12-2005

Leveraging ITIL to Govern AOC Information Technology

Robert V. Weaver III

LEVERAGING ITIL TO GOVERN AOC INFORMATION TECHNOLOGY

THESIS

Robert V. Weaver III, Major, USAF

AFIT/GIA/ENG/06-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GIA/ENG/60-01

LEVERAGING ITIL TO GOVERN AOC INFORMATION TECHNOLOGY

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Assurance

Robert V. Weaver III, BS

Major, USAF

December 2005

AFIT/GIA/ENG/60-01

LEVERAGING ITIL TO GOVERN AOC INFORMATION TECHNOLOGY

Robert V. Weaver III, BS

Major, USAF

Approved:

_____//Signed//_____	5 Dec 05
Dr. Robert F. Mills (Chairman)	Date
_____//Signed//_____	5 Dec 05
Maj Scott R. Graham (Member)	Date
_____//Signed//_____	5 Dec 05
Dr. Michael R. Grimaila (Member)	Date

Abstract

The Air Operations Center (AOC) is a complex system of systems that is resistant to traditional engineering controls and management strategies. The US Air Force (USAF) seeks to transform its antiquated AOC Information Technology (IT) management function into an agile enterprise capable of leveraging cutting-edge technology by aligning the AOC's infrastructure with its organizational strategies and vision. The USAF calls this effort a transformation. Private industry calls it IT Governance.

To achieve AOC IT Governance, the USAF must stop managing infrastructure *components* and start managing IT *services*. IT Service Management abstracts business processes from the technology supporting them by creating IT services. Those services resolve business process requirements and provide IT capabilities. Effective IT Service Management requires an all-powerful, centralized IT management organization focused on providing value to the enterprise through the monitoring and improvement of IT services aligned with enterprise goals and strategies.

This research will focus on the potential benefit of a service-centric collection of industry best practices known as the Information Technology Infrastructure Library (ITIL). The ITIL best practices are designed to enable the implementation of IT Service Management. The ITIL framework is a necessary step forward in the USAF's quest for IT Governance.

Acknowledgments

I would like to express sincere appreciation to my faculty advisor, Dr. Mills, for his guidance and support throughout the course of this thesis effort. His insight and experience was appreciated. I would, also, like to thank my advisors, Maj Scott Graham and Dr. Michael Grimaila, for the support, motivation and latitude provided to me in this endeavor. This research is based on the innovative ideas of Jeff Stanley, a fellow AFIT graduate student. I appreciate the hours he spent with me explaining the lack of a service-centric mentality in the US Air Force. Thank you all.

Robert V. Weaver III

Table of Contents

Page

List of Figures

Page

List of Tables

Page

LEVERAGING ITIL TO GOVERN AOC INFORMATION TECHNOLOGY

I. Introduction

1.1 Background

The US Air Force's (USAF) concept of operations relies heavily on centralized Command and Control (C2) capabilities and decentralized execution. This concept of C2 can be broken down into three main components: sensing, deciding, and executing mission capabilities. These three components of C2 happen inside a specialized command post known as the Air Operations Center (AOC). The AOC is a robust communications system used to receive and transmit vast amounts of accurate and timely information both vertically along the USAF chain of command and horizontally among peer organizations like Special Operations or Navy Command Posts.

USAF AOCs have evolved from simple command posts to become an intricate and complex system of systems. Each AOC differs significantly from each other due to the absence of a centralized AOC infrastructure management function to standardize them. The AOCs changed and scaled to accommodate the unique aspects of their theaters and tasking. The rapid pace of changing information technology (IT) has made it increasingly difficult to successfully incorporate new technology with AOC legacy systems and still provide reliable, integrated C2 capabilities to USAF commanders. The scale, scope, and complexity of the AOC have made the management of its infrastructure

resistant to conventional engineering definitions and control measures. [41]

1.2 Transformation

The Clinger-Cohen Act and the Information Technology Management Reform Act (ITMRA) are pressuring Department of Defense (DOD) agencies to achieve joint integration and efficient technology life cycles by improving their technology acquisition processes. DOD organizations must design and implement IT acquisitions and management processes that minimize risks while maximizing the value of IT. DOD IT acquisitions will now be evaluated using stringent metrics to ensure they deliver value throughout their life cycle. [9]

USAF C2 technology is under tremendous scrutiny due to its increasing cost and inherent vulnerabilities. General John P. Jumper, former USAF Chief of Staff, has demanded more integration, functionality, and performance at less cost. In fact, he ultimately wants to reduce the AOC infrastructure footprint to the point an entire AOC could be implemented using airmen with laptops. [36] This radical transition is not possible with current AOC IT management processes and procedures.

Therefore, the USAF seeks a 'transformation' in the way it acquires and manages technology. The USAF defines transformation as a "process by which the military achieves and maintains asymmetric advantages through changes in operational concepts, organizational structure, and technologies that significantly improve our warfighting capabilities or ability to meet the demands of a changing security environment." [31] General Jumper observed "Transformation expands the way we, as airmen think. It transcends just designing new systems. It is the integration of all our capabilities, old and

new, that elevates our operational effectiveness to new heights." [31] His comments about transformation capture the essence of what the private sector calls IT Governance.

IT Governance is the successful *alignment* of IT acquisition processes with the organization's strategic goals. It is the leveraging of information technology to support today's operations and to position the organization for dominance in the future. For the USAF, IT Governance is the key to transforming a reactionary, best-effort management organization into an effective joint integrator of cutting-edge technology. However, figure 1.1 shows IT governance requires a shift from managing technology *components* (Information Technology Infrastructure Management - ITIM) to managing *services* (Information Technology Service Management - ITSM). This intermediate step is difficult for organizations but it is necessary to achieve the transformation the USAF wants.

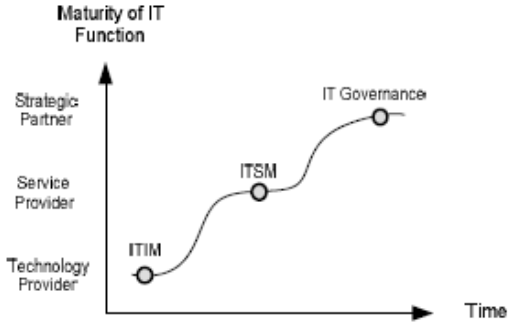

Figure 1.1 Steps to Governance [49]

At the operational level, the C2 infrastructure of the AOC is a natural focal point for IT governance. The USAF is attempting to overhaul its AOC design, acquisition and management functions. It seeks an IT acquisition strategy that relies on collaborative

requirements development, seamless requirements verification, and focused technological solutions to those requirements. [24: 2] However, AOC IT systems have enormous inertia and complexity, resisting efforts to control or modify them.

1.3 Complex System

The AOC is defined in several papers as a *complex system*. [5, 6, 41, 42, 51] Its infrastructure currently incorporates over 80 independent systems that must work together to produce functionality. Most of these systems do not share a common development concept or history. They are controlled by independent management bodies and budgets. Many of these systems have multiple DOD customers and government clients besides the AOC. More importantly, these independent systems evolve at different rates. The lack of central AOC control and influence over its subcomponents results in a reactionary relationship between AOC technology providers. [41:3]

The behavior of a complex system, like the AOC, is different from that of well-bounded single-owner systems like a submarine or aircraft. The independent elements of a complex system interact in ways that produce unpredictable behaviors. The collaborative behavior of the AOC infrastructure has proven difficult to predict when changing one of the sub-elements within it. Often the only way to understand the behavior of a complex system is to observe its behavior in response to a change in its elements. [51]

By their very nature, complex systems defy attempts to regulate and control them. Christopher Alexander noted that attempts to gain ‘total design’ control over a complex system tends to create unpredictable effects. [1:238] The more control you exert on a

complex system using traditional engineering methods, the more it resists those controls. This is true for all complex systems like governments, economies, and the AOC weapon system. While inputs can be made to stimulate a complex system, predicting specific resultant behavior is difficult or impossible.

1.4 Weapon System Integrator

The USAF recently attempted to apply strict configuration controls and standardization to the AOC infrastructure using traditional systems engineering methods. The attempts met with political, financial, and operational resistance due to the distributed and complex evolutionary nature of the AOC infrastructure. [41]

The USAF lacks the manpower, funding, and expertise to accomplish the desired transformation and integration of a complex system like the AOC. It plans to outsource the 'transformation' of the AOC infrastructure to a private contractor known as a Weapon System Integrator (WSI). While the USAF will retain the final approval authority, the WSI will research, integrate, test, deploy and maintain AOC systems in the future. [21:15]

The proposal to hire the WSI contains numerous requirements concerning the standardization, flexibility, and modernization of the AOC. Specifically the WSI will be asked to integrate, standardize, field and sustain the AOC Weapon System (WS) using a spirally developed baseline. The WSI will take over all key engineering roles while the Government retains oversight. [21:18]

The USAF is asking the WSI to resolve the AOC infrastructure management problem. However, a WSI contractor will have no more influence on the AOC than the

current AOC infrastructure management system. The WSI efforts will meet the resistance to control currently experienced by the USAF unless the AOC IT can be governed. The three factors needed to create AOC IT governance are…

1) Focused USAF leadership *empowerment.*

2) The establishment of a *single centralized enforcement authority*.

3) The adoption of an *IT Service Management* orientation.

1.5 AOC IT Governance

Managing rapid technological changes in a complex AOC weapon system is not possible using the decentralized management style of the past or the semi-centralized distributed management practices in place today. The AOC of the future requires a centralized management body with a focus on user requirements and IT services. The IT management body must be empowered by DOD and USAF leadership to enforce policies on subordinate AOC organizations. It must have the clout to leverage cooperation from peer organizations to provide services necessary to support critical AOC operations. A centralized, service-centric management organization able to enforce policies represents a significant change in the way the USAF thinks about the value, use, and function of its information technology. The adoption of a Service Management framework is a necessary step towards the IT Governance required for a USAF transformation into an agile IT management organization.

IT Governance through the application of a Service Management framework has been used successfully by large complex organizations like Proctor and Gamble, the US Navy, Johnson and Johnson, IBM, Caterpillar, Boeing, and the Internal Revenue Service.

[49:10] These organizations faced IT management challenges similar to those of the AOC and were able to use a service-centric framework to align their large complex infrastructures with corporate strategies and create agile IT management organizations. IT Governance has produced lower costs and higher profits for civilian companies. However, for the USAF, IT Governance represents the ability to control the rapid integration of new AOC technology enabling the warfighter to accomplish his mission.

The Information Technology Infrastructure Library (ITIL) is a collection of Service Management best practices. It creates and manages services to resolve business process requirements and provide capabilities. ITIL Service Management will not solve all the systems engineering challenges facing the AOC. However, it will lay a solid foundation for the agile technology acquisition required to meet the needs of the AOC warfighter. Under an ITIL framework, the AOC infrastructure requirements align with the needs of the AOC customer. Those needs will be resolved with IT services. The ITIL is a Service Management framework required to effect an IT governance transformation within the AOC infrastructure.

1.6 Problem Statement

Achieve an AOC IT management governance transformation through the effective application of ITIL Service Management principles.

1.7 Hypothesis

The USAF is seeking a 'transformation' by aligning the AOC IT infrastructure with its strategic vision and goals. This research will demonstrate the need for

- Focused USAF leadership *empowerment.*
- The establishment of a *single centralized enforcement authority*.
- The adoption of an *IT Service Management* orientation.

