Information Technology Customer Service: “Best Practice” Processes for Operations

By

M. Keith Wright, PhD, CISA, PMP
Visiting Professor of Computer Information Systems
University of Houston – Downtown
Finance, Accounting and Computer Information Systems Department
One Main Street
Houston, Texas 77002
wrightkm@uhd.edu

&

Charles J. Capps III, DBA, SPHR
Professor of Management
Sam Houston State University
Management and Marketing Department
P O Box 2056
Huntsville, Texas 77341-2056
capps@shsu.edu

Copyright by Author 2007
ABSTRACT

In today's information economy, information technology customer service managers require increasingly technologically advanced, but cost effective operations. These managers have a Byzantine array of standards, methodologies and best practice frameworks that offer hundreds of pages of detailed, but often confusing, guidance. This paper's goal is to summarize and clarify important key concepts from the literature, and also present lessons learned from our consulting experiences with several large organizations. We explore the common challenges encountered in the initial stages of customer service quality improvement initiatives. This article is a simple guide for IT managers beginning a formal program to increase the effectiveness and efficiency of the day-to-day operation of their customer support services.

INTRODUCTION

Does your information technology (IT) organization have the capability to provide the required service with the required quality? If your organization is growing fast, there is a good chance it does not. When you as an executive finally make the decision to try to do something about these growing pains, the first step is usually management education. At that point managers encounter a bewildering array of standards, methodologies and best practice frameworks offering to help guide them.

For example, Carnegie Mellon University’s Software Engineering Institute (SEI) now publishes a process standard that can be used for any management process, not just software development. Called the Capability Maturity Model Integration (CMMI), this new model is a process management standard, not a performance standard. Thus, the CMMI does not require organizations follow a particular process. Thus, the CMMI is not meant to be an initial cookbook. (Software Engineering Institute, 2002) Other standards focus less on the management process itself and more on the output of the process. An example is Motorola’s Six Sigma programs which focus on defect reduction to a high level of statistical reliability. (Motorola Corporation, 2007) In contrast, the Control Objectives for Information Technology (COBIT) approach focuses on auditable controls. (Information Technology Governance Institute, 2000) From a project management standpoint, there is the Project Management Body of Knowledge. (Project Management Institute, 2004)

The International Standards Organization (ISO 20000) standard defines the requirements for a service provider to deliver managed services, and can be used as the basis for an independent assessment. (International Standards Organization, 2005) It may also be used by businesses that are going out to tender for their services, to provide a consistent approach by all service providers in a supply chain, to benchmark IT service management, or to demonstrate the ability to meet customer requirements. ISO 20000 grew from the “best practice” framework, ITIL, the IT Infrastructure Library. (Office of Government Commerce, 2000) This relationship is often illustrated via a diagram like the one on the next page:
ITIL is a best practices framework outlining a number of processes for information technology services management. In ITIL, business processes are independent of organizational form or size and may be large and cross-functional, or relatively narrow. Today, Forrester (Garbani, 2006) estimates that 30% of $1 billion-plus companies are experimenting with ITIL or ISO 2000 and between 12% and 13% have implemented it.

The above literature covers more than several hundred pages of tedious and detailed guidance. The fact so much is now known about best practices for IT service delivery means that customers will soon come to expect high quality IT services just as they expect high quality in any commodity, like electricity. (Carr, 2003; Swanson, 2004; Davenport, 2005; Iverson, 2006; and King, 2006) As customer expectations evolve to that higher level, the low-quality IT providers we must tolerate today will become extinct.

To date, there have been few case studies published describing the early stages of ISO/ITIL initiatives. This article addresses that need, based on a perspective tempered by teaching IT customer service improvement to various large organizations in the United States including IBM, the U.S. Department of Veterans Affairs, the City of San Jose, General Dynamics, Technology Concepts & Design, and Lowes Home Improvement Centers. This paper describes lessons learned from these experiences. We use ITIL terminology wherever possible. However, we find certain ITIL terms confusing to practitioners. Thus, we occasionally use different terms and point these differences out explicitly throughout the paper (See Table 1 on the next page). Our methodology adds to the published literature a suggested practical ordering to the implementation steps.
Table 1: Key Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLMP</td>
<td>Service Level Management Process</td>
</tr>
<tr>
<td>SKMP</td>
<td>Service Knowledge Management Process</td>
</tr>
<tr>
<td>SDB</td>
<td>Service Database</td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Resolution Process</td>
</tr>
<tr>
<td>ICP</td>
<td>Incident Correlation Process</td>
</tr>
<tr>
<td>SMP</td>
<td>Solution Management Process</td>
</tr>
<tr>
<td>CCP</td>
<td>Change Control Process</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SIO</td>
<td>Service Infrastructure Object</td>
</tr>
</tbody>
</table>

