



ITIL for Government

Adopting IT Infrastructure Library guidelines can improve management strategies — especially with cloud computing initiatives.

Table of Contents

- 2 ITIL Fills a Need
- 2 Bring in the Clouds
- 3 Create a Game Plan: The 5 Steps

Executive Summary

First created in the 1980s to formalize best practices for well-run IT departments, the Information Technology Infrastructure Library (ITIL) has been helping public sector organizations refocus their resources on line-of-business services for decades.

Known as “service management” in ITIL circles, this strategy encourages IT departments to look beyond routine performance and uptime statistics for servers, storage systems and network gear. Instead, ITIL guides the IT group to think like their “customers” — the people inside an organization who rely on technology to do their jobs.

This emphasis on what it takes for organizations to attain their mission goals is finding common ground with another growing IT trend: cloud computing. Approaching services from a different starting point than ITIL, cloud computing offers a way for organizations to contract for applications, IT infrastructures or development platforms as services, for predictable monthly fees.

Certain gaps may exist between ITIL’s close attention to every detail of IT performance and cloud computing’s fundamental approach of turning this responsibility over to a third party, either to an internal organization or to a service provider.

For example, a government agency and a cloud provider have to work out how to handle key ITIL mandates such as change management and incident response. But some federal, state and local agencies are already finding ways to blend these two worlds by implementing key elements of the ITIL framework, such as service catalogs.

Any game plan for merging the best of ITIL and cloud computing begins with a working knowledge of how to identify, design, launch, maintain and improve high-value administrative and operational services.

ITIL Fills a Need

The Clinger-Cohen Act may have ushered in the era of the modern public sector IT department in 1996, but it didn't solve one of the biggest challenges: how to bring order and discipline to constantly changing and often ad-hoc IT strategies.

Subsequent federal and state legislation over the years added new pieces to the planning puzzle, including requirements for overarching enterprise architectures to break down information silos that deter government departments from sharing information and working more closely together. But in the crush of demands for new services or improvements to existing processes, government organizations still need the benefits that only a clear and versatile IT roadmap can offer. Enter ITIL.

This framework (first created decades ago by the British government) provides detailed guidance for documenting and managing each component of an IT infrastructure in a large organization. The most recent iteration of the framework, Version 3 (V3), calls for a disciplined dedication to what it refers to as service management.

Service management in the ITIL vernacular pushes an IT department to think not in terms of technology but from the perspective of the customers. These are the people in an organization who use technology-based processes for their work, such as analyzing terrorist watch lists for homeland security efforts or delivering food stamps to needy families.

A true service-management approach requires a bit of mental gymnastics for veteran hardware engineers and application specialists. In the ITIL world, performance benchmarks, network throughput and software modules aren't the first things to consider when serving an agency or organization's mission.

Instead, always top of mind are the processes that need to run and the innovations that could make them run better. In other words, don't focus on what new bells and whistles are available from the latest hardware and software, focus on how best to combine all the resources into the most effective operational process, the ITIL mantra says.

The dissection and examination of services is so important to ITIL that the authors of V3 created five volumes to describe the core concepts of a service lifecycle in detail. A service lifecycle covers everything it takes to launch and maintain an individual service.

To promote healthy lifecycles, ITIL V3 directs proponents to dedicate themselves to five building blocks: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

