

Issue Briefs are designed for practitioners with limited time and a need to know about the latest industry-based knowledge.

Improving Life Cycle Management Through IT Service Management

By **Bonnie B. Maney**
SEARCH

Introduction

Many agencies find that implementing technology is an expensive, underfunded, and uncoordinated requirement rather than an option. Public safety leaders are acutely aware of the financial impacts, as they have to budget for maintenance and support. There has been little time to analyze the business impacts these changes have on the quality, reliability, and efficiency of the organization. In short, *public safety technology requirements have outpaced information technology policy.*

As agencies have kept adding services one after the other, they have not had time to ask if the services are redundant or if a service already exists that can interface with incoming technology.

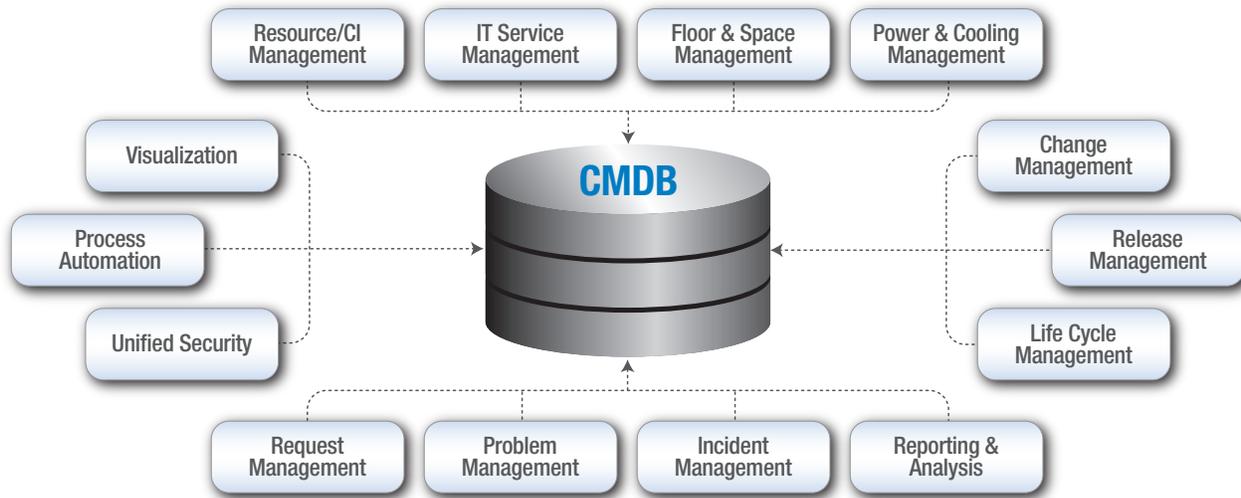
This *Issue Brief* looks at both the traditional and Information Technology Service Management (ITSM)¹ approaches to life cycle management, and highlights why it is important to

1. ITSM, as discussed in this Issue Brief, is based on the Information Technology Infrastructure Library (ITIL V3); ITSMF International, 2007. There is significantly more to ITSM than is practical to present in this brief. Rather, this brief presents a "quick-start guide" to managing the life cycles of technology services more effectively.



engage in a continual improvement process. It reveals how managing public safety services using elements of ITSM can increase service quality, reliability, and operational efficiency, resulting in cost savings. There are common themes between traditional life cycle management and ITSM; however, traditional life cycle management can be enhanced by including elements of ITSM. While the use of life cycle management as part of ITSM has been found to occur at the State and large county IT level, there is an opportunity to employ these strategies at the local level as well. This *Issue Brief* will identify numerous benefits to using configuration management, and provide information on how to get started. It will also explain the critical role life cycle management has in maintaining a configuration management database (CMDB) and the





relationship they have that results in improved information technology services (see Figure 1).

Information technology (IT) staff, public safety practitioners (especially those responsible for IT), and agencies considering consolidation are the intended audience for this *Issue Brief*.

Life Cycle Management

Life cycle management is a continual improvement process that consists of several stages that help improve the quality, reliability, and efficiency of technology services. When applied consistently, life cycle management can save an agency time and money. It is common for agencies to conduct the initial planning, purchase, and implementation of new technology, but then not to go any further.