1.8 Research Objectives

- Explore ITIL Service and Infrastructure Management principles
- Understand current USAF AOC IT management processes/constraints
- Propose specific ITIL solutions to the AOC IT management problem

1.9 Methodology

This thesis culminates eighteen months of research on the AOC management process and the ITIL framework. Information on these topics was obtained through Air Force Institute of Technology (AFIT) classes, ITIL publications, DOD documents and interviews with AOC IT personnel at the System Program Office. AFIT sponsored a site visit to the AFC2ISR Transformation Center to interview personnel involved with the AOC IT management process and see the test environment for CAOC-X. Other sources included an ITIL seminar and numerous Information Management publications.

1.10 Assumptions/Limitations

This paper targets an audience with influence on the AOC Weapon System IT management organization and processes. It assumes a basic knowledge of the AOC

purpose and function. Fundamental aspects of current AOC IT management practices will be investigated. ITIL Service Management principles will be explained along with their potential application to the AOC IT management process.

This research concerns AOC IT management; however, the AOC is not an island. It is a system of systems in a constant state of change and a subcomponent of a larger DOD command and control (C2) system. This research is limited to those areas within the AOC IT management team's influence.

1.11 Roadmap

Chapter two defines and describes various aspects of the ITIL framework. Chapter three presents a brief history of the AOC and the current state of AOC IT management. Chapter four applies ITIL Service Management concepts to a centralized, empowered AOC IT management organization. Chapter five provides a summary of the research and proposes areas for future research.

II. Information Technology Infrastructure Library (ITIL)

2.1 Overview

This chapter provides an overview of the Information Technology Infrastructure Library (ITIL) and its application within a large, technology-dependent organization. While the entire ITIL framework will be described, this chapter will focus on the specific components that enable IT Service Management. The key interactions between ITIL components will be explained to demonstrate how they create and maintain a stable, productive and service-oriented IT organization.

2.2 ITIL Background

The Information Technology Infrastructure Library (ITIL) started as a collection of IT management concepts, processes, and methods. It was originally developed by the IT provider for the British Government in an effort to reduce costs and improve services. The United Kingdom's Office of Government Commerce (OGC) published the ITIL as a collection of best practices later made available to non-government organizations. All current Service Management frameworks use ITIL as their foundation. ITIL is recognized around the world as the default standard in applying a service-centric management style.

Many of the ITIL best practices evolved after years of trial and error in the IT organizations supporting a large number of users. The ITIL framework has become the industry standard to guide IT departments around the world in providing improved IT management within their respective organization through the use of Service

Management.

ITIL has been revised several times since its creation and will continue to evolve due to the efforts of a large number of companies and support groups around the world. The IT Service Management Forum (itSMF) and other similar organizations provide ITIL education and consultation. An IT Service Management Specification, BS 15000-1:2000, is progressing toward becoming an International (ISO) standard for Service Management. [48:34] ITIL is here to stay and continues to gain recognition and support from large technology-dependent organizations using it to achieve IT Governance.

2.3 ITIL's Service Culture

ITIL provides common ground between business leaders and technically-skilled IT engineers to facilitate effective communication. This common ground is built on the concept of *services*. A business user typically thinks about his job in terms of business processes. These are the finite tasks he does repeatedly to accomplish an objective. The IT staff of the company typically thinks in terms of technology components (i.e. routers, servers, software packages, etc.). It is extremely difficult for these two groups to communicate clearly about achieving common goals because they do not share each others paradigm. The ITIL concept of services helps bridge the communication gap between business *consumers* of IT and the technical support *providers* of IT.

ITIL provides both the consumer and provider of IT services a common language and understanding upon which to build mutual goals. ITIL documents IT user expectations and IT provider capabilities in contracts used to specify the quality and quantity of IT services. ITIL educates the IT staff by exposing them to the parent

business' goals and strategies. It helps the IT staff understand the contribution they are making and instills in them a customer service mentality. ITIL helps the business leaders understand the IT infrastructure by abstracting away the technology and presenting the company's IT capability in terms of services.

The term *service* is defined by ITIL as "one or more IT systems which enable a business process." [39] ITIL defines a business process as a finite function of the business that uses IT to accomplish its objective. The business process resolves a business objective. An ITIL service uses technology to accomplish the business objective. The military would describe its business processes as *activities or functions*. Military *functions* support military *capabilities* or areas of expertise. Those functions have quantity and quality requirements. Therefore, in a military organization *IT services* would resolve *military function requirements* and provide a *military capability*.

ITIL teaches that each IT service has an intrinsic value to the organization. However, organizations rarely think in terms of services. An AOC Commander knows the efficient generation of an accurate target list is important to his operations. But what is it worth? What is the value of that target list? ITIL creates a service by identifying all of the technology required to generate a target list. It can now attach a dollar figure to the creation and maintenance of the target generation service. Now the AOC Commander will look at the target list as a product of a service with a specific value to his organization.

As an example, when an AOC commander looks at the AOC infrastructure he only sees computer components. If asked about the value of a Cisco router he will only

see its purchase price. If he was told that it enabled his target list generation process he would see it in a new light. That same router would now be seen as a contributor to one of the AOC commander's services.

Abstracting technological components into the services they provide is fundamental to IT Service Management. IT Service Management helps infrastructure users and providers learn to think in terms of the IT service financial and technological limitations instead of focusing on the technological component limitations.

ITIL defines the *customer* as the consumer of IT services and *users* as the personnel that actually interact with the services. The *customer* is the person paying for the IT services and who obtains value from them. He typically establishes the requirements for the systems. The *user* is the person that uses the IT services to do his job (i.e. hands on the keyboard). [44] These customers or users could be outside the company, however, typically these personnel are fellow company employees working in finance, shipping or acquisitions.

In an AOC, the customer would be the USAF commander of the AOC and the users would be his staff. The supplier of IT services is normally a company's IT department. The supplier of AOC IT would be the local personnel maintaining the system at the AOC site and the hundreds of system engineers and managers distributed across several offices at Langley and Hanscom AFB.

2.4 The ITIL Framework

Most companies struggle with implementing ITIL because they think it is IT Management in a box. The ITIL is a *framework* meaning it does not recommend specific

vendor hardware or software solutions. Instead, it provides guidance on how to implement repeatable and consistent processes designed to eliminate human error caused by trying to solve IT problems dynamically (i.e. putting out IT fires). It was designed to help an IT organization move from a reactive, best-effort methodology to a measured, customer-oriented management of IT resources. ITIL promises effective IT Service and Infrastructure Management. It requires a significant shift in the way an organization views IT Management. ITIL emphasizes its motto "Adopt and Adapt". It is not meant to be an IT management solution; it is a service-centered methodology used to provide IT solutions tailored to resolve customer needs.

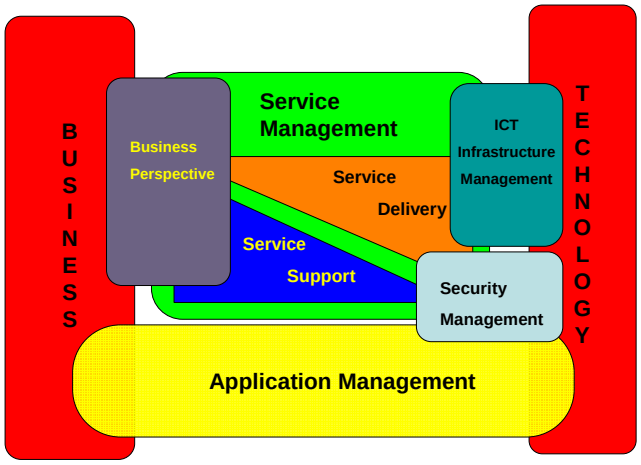

Figure 2.1. ITIL Framework [48]

ITIL is divided into five elements: *Business Perspective, Security Management, Application Management, Infrastructure Management, and Service Management.* These elements interact to provide an integrated and responsive IT service management organization driven by the business requirements of its users.

The graphic depicting the ITIL framework in figure 2.1 helps demonstrate the use of Service Management to abstract the technology from the business. Note that the Business Perspective overlaps both the Service Management and Business processes. This is because Business Perspective bridges the gap between the Service Managers and the organization leadership. Infrastructure Management overlaps the Service Management and the Technology processes. Infrastructure Management is designed to allow the Service Managers to interface with the maintenance and management of the technology components. The concept of separating or abstracting the technology from the business processes is powerful in terms of redefining the value of information technology within an organization. [48:10]

Application Management is a set of processes that deal with the development of software solutions designed to meet company business requirements. It aligns product capabilities with the needs of the company throughout the acquisition life cycle. This ITIL component helps achieve maximum value from applications built or bought by the company. [48:10]

The Business Perspective is the education and indoctrination of IT Service Management personnel. They are brought into the company's strategic planning functions as a partner and asked to contribute value to the business. This helps establish IT service value and builds collaboration within the company.

Obtaining and maintaining leadership empowerment of ITIL-based management practices is essential to effective ITIL implementation. It requires ITIL indoctrination at all levels of the organization. Clear communication between the IT management and the

company's leadership is required to create a *service culture*. The leadership must empower the IT organization to implement and enforce its policies designed to align the IT efforts of the company with the company's business needs.

Likewise, the Business Perspective requires IT management and support personnel to understand their operational and strategic role in helping the organization achieve its goals. The IT staff must be committed to providing IT services that empower the organization in obtaining its goals today and position the organization for success in the future. They must be motivated to provide the highest levels of customer service.

Security Management examines the risks and vulnerabilities of the IT services. It manages the confidentiality, integrity, and availability of the data and information utilized to provide IT services. Security Management develops response plans to mitigate service-based security risks and handle security incidents.

Infrastructure Management is the implementation of IT services on the organization's infrastructure. Most of ITIL is dedicated to the management of services rather than technologies. Infrastructure Management is oriented toward the technology required to provide the services. It is divided into four main sections: Planning, Deployment, Tech Support, and Operations. Infrastructure Management identifies the steps necessary to plan, test, install, deploy, operate, and optimize a service on a specific company infrastructure.

ITIL Service Management is divided into Service Support and Service Delivery. Service Support is the collection of processes enabling the infrastructure to *support* services. Service Delivery processes identify and monitor the *delivery* of services to the

end user. The combination of Service Support and Delivery capture the heart of ITIL Service Management. Most companies concentrate on these core processes as they adopt and adapt ITIL principles. The Service Management concepts of service-centric management, the Business Process, Service Delivery and Service Support are the focus of remainder of this chapter.

2.5 Service-centric Management

Progress towards IT Governance starts with identifying, monitoring and improving IT services. ITIL Service Management is designed to accomplish this progress. It is based on clearly understanding the IT-dependent business processes and being able to map IT services to those processes. ITIL is unique in the way it organizes around services instead of the technology. "The ITIL framework supports defining services in a way that is distinct from the technology that underpins them, allowing flexibility in what technology components are used to support and deliver the service." [52:1]

In a service-centric organization, architectures and platforms no longer define how one will do his job. The customer and user present their needs to an IT partner who agrees to provide IT services to meet those needs. These needs or requirements are captured in a contract expressing the user requirements and the service solution to those requirements in terms of quality and quantity.

The nature of the physical technical solution required to implement the service solution may change repeatedly without affecting the quality of the service provided. Requirements, capabilities, and corresponding IT services within an organization are

much more stable and predictable than the underlying technology used to provide them. This stability is what lends ITIL Service Management processes to an AOC application.

In the case of the AOC, a military requirement might be producing a list of 150 targets within two hours. The IT service resolving that requirement would capture all the necessary personnel and IT system interactions required to produce the target list. The target list production service would have measurable levels of quality associated with it (i.e. time constraints, accuracy, integrity, reliability, etc.). These measurable qualities or metrics are reviewed periodically ensuring that the service is provided at a level agreeable to the user and sustainable by the provider. The IT organization assumes the responsibility of providing that level of service to the customer. The technical solution is abstracted by the service contract. The technical implementation of the service may utilize a seamless interface into a satellite imagery system or access to stored screen shots of Predator video. As long as the customer/user is happy with the service and the contracted service levels are met, no attention is paid to the physical technology supporting his requirements.