6 Keys to ITIL Success

- 1. PREPARE FOR COMPLEXITY.** Even proponents acknowledge that the scope and complexity of the full ITIL library can seem daunting. Before delving into the details, make sure everyone is familiar with a high-level definition of the framework and its primary goal of aligning IT and organizational goals.
- 2. START SMALL.** Organizations will start to see benefits from the ITIL framework before they adopt the full library. Develop a piecemeal approach that focuses on the biggest pain points or opportunities for improvement. For example, starting with key ITIL components such as Service Desks and Configuration Management Databases (CMDBs) can jump-start efforts to mitigate performance problems and develop a detailed understanding of the entire IT infrastructure.
- 3. PREPARE FOR CULTURE SHOCK.** ITIL requires IT personnel to revise their thinking about managing technology — and, in some cases, their work habits. Document and use each success in a gradual ITIL implementation to gain buy-in from skeptics.
- 4. BUDGET FOR TRAINING.** Training and certification classes are important pieces of the ITIL adoption process and act as stepping stones for building teams that can introduce and implement the framework throughout an organization.
- 5. GAIN EXECUTIVE COMMITMENT.** Another antidote for culture shock is a senior manager who understands the value of ITIL and regularly communicates commitment to others in the organization. To develop senior-level evangelists, some organizations send top managers to certification classes before educating those who will be closest to day-to-day ITIL activities.
- 6. SEE THE BIG PICTURE.** The management areas defined by ITIL don't exist in a vacuum. Look for crossover among related areas — incident and change management, for example — which can be the keys not only to greater efficiencies but also to finding the root causes of long-term problems.

Bring in the Clouds

But ITIL doesn't have a lock on services. There's another trend happening in the data center that's also focused on services, but instead of promoting complex blueprints, rigorous training sessions and new nomenclatures, it offers a flick-of-the-switch way to implement new operational processes.

Cloud computing, in all its various manifestations — public versus private; focused on software, infrastructures or platforms — allows government IT managers to figure out what IT component they need and sign up to have it delivered for a monthly fee, just like electricity from the power company. What about all of that IT complexity? Let the provider and its dedicated staff worry about architectures, upgrades, uptime and ongoing maintenance.

Cloud computing isn't just a hot new trend. It has some friends in high places. Vivek Kundra, the federal government's CIO, and Aneesh Chopra, its CTO, have championed the virtues of cloud computing since taking office in 2009. "Why should the government pay for and build infrastructure that is available for free?" Kundra has been quoted as saying. "In these tough economic times, the federal government must buy smarter."

Points of view such as this are fueling a surge in cloud computing across all types of organizations at all levels of government. In fact, public and private interest will spur cloud-provider revenues from \$8.7 billion in 2010 to almost \$17 billion by 2013 — a 24 percent compounded annual growth rate — according to the 451 Market Monitor, an independent IT research and analysis organization.

The rigor of ITIL and the big-picture simplicity of clouds may appear different on the surface, but their mutual focus on services provides plenty of common ground. Managed effectively, clouds can become a welcome resource for delivering the operational processes at the core of the ITIL framework. At the same time, ITIL's attention to detail offers a blueprint for agencies when negotiating and enforcing cloud service-level agreements (SLAs). And that's just the beginning.

Because each government organization has unique needs based on its existing IT investments, regulatory requirements, security concerns and other factors, ITIL offers a formal and consistent way to make the most fundamental decisions of all: which services should run in the cloud and which should remain under more traditional control.

Plus, there's another consideration. If an e-mail system or a claims processing application eventually does fall under the purview of an outside cloud provider, ITIL can help agencies maintain the high-bandwidth network connections and related resources that ensure staff members and constituents alike have the services they need.

Create a Game Plan: The 5 Steps

Agency IT managers need some dexterity to actually merge ITIL's formality within the evolving world of cloud computing. Total control is how ITIL enables IT departments to deliver reliable computing services. But that doesn't necessarily translate well in the cloud context.

For example, should agency IT managers receive a notice every time a cloud provider makes a change to the inner workings of its data center? Under most conditions, that would not be practical. The best answer is a strategy that applies ITIL rigor to cloud service contracts that spell out how change management and service disruptions go through triage, then are documented and handled.

This blending of ITIL and cloud is already under way. For example, IT service catalogs, a component described in ITIL V3 that provides a "storefront" for choosing new IT services, are up and running in federal agencies such as the General Services Administration (GSA), as well as state government agencies in North Carolina and Kentucky.

How to begin? The first step in seeing the potential of ITIL and cloud computing is to gain a working knowledge of ITIL V3 and its vision of a service lifecycle. Here's a closer look at ITIL's process for identifying, designing, launching, maintaining and improving IT services.