Life cycle management is similar to planning for a building to last long after the mortgage is retired. If the foundation, walls, plumbing, and appliances are going to last, plans and budgets are required to maintain and replace and upgrade those items. As needs change, the owners may update the electrical so it is more efficient, or add rooms or accessibility features. They make renovations so the building continues to meet the changing needs of the occupants (users).

Engaging in a life cycle management methodology will enhance partnerships and planning efforts. By employing a life cycle management methodology, agencies are better able to forecast long-term funding requirements, and help set the framework to establish and maintain new or existing technology systems. Beginning with a product's life cycle in mind increases an agency's ability to accurately determine and budget project costs, and provide opportunities to successfully manage technology over the lifespan of the system.

Figure 1: Life Cycle Management role in the Configuration Management Database

Adapted from NetCracker Technology Corporation; www.NetCracker.com 2011

Approaches to Life Cycle Management

Information technology specialists know life cycle management as **service management**. Municipal planners are probably familiar with the concept of life cycle management, but public safety personnel for the most part are not. One thing is for certain: Even if they are not familiar with either term, they are probably intimately aware of what happens—what works and doesn't work—when the life cycles of the services they rely on everyday are not adequately managed.

Does it make sense to have a request to upgrade three different email servers—in the same organization? In many agencies, this is exactly what is happening.

Consider these situations:

- You enter an equipment room to find old equipment on the walls, and cables to nowhere.
- IT staff are notified of a new system installation when the vendor arrives and asks where the equipment room is so they can connect into the network.
- Responders complain regularly that their equipment is outdated or always needs repair.
- Dispatchers routinely advise that responses have not come back yet because the system is running very slowly.
- Records managers complain they have several programs with the same capabilities but they have to use different computers to get to the records they need.

- Agency executives complain about the cost of service agreements.

These situations are just a few of the possible consequences of years of adding technology without effective life cycle management and clear IT policy. The solutions range from simple to complex. In some cases, simply engaging in basic life cycle management techniques where previously there were none will produce results. Other situations are part of a bigger problem—problems that require a more comprehensive approach that exists within ITSM.

Traditional System Life Cycle Management and IT Service Management

Traditional System Life Cycle Management and Information Technology Service Management are nothing more than different roads to the same destination. The intended outcome of both approaches is continuous service/system improvement. Both have multiple phases that involve activities designed to create an environment of *continuous improvement*. A difference is the perspective of the two main groups of stakeholders—public safety practitioners and IT staff—about “what” is improved.

- **Traditional life cycle management** is the process most familiar to the public safety practitioner (see Figure 1 on page 2). It is a cyclical process focused on continual improvement of a system, such as computer-aided dispatch (CAD), records management system (RMS), 911, radio, etc. It goes beyond purchasing, installing, and operating computer systems and software applications, but it does not focus on technology development such as writing software programs. Traditional life cycle management phases include planning, acquisition, implementation, support and maintenance, refresh, and disposal of the system (see Figure 2).

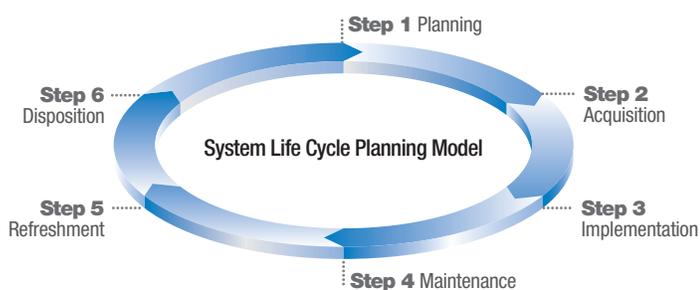


Figure 2: Phases of Traditional System Life Cycle Management (OEC)

Adapted from U.S. Department of Homeland Security Office of Emergency Communications, Emergency Communications System Life Cycle Planning Guide (Washington, D.C.), August 2011. www.safecomprogram.gov/sitecollectiondocuments/oec_system_life_cycle_planning_guide_final.pdf

This viewpoint of life cycle management looks at systems as a whole and does not delve deeper into the relationships between the systems. Nor does it focus on the efficiencies between systems. Usually the focus on these systems is primarily from an equipment and operational perspective. Is the mobile data computer (MDC) in a patrol car working today? When a button is pushed, does the radio transmit? Does information entered into CAD go to the right place?