The *stability* of the ITIL service-centric framework allows the IT organization the *agility* to demonstrate critical contributions to business requirements achieving strategic business goals. This is because the customer's business process requirements and their accompanying *services* are less transient than the technological *components* used to provide the services. The focus on services is more stabile than a focus on the technology that supplies that service. New technology is incorporated into the infrastructure because it supports a customer/user requirement for a service not simply because it is available.

Every change to the infrastructure is deliberate and necessary to provide customer support. The service-centric philosophy allows levels of efficiency, reliability, and agility that are unattainable under a technology-centric IT organization.

2.6 Business Processes

ITIL Service Management is process-oriented, meaning that the first step to implementing ITIL is to identify the business processes it will support. ITIL identifies a business process as a logically related series of activities conducted to accomplish a defined objective. [44] Most business processes in technology-dependent organizations, like the AOC, use IT.

ITIL Service Management requires that all IT business process system requirements then be translated into IT services. This includes all of the people and activities accomplished when performing a business process. The people associated with a process are the users/customers that will use the IT services provided to support the process.

Previous inter-company boundaries often interfere with properly identifying the people associated with a specific process. Users/customers from different offices often work together to perform activities or functions. It is important to ignore the inter-company structures or office assignments when identifying all the activities people that implement a specific process.

An AOC example will help illustrate this concept. The AOC has numerous business processes dependent upon IT. Most of these business processes are accomplished by the efforts of personnel from different offices working together to create

a product needed by others in the organization. One AOC process titled "Produce and disseminate the Air Tasking Order (ATO)" requires cooperation from several different teams and systems within the AOC to generate and distribute an ATO.

ITIL Service Management organizes its efforts around the business processes and the associated personnel. It ignores preexisting organizational divisions when it isolates a business process. Service Management identifies the needs of those business processes and provides effective and sustainable IT solutions to resolve them. Service Management is divided into Service Delivery and Service Support.

2.7 Service Delivery

Service Delivery is the first of the two ITIL Service Management areas and focuses on identifying and providing IT services to customers. It is an essential part of aligning IT services with organizational strategies and vision. Service Delivery is specifically concerned with discovering, predicting and documenting the customer's IT needs. It is sub-divided into five areas: *Service Level Management, Capacity Management, Financial Management, Availability Management and IT Continuity*.

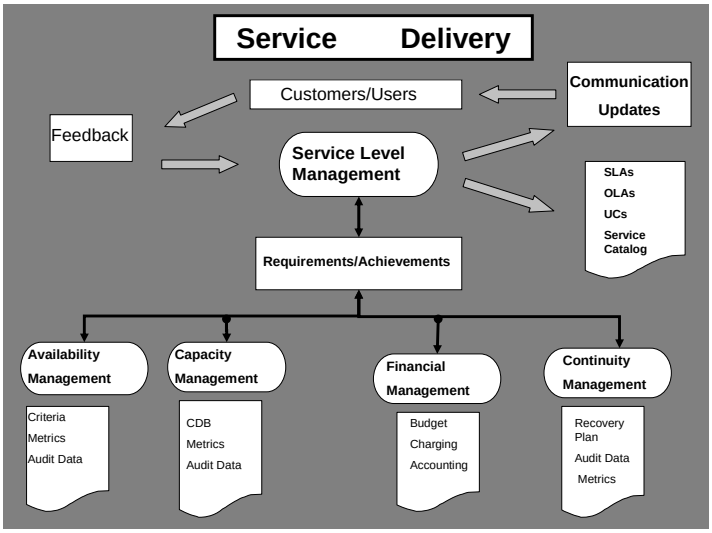

Figure 2.2. Service Delivery [48]

2.7.1 Service Level Management

Effective Service Level Management establishes a mutual understanding between the consumer and provider of IT in terms of quantity and quality. It documents the user's service expectations in clear unambiguous terms. It also documents the capabilities of the IT providers to supply that service. Service Level Management ensures the continual identification, monitoring and reviewing of the documented levels of IT services as required by the organization. [2:2] The business process requirements and IT service solutions are captured in written contracts called Service Level Agreements (SLA), Operational Level Agreements (OLA), or Underpinning Contracts (UC).

These contracts describe the customer's IT service requirements and the corresponding IT services in clear language used for planning, monitoring and reporting the level of service provided to the customer. The user/customer gives feedback to the Service Level Management staff to establish customer satisfaction levels. Customer

satisfaction surveys are often used by ITIL companies to accomplish this function. The goal of Service Level Management is to generate a constant cycle of improving IT services by repeatedly stimulating agreement and collaboration between the supplier and consumer of the IT services. The SLAs, OLAs, and UCs document this agreement and collaboration.

ITIL describes an SLA as a written agreement between an IT Service Provider and the IT Customer(s). It defines the key service targets and responsibilities of both parties. [45:28] Service Level Management examines metrics to identify a breach of promised service levels. These service levels are enforced using an internal economy between the users and providers of IT services. If a breach is identified, the SLA penalties are imposed by ITIL's Financial Management function. The IT Service Management organization works with other ITIL's Incident Management to restore the substandard service to specified SLA levels. Most companies enforce breached service target levels with direct financial penalties levied against the IT provider (i.e. a user discount for the affected service). [2:3] This provides an assurance to the customer that the IT service provider is motivated to supply the level of service agreed upon.

Customers typically pay for each IT service provided based on its value. The value of a service is calculated from the cumulative costs required to provide the technical solution to the customer requirements. These costs include the purchase, installation, and maintenance of the technology required to meet the SLA service level targets. Software licenses, hardware warrantees, and contractor fees are included in the

costs used to determine a service's value. That value can be expressed in terms of monthly costs which are passed down to the user as a bill for the service.

For example, a specific service guarantees 99% availability for a certain printer. If that level of availability is not met, the customer is compensated with a 30% discount for the services using that printer. The internal economy financial penalty highlights the service level breach and pressures the IT staff to respond rapidly to restore service levels based on customer feedback. If implemented properly, the penalties stimulate the IT organization to resolve the problem. Positive incentives could be applied in the same manner.

Identifying the business process owner and the owner of the corresponding IT service is essential to managing IT services because these parties establish the SLA. This identification process helps initiate and sustain productive dialog between the people that must work together to provide and consume an IT service. The process owner understands the business requirements. The owner of the IT service understands the service expectations and the technology required to support it. The IT service owner becomes accountable for providing the IT service solution and is financially motivated to solve problems associated with his particular IT service.

ITIL emphasizes that the SLA serves as a treaty between partners rather than a lawsuit between enemies. The idea is to clearly document both the customer expectations and the IT provider capabilities in an effort to provide a necessary service. The SLA is modified through a controlled and equitable process if the IT service supplier or consumer perceives additional needs or limitations.

An OLA is a sub-component of an SLA. It breaks the SLA down into atomic (indivisible) activities required to provide service at the specified level. Normally, the OLA is internal to the IT department of an organization. It tasks individual sub-departments with the specific measurable tasks that provide the services described in the SLA. The OLA tasks should use metrics similar to the SLAs that provide OLA performance feedback for IT service managers.

For example, an SLA may state that printers for an AOC target generation service must be serviceable within thirty minutes of a failure. The related OLA at the Service Desk may state they have five minutes to contact service personnel directing them to respond to the problem. An additional OLA in the technical service department would specify that the service technicians must have a replacement printer and ink cartridge on hand and that they be able to deliver these items and configure the printer within fifteen minutes of notification. Thus the combination of OLAs provides the IT Department with the capability to meet the overarching printer service level agreement requirement of thirty minutes to restore the printer required by the AOC service.

Underpinning Contracts (UCs) are similar to OLAs except they define the duties of an external supplier of IT services. This applies to large complex systems that outsource IT requirements. In the printer example above, suppose the company IT Department contracted out its printer services to an external printer business. The UC documents the same time constraints as part of the contract between the organizations IT Department and the external printer business in clear and measurable terms. Failure to meet the service levels results in financial penalties or breach of contract.

Effective management of SLAs and OLAs prevent a “blame culture” because the expectation and capabilities of both the supplier and consumer of IT services are clearly documented. The identification of process and IT service owners is critical. Numerous ITIL implementations have failed miserably due to a lack of ownership of either the process or the IT service.

ITIL recommends the creation of a Service Catalog. The catalog lists the services available on the IT infrastructure. This provides a good starting point for new customers by providing an index of available services. The catalog serves as a good place to track the value of associated services as well (i.e. cumulative costs).

Service Level Management measures IT service performance by tracking relevant metrics and comparing them to Service Level Agreement targets. These results are reported to IT and organization management as feedback on the company’s investment in IT services. This feedback can either validate outstanding IT service or condemn lacking performance. The desired end state is a clear understanding of customer's business needs vetted against the capabilities and limitations of the IT providers.

2.7.2 Financial Management

Financial Management establishes a micro-economy within the organization to allow an internal IT department to operate as a separate business. This business within a business facilitates an understanding of the true value of IT services. Understanding IT service value is essential to the effective transformation of IT component management into IT governance.

ITIL Financial Management determines the cost and return on IT investments in terms of *services* instead of individual infrastructure *components*. Most IT organizations budget for components. ITIL Financial Management budgets for services. They must work closely with other financial processes in the organization to develop IT budgets and track the true costs of IT services within the organization. ITIL divides Financial Management into three sub-categories: IT Accounting, Budgeting, and Charging. [45:61]

Budgeting is the prediction of money required to provide specific IT services for a specified period of time. Typical IT organizations budget for hardware, software, personnel, infrastructure (i.e. facilities, utilities, network connections, etc). However, ITIL Financial Management translates the costs of the individual hardware and software components into a cost for a service. Financial Management uses a Total Cost of Ownership (TCO) mentality when establishing IT service value. TCO incorporates the initial purchase price along with testing, deployment, maintenance, upgrade, and disposal costs for all of the components used to provide a service. [45:86]

IT Accounting is the ability to document the money spent on IT services. According to Microsoft ITIL documentation, "it is impossible to quantify IT value without the ability to equate services with the costs associated with them." [40:4] Accounting should track the cost of a specific service against the IT budget and provide prioritization for future investment. Accurate accounting provides data for a Return-On-Investment analysis in terms of stable services. This analysis allows management to understand value derived from IT investments in terms of business requirements and IT

services. This helps bridge the gap between corporate leadership and IT service providers in identifying and prioritizing changes in the IT infrastructure.

Budgeting by services motivates the business to be cost conscious as it incorporates new technology. The organization can now look at IT expenditures in terms of services provided and not individual components like printers and servers. The service-based budgeting process is more intuitive for organization leaders. A service-oriented budget reduces the risk of over-spending on impressive technology; ensuring necessary funds are available for required service-related expenses.

Charging is the process of billing customers for specific services. It forces the organization to curb its appetite for more IT capability without paying for it. Charging consumers for services highlights inefficiencies by documenting the costs of the IT services used by the organization. IT providers are constantly trying to resolve IT services with more efficient and more capable technology. If a customer wants additional functionality in a service, they must modify the SLAs service expectations. The IT service provider must find technology capable of meeting the higher expectation. The IT provider will increase the cost of the service to pay for the new technology required to increase the functionality. Charging keeps the customer focused on business requirements instead of new technologies.

Charging helps focus the IT provider as well. Financial penalties associated with service level breaches put pressure on IT service staff to maintain excellent customer service. Their ability to deliver services directly impacts the money they can charge for a service. The internal economy can be a powerful motivator if implemented properly.