Step 1: Create an Overall Service Strategy

In the ITIL world, Service Strategy defines what services an organization needs, who needs them and what resources are required to create and run the services. As such, everything in the ITIL service lifecycle begins with the Service Strategy.

These overarching policies guide IT departments and program people in deciding what services to invest in and how to prioritize those investments. Agencies looking for a way to include cloud computing in the investment mix can take heart: In its description of Service Strategy, the British government's Office of Government Commerce (OGC) — the official source of ITIL guidelines and updates — already acknowledges that services are running in what are becoming commonly referred to as private and public clouds.

“The service provider may exist within an organization solely to deliver service to one specific business unit, to service multiple business units, or may operate as an external service provider serving multiple external businesses,” the ITIL group noted in its V3 update in 2007.

Service Strategy Best Practices

The overarching nature of the Service Strategy process makes it a big job that requires three distinct job titles.

Product managers take charge of creating and managing services from conception to rollout.

Operations relationship managers act as liaisons with program departments to understand service requirements and keep tabs on how well existing capabilities are fulfilling those needs. These managers also work to make sure their colleagues receive adequate IT resources to meet service demands.

The *chief sourcing officer* works with the CIO to develop a sourcing strategy for service and puts the plan into action.

But before organizations get as far as determining who’s responsible for a service, the Service Strategy walks them through a checklist of fundamental questions, including:

- What services are needed?
- Who needs them?
- How will service performance be measured?
- How will users of the services measure their value?
- How will the IT infrastructure be used to keep all services running successfully?

The list goes on, but the goal is clear: Gone are the days when IT departments found themselves reacting primarily to the ad-hoc requests from individual groups or offices for new capabilities. Instead, the Service Strategy attempts to create a game plan for defining the organization’s larger goals so the IT department can launch or even proactively recommend services to reach those goals.

The guidance also lays out three key processes that are important to Service Strategy success. The first, Financial Management, homes in on exactly what would be expected by the name: the budgeting, accounting and charging processes of the service provider, whether that’s the in-house IT department or an outsider, such as a public cloud vendor.

These processes are important components for helping the IT department and program managers quantify the financial value of the IT services themselves, as well as the underlying technologies that make the services possible, the OGC points out.

Once a mechanism for determining the financial value of services is in place, the second process, Service Portfolio Management, works to make sure the organization protects its investments. This process addresses a service’s entire lifecycle, from the conceptual phase to ongoing improvements in fully functioning production services. Components include creating an inventory of available services, validating their business cases and assigning resources to support the services.

Finally, the ITIL guidance calls for a Demand Management process. This process determines the optimum level of IT resources to support the necessary operational services.

The challenge? Over-provision the underlying resources, and the organization will incur unnecessary expenses from underutilized equipment. Under-provision the services, and users struggle with unreliable or poorly performing services, which in a public sector context could mean unemployment benefits aren’t paid on time or a first responder isn’t made aware of a new environmental hazard arising at a toxic spill site.

The ITIL literature doesn’t view Demand Management as a passive process. In addition to monitoring demand for services, it encourages IT departments to actively influence demand with, for example, off-peak pricing to mitigate spikes in demand.

Step 2: Design the Individual Services

Service Design is the second phase in ITIL’s vision of the Service Lifecycle, and it’s where the hands-on work begins for creating the high-value services identified in the Service Strategy. It’s also the stage at which organizations lay the groundwork for the underlying processes that will run the new services.

Service Design addresses how a planned service will interact with all the layers of the larger administrative and technical environments for support services, associated workflow processes and underlying IT resources. This stage is also where the IT staff identifies inherent risks to the service, ranging from security breaches to infrastructure problems that cause reliability issues.

To reach these goals, ITIL outlines five important processes. At the top of the list is Service Catalog Management. This activity ensures that a central catalog of available services is available to any authorized members of the organization who may need them.

Operations-related data flows in from the second of Service Design’s five main processes, Service Level Management. This activity organizes the discussions between the IT group and program units around service

performance. It also documents how well these service guarantees are being met.

