

## CareGroup ITIL Action Plan<sup>†</sup>

### Executive Summary

The Information Technology Infrastructure Library (ITIL) provides a framework of best practices for managing information technology services. Adopting the ITIL Service Support model can help CareGroup avoid another incident like the network collapse of November, 2002. Because implementing the entire service management framework will take years and is an expensive proposition, the author recommends starting with the five aspects most relevant to CareGroup's situation just after the incident.

Establishing a service desk is the best first step; all of the other service support processes take advantage of this single point of interface between IT providers and customers. From there, based on CareGroup's specific needs, it should implement the ITIL incident management process. This focuses on improving the way services are restored following a disruption. The IT department should establish policies for logging, prioritizing, dispatching, investigating, and communicating the resolution to incidents that are reported to the service desk. Incident management is a relatively “quick win” that will help restore confidence in IT and build internal support for the entire initiative.

The next step is to implement a change management process. CareGroup already recognizes this as a high priority given the causes and response to the network collapse. ITIL best practices recommend expanding the change control board CareGroup has established to be more proactive and holistic.

Third, CareGroup should develop a formal problem management process that incorporates guidelines for quality management best practices as well as data from and

---

<sup>†</sup> This paper is a class exercise based on the 2005 Harvard Business School case about CareGroup, prepared by F. Warren McFarlan and Robert D. Austin. It was not commissioned or delivered to the actual CareGroup organization.

communication with the service desk. The final step should be to establish and maintain a configuration database as part of a configuration management process that informs each of these other processes.

Adoption will entail significant costs in terms of staff time, consultants, new positions to fill, and software licensing. It will also require some changes to organizational structure, like creating the service desk. I believe that CareGroup will benefit greatly from this transformation, but key performance metrics should be measured and reported throughout the implementation process to allow managers to make better decisions about the initiative.

Once these high priority processes have been established, CareGroup should evaluate the experience and decide whether to pursue the service delivery model part of the ITIL framework.

## **ITIL and CareGroup**

This plan is a response to the CareGroup network collapse of November, 2002. During that time, emergency backup procedures helped the organization to function for three days while it was without reliable IT systems. The following analysis details steps CareGroup should now take to avoid a similar incident in the future.

An ITIL implementation aims to improve the quality, availability, and cost of information technology (IT) services by better managing problems with and changes to the configuration of IT resources. In this context, an IT service is a technical or professional capability provided for a non-IT customer. At CareGroup, these customers include, for example, medical and research staff, managers and back-office employees. IT services include the basic computer and network infrastructure as well as the computer-based applications that employees and even patients use to carry out business processes.

The two main components of ITIL are service support and service delivery.

Implementing the framework can be a long and expensive process involving significant organizational change. It should be done in deliberate steps. This plan focuses on the service support components because they best match CareGroup's immediate needs and lay the foundation for the rest of the framework.

## **Implementing ITIL Service Support**

### Service Desk

In adopting ITIL service support best practices, CareGroup will develop processes for incident management, change management, problem management, and configuration management. Before these can be tackled, however, the IT organization should be structured to provide what ITIL refers to as a *service desk*. This functional unit will provide a single point of contact between IT customers - employees within CareGroup and, in some cases, patients or external partners – and the entire IT service organization. The service desk will be responsible for logging, tracking, and answering or forwarding all user support requests (whether calls or emails). Not only will this allow for more efficient and effective communication, but the service desk will play a vital role in enabling all the other ITIL service support processes.

Establishing a central service desk will require bringing together customer-facing IT staff members from each of the four CareGroup hospitals and the corporate office. Since the supported facilities are geographically separated, service desk employees should remain physically distributed, at least to start. In order to encourage consistency and group cohesion, however, they all need to be trained together and report to the same senior manager. They should think of themselves as CareGroup IT support, and not Mount Auburn support or Beth Israel support.



## Incident Management

Change management is one of the highest priorities for CareGroup given that out-of-date infrastructure documentation and an unauthorized software installation contributed to November's network collapse. However, a quick win is important to build momentum and support for the ITIL implementation initiative. Since managing incidents is a relatively easy process for CareGroup to improve and can have high-profile results, I recommend starting with incident management. This process seeks to restore normal IT services quickly when those services are disrupted.