- **IT Service Management** is a life cycle perspective of the IT practitioner. Reflected in service quality, IT Service Management is a cyclical process focused on *continual improvement over the life cycle of a service formed by the relationships between the services and the resulting operational efficiencies*. It goes beyond purchasing, installing, and operating computer systems and software applications. Like traditional life cycle management, it also does not focus on technology development such as writing software programs. The phases of ITSM include service strategy, design, transition, and operation, and are surrounded by continual service improvement (see Figure 3).

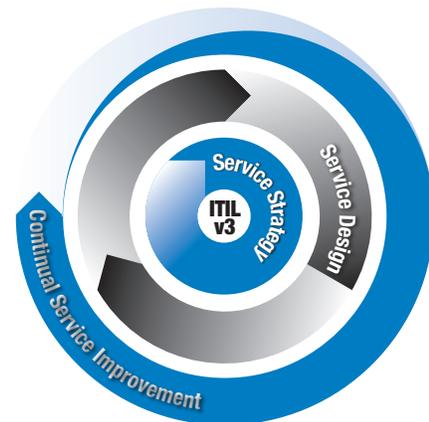


Figure 3: Phases of IT Service Management

Adapted from American Internet Services; www.americanis.net/service-architecture.

From the IT perspective, life cycle management does not focus on an individual system. Rather, it focuses on services and their relationships to each other. These relationships create reliable and efficient systems that meet the users' needs in a way the users like. In ITSM, this means a constant planning cycle of identifying needs, acting on those needs, checking to make sure that needs are met, and adjusting the plan to achieve the goal of providing effective and efficient IT services.² A continuous service cycle is concerned with adding and retiring services to maintain alignment to the business needs of the users.

2. "Guide to IT Services for Justice Agencies" is a companion white paper that discusses the principles and capabilities of ITSM for justice agencies. It is available at www.search.org.

What is a service? A service is anything used to support a business process. Services are a staple of any public safety agency today. When trying to identify a service, think of a vendor. A vendor sells a service or they support a service. Examples of common public safety services include:

- E-mail service
- File and document management services
- Local Area Network (LAN) service
- Database hosting
- Internet service
- Criminal Justice Information System (CJIS) interface
- Telephony (could be broken out into desktop and mobile telephony)
- Hosting services (could be broken out into web, server, and mainframe)
- Help desk services
- Application development
- Land mobile radio (LMR)
- Mobile Data Computers (MDC)
- CAD
- RMS
- Payroll software application

Several items from this list (computers, servers, software, interface, etc.) make services work. If a software application—such as CAD or RMS—is a service, then there are services that support the applications that are *also* services. Other services, called *shared services*, support more than one service. Leveraging such characteristics across more than one service creates efficiencies.

In the world of technology, services provide people with the functionality they need to complete some sort of public safety business process with the aid of technology instead of manually. Engaging in ITSM to manage the life cycle of IT services can help your agency or jurisdiction adapt services to rapidly changing business needs and provide for continued support of IT services.³

There will be controversy about where the continuous cycle of improvement begins, regardless of which approach to life cycle management is used. As a cycle, an end does not exist; however, life cycle management does need to start somewhere in the cycle. Unless you are starting a public safety agency from scratch, which more than likely is not the case, then the starting point within the cycle may be different for the management of each service. For new services, the life cycle based on ITSM starts with developing the service strategy.

Both traditional life cycle management and ITSM start with a *planning phase*. This phase gets stakeholders strategizing about governance and organizing the purchase, operation, maintenance, and future improvements for a service so it is reliable and efficient for users. Both methodologies require a strong foundation of governance. Through governance, decide how to manage those responsibilities. Decision-making is going to be important both during this phase and in the future. Then work through the process of identifying supporting services. Planning also includes configuration management to leverage shared services and ensure alignment of services for optimal performance. Configuration management forms a foundation for successful life cycle management; however, it is commonly forgotten in public safety IT management when a traditional life cycle management methodology is used.