The third process, Capacity Management, reconciles IT resources with program requirements. It does this in part by using a Capacity Management Information System, which houses relevant data for analysis and reporting. Fourth is the Availability Management process, which acts as a central clearinghouse for issues related to services uptime.

Last is the Supplier Management process. This process outlines how to gather data and assesses the performance of suppliers. As a result, it may become an important component for assuring that cloud service providers meet their SLAs. ITIL calls for organizations to create a Supplier and Contract Database (SCD) to maintain an up-to-date record of suppliers, services and contract details.

A dedicated service design manager should lead these efforts by taking the top-level responsibility for seeing that effective designs for services and processes are in place. Aiding this person are a number of specialists, including an IT designer or architect, who acts as the technology lead; an IT security lead; and managers for each of the five key processes.

Step 3: Develop Services

The Service Transition phase of the ITIL Service Lifecycle tackles the important task of actually creating or updating program services, then testing them to assure they're ready for use before finally releasing them.

As ITIL guidance notes, this requires a multipronged strategy that encompasses everything from change management to damage control when, despite an organization's best efforts, things don't go as planned.

The Change Management process within this phase seeks to implement standardized methods to make sure that when new or updated services reach production level, the organization applies consistent strategies to implement these revisions. To encourage this consistency, ITIL calls for a Configuration Management System, which acts as a central storehouse for recording change management methodologies.

Related to the Change Management process is the Service Asset and Configuration Management process, which gathers information about service-related resources throughout the organization and beyond, including resources outside of IT and from third-party service providers (outsourcers and cloud vendors).

Service Design Best Practices

A growing number of ITIL-savvy tools from commercial vendors are available to help organizations with the Service Catalog Management process that is key to Service Design success.

There are two components to the process: a service catalog that displays services and allows users to select among them, and a related technical service catalog that lists the underlying resources the IT department needs to manage and run available services.

When shopping for an electronic service catalog, look at platform compatibility to make the first cut of potential solutions. Some support only Microsoft Windows, for example. Next, choose delivery methods: Some vendors sell only on-premises applications, some offer their applications as a software-as-a-service (SaaS) model, and others give organizations a choice between the two options.

Finally, evaluate the user interface. A familiar interface will be easier to navigate for the people who will use the catalogs regularly. Support for mobile applications is becoming increasingly important for some government offices, particularly if their users value the ability to shop for services from their smartphones and tablet computers.

Other must-haves include a wide selection of templates for quickly mapping business-process workflows. Service catalog solutions should also offer customization and integration tools that make it easy for organizations to plug the application into existing enterprise management systems.

As with Change Management, ITIL specifies a Configuration Management System that serves as a dedicated asset and configuration storehouse for centralizing information about IT services and underlying resources.

Finally, the Knowledge Management process makes sure all the information gathered in the preceding two processes is readily available to people who may need the data. This is to make sure each service is providing the right level of support to the organizations' users.

Unlike other core components in the five-part Service Lifecycle, ITIL doesn't call for dedicated job titles for Service Transition. Instead, the OGC assumes that people closely involved in the associated lifecycle levels also will apply their expertise to Service Transition.

Step 4: Launch Services

After defining strategy, preparation, planning and change management, the ITIL Service Lifecycle guidance culminates with Service Operation, where organizations actually deliver their well-nurtured

services. Integral to this phase is the coordination of all the supporting software, hardware, networks and other IT infrastructure components that make a service run efficiently.

Once a new or revised service is launched, people responsible for Service Operation continue to monitor the resource for any problems. A portion of that group staffs the Service Desk, a central resource for resolving or performing a triage during breakdowns, maintaining records of events and incident reports, and acting as a point of contact for all Service Operation processes.

Service Transition Best Practices: The CMDB

Configuration Management Databases have been an important part of ITIL guidance for years. In the latest version they continue to serve a key role as the central storehouse that pulls information from across an organization to maintain an up-to-date record of services, processes and related hardware, software and networks.

CMDBs are critical in part because they benefit such a wide variety of job functions. This ranges from financial managers who slice and dice CMDB data to monitor IT costs, to the Service Desk technicians who need an overview of all IT resources to quickly resolve performance problems.