The case writeup does not describe CareGroup's IT support staff organization in detail, but I assume they are already mostly centralized under the CIO, John Halamka. I further assume that the Meditech automation system does not have a robust incident tracking function. Thus, incidents are currently passed on and handled as they come to support staff in an ad-hoc fashion. There are probably already general instructions about prioritizing and routing incoming user communications, but CareGroup is unlikely to compare incoming calls with already resolved problems or known issues in all but the most informal ways. A help desk staffer might know, for example, that a complaint about intermittent access to digital X-ray storage should be a high priority and be routed to the clinical support technicians, but would be unlikely to correlate that complaint with other reports of network problems in other areas or that came in to other support people.

Following ITIL best practices, CareGroup should decide on and document policies for (1) reviewing and logging user communication to the service desk. (2) Prioritizing these communications and categorizing them as incidents (calls for help or reports of trouble) informational requests, or service requests (requests for new or exceptional IT services like granting special user access or supporting video-over-IP). (3) Assigning these communications to appropriate staff who can investigate them with timelines for escalating

unresolved incidents to managers' attention. (4) Tracking, closing, and learning from these requests.

When these incident management policies are operating at CareGroup, that digital X-ray storage access complaint will be handled differently. First, the service desk staffer would log the call according to policy as an incident and check for already known resolutions or work-arounds. If there were none, she would send a message to the predefined appropriate technician, clinical systems support in this case, with the appropriate priority flag. That technician would communicate a resolution, work-around, or known error for that incident back to the service desk once it had been investigated. Perhaps this investigation discovered high network utilization was a problem; the service desk learns that users should try accessing a different storage mirror and network support is notified about the high utilization issue. Finally, the service desk staffer would contact the original customer to let him know how to work-around this issue and that a deeper issue is being investigated. While this is an idealized situation, a formal process is more efficient and valuable than the current situation.

To gauge the performance of this process, CareGroup IT management should track a few key performance indicators. Comparing these to historical data may also be helpful to demonstrate the value of implementing incident management best practices. Speed of incident resolution can be measured by the average time to for service desk staff to respond to a request or by the percentage of results categorized correctly and assigned to the right technician. Overall IT service quality can be measured by total time IT services are unavailable or by the average number of open incidents. User satisfaction can be measured directly with surveys of employees. These examples should be tailored for the performance indicators decided upon by incident management group and should be communicated to the IT department to build camaraderie and support for the process. IT employees should be incentivized to meet performance goals, possibly with cash bonuses.

Implementing a solid incident management process will require two significant expenditures in addition to the time required to create the new policies. CareGroup should purchase a purpose-built software system to facilitate incident logging, tracking, and communication. Also, most CareGroup employees will need to be educated about the new policies. IT staff, and especially service desk staff will need in-depth training of these new procedures and software tools. The whole IT organization, from first tier support to technicians to managers, needs to participate in incident management for it to succeed. Even non-IT staff should understand the new process so that they know to how and why to follow it. And also so they know what to blame for any increased frustration or satisfaction.

The costs of implementing ITIL's incident management framework will be balanced by CareGroup's overall improved responsiveness to incidents. While this won't, by itself, prevent a major network outage, it can lead to improved IT service quality, improved productivity, and higher user satisfaction amongst all employees. More information about all the group's IT services will be available to be acted upon, accountability for resolving or escalating incidents will be increased, and there will be less duplication of effort. Not only are these improvements valuable for the efficiencies and cost savings they will bring, but also because a solid incident management process will demonstrate to CareGroup IT and managers the value of the ITIL initiative.

### Change Management

Alongside incidents, better managing changes to its information technology environment is the highest priority for CareGroup. The variety and distribution of IT services in the organization - ranging from doctor email to clinical systems to the datacenter all on a complex multi-segment networking infrastructure – combined with the research-orientation of some of the hospitals in the group makes it likely that another catastrophic IT failure will

occur in the absence of an informed change approval and scheduling process.

It was an unmanaged change – untested and unapproved software installed onto the network without notification or supervision - that triggered the network collapse of November, 2002. And unmanaged changes to the physical network had crippled IT troubleshooters' attempts to diagnose and recover from that problem. CareGroup has learned from its IT mistakes and is already moving to establish a Change Control Board (CCB). In addition, the organization is working towards keeping its knowledge of its own IT systems current.