Configuration Management System

This discussion started with the problem created by the rapid rate at which technology has been thrust upon public safety, and the reactive response public safety has had to meet the public's expectations. Being reactive costs money, and with the ongoing reductions to federal, state, and local funding, agencies have a renewed drive to reduce costs wherever and however possible. With a **Configuration Management System (CMS)**, time becomes available to be proactive, enabling people to prevent problems before they happen—breaking the reactive cycle. Using a CMS reaps many benefits that ultimately lead to cost savings, including improved reliability and efficiency.

A CMS is a holistic approach to planning, identifying, configuration control, status accounting, verifying, and auditing of the relationships that services have to one another. A CMS identifies and captures this information. At a very rudimentary level, a CMS is concerned with the asset; what the asset does, and the relationship each asset has with other assets and what they do. No matter what size of agency, configuration management starts with asset management; then, objectives and priorities are set based upon a level of detail in line with that agency's business needs.

There are two pieces to configuration management: setting up the CMS, and running the CMS. Set-up involves the planning and identification activities. Running configuration management involves control, status accounting, and verification and reporting.

Set-up includes creating a Service Catalog and a Configuration Management Database (CMDB). Similar to a menu in a restaurant, a Service Catalog documents the different types of configuration items (CIs). Configuration items can be any part of the service that makes delivery of that service possible. Types of CIs include business practices (entering calls

3. ITSM is based on ITIL®, which was developed in the UK to document and standardize IT processes across government.

for service) along with software applications (call-processing software), computers, servers, and others. The CMDB contains detailed information on the attributes of each CI in the Service Catalog, including its purpose and what network elements it uses. By managing the CMDB, a configuration item is associated to a business process. This allows evaluation of the business impact of any asset or CI before a change takes place.

There are two classifications of relationships: *physical or logical*. The relationships identified between services and CIs using the Service Catalog and the CMDB are what makes a CMS valuable. The relationships establish a starting point for impact assessment, which drives the overall process of configuration management in which staff identify technology needs, identify costs, and then add, modify, or remove services.

Units and departments within the same organization may be independently tracking their own services but functioning autonomously when it comes to IT policy. By bringing these separate CMDBs together under one umbrella, staff start understanding each other's needs, and recognizing redundancies and inefficiencies. Using this awareness to facilitate change translates into saved time and money, and provides a foundation for inter- and intra-agency information sharing.

For practical purposes, a CMDB is to service management as a project plan is to a project or a governance charter is to governance. The CMDB is the foundation for all of the other ITSM elements, including life cycle management (see Figure 3 on page 3).

The other ITSM tasks and processes need information from the CMDB to execute their functions, use information from the CMDB to identify a CI, or provide information to the CMDB to assess impacts and manage change. The latter, change management, is essential to successful configuration management.

Traditional life cycle management focuses on improvement of individual systems. ITSM focuses on improvement of services as a whole based on their relationships to each other.

In relationship to the CMDB, the life cycle of a CI can be split into seven stages: planned, received, tested, implemented, operational, maintenance, and archived—essentially a life cycle within the continuous service management cycle (see Figure 4).