Attesting to the importance of well-functioning CMDBs, a number of solutions are now available. Here's what to look for:

- **FEDERATION:** Rather than relying on a single, hard-to-maintain database for storing all the IT resource information an organization may have, federation allows CMDB solutions to house high-level data about individual systems while storehouses associated with each system remain the source for more-detailed information. ITIL Version 3 has come out in favor of the federated approach.
- **VISUALIZATION:** The CMDB solution should offer graphical tools to help users quickly visualize the IT infrastructure and configuration data.
- **ANALYSIS:** To make use of the raw data associated with CMDBs, commercial solutions should offer analytical tools to help managers create both standard and custom reports. These can help them spot solutions to technical problems and find optimization opportunities.
- **INDUSTRY STANDARDS:** Recent industrywide standards, such as the Distributed Management Task Force's Common Information Model, have arrived to facilitate data interoperability among the applications that feed information to CMDBs.
- **INTEGRATION:** Look for interface hooks that can connect the CMDB solution with other enterprise applications for out-of-the-box integration.

ITIL takes a multipronged approach to monitoring service performance. First, there's the Event Management process, which oversees what ITIL defines as "a change of state that has significance for the IT service." This can range from something big (a breakdown in an underlying piece of hardware, for example) to something less debilitating (a prompt to perform some routine maintenance on an IT component).

When a concern rises in importance beyond an event, ITIL classifies it as an incident, which may lead to unplanned service downtime or reduced service quality. The Incident Management process kicks in to handle these occurrences, with the ultimate goal being to get services up and running quickly so as to mitigate problems for users.

ITIL best practices call for ranking the importance of incidents and the urgency of their repair, depending on the relative value of the service to overall operations. Technical support staff also stand at the ready to step in if the incident surpasses the expertise of first responders in the Incident Management process.

Related to these activities are three associated processes. The Request Fulfillment process captures requests from users seeking information, access to a service or a change to the service.

The Access Management process assigns usage privileges to make individual services available only to authorized personnel (this process also tracks users of services and updates access privileges when users change responsibilities).

The Problem Management process works to end problems that eventually lead to full-fledged incidents, with the overall aim being to break a cycle of chronic incidents. Aiding these activities is a Known Error Database, which stores solutions to incidents for future reference.

Step 5: Continuous Improvement

Continual Service Improvement, the last step in the Service Lifecycle, is arguably the most important of all. According to the ITIL Service Lifecycle, creating and launching high-value services isn't an exercise with a clear beginning, middle and end.

Instead, organizations must constantly look for ways to improve upon the services they've created. True to the highly structured and detailed character of its other guidance, ITIL doesn't just make the case for

continuous improvement, it offers prescriptions for embedding the activity into an organization's cultural identity.

Reliable data is at the heart of the Continual Service Improvement phase. The IT department should continuously collect information about the performance of services, related technologies and processes as the first step in looking for ways to boost efficiency and identify optimization possibilities.

As the OGC rightly points out, many organizations aren't hearing this idea from ITIL for the first time. Most managers intuitively know that measuring and analyzing performance for improvement opportunities is the right thing to do. But with everything else going on in a modern IT department, this concept is a little like understanding the importance of eating your vegetables: The theory is sound, but fast food is quicker when meetings run back to back.

The crush of daily activities is one reason why continuous improvement is so hard to achieve. IT industry researchers such as Gartner estimate that the vast majority of IT resources (upward of 80 percent in some cases) may be allotted to "keeping the lights on" — that is, maintaining the operations already in place. Continuous performance improvement can easily fall into that nice-to-have category, becoming a must-have only when a crisis hits that threatens the organization's core mission.

This doesn't have to be the case. ITIL offers a model for continuous improvement that can help both with in-house systems and services that government organizations move to the cloud. It organizes the action within the context of maintaining the momentum created by the overall Service Lifecycle sequence.

To do this, the ITIL model asks IT managers to compare the overall vision of the organization with its current performance levels. Any shortfalls that are exposed become prime areas of focus for improvement specialists.