The CCB and up-to-date documentation are good steps. I'll touch on the later below in discussing configuration management. As for the former, while controlling change through notification and scheduling is important, ITIL best practices recommend a more proactive and holistic practice. CareGroup's change management process should review proposed changes to ensure that they have been tested, that they are consistent with technology architecture policies and goals, and that all the relevant documentation has been updated to reflect the new state. The process should involve people from many different parts of the organization to anticipate the consequences of any proposed change. This includes the IT department and project management office, but also includes employees with clinical and back-office responsibilities like nurses and accountants. Changes and their consequences should be communicated to the service desk as soon as they are scheduled. This will help the whole organization prepare for a smooth transition.

Like incident management, CareGroup should track and report on performance metrics for the change management process. The percentage of changes implemented on time and on budget can be a measure efficiency and effectiveness. Likewise, the number of changes that have to be undone or that cause incidents can be tracked to measure improvements in service quality.

A rigorous management role for the CCB is expensive in terms of staff time away from other responsibilities. If this involves nurses and doctors, it will take buy-in and support from influential executives and practitioners. There will also be a cost associated with auditing the process to ensure that these policies are being followed. Control over changes comes at the price of limited freedom to experiment on the network and a slower IT project cycle. This is not insignificant from a strategic point of view at an institution that prides itself on research and state-of-the-art technology in support of its medical services.

Some of these costs can be mitigated. To the extent that the IT environments at individual CareGroup facilities are different, it may be advantageous to establish a federated change management system. In such a system, less significant changes and ones that only affect a local facility can be approved and scheduled by a subset of the CCB or by a local CCB. Also, reoccurring or common changes can be pre-approved. These steps can reduce the time required by members of the CCB and the time it takes to get some projects approved. In addition, the improved responsiveness provided by the service desk and incident management procedures will offset some of the project cycle slowdown.

As it matures, though, CareGroup should be willing to accept some of the costs of good change management. The risks of a poorly managed change process are too high, especially in a medical environment where health is on the line. More generally, though, the benefits of improved reliability and planning ability outweigh the costs.

### Problem Management

With three important IT service processes now aligned with best practices, CareGroup should turn to improving its foundational processes. The recent network collapse was a large incident – all services were disrupted for three days – and the response would have fallen under CareGroup's incident management process. But there were a number of problems that

caused the incident and could cause further incidents if allowed to continue. In the ITIL framework, problem management focuses on correcting those underlying problems and removing the causes of incidents. Because it requires data about service disruptions, this process should be implemented only after CareGroup's incident management process is running smoothly.

Halamka and the IT team, along with the Cisco consultants, did an admirable job resolving many of the problems responsible for the recent crisis. Still, a formal proactive problem management process is important to improve overall IT reliability and reduce the costs associated with recovering from incidents. Having a support contract from with engineers on site will help ensure that network problems can be identified and corrected quickly. Even with this new experience and resource, CareGroup will be reacting to problems in an ad-hoc fashion and only after they have caused enough trouble to catch someone's attention. Further, service problems can occur in IT resources not under Cisco's purview.

In adopting an ITIL problem management process, CareGroup should establish formal guidelines for how to identify and diagnose problems. These should include general quality management best practices like root cause analysis but should also leverage the knowledge that is generated by incident management and that is routed through the service desk. Actual correction of problems will be done, as it is currently, by experts using the best methods of their domains. The communication loop should be closed, though, by documenting the results and new status of any changed resources and sharing that information with the service desk. See the discussion of configuration management below for more on this. The process should also involve proactively analyzing incident management data to identify and prevent hidden problems.

With an active and formalized problem management process, CareGroup can expect fewer problems that produce major incidents and a shorter time to recovery because all

available data will be brought to bear identifying and solving those problems. It also ensures that problems are tracked well and that they feed into the organization's change management process. As problems are solved more quickly, the service desk will receive fewer complaints about the same incidents and productivity in other parts of CareGroup operations will improve.

Problem management success can be difficult to measure because most of the improvements show up in incident management metrics. For example, a reduction in reported incidents for a period is difficult to attribute directly to problem management. But managers can measure a reduction in repeat incidents (which would point to the same problem causing a disruption) or a reduction in the average time to diagnose a problem.

Ad-hoc problem solving requires fewer resources up front, but, as CareGroup discovered, the bill for labor and downtime when a big one surfaces can be dramatic. There is a staff time cost to implementing an ITIL problem management process, as well as a cost for any quality management professionals to consult on the guidelines that will be established. Once the process has begun reducing demand on the service desk, some of those employees can be transferred to or split with problem management, which will offset some of the cost of investigating potential problems.