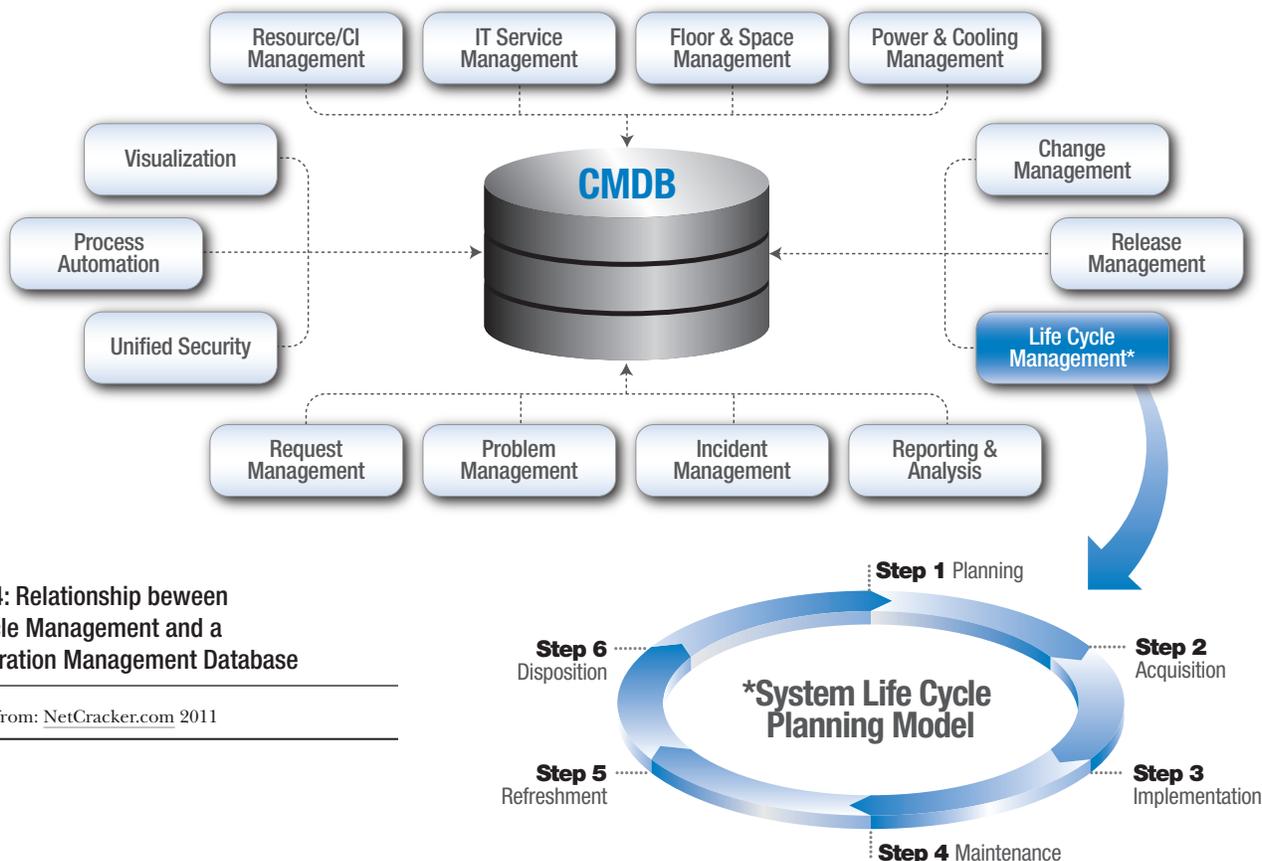


Figure 4: Relationship between Life Cycle Management and a Configuration Management Database

Adapted from: NetCracker.com 2011

Benefits of Configuration Management

- **Better support for IT asset life cycle management** – results in more precise expenditure planning, tracking and forecast maintenance, upgrade, and other costs
- **Improved IT components management** – provides access to information to deliver IT services, contract records, and service-level agreements
- **High-quality IT services** – promotes communications between agency staff and IT, which reduces errors and duplication of effort
- **More accurate problem solving** – manages CI modification and replacement
- **More rapid processing of changes** – supports impact analysis and risk assessment
- **Better control of software and hardware** – minimizes risks associated with rollouts, releases, and updates
- **Improved security** – captures information on authorized changes to CIs, protects systems from intrusion, viruses, and other security concerns
- **Better support for Availability Management and Capacity Management** – improves analysis and planning
- **A solid foundation for IT Service Continuity Management** – uses CMDB for disaster response and recovery activities

Potential Pitfalls When Implementing Configuration Management

- **Wrong scope of CI level of detail** – If the scope is too narrow, critical attributes will not be collected. If it is too broad, it will be cumbersome and difficult to manage.
- **Effect of urgent changes** – If changes will have to be made outside of normal hours, make sure a process is in place to manage them.
- **Overambitious schedules** – Draw up realistic schedules so time is included for CMS activities.
- **Management acceptance** – Configuration management is not familiar to most executives. To gain their support and commitment, people responsible for IT will likely have to sell the benefits.
- **Bypassing the process** – When rushed, people may try to bypass the CMS. At some point, disciplinary action may be necessary.
- **Right skills, wrong outlook** – The people selected need the right skills and the right outlook.