The point of view is based on the ideas of W. Edwards Deming. (Deming, 1966; Deming, 1986; and Deming, 2000) He observed that quality business processes consist of five key steps: plan, execute (do), measure (check), improve (act), and consolidate. (See Figure 1) The consolidation phase enables the organization to take stock of what has been taking place and to ensure improvements are documented and formalized through human resources, so they are repeatable.

![ITIL Process Model](image-url)

Figure 1

This approach can be adapted to both small and large organizations. Regardless of an organization’s size, the secret to a successful service improvement program is the financial strategy.

**Best Practice #1: Manage the Financial Expectations**

A major challenge a manager faces when starting an IT customer service improvement initiative is maintaining positive expectations for the project. The first step is to learn how much expense is justified. To do this, managers need to understand how much waste and/or lost opportunity exists in the current operation. This in turn requires someone be assigned responsibility for a separate and distinct IT cost accounting system. Because this is a full-time job, this person ideally should **not** be the same person responsible for the organization’s overall financial management. We call this new role the IT Financial Manager. This role should be charged with designing and documenting an IT Financial Management Process that provides accurate cost accounting to the other IT service managers. The inputs for this process are the business requirements, policies
and cost control methods. The IT financial manager develops a cost model used to allocate IT services costs to the customers receiving the services. Whether or not internal users are charged for IT services is optional although it is an excellent way to manage demand for IT services. Suggested cost elements are hardware, software, payroll, transportation, relocation, overtime, consultancies, offices space, storage space, security, and utilities.

If the IT Financial Manager can prevent the actual costs of the initiative from exceeding the predicted costs, this will go a long way towards maintaining positive expectations. A steady stream of accurate cost-benefit analyses to stakeholders helps immensely. Earned value analysis is especially useful for this purpose. A word of caution here: if the analysis does not show a potential for a huge benefit, go back to the drawing board and simplify something. Quality initiatives are risky, even when kept simple. Once managers grasp how much money is to be spent on the customer service quality initiative they are ready to get human resources involved.

Best Practice #2: Get Human Resources Involved

Before undertaking a process improvement initiative, it is vital to get the human resources department involved, so compensation systems can be altered to include new responsibilities for key personnel. Several new job roles must be formally defined including Process Managers and Process Owners.

HR often requires key personnel be assigned the goal of getting certified in a related quality improvement methodology. Along these lines, we have found that unless certification exams are challenging, the training will not be fully effective. Our consulting practice licenses the ITIL practitioner’s exam.

The key prerequisite for repeatability is Assigned Responsibility: there must be somebody accountable for defined processes covering objectives outlined in the financial planning effort. A formal project manager makes the design and implementation of any process more effective. This implementation manager may become the eventual “process owner.” Once the implementation project ends and the process become operational, the “owner” remains responsible for the process outputs during its lifetime. From an audit standpoint, separation of duties is a consideration when making the decision to select the original project manager as the eventual process owner (See Figure 2 on the next page).

Processes, whether very simple or complex, are always more effective if carefully guided by the organization’s strategy and policies. Furthermore, effective processes often cross organizational unit boundaries.
Best Practice #3: Create a Service Level Management Process

Once human resources have established the new job roles and incentive systems, the next step is to implement a Service Level Management Process (SLMP). Its purpose is to align and balance IT services with internal business needs, and to continuously improve the relationship between the IT services provider and its consumers. (See Figure 3)

The “owner” of this process is often the same person as the IT financial manager. The SLMP is responsible for a written description of all services the IT organization is capable of and willing to provide for any consumer. Called the Service Catalogue this document is analogous to the menu in a restaurant.

Inputs to the SLMP are the consumer requirements and the provider’s capabilities. It is important to remember that consumer here means any user of the IT services, whether they are paying customers, or those who support paying customers. This includes users inside the provider organization. Their needs must not be ignored because degradation in
paying customer service will result. For example, IBM, once known for its royal
treatment of employees, now has quite a different reputation and struggles to keep its
employees well supplied with access to information systems needed to support the paying
customers. Often this results in frustrations and lost service business. In IBM's case
these communication issues have been exacerbated by the off-shoring of key software
development programs.

