative to the CAB. This facilitates the communication and the coordination of tasks between the vendor and organization. Having a vendor representative on the CAB also eases the resolution of problems during the change and release processes.

In general, the CAB should be composed of individuals with a wide range of expertise. Collectively, the individuals should be familiar with business requirements, the user community, IT system technology, and the organization's application development, testing, and support staffs.

8. CAB Responsibilities
The CAB should meet at regular intervals (perhaps weekly for a large organization) to review, prioritize, approve, and schedule RFCs. It is common for the CAB to consider

more than one RFC in a session. In this case, members might come and go during the meeting as the changes relevant to their area of concern are considered.
The change manager directs the CAB in a vote to approve or reject changes. In order to approve RFCs, the board must have the authority to make budget- and resource-related decisions. The board also reviews the status of each change throughout the change process, assesses the progress with respect to the approved schedule, determines how to correct any identified problems, and communicates its findings to appropriate managers and stakeholders.

Those major or significant changes that are not decided upon by a majority vote may be referred to the IT executive committee. The change manager is responsible for deciding if the disputed change is rejected or should be forwarded to the IT executive committee.

9. Change Advisory Board Urgent Committee
The Change Advisory Board Urgent Committee (CAB/UC) is a subset of the CAB and is responsible for assessing and approving any changes classified as urgent. Members of the CAB/UC must have the flexibility to meet at short notice or to provide recommendations using e-mail or other forms of communication.

10. IT Executive Committee
The function of the IT executive committee (ITEC) is to approve disputed changes that have been escalated to the ITEC by the CAB or changes that the CAB does not have the authority to make. Under these circumstances, the committee performs the same tasks of analysis and authorization that the CAB conducts. Following authorization by ITEC, the CAB has the responsibility for scheduling the RFC and monitoring the change process. Representatives from all of the IT groups within the organization are on the executive committee. Typically, managers who have the authority to make decisions regarding budgets and resources fill these positions.
The following table summarizes the responsibilities of each role in change management.

11. Service Manager
Ultimately, the responsible entity for day to day provision and monitoring of an individual service across all relevant sites; responsible for provisioning SLA compliance measures and for ensuring that the service review is carried out. Normally there is one service manager per service

Appendix D: Key Words Definitions

CAB urgent committee (CAB/UC):
This is the subgroup of the CAB that deals only with urgent changes. It is established to be able to meet on short notice to authorize or reject changes with urgent priority.

Change
Any new IT component deliberately introduced to the IT environment that may affect an IT service level or otherwise affect the functioning of the environment or one of its components.

Change Advisory Board (CAB)
The CAB is a cross-functional group set up to evaluate Request For Change (RFC) for business need, priority, cost/benefit, and potential impacts to other systems or processes. Typically the CAB will make recommendations for implementation, further analysis, deferment, or cancellation.

Change Impact (sometimes referred to as Change Category)
This a measurement of a change's deployment impact on IT and the business. The change complexity and resources required, including people, money, and time, are measured to determine the category. The risk of the deployment, including potential service downtime, is also a factor.

Change Initiator
A person who initiates a request for change; this person can be a business representative or a member of the IT organization.

Change Manager
This role has the overall management responsibility for the change management process in the IT organization.

Change Owner
The role that is responsible for planning and implementing a change in the IT environment. The change owner role is assigned to an individual for a particular change by the change manager and assumes responsibilities upon receiving an approved RFC. The change owner is required to follow the approved change schedule.

Change Urgency
This is a change classification that determines the speed with which a requested change is to be approved and deployed. The urgency of the need for the solution and the business risk of not implementing the change are the main criteria used to determine the priority.

Configuration Item (CI)
This is an IT component that is under configuration management control. Each CI can be composed of other CIs. CIs may vary widely in complexity, size, and type, from an entire system (including all hardware, software, and documentation) to a single software module or a minor hardware component.

Release
This is a collection of one or more changes that includes new and/or changed configuration items that are tested and then introduced into the production environment.

Request For Change (RFC)
This is the formal Request For Change (RFC), including a description of the change, change requirements, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.

Appendix E: CAB Members List

CAB Members As Of 03/24/08		
Department	Primary, Title	Secondary, Title
Information Technology		
Property Management		
Enterprise Applications		
Information Management		
Architecture		
Security		
System Engineering		
Network Engineering		
Service Desk		
Operations		

Appendix F: CAB Timelines

CAB Timelines As Of 03/24/08	
RFC shall be published by	Monday, 5PM
Agenda shall be published by	Tuesday, 1PM
CAB meetings	Wednesdays, 10-11AM
Meeting notes shall be published by	Wednesday, 5PM

Appendix G: CAB Documentation Templates

CAB Templates As Of 03/24/08		
Purpose	Name	
CAB Agenda		
RFC Status Report		
Request For Change	TBD	
Release Readiness Review	Release Readiness Checklist	
Post Implementation Review	PSF Project Close-Out Template	
Known Changes Type List	Know Change Type List Repository	

Appendix H: Linkage Between Risk Assessment, Change Category and Approval Process

Risk Assessment	Change Category	Approval Process
Low	Standard Change	Pre-approved
Medium	Minor Change	Change Manager Approval
High (non-PSF)	Significant Change	CAB - Release Readiness Review(RRR)
High (Large PSF)	Major Change	CAB - CIR and RRR