Adding ITIL Financial Management practices may seem like excessive overhead. However, the purpose of this important aspect of ITIL is to highlight the value of IT *services* instead of the technology *components* that supports them. This best practice forces all parts of an organization to prioritize their IT service needs. The internal economy created by ITIL Financial Management promotes efficiency and proper resource prioritization based on stable business requirements.

2.7.3 Capacity Management

Capacity Management ensures there are adequate IT infrastructure resources to meet the customer's service needs today and in the future. This ITIL function strives to understand a business process requirement eliminating the possibility that the current and future IT service implementations will exceed infrastructure *capacity*.

Capacity Management endeavors to strike a balance between the economy of having just enough IT service related capability and shortfalls that force panic purchases to enable critical IT service functionality during peak usage. [35:145] Providing the right IT resources at the right cost and at the right time achieves the correct balance. This capability requires an intimate knowledge of organization IT service need priorities and infrastructure requirements.

Measuring resource utilization and capacity in terms of services separates the idea of Capacity Management from other forms of network monitoring and management. ITIL's Capacity Management is divided into three disciplines: Business Capacity Management, Service Management and Resource Capacity Management. Each area

contributes knowledge to a Capacity Management Database (CDB) used for analyzing infrastructure usage and predicting future capacity needs. [45:131]

Business Capacity Management tracks the business' expansion plans and changes to IT service implementations to ensure the IT department understands the role IT will play in meeting service needs and expectations of the organization's users. Business Capacity Management must advise company leaders and infrastructure managers on resource consumption in terms of services and the potential impact changes to business processes or the infrastructure will have on those services.

Service Capacity Management focuses on end-to-end services to understand exactly what software and hardware is used by a service as well as the maximum number of users the service can support. Resource Capacity Management is similar except that it focuses on the throughput of an individual component of the infrastructure like a router or a server.

The three sub-components of Capacity Management work together to monitor, analyze, tune and recommend changes to the infrastructure to meet the business demands. Monitoring is accomplished using automated sensors throughout the infrastructure to collect utilization information and report that data to the CDB. The CDB data is analyzed to predict shortfalls in capacity. The CDB will eventually contain a usage history capable of identifying peak and low usage periods. Capacity Management identifies services that over or underutilize resources in the infrastructure. Some services can be rerouted to balance the load across the entire system. Metrics and saturation tests establish "redline" thresholds that help IT organizations determine shortfalls or excess capacity. This data

allows Capacity Management to forecast future IT needs based on current utilization prior to an IT crisis.

In a proactive role, Capacity Management examines proposed business process and service level changes to eliminate negative impacts on IT service delivery levels. Capacity Management must watch for cumulative degradation of infrastructure capacity due to numerous changes over time. These cumulative effects are detected and mitigated to prevent inexplicable exhaustion of infrastructure capacity and related declines in service levels.

2.7.4 Availability Management

Availability Management confirms that service-related data is accurate and accessible within strict time constraints. Availability Management compares the service data accessibility expectations with infrastructure capabilities. Availability requirements are derived from user/customer business needs.

Availability Management verifies that IT services are provided to the customer/user at the levels specified in the Service Level Agreements. In fact, every Service Level Agreement should have availability expectations and metrics associated with it. The Service Level Agreements are written with specific availability targets or metrics used to determine if the service level contract has been met. Availability Management works with Service Level Management by measuring these metrics to highlight problem areas and suggest areas for improvement.

Availability Management researches technology alternatives to close the gaps between the service availability expectations of the business and the capabilities of the IT

provider. If data required by a service is extremely important, Availability Management may require the implementation of frequent off-site backups. A mirrored distributed database may be required if the data must be available to a service supporting a large numbers of users within tight time constraints.

2.7.5 Continuity Management

Continuity Management is the ITIL Disaster Recovery Plan for IT services. Continuity Management is concerned with the rapid prioritized recovery of IT services following a major breakdown in the system infrastructure (i.e. a computer virus or natural disaster). Continuity Management makes certain that the services associated with critical/essential business processes are identified and supported by a rapid recovery capability.

The prioritization of critical services must match organization business goals and objectives. After a service is identified as critical, Continuity Management performs a service-based risk analysis. A risk analysis is the mapping of a threat to a service vulnerability. [45:177] After a risk is identified the reactions or countermeasures to that risk are determined. The reaction might be to ignore the problem, work around it or bring up spare back-up systems to compensate for equipment losses. Service restoration priorities, vulnerabilities and countermeasures are captured in a Continuity Plan. The plan is designed to provide a step-by-step process to recover critical services.

2.7.6 Service Delivery Summary

Service Delivery uses IT to address the needs of an organization. It identifies what IT services are needed to resolve the business requirements of the organization. It focuses on delivering the quantity and quality of service expected. Service Level Management monitors the creation, modification, and performance of IT services based on contracts between the provider and consumer of IT services. Financial Management establishes an internal economy based on the value of the IT services. Capacity Management looks at the present and future ability of the infrastructure to support service-related demands. Availability Management helps measure the accessibility of services to the user. These services rely on an infrastructure to enable them. The Service Support function of ITIL provides controlled and repeatable processes to manage change within that infrastructure.

2.8 Service Support

Service Support is the second half of Service Management. Service Support focuses on the IT infrastructure and helps manage change in the organization. Service Support provides mechanisms for the safe and efficient integration of new technology necessary to provide the expected level of IT services to the organization. This ITIL element is subdivided into five areas: *Incident Management, Problem Management, Change Management, Release Management, and Configuration Management.*

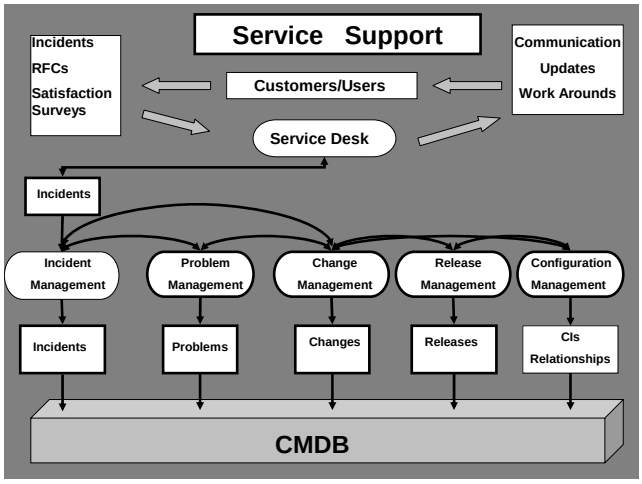

Figure 2.3. ITIL Service Support [48]

2.8.1 Incident Management

An *incident* is defined as an event that is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in the quality of that service. [46] Incident Management is the resolution of incidents to restore services. The implementation of effective Incident Management through a responsive Service Desk provides a rapid and tangible return on investment. Lockheed Martin chose to implement Incident Management first in their transition to a service-centric IT management organization for this very reason. [52:2]

The overall objective of Incident Management is to return to the promised levels of service as quickly as possible after an incident. This requires efficient identification and correction of the service interruption. Each incident is classified, prioritized, and escalated based on the priority of the interrupted service. [2:3] This creates a triage-type mentality in which Incident Management resources are brought to bear on the highest priority incidents in an effort to restore critical services first.

The Service Desk is Incident Management's primary interface to the organization's users and customers. Incidents are usually identified by users or customers as a lapse in service and reported to the Service Desk. The Service Desk starts the service restoration efforts of IT Service Support. Efficient documentation and incident classification is essential to quickly restore service.

ITIL places a great deal of emphasis on the Service Desk because it is often the first point of contact users and customers have with the IT Management. It is important that the Service Desk not be viewed as a barrier. A positive user perception of IT service-orientation is created or destroyed at the Service Desk. It must be more than a simple answering service that logs customer complaints about computer problems in a polite manner. The Service Desk must make the user feel understood and that their problem is important. This is accomplished with tight integration and continuous feedback to the user. The user's problem must be communicated quickly and efficiently to the IT professionals qualified to provide solutions. The user's perception of prompt and professional help is as critical to the ITIL customer service culture as the prompt resolution of the incident.

Most Service Desks are organized in one of three different configurations: centralized, distributed or federated. The centralized Service Desk is appropriate for smaller organizations with a single site IT staff and infrastructure. This approach allows a company to concentrate its expertise in one location. It sets up a single Service Desk to cover all IT service requests from its organization. The drawback to the central help desk

is inadequate response time during peak demand or wasted resources during periods of low demand.

The distributed Service Desk approach is tailored for larger organizations. This scheme allows companies to have immediate, on-site assistance at remote locations. However, this approach is more costly in terms of personnel and infrastructure. It forces a company to spread its IT expertise across multiple sites thus surrendering the economy associated with the central Service Desk configuration.

A federated Service Desk allows for a combination of the centralized and distributed Service Desks. The federated configuration allows for on-site assistance by small IT service teams for simple problems and centralized support from more experienced system engineers for challenging issues. Additionally, the federated approach utilizes a central Service Desk that can serve as a back-up facility in the event of a local site Service Desk failure.

Incident Management should implement and maintain a repository of expert knowledge obtained from solving past incidents. This database of knowledge will serve IT technicians in diagnosing future problems of a similar nature. This system allows Incident Management personnel at the Service Desk to achieve rapid resolution of repetitive incidents without repeatedly tasking technicians to solve the same problem over and over. This knowledge should be stored in the Configuration Management Database (CMDB) which will be described later.

The Service Desk should be staffed with qualified technicians that realize the importance of quickly restoring service and have the training to triage the incident

correctly and efficiently elevate incidents to the proper level of attention. If the incident is beyond the ability of the Incident Management personnel at the Service Desk, it is quickly assigned to a support team. The handoff to more technically capable personnel should be automated and use standardized, detailed documentation for more efficient resolution of incidents. Restoring service within an allotted time is the goal of optimal Incident Management.

2.8.2 Problem Management

Problem Management is different from Incident Management because it focuses on the root cause of an IT service disruption. Incident Management is concerned with restoring service as quickly as possible and their solutions often fix symptoms of a problem without ever discovering the root cause of the problem.

An Incident Management solution will probably be a “work-around” designed to reestablish desired service levels. The work-around may not utilize the infrastructure or personnel in the most optimum way. Discovering the root cause of service disruptions is the domain of Problem Management. Effective Problem Management is both proactive and reactive in its focus to prevent future disruptions.

In a reactive role, Problem Management studies data from Incident Management’s Service Desk to locate infrastructure components that are involved in numerous incidents. This can lead to the identification of full hard drives, failing hardware, or software bugs. Problem Management continues to study incidents after they are resolved to discover why they happened in the first place.

To be proactive, Problem Management uses extensive metrics to locate IT problems. Metrics set performance baselines that can be studied for bottlenecks or single points of failure. The analysis of these resources helps the Problem Management staff stay proactive in predicting problems instead of solely reacting to incident reports from the Service Desk.

2.8.3 Change Management

Change happens. It is unavoidable. Managing change is the key to success in any competitive market. In many organizations, there is a resistance to change or it is perceived as a necessary evil. Those organizations lose the ability to compete because they do not adapt with technology. Other organizations incorporate new technology so fast there is no chance to establish efficient procedures or processes.

Managing change with respect to *services* allows a company to establish a balance between *flexibility* and *stability*. Flexibility allows a company to incorporate new techniques and technology while phasing out older material. Stability is the inertia that resists change to allow a company to train and execute as a team using common terms, knowledge, and equipment. Too much change too quickly can cause incompatibility, confusion, and chaos. Too little change results in stagnation.