The principal output of the ITSM process is the Service Level Agreement (SLA) -- a
clearly written statement describing the deliverables to a consumer including the agreed
service hours, incident response times, service availability times, security requirements,
continuity targets, customer responsibilities, and the next SLA review date. (See Figure
4) Although not a legally binding document, a clearly written SLA can avoid lawyers
and courts by setting clear consumer expectations and promoting win-win trusting
relationships with the paying customers.

![Service Level Management Diagram](image)

Figure 4

However, if the service level agreement depends upon external vendors, appropriately
referenced underpinning contracts can protect against legal liabilities. Further, if the
service level agreement depends upon multiple internal organizational units,
appropriately referenced operational agreements improve communications among
cooperating internal units.

It is important that service level agreements have a section documenting the escalation
procedures for use in case of service outages. What's more, this section should
distinguish between functional and hierarchical escalation, the former being cases where
more expertise is needed, and the latter being when more institutional authority is needed.
Functional escalation can be automatically triggered when agreed down-time intervals
elapse. Hierarchical escalation procedures allowed any time during the incident
resolution process can increase customer trust in cases where customer service cannot be
restored within agreed lower limits. Automatic hierarchical escalation can be considered
when it is likely that timely resolution will fail. If service level managers can work out
these details before the agreed resolution time is exceeded, line management can take early corrective action, for example by the hiring of third-party specialists.

If the service level targets are not measurable and monitored, stakeholders will likely not take them seriously, and service will not improve. Customer surveys are very useful here. Regularly held service level review meetings attended by paying customers, the service level manager, and other stakeholders provide an excellent forum for airing grievances and promoting a win-win relationship between the provider and consumer. This is the appropriate time for stakeholders to discuss possible amendments to the service level agreement (SLA). Possible reasons for such amendments include additional charges for services not within the scope of the original SLA, such as office moves, major hardware and software roll-outs, unplanned hardware upgrades, etc.

**Best Practice #4: Create a Service Knowledge Management Process**

Once managers understand the costs involved and have assigned a single person responsible for service level management, the next -- and most critical -- process the IT organization must implement is the *Service Knowledge Management* process (SKMP). (We use the term *service knowledge management* in preference to the analogous ITIL term, *configuration management*, which clients often find confusing). This process provides complete, timely and accurate information to all the other stakeholders in the IT services organization. Accordingly, this process covers the identification, recording, relating and reporting of all service-related infrastructure objects (SIOs) whether they are hardware, software, service level agreements, or other documentation.

The inputs to the service knowledge management process (SKMP) are the service level agreements, other business objectives, and IT infrastructure details. The SKMP helps control the IT infrastructure through the identification, registration, monitoring and management of all SIO documentation.

Thus, the principle output of the SKMP is the service database (SDB). As well as an understandable and accurate logical model of the relationship among the SIOs, the SDB contains the kind of information shown in Table 2 on the next page. Although the SDB can be initialized with data from existing asset management systems, it should extend this to include logical *relationships* between SIOs. For example, a disk drive is *part of a* PC. A PC is *networked to* a server. A program is *a copy of* the master. A manual *describes* a program.
Table 2: Contents of the Service Database (SDB)

<table>
<thead>
<tr>
<th>Service catalog</th>
<th>Telecommunication services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures</td>
<td>Service level agreements</td>
</tr>
<tr>
<td>Business units,</td>
<td>Servers</td>
</tr>
<tr>
<td>Supplier locations</td>
<td>Network components</td>
</tr>
<tr>
<td>Employee contact information</td>
<td>Desktops</td>
</tr>
<tr>
<td>Changes</td>
<td>Mobile units</td>
</tr>
<tr>
<td>Solutions</td>
<td>Software applications</td>
</tr>
<tr>
<td>Problems</td>
<td>Software licenses</td>
</tr>
<tr>
<td>Incidents</td>
<td>Facilities descriptions</td>
</tr>
<tr>
<td>Manuals</td>
<td></td>
</tr>
</tbody>
</table>

If support personnel can use the SDB to quickly identify all related service infrastructure objects pertaining to the SLAs, service levels will improve dramatically. Further improvements will occur if personnel can trace changes to service infrastructure objects (SIOs) from one state to another, for instance “under development,” “being tested,” “live,” or “withdrawn.”