### Configuration Management

The fifth stage of CareGroup's ITIL implementation should focus on better managing IT configuration. This is related to change management and directly impacts problem management and the service desk. Because CareGroup has just updated its technology infrastructure documentation as part of rebuilding its network, configuration management is a lower priority than it might be for other organizations. Nonetheless, it is important to implement because most IT management processes rely on current data about configuration.

Like it or not, the rapid pace of technological change and hospital research will soon make CareGroup's current documentation out of date.

Following best practices, CareGroup first needs to fully document all of its IT assets, configurations, and services. This should be done via an audit of each of its facilities and interviews with IT managers and employees with a long CareGroup employment history. The goal is to identify everything relevant to the IT environment, including individual PCs with serial numbers and operating system version, servers with what services are exposed on which ports, network switches with software version numbers, and physical and network location information for each item.

This configuration information, along with documentation of the new physical network should be added to a customized *configuration management database (CMDB)*. Specialized consultants should be brought in to help define the structure and labels for that database; architecture and naming practices are difficult to get right. Getting it right is important because the CMDB needs to connect to software systems that manage these other IT management processes and needs to be understandable by the change control board.

Once created, the configuration database needs to be maintained and its accuracy verified. During creation and maintenance, CareGroup should establish two new staff positions that ensure the quality of the data and this initiative. First the configuration management *process owner* will be the project's champion and lead the entire process. This person will work with the IT department to make sure that policies are carried out and with other departments to encourage participation. This process owner role should be filled by a senior manager with influence across the organization.

The second position, *configuration manager*, will be responsible for carrying out the operational aspects of this process: conducting the initial and verification audits, helping develop the database structure, and integrating with the other processes like incident

management. This role will produce performance data and report on the status of configuration management to the senior IT management. This person will also be a steward for configuration data, personally responsible for its integrity and currency.

In addition to the consulting and new staff salary costs, a successful configuration management process will require CareGroup to think about its IT projects throughout their lifecycle. If projects to upgrade network segments or deploy new surgery webcasting software are approved, added to a simple list of technology inventory, and just then handed off to the service desk for support, all the management processes described above will continue to struggle with compliance. Once configuration management is treated as an important component of IT strategy, all four of these ITIL processes will interoperate smoothly and CareGroup's IT will have matured to a more reliable and efficient level. Fortunately, Halamka and the CareGroup management team seem eager to make IT improvement a priority.

### **Where To Go From Here**

Having implemented the core of the ITIL service support model, CareGroup should evaluate its experience. Has the IT department gotten behind the initiative or are feet dragging? Has the organization seen real improvement in the quality and reliability of IT services as a result of the initiative? Have the costs been justified by these improvements? Does the organization have the stomach for further IT service transformation?

In addition to improving the processes already implemented, CareGroup should consider adopting the ITIL service delivery model. Like the service support model, this is a set of best practices, but for five processes involved in actually delivering services. It consists of the following processes: (1) Service level management, which defines agreements about metrics and monitoring between IT service providers and customers. (2) Availability management and (3) capacity management, which ensure that IT resources can support the

service levels that have been agreed upon. (4) Service continuity management, which is concerned with restoring services following a serious incident like a network collapse. Finally, (5) financial management for IT services brings accounting and budgeting into the service mix.

These should be thought of as longer-term goals for CareGroup. The IT department has already begun updating its emergency backup procedures, so implementing service continuity management is a lower priority. Similarly, CareGroup has been very conscious of its IT spending over the past five years as evidenced by figures in the case. Nevertheless, if the ITIL framework has proved to be a good fit with the strategic goals, operational realities, and organizational culture of CareGroup, continue with enthusiasm!

## **References**

DuMoulin, Troy. "The Hitch Hiker's Guide to the ITIL Galaxy and Beyond: Don't Panic Blog." Pink Elephant. Retrieved from <http://blogs.pinkelephant.com/troy> on May 11, 2007.

McFralan, F. Warren and Robert D. Austin. "CareGroup." Harvard Business School. August 11, 2005.

McGrath, Patrick. "ITIL Awareness: ITIL Process Follow-up Slides." From Service Implementation (INFO 290-10), class 14 at UC Berkeley School of Information. April 24, 2007.

Pink Elephant International. "Critical Success Factors (CSF) And Key Performance Indicators (KPI). 2004