Change Management works like a thermostat between flexibility and stability. It attempts to balance the need for change with the discipline to accomplish that change in a controlled and planned manner. [35:85] That balance provides agility to the change process. Agility is the ability to efficiently utilize current systems to support service

needs while incorporating new technology. Agility requires a balanced Change Management process.

When new technology becomes available, it is tempting to just plug it into the organization's infrastructure and hope for the best. However, in the complex environment of today's IT infrastructure the results could be disastrous. Changes to a company's infrastructure (i.e. hardware, software, etc.) must be clearly understood and carefully weighed in terms of risks and benefits. Change Management's objective is to incorporate change efficiently with the least impact on IT service quality.

There are two groups within the Change Management department that can authorize changes. The first consists of the Change Manager. He provides broad oversight and continuity to the Change Management process by sitting on committees and interfacing with other ITIL areas. The second group is a collection of Change Advisory Boards (CABs). A CAB is the Change Management committee that approves or denies changes based on pre-existing metrics and criteria. These committees are made up of the Change Manager, organizational leadership, technical experts, managers, contractors and customers in an effort to give the group the expertise needed to make effective decisions regarding change in the organization.

CABs come in different sizes and compositions. The organization can designate large or small CABs to deal with different types of change within the company. The changes may be urgent and require a small emergency CAB capable of quickly analyzing the change and giving approval. Whatever the case may be, ITIL emphasizes the importance of changing the composition of the CAB to match the nature of the changes

being considered. This is how ITIL ensures that the changes made to the system are closely aligned with the needs of the organization and that they will be both cost effective and supportable.

Change Management assesses the impact, cost, benefits, and risks of changes through extensive testing. The testing may be performed by organization engineers or performed by the developers of off-the-shelf systems. This testing is normally accomplished on test equipment separated from the company's live environment to mitigate risks to the organization. They should utilize the appropriate equipment and personnel for this task to allow rapid test of proposed changed to the infrastructure. Service users/customers should be heavily involved with acceptance testing prior to a change approval. After a change has been analyzed, the Change Management process recommends an implementation strategy.

Change Management is time consuming and expensive. However, it is essential to a company that expects to balance stability and flexibility. Change Management must constantly strive to find ways to make its process more efficient. This is because Change Management can be considered a roadblock to progress if the process takes too long. Users and customers will find a more efficient means to incorporate change unless they feel Change Management is responsive to their needs. Efficient Change Management is critical to maintaining a safe and secure IT environment.

If changes were incorporated as soon as they were approved by Change Management, the infrastructure would be in a continuous state of change. Users and

maintainers of the systems would be constantly relearning how to do familiar tasks. Human users adapt to change better if it is organized into periodic ‘releases’.

2.8.4 Release Management

A ‘release’ is a collection of changes to an IT service or component authorized by Change Management. Release Management combines numerous changes into a periodic release in an effort to provide safety and stability to the change process. Releases are planned for specific intervals (i.e. every six months, quarterly, etc.) The changes contained in a release might affect training, functionality, and interdependencies between infrastructure components. These effects on the infrastructure must be known and coordinated before changing the company’s IT services or components. Additionally, all documentation and training functions associated with the release must be updated to reflect the changes. Release Management must then monitor and report on the implementation of the release within an organization.

Release Management must provide a “back out” strategy if unforeseen consequences require the reversal of an approved change or release. The back out strategy is a necessary risk management function that allows the IT staff to return the organization's production IT environment back to a specific state prior to the implementation of a change. This back out solution must be carefully planned and tested prior to the implementation of the change in the production environment. [46:205]

2.8.5 Configuration Management

Configuration Management is the discovery, inventory, and documentation of an organization's IT infrastructure. Configuration Management ensures that the components and the relationship between them are recorded in a database called the Configuration Management Database (CMDB). These components may be hardware, software, documents, services or processes.

The CMDB can be thought of as a Common Operational Picture of your organization's IT infrastructure. The CMDB is the single most critical component of the ITIL Service Support solution. Every other ITIL Service Support component will reference or interact with it. An incomplete or inaccurate CMDB will impede other ITIL Service and Infrastructure Management processes.

ITIL calls a component a Configuration Item (CI). The granularity and scope of the CMDB refer to the amount of detail recorded about the infrastructure. Scope refers to what components are tracked (i.e. desktops vs. the components within the desktop). The granularity of the CMDB is the amount of information contained within individual records or CIs. The granularity and scope of the CMDB determine the effectiveness of the Configuration Management process. If too much detail is recorded the system gets bogged down and out of date because it cannot keep up with the changes in the IT infrastructure. It is possible to track so much detail that the CMDB will not scale properly. If too little information is tracked then the CMDB picture is of little use to the organization.

The CMDB is used to track more than just the components of the IT infrastructure. It captures the *relationships* between the *components* and the specific *services* they provide. SLAs, OLAs, and UCs are tracked in the CMDB along with changes and release information. Incident and Problem Management use the CMDB to investigate problems and then to store their solutions. The CMDB is to be integrated into every aspect of Service Management. It is the common repository of information related to the organizations ability to provide IT Services. This integration is not easy but it is essential to the ITIL Service Management framework.

The CMDB is the primary ITIL component used to integrate IT Service Management into an organization. All other ITIL elements rely on accurate CMDB data to make decisions, provide service and solve problems. The CMDB must be kept current and available for ITIL to deliver effective IT Service Management. This means the CMDB must be seamlessly integrated with other IT Service Management products and tools.

There is an ongoing debate in industry over the proper way to implement a CMDB. One group advocates a new, scalable enterprise CMDB that must be built from scratch. Obviously, this is more costly but may be easier to integrate with future systems. There are a few companies that offer proprietary CMDBs designed to provide the integration required by the ITIL framework like assyst™ by Axios Systems.

However, Forrester Research's Thomas Mendel, Ph.D., believes that the only sensible way to implement CMDB architectures is to use a federated approach. This enables companies to construct different views of the data for different purposes while at

the same time storing and updating the data in legacy data stores. [38] The federated approach uses a centralized middleware database to combine legacy data stores containing the configuration data to create a virtual CMDB. These legacy data stores may be proprietary databases from older systems or data from self-discovery network software. The attraction here is the ability to use existing hardware and software that contains the necessary information in various formats.

Regardless of the type of CMDB, the data in the CMDB should be recognized as the authorized configuration of the infrastructure. No changes should be made to the infrastructure without a corresponding change in the CMDB. This policy must be *enforced* to retain a credible Configuration Management system.

If you do not track changes to an infrastructure component in your CMDB then you cannot utilize ITIL Service Management to address possible impacts of that change. The challenge is to keep the CMDB synchronized with the actual infrastructure with enough detail to be relevant. The CMDB must be tightly integrated with all IT Service Management functions to make the update process natural and user friendly.

2.8.6 Service Support Summary

Service Support is concerned with ensuring users have access to appropriate IT services by providing an agile IT infrastructure that can adapt quickly to a changing environment. Change and Release Management strike a balance between flexibility and stability. Configuration Management captures infrastructure components and the relationships between them. Incident and Problem Management resolve short and long term problems within the infrastructure by restoring service if incidents arise and

preventing problems from occurring again. All of the Service Support components integrate heavily with the CMDB to ensure users have access to required services.

2.9 ITIL Component Interaction and Integration

Companies often elect to install one or two ITIL Service Management components at a time. The process of shifting from a technology-centric methodology to a service-centric one takes time. However, many ITIL implementation efforts fail because the companies do not understand the importance of tight integration between the different components within ITIL Service Management. A lack of integration and cooperation between and within the ITIL areas can create ITIL silos or stovepipes that prevent the realization of the potential benefits of a service-oriented approach to IT management.

Change Management processes require close integration with Incident/Problem Management, Capacity Management, Configuration Management and Release Management processes. Incident/Problem Management may determine that a change to the infrastructure is required to fix a problem. It is essential that Change Management work closely with Incident/Problem Management to test, evaluate, and implement Incident/Problem Management fixes in a manner that prevents an unintentional cascading set of new problems that could cripple the IT services they are trying to provide.

Capacity, Release, and Change Management work together to assess the cumulative impact of adding or removing IT capabilities from an organization over time. [35:89] Release Management attempts to provide stability by collecting approved IT

solutions from Change Management and grouping the changes into a predictable and scheduled release. [46:167]

The Change, Release, and Configuration Management process are the most tightly coupled of the ITIL paradigm. This is because every change to the infrastructure must be documented. ITIL organizations must be able to trace what has changed and why. The Configuration Management process documents any authorized changes in the organization infrastructure through the CMDB. An effective CMDB will capture a history of the organization's infrastructure as it changes over time. Additionally, many companies incorporate Change and Release Management into Configuration Management to facilitate the flow of critical configuration information between them. [46:165]

An integrated CMDB is the linchpin of the entire ITIL Service Management solution. It provides different views of the organization infrastructure necessary for technicians in Incident and Problem Management to troubleshoot break downs in IT service. The CMDB helps organization and IT managers see the effects of proposed changes to the company’s IT services in terms of cost and potential problems. It helps ITIL Availability and Continuity Management identify weak links in the infrastructure and create plans to deal with failures in the system. Thus, an integrated, accurate, current and available CMDB is critical to an organization’s ability to understand its infrastructure capabilities and limitations. The interaction between the CMDB and the other elements of ITIL must be seamless and efficient.

Incident Management interfaces with all other ITIL Service Support components to stay abreast of changes within the infrastructure. Incident Management provides important metric data to Capacity, Availability, Service Level and Financial Management for planning and advisory purposes. The need for a close working relationship between Incident, Configuration, Change and Service Level Management is obvious. Incident Management ties the Configuration, Change, Release, and Problem Management areas together and presents the user with a Service Desk single point of contact for them all. [35:109]

Problem Management indirectly enables Availability and Capacity Management by proactively or reactively solving problems that interfere with system availability and IT resource utilization. Additionally, Service Level Management may not provide promised levels of service if problems in the infrastructure are not identified and resolved by the Problem Management team within the organization.

Capacity Management interacts with all of the other areas of Service Support in a proactive and reactive manner. The Capacity Management staff looks for actual and potential breeches of Service Level Agreements to identify IT components and resources that do not provide the promised level of performance for specific services. Capacity Management monitors trouble tickets generated by the Service Desk as well as monitoring data reported by various sensors throughout the infrastructure. Capacity Management then works closely with Incident and Problem Management to determine the capacity implications of the incident/problem and submit a fix through Change Management.

Service Level Management works closely with other ITIL elements in providing the level of service promised in the SLA. For example, Change Management must determine what effects an infrastructure change will have on IT services. Change Management would then work with Service Level Management to ensure proposed and implemented changes in the system will not cause Service Level Agreement breeches. Release Management shares a similar relationship with Service Level Management by ensuring that large scale changes in the organization infrastructure do not impact required IT service levels.

In fact, every ITIL Service Management area impacts every other ITIL Service Management area. Some impacts are explicitly described like the role the Service Desk will play in correcting a lapse in service. Others are implicit like the requirement for Capacity Management to monitor service impacts on infrastructure utilization. However, the interaction between Service Management areas cannot be overlooked in the implementation of the ITIL framework.

Service Management relies on the integration of Service Delivery and Service Support to identify, monitor, and improve IT services. However, each service relies on the IT infrastructure to enable it. There must be a tight coupling between the service management philosophies and the physical implementation of infrastructure technology. ITIL Service Management must work with IT providers and maintainers to properly manage an organization's infrastructure because of the expense associated with losing control of this fundamental function.

2.10 Summary of ITIL

Governance is the ability of an organization to align its IT investments with over-arching business strategies. The ITIL framework allows a company to align its IT investments with its corporate goals. It allows a company to exploit IT functionality by understanding the IT services in terms of their value to the organization. It requires an organization's leadership to embrace IT's partnership role in supporting and even shaping the overall business strategy.