A project manager plans the initial scope and level of detail to be included in the service database (SDB). For example, s/he may not deem it economical to track each mouse and keyboard or to track SIOs proposed for future services. We recommend implementing the SDB incrementally, perhaps only including SIOs related to existing service level agreements. A full blown SDB software package can cost millions, so one should select tools carefully. One can use inexpensive existing software in a prototyping approach to help flesh out the details of the requirements for a major automation upgrade. A cost effective service knowledge management process (SKMP) will eventually make or break the entire service quality improvement initiative.

After a simple SKMP is operational, its owner remains accountable for continuous accuracy of the service database (SDB). Thus s/he should control access to it and ensure no SIO record is added, modified, replaced, or removed without appropriate controlling documentation. Moreover, the SKMP should audit the SDB against the IT infrastructure after SDB implementation, after major infrastructure upgrades, and at regular intervals in between.

To briefly summarize, the outputs of the service knowledge management process (SKMP) are the service database and the periodic audit results. (See Figure 5) The SKMP should start very simply and become more complex as SLAs are added. Key SKMP performance indicators are the number of untracked SIOs detected in use, the number of SIOs used but not tracked in the SDB, and the number of changes to the SDB by type. Finally, if the SDB can save, protect, and report on historical time point
snapshots quickly, it can be used to quickly restore the IT infrastructure to prior states, in case a change in the infrastructure causes unforeseen incidents.

**Best Practice #5: Have a Service Desk Department**

After the financial management, service level management and knowledge management processes are defined and partly operational, the next step is build an appropriate service desk department complete with a budget for staff. This department advocates purely for the consumer and is their single point of contact. All consumer service requests, information, wishes, claims, complaints, requirements, quick fixes, and permanent solutions flow in and out of the service desk. The service desk often escalates incidents to other relevant departments and processes.

A customer facing staff skilled in communication and conflict resolution can improve customer expectations enormously. Many individuals with career interests in computer technology are not suitable in customer facing roles. Nevertheless directly supporting the customer facing staff is a group of specialists with the required knowledge, skills and authority to facilitate any kind of request or outage incident from a consumer. These first level positions are excellent entry level slots for employees interested in careers in computing technology.

Without a service desk, consumers may not know where to request service and may interrupt technology specialists. Then outage incidents will likely not be reported completely and accurately. This prevents proper incident escalation and will likely cause the entire quality initiative to fail. Globally dispersed service desks can provide access 24 hours a day, 7 days a week. If so, it is vital that a common agreed upon language is used for incident recording, which is the first step in the incident resolution process.

**Best Practice #6: Have an Incident Resolution Process**

Chiefly reactive, the mission the *Incident Resolution Process* (IRP) is to restore service outages as quickly as possible, not necessarily to find the root cause of the outage. (We use the term *incident resolution* in preference to the ITIL term, *incident management.*) Often this means simply reporting temporary quick fixes or workarounds found in the service database. An *Incident Manager* owns the IRP process. This manager is often the person holding the service desk budget. ITIL defines an *incident* as an alert about a service disruption, or a potential service disruption. Examples would be calls about printer failures from either a customer or internal support, or an alert about a disk overflow from a computer monitor. Efficient and effective incident reaction demands a formal method of working that can be supported by software tools.

First and foremost, the IRP should accurately and completely record all incidents. Examples of data to capture are incident ID, reporter, affected persons/systems, time, brief status description, and inventory number.
The next activity is prioritization. And it is vital that incident prioritization be a function of three things: the category, urgency and impact. The category and urgency are spelled out in the customer service level agreements. For example, category A48 might mean a service is now unavailable and must be restored within 48 hours to avoid payment delays. Category T3 might be a training incident that must be resolved within three months. Category S6 might be a request for an equipment relocation to be completed within six months. Additionally, the impact of the incident measures its potential effect on the entire service catalogue. Although criteria for assigning impact is set up in advance via consultation with the provider’s managers and formalized in service level agreements, the initial impact measurement is the subjective judgment of service desk employees assigned to the incident.