The relationship of this sub-life cycle to the overall ITSM cycle is similar to a project charter and a governance charter. A project charter ends when the project ends, but the governance charter provides guidance beyond the individual project. Likewise, a system life cycle may end but the continuous service management cycle continues beyond each system to oversee the whole.

The Importance of Understanding Services

When decision-makers understand the services they rely upon to support their agency operations, they have more information on which to base decisions. When IT staff and service providers understand how the services they provide fit into the overall business picture, they are able to better align the services they provide with an organization's unique business goals and practices. This sets the stage for delivering the functionality users need.

Public safety business practices have become so reliant on IT services that it is hard to separate the two. On the public safety side, technology implementation has taken place so rapidly that it has happened as silos rather than guided by IT standards. Adhering to standards will improve operations "if" IT staff, decision-makers, and users practice IT implementation in a systematic way that does not outpace standards and policy.

Making the CMS Happen

The key to successfully implementing a CMS is to make *gradual progress*. Like the individual who attempts to exercise 7 days a week after being sedentary for many years, if you dive headlong into the effort, odds are that the new routine will not last long. Unfortunately, the individual will likely get frustrated and give up. Start simple, and remember: *gradual progress*.

The first step to make the CMS happen is to set up governance and determine who is responsible for making this transition happen. This depends on organizational structure, as well as the reason configuration management had not been previously accomplished. Part of the responsibility of managing IT is to keep track of configuration items, but there are many reasons an organization may not have developed a CMS.⁴ The initial problem is likely the need to be reactive to the rapid introduction of technology. IT staff coming in from the public safety ranks in a "learn as you go" situation (borne out of necessity rather than design) often contribute to missed steps. Agency culture may have played a role, and staff may lack project management skills. All of these may lead to missed life cycle steps. There could also be limits on staff availability or budget for dedicated IT staff.

4. Foundations of IT Service Management, based on ITIL V3; ITSMF International 2007.

Whatever the reason, moving forward, it is critical to identify whose responsibility it is.

The second step is to create the Service Catalog. If you need to demonstrate the benefits of CMS quickly, this is a quick win. If the service is currently in use, ask the following questions about each service to help determine if it should be included in the Service Catalog. If the service is not in use, follow established policies to remove the unused components of the service to free-up valuable console and back-room real estate.⁵

- Is the service still in use?
- Does the service still meet business objectives?
- How critical is the service to the business?
- Does the business have a need to improve the service?
- Is there funding in the budget for needed improvements?

Setup a Basic CMS

- 1 Establish governance.
- 2 Create a Service Catalog.
- 3 Start simple, use templates, and one at a time, identify attributes for each service.
- 4 Organize completed templates in a paper or electronic file to create a CMDB.

Once the Service Catalog is underway, the third step is to gather descriptive information (attributes) for each CI. Start simple, with one service at a time, and capture the attributes for each CI. Large enterprise organizations may spend money on software programs and advanced Configuration Management services. However, that is probably an unnecessary expense for most agencies. The goal is to start somewhere. Use index cards, Excel, Access, Word templates,⁶ or sheets of paper—whatever is available. To facilitate this step, SEARCH has created a series of templates to help identify and capture the attributes for each CI commonly used in public safety.⁷

The information requested in the templates may initially appear daunting. Each template provides sample language for each service and CI, and is customizable to meet agency needs. The templates are easy to use by public safety practitioners new to configuration management, but comprehensive enough to establish a solid CMDB foundation. IT staff and others responsible for managing an agency's technology and information systems are logical sources to acquire the information needed. If support and maintenance is outsourced, vendors should have the information related

to their services. Financial and IT infrastructure records are additional sources. In addition to attributes of configuration items (CIs), unit managers and end users are potential sources to determine relationships with other services.

As the attributes for each service in the Service Catalog are documented, the completed information for each is organized into one CMDB. The Service Catalog and CMDB are dynamic documents that will change as the cycle of continuous service improvement revolves. At this point, the CMS is set up and the focus turns to running the CMS.

The situations presented earlier have several factors in common. Implementing a CMS that includes a Service Catalog and CMDB can lead to improvement across several areas. Unnecessary spending stops when reliability, efficiency, and quality of services are improved. After cataloging even a few services, describing attributes, and identifying the relationships, there will be measurable improvement. Moving forward, configuration management—in particular the CMDB—should be the nucleus of your IT program, and the principal source of IT information for everyone.