ITIL Service Management requires an organization to identify critical business process needs and then creates IT services to resolve them. Those services must be provided, measured, and improved in a continuous manner to secure value from IT investments. The IT providers become partners with the business in providing value and generating new business. ITIL Service Management is a required intermediate step towards IT governance.

Chapter three will describe the function of an AOC. The history and current operating practices of AOC IT management will be examined. Finally, ITIL Service Management principles will be applied to AOC IT management processes in chapter four.

III. AOC IT Management

3.1 Introduction

In 1912, Lt Henry “Hap” Arnold used an aircraft to achieve greater accuracy in the employment of field artillery. He would observe friendly artillery impacts and drop weighted notes containing impact information to cavalry officers below. The cavalry officers would then collect the notes and gallop back to the artillery pieces to deliver the intelligence. The artillery would then adjust their fires based on that information. [7:5]

Hap Arnold was using airpower to find, fix, track, target, and kill (F2T2K) objects on the battle field. This is known today as a kill chain. The US Air Force (USAF) is looking for ways to shorten the F2T2K kill chain by communicating more efficiently up and down the chain of command. However, technology keeps getting in the way.

The USAF has moved the kill chain into a facility known as the Air Operations Center. The Air Operation Centers (AOCs) are typically called Joint AOCs (Multi-service), Combined AOCs (Multi-nation), or a combination Joint/Combined AOC depending on their location and function. For the purpose of this paper, the term AOC will be used to refer to any of the above systems.

This chapter will describe the evolution of the AOC and its management functions. The current semi-centralized AOC management organization will be explained along with the processes used to incorporate new technology into the AOC.

3.2 AOC Structures and Processes

The USAF uses a command and control (C2) concept known as centralized planning and decentralized execution. The AOC is the centralized C2 command post

used by the USAF to conduct air operations in a specific theater. The AOC provides operational-level control of theater aerospace forces and is the focal point for planning, directing, and assessing aerospace operations. It uses Information Technology (IT) to ensure dominance of the battle space through seamless integration of C2 communications. The AOC includes the hardware, software, databases, communications gear, and interfaces utilized to exercise command and control over aerospace forces.

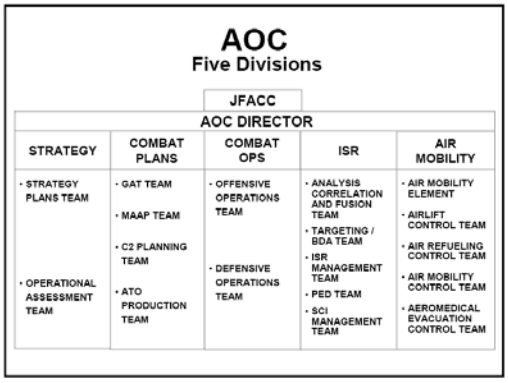

Figure 3.1. AOC Divisions [29]

The theater Joint Forces Air Component Commander (JFACC) uses an AOC to gather information, deconflict his plan with peer service component commanders, and communicate his instructions down to the warfighters. Therefore, the AOC is the destination or origin of the majority of USAF C2-related communications in a theater.

The AOC work load is divided among five main divisions: Strategy, Combat Plans, Combat Operations, ISR (Intelligence/Surveillance/Reconnaissance), and the Air Mobility Division. These divisions and their staffs are depicted in figure 3.1. The five divisions work together to coordinate the warfighting effort.

The AOC operates continuously twenty-four hours a day, three hundred and sixty-five days a year. The JFACC and his Strategy division staff formulate an operations plan. Target lists are generated by the Combat Plans division to match the objectives in the strategic plan. Weapons experts map appropriate weapons to the targets on the list and select aircraft to perform the strike. The Air Tasking Order (ATO) containing the JFACC's attack plan is generated and distributed.

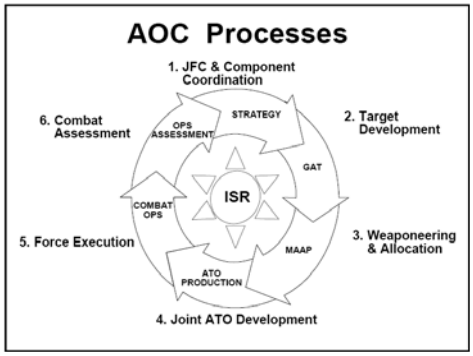

Figure 3.2. AOC Business Processes [29]

The execution of the plan is monitored and modified by the Combat Ops division within the AOC. Intelligence is gathered by ISR to validate the success of the executed ATO. The Air Mobility division coordinates the use of airlift and air refueling into the operational plan. This cycle takes three days and repeats over and over throughout the execution of a campaign. Typically there are three parallel cycles going at the same time to generate an ATO every day.

Over the past forty years, the AOC has developed an insatiable appetite for cutting-edge technology. The increased operational tempo, high turnover of AOC support personnel, rapidly emerging technologies, complex infrastructures, and the need

for the USAF to operate in joint and coalition environments have made managing change within the AOCs incredibly difficult. As a result, each AOC command post evolved to the point where it has little in common with other AOCs around the world. This segregated 'Darwinian' approach to AOC IT management has been expensive and difficult to modernize.

3.3 AOC Diversity

The lack of standardization hampered the development of doctrine, tactics and procedures. Each AOC was so specialized and unique that personnel with experience in one AOC were not able to perform the same job in a different AOC. The USAF could not effectively train AOC personnel due to a lack of standardization. [27:8] The lack of standardization also prevented communication and cooperation among the AOCs due to incompatible technology. The AOCs could not effectively integrate with sister services like the Navy or Army without excessive improvisation and workarounds.

Historically, the AOC was always considered a Command Post that housed essential communication and planning gear. It was simply a data and communication center. Localized USAF AOC IT management staffs solved AOC infrastructure problems by simply purchasing or developing individual IT solutions for each theater AOC. As the AOC scaled and became more technologically complicated, this approach resulted in stove-pipe, proprietary systems that were expensive to maintain and difficult to integrate with other internal AOC systems or external joint/coalition systems.

General John Jumper discovered this during a conversation he had with an AOC airman who required three separate terminals at his workstation. When asked why he had

three separate terminals, the airman responded “Well, sir, I get the data off of this one, then I have to reenter it over here, and then once I get that, I’ve got to reenter it over here and that gives me my answer.” When pressed for an explanation of the convoluted process, the airman replied that three separate companies built the terminals. The companies did not work together and simply supplied separate parts of a solution. This acquisition of stove pipe solutions has been prevalent throughout AOC acquisition history. General Jumper was not impressed. He insisted the USAF do better in the future. [37]

3.4 AOC Transformation

The pressure to change the management of the AOC did not start with General Jumper. AOC management transformation has been taking place over the past decade. In 1995, General Ronald R. Fogelman assessed the AOC IT management problems. He pronounced the USAF was behind the technological power curve because it could not keep pace with the rapid advances in technology. General Fogelman wanted to dominate battlespace awareness by redesigning the way the USAF identified its technology requirements and acquisitions processes. He wanted to improve the exploitation of technology so the USAF could rapidly field capabilities instead of simply demonstrating them. Specifically, he instructed the USAF to focus on the management of C2 functions. [33]

In October of 1997, the USAF initiated an Expeditionary Force Experiment (EFX) to explore new C2 capabilities within an AOC. The EFX showed that a *standardized* management approach to building and maintaining AOCs would provide

more efficient command and control of air power in future wars. [21:3] As a result of this experiment, the USAF sought to standardize and consolidate its IT resources.

In July of 2002, General Michael E. Ryan directed the Air Force to build a new AOC at Prince Sultan Air Base (PSAB). General Ryan attempted to bring standardization to all USAF AOCs by declaring the PSAB AOC a "Weapon System" designated the AN/USQ-163 Falconer. The PSAB AOC became the default baseline for defining what an AOC should be. The USAF decision to centralize the AOC IT management process was intended to create universal IT solutions for all of the various AOCs. The declaration of a "standard" AOC was necessary to save time, money and training. [27:8] It gave the USAF a starting point on which to begin shaping the AOC of the future.

The new AOC would be standardized, tailorable and able to integrate with other joint, coalition, and allied warfighting components. [25:10] The weapon system approach would allow for accreditation, clarify funding decisions and improve IT management. Unfortunately, the PSAB facility was the only AOC in the USAF that met the definition. The USAF was anxious to baseline all of its AOCs. However, they could not afford to abandon all of the AOCs around the world and rebuild them from scratch. It decided to reshape the older AOCs into the new baseline model. This effort has proved difficult, expensive, and time consuming.

3.5 AOC Reorganization

This controversial decision to declare the AOC a weapon system was a step in the right direction. However, it did not change the AOC Command Post into a weapon

system over night. Numerous Air Force and DOD agencies were required to cooperate in an effort to bring order to the initial chaos created by the AOC weapon system decision. A plan was developed to have all operational AOCs meet a standardized minimum baseline of equipment and capabilities through a series of "spirals". Subsequent spirals would then build on the base line in a controlled and budgeted manner. However, the reality of the transformation differed from the plan.

Behind the scenes, there was significant resistance to the changes in AOC IT management from users of the AOC and from agencies that perform the management function. Much of the resistance was due to the radical departure from the traditional weapon system development process. Continued resistance on the part of the warfighter or USAF leadership will result in increased costs and risks to future AOC systems.

Most weapon systems start by defining the customer's requirements for the weapon system and then designing the architecture of the system to meet those requirements. Those architecture products are then used to construct the physical weapon system. The architecture products serve as a blueprint for measuring the effectiveness of the final product in meeting the initial customer requirements. However, the AOC had to be reverse engineered and the unique capabilities of the nine operational AOCs made the initial task of defining AOC requirements and determining its boundaries very difficult.

The plan to convert the AOC Command Posts into Falconer Weapon Systems utilized an evolutionary "spiral" acquisition approach. The first spiral focused on an equipment inventory and capturing the existing AOCs on paper using architecture frameworks. The inventory process required a "lockdown" to freeze the individual AOC development. This spiral was labeled 10.0 and it established a baseline or a common

sub-set of equipment required for a Falconer Weapon System.

Spiral 10.1 was an accreditation process in an attempt to stop reverse-engineering and start managing the weapon system. The USAF was able to measure AOCs against an approved standard and declare them operational. Subsequent spirals will attempt to improve airspace deconfliction, coalition interoperability, and multi-level security capabilities. Additionally the footprint and manning requirements will be reduced while the number and scope of machine-to-machine interfaces will increase. There will be a requirement for interoperability and reach back that will allow the AOC to cooperate with other AOCs in an effort to provide increased capacity and continuity. [21:1]

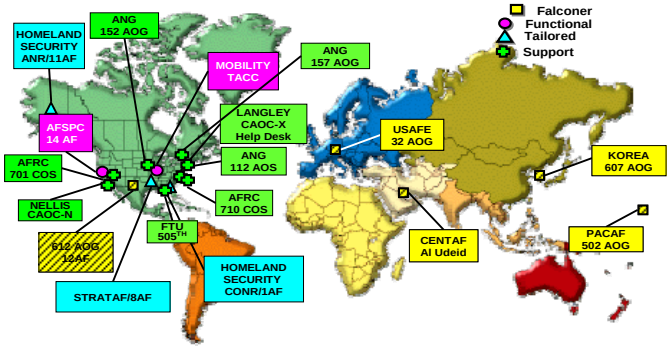

Figure 3.3. AOC Locations

In Dec 2003, the USAF selected five AOCs to be converted into Falconer Weapon Systems plus a centralized Help Desk and a Formal Training facility. This decision is referred to as the 5+1+1 configuration. The AOC at PSAB was closed and the Al Udied AOC became the USAF baseline AOC. Currently, there are five *Operational* Falconers. There are two fixed sites in CENTAF at Al-Udied, QATAR and 7th AF

located in the Hardened Theater Air Control Center (HTACC) at Osan Air Base, Korea. The remaining three Falconers are deployable. They are based at 12th AF (Davis Monthan AFB, AZ), 32nd Air Operations Group (Ramstein AB, Germany), and 502nd Air Operation Group (Hickam AFB, HI).