Parallel with incident prioritization, the incident resolution process (IRP) addresses the incident queue in order of priority. At this point, initial investigation and diagnosis is performed. If an immediate solution is not apparent in the service database, the next step is to transmit escalation alerts to one of the target processes we detail later. Conversely, the IRP periodically monitors the output of the target process to determine incident status and report to the consumer. Examples of status include new, accepted, scheduled, assigned to specialist, impact, urgency, priority, work in process, on hold, time spent, specialists involved, costs involved, resolved, and closed. Support personnel should augment the incident description as the incident progresses towards resolution.

To review, the inputs to the incident resolution process (IRP) are incident reports from the service desk or monitors, the service database, service level agreements, and incident status. The outputs are escalation alerts, incident reports to the service database (SDB), routine requests for changes in the infrastructure and status information to consumers (via the service desk). IRP personnel are responsible for closing an incident, but should never do so without the consumer’s permission.

Consumer satisfaction surveys are excellent ways to measure performance of the incident resolution process (IRP). Possible survey questions include: Is the telephone answered courteously? Are services restored in accordance with the Service Level Agreements? Are you given good advice to prevent future incidents? Are you advised in a timely manner about current and future changes? Other performance indicators are the total number of incidents registered, the percentage of incidents resolved during the first alert, average incident resolution time, percentage of incidents handled within agreed response time, and number of incidents escalated correctly.

During normal IRP operation, incidents are escalated to the incident correlation process, detailed next.

**Best Practice #7: Have an Incident Correlation Process (ICP)**

The primary mission of the Incident Correlation Process (ICP) is to constantly scan the service database vetting and grouping related incidents into problem records. (A single sufficiently informative incident can also be declared a problem. We use the term
incident correlation in preference to the ITIL term, incident trend analysis, which clients often find confusing). This can be automated via modern statistical and data mining tools. Employees in ICP roles are typically engineers.

When beginning a consulting engagement with organizations we usually find informal processes covering incident management. These are often called 1st or 2nd line support. For two reasons however, most of our clients do not have an effective ICP. First, they are often unaware of the latest data mining tools available. Second, they have trouble distinguishing between the following concepts: incident, problem, root causes, and defects. Part of this confusion arises from the terminology introduced by ITIL and ISO 2000 where root causes are referred to as errors, and correlated incidents are called problems.

A problem is best conceived as the state of existing knowledge between the time point incidents are correlated (when problems are discovered) and a solution is discovered. Consider this example. Suppose a service desk employee receives a call about a printer failure. S/he would then record and prioritize an incident in the service database (SDB). Then suppose there are soon several more similar calls about different printers. An effective incident resolution process proactively and constantly scans the SDB using data mining tools and quickly discovers that each of these failed printers are located on the same building floor. At that point a single problem record should be opened in the SDB. Subsequent similar incidents can then be added to that single record.

Therefore, the key performance indicator for the incident correlation process (ICP) is the ratio of incidents to problems. This ratio should be much greater than one. Without a formalized ICP the ratio of incidents to problems can approach one, and the sheer number of problems can overwhelm the entire IT service organization.

After the ICP associates incidents with problems in the SDB, the ICP prioritizes and escalates them to the next prescribed process, Solution Management. (We use the term solution management in preference to the ITIL term, error control).

Best Practice # 8: Have a Solution Management Process (SMP)

The two purposes of the Solution Management Process (SMP) are to find the root cause of problems and then to recommend their solutions. Obviously the personnel usually assigned to this process are engineers. To continue with our earlier example, suppose the engineers eventually discover faulty building wiring responsible for the printer failures on that building floor. The SMP then documents a defect in the SDB. (ITIL does not use the terms root cause, solution or defect, but rather the term error, which managers find confusing). The solution team then begins a complete analysis and documentation of a set of possible solutions.

The primary inputs to SMP are the escalation alerts from the incident correlation process (ICP) and the infrastructure configuration details from the service database (SDB). The most important outputs are the solutions, workarounds and request for changes (RFCs) --
all recorded in the SDB. The RFC contains the set of possible solutions. An effective SMP also includes a proactive step to recommend RFCs for improvements to the IT infrastructure prior to any reported incidents.

The critical SMP performance indicators are the average time between problem entry and solution definition, and the ratio of successful to failed solutions. However, the eventual success or failure of solutions will not be discovered until the solution is implemented -- by the Change Control Process which we discuss next.