In addition to offering a model for maintaining momentum, the ITIL approach outlines some processes that can further the goal of continuous improvement. The 7-Step Improvement Process includes advice for collecting hard data about performance gaps so the IT department has tangible reports to help make their case to upper management for improvements.

Service Operation Best Practices: Service Desk Solutions

It's not enough to just have a formal way of describing events and incidents that can arise in large-scale IT operations. Agencies also need a plan for addressing these issues when they're numerous and coming from a variety of sources.

In the ITIL world, the Service Desk acts as the command center for these responses, and it's one of the ITIL elements that can help government organizations transition to well-managed cloud services. Note that ITIL doesn't consider Service Desks to be synonymous with traditional help desks, which mainly act as the first point of contact when an incident arises. Service Desk personnel not only record incidents, they take action to resolve problems.

The Service Desk personnel manage incidents through four main steps:

1. TRIAGE: When an incident strikes, agencies first need to assess which services are affected, which departments or offices are feeling the pain, and how significant the problems are for the overall functioning of the organization.

Prioritizing incidents is key to helping the organization decide how to allocate resources when multiple unrelated incidents arise simultaneously. Service Desk solutions can speed decision-making by enabling organizations to create response matrixes using predefined triage criteria.

The best products prioritize incidents automatically but also give Service Desk personnel an option to override these determinations manually depending on the organization's needs and other prevailing conditions.

2. ACTION PLAN: Some incidents are unique, and their solutions require the combined efforts of technical and program personnel to find the right fixes. Other problems may be the same as or similar to previous breakdowns.

Look for Service Desk software that can match symptoms to an incident database that contains previous fixes and workarounds. This capability draws on the collective knowledge of an organization to help service personnel resolve problems and reduce service downtime.

3. ESCALATION: When unique or especially large-scale incidents arise, front-line technicians may not have ready solutions to the problem. Organizations should formalize when and how to escalate these problems to upper-level technical specialists.

4. DOCUMENTATION: Service Desk personnel should be equipped with tools for capturing fixes to new problems and entering them into a central knowledge base to ensure response times will be kept to a minimum if a comparable incident arises in the future.

An integrated Service Measurement Framework defines what information should be gathered and then goes about collecting the data. In traditional environments, ITIL followers diligently measure the performance of each IT resource. Subsequent reports show the processing times of individual servers, for example, or the data throughput rates of network switches.

For the service-management philosophy to work, IT departments need to monitor performance from the point of view of end users. The goal: to see the actual value of these services to the overall mission of the agency or organization. So in addition to data about the individual IT components, organizations should collect what ITIL calls “service metrics,” which measure end-to-end speed and availability for processes.

ITIL’s Service Reporting process then helps organizations build on their data-gathering activities with action plans designed to improve service and avoid known performance issues.

Continuous improvement may extend to ITIL itself. Already CIOs are anticipating revisions and supplementary guides to augment the last library update in 2007. Wish lists include guidance that looks beyond internal data centers with specifics about mobile applications and decentralized storehouses of applications and organizational data.

Best Practices for Continuous Improvement

The ITIL Service Lifecycle isn’t complete once a new service is launched or an existing service receives an important update. Strive for higher performance by initiating a continuous service improvement program that reflects the following values:

- **ITERATIVE:** Use the latest performance data to determine how well service levels are living up to predetermined goals.
- **FORWARD-LOOKING:** Don’t just fix existing problems; proactively look for new opportunities for performance optimization.
- **STRATEGIC:** Don’t view improvement as merely a tactical undertaking; make a commitment to constantly improving quality. That way, it becomes a strategic approach that can differentiate an organization in its ability to meet mission goals.

Revisions may also have more to say about the growing phenomenon of cloud computing beyond the “external service providers” referred to in the current ITIL volumes.

In the meantime, ITIL’s focus on services and monitoring from the end user’s perspective is becoming engrained in IT departments. ITIL V3 provides one of the best frameworks to date for deriving real value from the cloud.