Tailored AOCs are adapted versions of the Falconer AOCs designed to meet unique theater requirements for both STRATCOM and Homeland Security. Functional AOCs provide specific capabilities in support of Homeland Security, Global Mobility, Nuclear Response and Intelligence agencies. They manage specific operations around the world like Military Airlift/Tanker Support, satellite ops or Nuclear Deterrence. [15:4]

Table 3.1. AOC Types and Locations [21:5]

AOC TYPE	SITE	MAJCOM	BASE
Falconers	9th AF	CENTAF	Al Udeid AB, Qater
	607th AOG	PACAF	Osan AB, Korea
	32nd AOG	USAFE	Ramstein AB, Germany
	502nd AOG	PACAF	Hickam AFB, HI
	12th AF	ACC	Davis Monthan AFB, AZ
Tailored AOC	8th AF	ACC	Barksdale AFB, LA
	11th AF	NORAD/NORTHCOM	Elmendorf AFB, AK
	1st AF	ACC	Tyndall AFB, FL
Support AOCs	152nd AOG	ANG	Syracuse, NY
	157th AOC	ANG	St Louis, MO
	701st COS	ARC	March ARB, CA
	112th AOS	ANG	State College, PA
	710th COS	ARC	Langley AFB, VA
	505 TRS FTU	ACC	Hurlburt Field, FL
	Help Desk	ACC	Langley AFB, VA
	CAOC-X	AFC2ISRC	Langley AFB, VA
	CAOC-N	ACC	Nellis AFB, NV
Functional AOCs	TACC	AMC	Scott AFB, IL
	14th AF	AFSPACECOM	Vandenberg AFB, CA

Support AOCs perform training, testing, or technical functions to support AOC operations around the world. There are five Air National Guard and Air Reserve

Component AOCs that maintain operator and maintainer readiness. CAOC-N is used for continuation training, joint force exercises, and experimentation. The CAOC-X facility provides test facilities to check new systems prior to fielding. The Formal Training Unit is used for initial training and qualifications. The Help Desk provides global IT technical support for the AOCs around the world. [21:5]

3.6 Centralized AOC IT Management Organization

The intention of the reorganization of the AOC IT management function was to centralize its management. However, in the process of centralization, accountability for the AOCs and the systems within them has spread out among many stakeholders. There are eleven different stake holder organizations tasked to assist with the management of the AOC WS. These are: Air Force Material Command (AFMC), Air Force Command & Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC), Air Combat Command, Air Force Operational Test and Evaluation Center (AFOTEC), Headquarters Air Mobility Command, Assistant Secretary of the Air Force for Acquisitions, Capabilities Directorate for Information Dominance, Deputy Chief of Staff for Warfighting Integration, Deputy Chief of Staff for Air and Space Operations, Air Force Communications Agency, and Air Force Operational Commands that own an AOC. [26]

All of these stake holders have mandated roles in managing IT within the AOC. They also present diverse interests and pressures that compete with each other. This competition slows or even prevents effective collaboration. The large group of diverse stakeholders creates a *semi-centralized* AOC IT management organization. The AOC IT

management organization does not have a single, all-powerful commander empowered to provide a clear vector or enforce policies. [41:4]

The Staff and Secretariat organizations provide general direction for policies and budgets. The Air Force Communications Agency provides interface guidance to ensure infrastructure integration with government networks. Air Combat Command (ACC) was designated the lead Operational Command and represents the interests of the AOC warfighters. ACC injects the warfighter's needs into the requirements review process used to change the AOC Weapon System. They are also tasked with developing training, tactics, techniques, and procedures to be used by the operators of the AOC. [26:5]

The AFC2ISRC was created to help the Air Force manage emerging command and control technologies. They were tasked to be the lead agent for generating and validating AOC requirements. The AFC2ISRC maintains a large testing facility and spearheads the acquisition and integration of new technology into the AOC baseline.

AFMC was tasked to be the implementing command and to manage the life cycle of AOC technology. [17:3] AFMC's mandate is to execute an evolutionary acquisition program that reduces risk, enhances maintainability, reliability, and security while providing continuous technology refresh. They prototype, develop, produce, test, install, field and sustain AOC WS IT. [26:3] AFOTEC provides the testing capability for AFMC by working with several military test organizations to capture the broad array of expertise necessary to test a complex system like the AOC. Electronic Systems Command (ESC) is responsible for the initial purchase and annual maintenance of AOC systems. A System Program Office (SPO), under the direction of ESC, keeps track of the baseline AOC configuration and audits the configuration management of the Falconer AOC

Weapon Systems. [17:3]

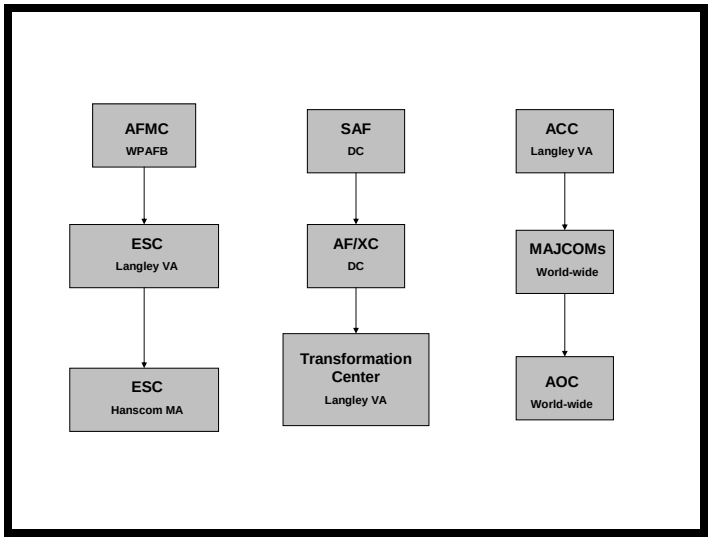

Figure 3.4. AOC Stake Holder Chains of Command

As you can see, the management of AOC IT is spread out among numerous agencies and offices and the number is expected to grow. The chain of command and accountability relationships between these offices are complex. The large number of stake holders and the complexity of the chains of command add to the difficulty of managing AOC IT.

The change management process of the AOC is presented in Fig 3.5. Its primary teams are the C2 General Officer Steering Group (C2 GOSG), the Spiral Development Integrated Product Team (SDIPT) and the Configuration Change Board (CCB).

Twice a year, a group of Three-Star General Officers meet to discuss USAF C2 issues and provide guidance to the AOC management community. This group is referred to as the C2 GOSG. The GOSG is tasked to set C2-related goals, objectives, investment

strategy and plans for the USAF. They review the SDIPT requirements and give periodic inputs to the AOC IT management process. The C2 GOSG is the most senior USAF leadership with direct input into the evolution of the AOC infrastructure.

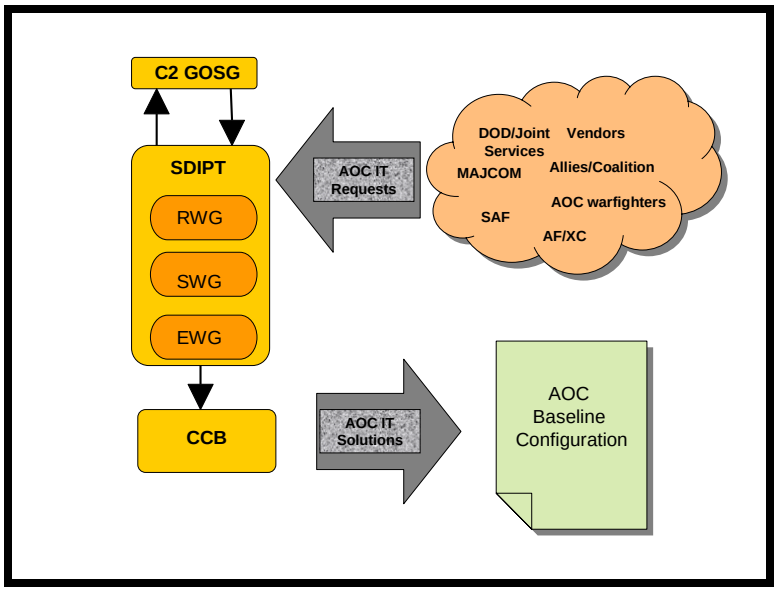

Figure 3.5. AOC IT Management Process

The SDIPT defines, validates, and prioritizes requirements for the AOC Weapon System. It consists of Colonels from various MAJCOMS, the Transformation Center and ESC that "present a harmonized authoritative view of the joint requirements" for the AOC. These requests may come from the war fighting customer, technology vendors, or DOD Leadership. [16:1]

The task of identifying and validating AOC requirements is divided among three specialized teams that directly support the SDIPT. They are the Requirements Working Group (RWG), the Sustainment Working Group (SWG) and the Engineering Working

Group (EWG). These teams help the SDIPT develop a user/customer request into an AOC requirement and then propose an IT solution. Each working group is made up of individuals from ESC, MAJCOM staffs, AFC2ISRC, and government contractors.

The Requirement Working Group (RWG) is an 'action officer' level (O-5 and below) forum used to create the requirement by validating the need for a solution and prioritizing the request with others being considered. It is chaired by the AFC2ISRC with representation from MAJCOMS, Air Staff and supporting agencies. [16] The RWG starts the process by taking the inputs from the outside agencies to "define, review, validate, and prioritize operational requirements." [16] The RWG translates a user/customer's request into an AOC requirement that the SWG and EWG can solve. Often a solution to a request is obvious or already present. However, the idea is to change the request into a language that defines the requirement and allows the three working group teams a chance to investigate alternative solutions.

The Sustainment Working Group focuses on budget and maintenance issues with the proposed solutions from the RWG. Often IT solutions may have complicated warranties or maintenance contracts that make them infeasible or undesirable. The SWG investigates the long-term costs of an IT solution.

After the SWG signs off on a solution, the Engineering Working Group will study the solution for accreditation, security and feasibility issues. This step prevents a solution from causing new problems and prevents the purchase of incompatible technology. The EWG uses testing facilities and architecture standards to ensure new technology will integrate successfully with the baseline AOC infrastructure. The EWG is unable to replicate all AOC infrastructures due to numerous site variations from the baseline.

However, the ability to test products against the common baseline helps mitigate some of the risks to the individual AOCs in the field.

Once a requirement has been published by the three working groups, it must be approved by the Change Control Board. The CCB reviews the requirements and solutions and makes the final decision whether to incorporate changes into the AOC baseline. The CCB delegates the approval authority for minor modifications to subordinate members of the SDIPT. However, the CCB is the final review authority for any change to the AOC baseline. [16]

Ideally the AOC Falconer Weapon Systems in the field will match that baseline. However, the requirement to tailor the AOC to its environment forces the USAF to deal with variations to the baseline. The variation might be a specialized system or the absence of an approved system that interferes with the AOC operation in a specific location. An authorized variation is an approved deviation from the baseline; however, not all AOC variations are authorized.

3.7 Summary

The last ten years have been a period of reorganization and change in the way the USAF manages the AOC. The organization for managing the AOC IT has been changing almost constantly since 2003. Most of the documents used to research AOC IT management were still in draft form. Many AOC organizations have recently written charters or guides to help communicate their roles and responsibilities to both themselves and other AOC organizations.