**Best Practice #9: Have a strict Change Control Process (CCP)**

ITIL refers to solution implementations as *changes* to the information technology infrastructure. Changes to a high technology infrastructure can be extremely risky. However an appropriately strict Change Control Process (CCP) can effectively manage this risk. Thus, the CCP’s purpose is simply to minimize the number of future incidents caused by changes. (ITIL uses the term change management, rather than change control). The key to minimizing change related incidents is using a strict standard approval process for each solution, no matter its nature. Accordingly the CCP should take a high level view of a change to an IT service and ensure that all aspects of the change, both technical (deployment) and non-technical (training) are considered.

To continue the earlier example, an effective CCP would ensure that a change to the wiring affecting the fourth floor would not cause incidents on other floors. If IT organizations do not control change, they will be overwhelmed by it. Lowe’s Home Improvement Centers, in an aggressive effort to open one new store per month in the U.S., was recently overwhelmed by IT change related incidents.

As a result, the first step in the CCP is to scrutinize and prioritize the requests for changes (RFC’s) input from the service database (SDB). The RFC must contain all the information necessary for the change manager to determine its priority. At a minimum this includes an ID, change details, requester, change purpose, proposed priority, infrastructure objects affected, resource requirements, opportunity cost discussion, and related incidents/ problems.

If the change request (RFC) does not meet minimum requirements, a change manager acting alone rejects the RFC for re-submittal to the solution management process. Further approval process steps depend on the category and priority of the RFC. The approval process should *always* include a careful deliberation involving a committee of more than one person. (ITIL calls this committee the change advisory board.) The size of the committee depends on the priority and impact of the change. At a minimum the committee consists of the change manager plus people involved in all the earlier described processes, especially solution management engineers. Major change approvals always require senior executive sign-offs. Finally, the change control process (CCP) is responsible for planning, design, building, configuration, and testing of hardware and software prior to deployment. Testing should be done on non-production equipment.
For these reasons, an effective CCP is often both capital and labor intensive. Unfortunately in today’s cost cutting economy, many (even large) organizations try to short circuit the change management process by testing on production equipment, perhaps during off hours. These short cuts often increase rather than reduce long term costs. Back-out plans -- proven procedures to follow in case change related incidents overwhelm the service desk -- further insure against failed changes.

The change control process (CCP) schedules implementations and manages consumer expectations before deployment. Deployment of changes includes a sub-process called the Release Process (RP). This important sub-process is responsible for grouping internally compatible RFCs into Releases, which are sets of RFCs that are best implemented at the same time. Complex software releases, for example, often involve intricate internal dependencies, best handled by specialists, and bundled into a testable unit. The RP should treat the release as a unit and record it as such in the service database. However the overall CCP approves the timing and contents of releases.

The release process (RP) maintains and controls the Definitive Software Library (DSL) -- a secure storage area containing all official, tested, licensed, and authorized software, along with associated documentation. This storage area is kept separate and distinct from the development, test, and live storage areas. The DSL includes definitive copies of purchased software as well as internally developed software. The RP is thus responsible for all legal and contractual obligations for all hardware and software in use within the organization.

The RP also maintains and controls access to the definitive hardware reserves. (ITIL calls this the definitive hardware store). This is an area set aside for the secure storage of authorized hardware spares. Its size depends on the scope of the quality initiative. These spare components should be maintained at the same version level as those in the production environment. The RP records details of the definitive hardware store in the service database. These spares can then be used in a controlled manner when needed for additional capacity, or in recovery from major incidents. Once their (temporary) use has ended, the RP returns them to the DHS, or obtains replacements.

Finally, the change control manager chairs the Post Implementation Review (PIR) committee. This committee meets periodically by teleconference to verify that previously implemented changes continue to resolve their related incidents. Members of this committee include representatives from all the process areas previously discussed, especially the engineers from solution management process (SMP). Only after the PIR should the solution management process close the associated problem and defect records.

The main outputs of the change control process (CCP) are successful releases to the production environment. Other outputs are the forward Schedule of Changes (FSC), Planned Service Availability (PSA), PIR meeting minutes, and action items.

The key CCP performance indicators are the number of change related incidents, number of releases deployed within budget, number of release failures, incidents of unauthorized
software use, number of urgent changes, rate changes implemented, and the average cost per change.