Conclusion

Both the traditional and ITSM approaches to life cycle management target how to keep things running in order to provide users the best IT availability. Agencies are encouraged to commit to a life cycle methodology and apply it. The benefits will be greater if that methodology involves an element of *configuration management*. Simplifying and reducing complexity means that staff will not have to remember multiple ways of doing things, and users will have a better experience using the services they rely on daily. Identifying which processes to reuse, and eliminating redundancies that clog up networks and reduce capacity, will make the technology easier to maintain and defend. This leads to increased productivity due to reduced down time and streamlined business processes.

Where an agency ends up in ITSM implementation is decided within their IT governance structure. Implementing a full-fledged ITSM process or a computerized CMS is not the right fit for every organization working to improve their life cycle management processes, as it may be overly complex and cumbersome for their actual needs.

There is much more to ITSM than can realistically be addressed here. This brief is a quick-start guide for agencies of all sizes to start thinking about life cycle management from a more holistic perspective, from identifying the IT services as part of a Services Catalog to creating a CMDB to develop a Configuration Management System as the foundation for future IT service management in your organization.

Agencies can increase service reliability, efficiency, and quality and reduce costs if they embrace life cycle management in general. Engaging in ITSM as a business practice can

5. Do IT Yourself Guides, 2011, www.itsmsolutions.com/dity.asp.

6. Software products referenced herein are registered trademarks of their respective owners.

7. The Service Catalog and CMDB templates are available for download at <http://search.org/files/pdf/TechBrief-ServiceManJusticeIT.pdf>

increase project success, as the practice becomes merged within the planning process. Using ITSM can help manage risk during the planning stages **before** IT implementation occurs rather than after, thereby inhibiting incidents and problems that previously could have resulted in project delays. Embracing the aspects of ITSM that are manageable will take life cycle management to the next level. The way to accomplish this is to start with those areas in which you can achieve successes quickly, such as configuration management—specifically a service catalog and CMDB. Use templates to start a service catalog and configuration management database. Collaborate to share services with other agencies to further increase efficiencies and cost savings.

To learn more, visit the SEARCH website at www.search.org.

Policy Development, Training, and Technical Assistance Resources

- **U.S. Department of Justice, Office of Community Oriented Policing Services (COPS Office):** The COPS Office is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, and tribal law enforcement agencies. The community policing philosophy promotes organizational strategies that support the systematic use of partnerships and problem-solving techniques to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime. The COPS Office does its work principally by sharing information and awarding grants to law enforcement agencies around the United States to hire and train community policing professionals, acquire and deploy cutting-edge crime-fighting technologies, and develop and test innovative policing strategies. See www.cops.usdoj.gov/.
- **SEARCH, The National Consortium for Justice Information and Statistics:** SEARCH offers technical assistance to local and state justice agencies to develop, manage, improve, acquire, and integrate their automated information systems. SEARCH not only works with individual justice agencies (such as a police department that is implementing a new records management system, or a court acquiring a new case management system), but also works with multidisciplinary groups of justice agencies to assist them in planning for and integrating their information systems at local, state, and regional levels. For more than 4 decades, SEARCH assistance programs have provided both on-site and in-house, no-cost technical assistance to justice agencies throughout the country. See www.search.org.

This *Issue Brief* is part of a series that SEARCH developed for the public safety/justice community in partnership with the U.S. Department of Justice, COPS Office.

Questions, comments, or feedback: Please contact SEARCH at www.search.org/about/contact/.

This project was supported by Cooperative Agreement #2007-CK-WX-K002 by the U.S. Department of Justice, Office of Community Oriented Policing Services. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

Captain Thomas W. Turner
Chairman, SEARCH

Ronald P. Hawley
Executive Director, SEARCH

Scott M. Came
Deputy Executive Director, SEARCH



COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE



U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street, N.E.
Washington, DC 20530
www.cops.usdoj.gov

© 2012 SEARCH Group, Inc. The U.S. Department of Justice reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use this publication for Federal Government purposes. This publication may be freely distributed and used for noncommercial and educational purposes.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author nor the COPS Office can vouch for their current validity.