Inter-Process Communication

Now that we have briefly sketched the best operational processes in IT service management, it is important to note that they execute in parallel with each other and thus require intricate inter-communication, depicted in Figure 5 on the next page. Communication is both synchronous, via an alert system; and asynchronous via the service database. A particularly common challenge is establishing effective communications between the Incident management, Solution management, and Problem management processes regarding solution definition. Smaller companies often attempt to deal with this by assigning employees to multiple processes. However, auditors may assess this practice as a separation of duties risk.

![The Operational Processes Diagram](image)

Figure 5

Implementing the Processes

The best way to implement these processes is to take small steps in all processes concurrently, coordinated by one overall Continuous Service Improvement Program, with individual project managers responsible for their own process implementations. We stress that implementing these processes is labor intensive in the short term. And it is easy to underestimate the scale of work required. Effective financial and service level
management processes are the foundations for all quality initiatives. The SDB is of major importance.

Even if the organization is not purely an IT services organization, the change process must be managed from the highest levels of the organization. Top management has the key role in avoiding the ‘Silver Bullet Lifecycle’ where new processes and increased accountability are introduced and then later abandoned during the critical initial period where costs are outstripping observable benefits.

Regrettably, many top managers do not like to get involved in IT service improvement programs because they erroneously think they are only the concern of IT specialists, rather than an integral responsibility of modern effective strategic management.

These suggested best practice processes will likely be perceived as a bottleneck by some, especially if schedules are overly-ambitious. When there is resistance it must be overcome, preferably with education. Employees who follow best practice processes correctly need to be compensated more than those that do not. In some cases, penalties may be needed as a last resort. For these reasons, the human resource department must be involved from the beginning.

Top management should take pains to avoid overambitious schedules and unrealistic expectations. Automation tools cannot and should not be expected to make up for poor process management. Poorly controlled infrastructure changes will greatly, if not fatally affect the quality of services. Alternatively, if the IT infrastructure is excessively controlled, staff becomes involved in unnecessary work. Adequate time must be built into schedules to allow staff to carry out their duties.

Expensive automation tool purchases should be delayed until their requirements are fully identified. Often this is done via prototyping with either manual methods, or inexpensive existing tools. We caution that staff and managers may end up blaming failed programs on tools instead of the processes.

**CONCLUSION**

In conclusion, this paper sketches a brief consensus view of what the Information Technology (IT) community usually considers “best practice” processes in consumer service operations. It does not claim to be a comprehensive description of everything within IT service support, but we believe it is IT management’s “best practices” generally accepted in industry.

These processes are proven, practical, cost-effective, and the result of our many lessons learned. However, you should consider the information herein as guidance – not rules!

Companies who adopt the framework presented here can expect their IT services to become more competitive. This will be due to the improved alignment of its IT with the business strategy because roles and responsibilities will be better understood. IT service providers will see improvements in service delivery because they will have a single
definable, repeatable, scalable, and consistent set of IT processes. This will result in a long-term reduction in the cost of IT services, as well as better service quality and responsiveness.

Customers will see fewer service outages, as proactive planning and quality measures are implemented. Customers will see their requested IT infrastructure changes implemented more quickly as needed to support new business requirements. Customer satisfaction will increase because service providers better understand what is expected of them. Customers will better understand the capabilities of service providers, and will therefore have more reasonable expectations.

More successful releases will result in less disruption to the internal business operation and assure that hardware and software in use is of known quality. Bundling changes into effective releases will reduce the number of required urgent deployments and businesses will be able to cope with higher levels of change.

Communications between IT departments will improve because the linkages between processes are documented and understood. Service providers will see better resource utilization with resources allocated based on business demands. Staff will be better motivated and behave more professionally because skill requirements and job expectations are better understood. A much more productive IT environment will be the result. For that reason, future applied research should continue to focus on increasing that productivity in logical, practical ways.
REFERENCES

About the Authors:

Information Technology Customer Service: “Best Practice” Processes for Operations

M. Keith Wright, PhD, CISA, PMP
Visiting Professor of Computer Information Systems
University of Houston – Downtown
Finance, Accounting and Computer Information Systems Department
One Main Street
Houston, Texas 77002
wrightm@uhd.edu
713-221-2788

And

Charles J. Capps III, DBA, SPHR, Contact Person
Professor of Management
Sam Houston State University
Management and Marketing Department
P O Box 2056
Huntsville, Texas 77341-2056
capps@shsu.edu
936-294-1895

* This unpublished article submitted to JABR on March 16, 2007, is not under review by another journal.