This period of reorganization is a perfect time to assess the potential role ITIL can

play in the AOC IT management. The next chapter explores the application of ITIL framework to the AOC IT management structure to show benefits and shortfalls.

IV. Application of ITIL to AOC IT Management

4.1 Introduction

The USAF drafted a 2004 AOC “Roadmap" describing the AOC of the future. The AOC of the future is to have a reduced forward footprint, automated coalition interoperability, fused correlated picture, uniformly trained personnel, time critical targeting, scalability and a rapid deployment capability. The AOC must be integrated vertically and horizontally. Vertical integration must link the AOC to both superior joint force elements and subordinate units within the theater to move information rapidly up and down the chains of command. Horizontal integration must link to lateral peer organizations of other services or even other USAF AOCs. [20]

The future AOC must be able to conduct distributed operations spread across multiple independent nodes in a team effort. They will also need the ability to split operations across dispersed locations under the control of a single commander. [29:4] This is not achievable with the existing AOC infrastructure and business processes.

4.1.1 IT Governance

Like numerous civilian companies, the AOC is so dependent on information technology that IT no longer supports the business…IT is the business. In other words, the loss of IT integration and innovation will prevent the AOC from accomplishing its primary C2 function. IT is no longer an enabler of AOC C2; it has become essential to it.

The USAF can no longer simply manage its AOC infrastructure. It needs an IT management contribution to its current warfighting ability. Moreover, the USAF needs

an AOC IT management organization that transforms and positions the AOC to meet the needs of tomorrow's JFACC. The dual need of effective IT contribution and IT positioning captures the difference between IT *component* management and IT *Governance.* [2:1]

IT Governance is the morphing of an organization's IT provider into a strategic partner. Establishing collaboration between IT providers and consumers using a service-centric framework provides the foundation to establish the partnership. IT governance decides who will make the IT decisions and how those decisions will be implemented by the partnership. ITIL Service Management defines "how" the organization should achieve the alignment necessary for the partnership. [49:20]

4.1.2 ITIL Stepping Stone

Tech-centric organizations become dependent upon their respective IT departments. They soon recognize the need to move from efficient management of IT resources to IT governance is necessary to stay competitive. However, the change from IT infrastructure component manager to an IT strategic business partner is a complex and time consuming process for an organization. Most companies follow a three step approach to achieving an IT Governance level of maturity.

First, they attempt to manage their infrastructure by maximizing return on IT investments and applying positive controls to infrastructure components and data. This is called IT Infrastructure Management (ITIM). ITIM describes the traditional network management functions found in most small organizations. There are intense pressures to establish control of the infrastructure to simply keep it available to it users. As the

infrastructure grows more complex this approach becomes less feasible. Many IT management organizations, like the AOC, get stuck in this phase because they do not understand the benefits associated with a change from managing infrastructure *components* to managing user *services*.

The next step is IT Service Management (ITSM) in which the organization identifies the IT services used by its customers. The organization focuses on delivering those services at acceptable levels of performance to meet availability, performance, and security requirements. These services are governed by external and internal contracts to meet mutually acceptable quality and cost targets. "The evolution of IT organizations from technology providers into service providers requires taking a different perspective on IT management. IT Service Management puts the *services* delivered by IT at the center of IT management." [49:9]

Finally, the organization achieves enterprise maturity as the IT organization is incorporated as a business partner that delivers value by offering new business opportunities. [49:2] This is where organizational leadership and organization IT management are aligned in a synergistic and empowering partnership. The leadership understands the limitations and value provided by IT. The IT providers understand the strategic goals and are able to provide innovative IT solutions to solve today's challenges while positioning the organization to achieve growth in the future. This concept of IT partnership is dramatically different from the paradigm in place today within the AOC organization.

4.1.3 Overview

AOC IT management must be *governed* to ensure USAF commanders have the most capable AOC available. The AOC infrastructure must maximize the capabilities of legacy systems and seamlessly incorporate new technology. Current management practices are not achieving IT Governance due to a lack of *leadership empowerment*, *centralized management*, and *service-oriented processes*. These three discrepancies will hamper AOC transformation until they are resolved. This chapter will discuss IT Governance transformation and the use of ITIL processes to establish an empowered, centralized, service-oriented AOC IT management organization. First, the need for centralization and empowerment will be discussed. Then AOC resistance to traditional management controls and tools will be explained. Finally, specific applications of Service Delivery and Support will be covered in an effort to illustrate the enormous potential offered by an ITIL transformation of AOC IT management.

4.2 AOC IT Infrastructure Management Organization

In 2003, the USAF published a “Transformation Flight Plan”. In this document the USAF declared it intention to “break out of industrial age business processes and embrace information age thinking" to create “flexible, agile organizations that continually collaborate to facilitate transformation and institutionalize cultural change.” [31:3] The creation of that flexible, agile AOC IT management organization requires a centralized management organization empowered to manage change within a complex AOC infrastructure.

4.2.1 Centralized Planning – Decentralized Execution

The USAF knows the value of centralized control and decentralized execution; however; it has not achieved it with the AOC management process. The USAF has lost *agility* by failing to fully centralize the management of the AOC weapon system. Centralized Command is defined as the placing within *one commander* the *responsibility* and *authority* for *planning, directing, and coordinating* a military operation or group or category of operations. [18] The current distributed network of AOC stakeholders compounds the complexity of the AOC IT management problem by dividing the planning and purchasing authority between numerous offices.

While, a competition-based system of checks and balances is suitable for our Nation's government, it is no way to manage a federated AOC IT network designed to use cutting-edge technology and yet provide agile, stable, and reliable services to its users. The USAF primary AOC management organizations ACC, ESC, AFC2ISRC work as peers with little authority or leverage over each other. They have established a complex political structure where decision making, funding, and accountability are distributed across dozens of different offices and organizations. Consensus and accountability are difficult to achieve with this management confederacy.

The authority to plan, test, purchase, and deploy IT solutions must rest with a single accountable organization. The proper organization structure would concentrate all funding, development, integration, fielding, maintenance, and training functions in a single, all-powerful commander. [41:4] That commander would provide a clear vector for all AOC Service and Infrastructure Management activities. The central management body would then provide clear guidance to a distributed federation of AOC sub-staffs to

accomplish the AOC management at the individual sites. This arrangement will yield the accountability and alignment necessary for IT governance within the USAF Air Operations Centers.

4.2.2 Empowerment

The central AOC IT management organization must be *empowered* to enforce policy and punish non-compliance. This is not the case with today's AOC infrastructure. Early AOC configuration control attempts by ESC provide a good example of this point.

There is an inherent need to "lock the system down" in order to centrally manage it. A lock down is simply the application of configuration controls to accurately document system components within the infrastructure. It creates a baseline list of approved components and prevents infrastructure modifications without approval from a configuration manager. The configuration lock down was largely ignored by the warfighting customer/user.

The AOC at Audib was the first AOC to be locked-down and baselined. However, configuration controls were viewed by the warfighter as a 'speed bump' to progress. The AOC personnel at Audib continued to incorporate new systems into the AOC and altered the baseline without utilizing the centralized configuration processes then in place.

The people modifying the AOC were professional soldiers and felt they were acting in the best interest of the military. This practice of unauthorized modifications has occurred and continues to occur in other AOCs as well. The USAF has created this conflict by tasking an AOC management organization to standardize the AOC and telling

the AOC commander to do what it takes to get the job done. [41:3]

The USAF has given AOC commanders the authority to modify their AOC if the benefits outweigh the risk. This authority has been used to overcome the delays of getting new systems approved by the AOC management organization at Langley AFB, VA. Additionally, AOC Commanders have access to independent funds that allow them to purchase IT solutions to their own problems. In fact, the OIF AOC was built entirely using Commander's Incentive Funds. [41:4]

The authority to bypass configuration controls and the financial means to do it combine to create the most formidable obstacle to successful centralized management of the AOC infrastructure. Bypassing the configuration control of the AOC infrastructure management organization is known as an unauthorized variation or a '*drive-by fielding'*.

A drive-by fielding takes place when a vendor simply bypasses the AOC configuration control process at Langley AFB by peddling their products to the AOC commanders directly. If the commander likes the product, he purchases it. He then asks his local AOC IT personnel to plug in the new system and expects them to maintain it. This risky practice has caused significant disruptions of AOC operations and will continue to pose a threat to system safety and stability with current management policies. [27:18]

Drive-by fieldings and unauthorized changes to the individual AOCs significantly degrade efforts to manage the AOC Weapon System because the AOC in the field continues to evolve without the knowledge or approval of the personnel tasked to manage it. The physical AOC never matches the AOC on paper. Testing and planning become

impossible because of the undocumented hardware and software variances among the AOCs in the wild.

IT Governance of AOC IT requires a strong central manager of the AOC infrastructure. He must be empowered by the USAF to establish and enforce AOC IT management policies. Proper centralized management of AOC IT would require the JFACCs to work with the AOC Weapon System's authorized configuration. The authority and funds necessary to modify it must be removed from the customer (JFACC) and given solely to the central management authority. [41:4] The decentralized execution of a centralized Service Management plan would allow the AOC to meet the needs of AOC IT customers and users. While painful, this step is necessary to implement a service-based governance over AOC IT.

4.2.3 Complex System

Managing the information technology within an AOC represents an unbounded, unpredictable engineering activity. The USAF has attempted to apply traditional systems engineering concepts to centralize the management of the complex AOC system. However, the AOC has resisted those management and engineering efforts. [41:3]

Several studies [5, 6, 41, 51] concerning the AOC infrastructure have discouraged the use of traditional system engineering attempts to control the evolution of the AOC. They identify the AOC as a complex system. A complex system integrates independent systems to achieve functionality. It is typically made up of several independent systems that evolve at their own pace.

The AOC is a complex system of systems. It has evolved to integrate numerous

joint and specialized intelligence systems. There are many systems within the AOC that develop independently of the AOC acquisition process. These independent systems, like the Theater Battle Management Computer System (TBMCS), have their own management process and development teams. The AOC has no influence on the release schedules for the other systems. There is potential for these groups to work in isolation or even in competition with each other to manage IT within the AOC. AOC IT management must adapt to the schedules of these independent systems and this creates a reactionary process instead of a proactive approach.

Traditional systems engineering focuses on every detail of a single system or finite number of systems with known states and interactions. However, managing a complex system has been compared to the function of a gardener. A gardener must focus his attention on the growth of the garden as a whole. He accomplishes this by nurturing individual plants and providing a hospitable environment that encourages growth. The gardener cannot force a single plant to do anything. He can only apply positive pressure to encourage growth (i.e. fertilizer, water, light, etc.). The gardener can always 'weed' out the plants he does not want and, therefore, manages the harvest of a flourishing garden. [41:2]

The complexity of the AOC system makes a management focus on emerging technology or the acquisition of individual infrastructure components impractical. Under an ITIL framework, all AOC IT development and acquisition would be based on IT service needs previously identified and documented. The individual IT components would be viewed in light of what service-related capabilities they provide to the AOC customer. Independent AOC SPOs and technology providers would be tasked to provide

services not components. The service requirements focus would allow the AOC gardener to manage the growth of the diverse AOC infrastructure without controlling the specific development and behavior of each component.

4.2.4 AOC Service Requirements

The implementation of ITIL relies on achieving a "customer service" culture. This means that everyone involved with AOC IT must embrace the question "What do the customers need?" Satisfaction of customer needs is the highest priority throughout the ITIL framework. The identification of customer/user requirements and their corresponding services is a prerequisite for the implementation of ITIL.

Table 4.1. AOC Functional Decomposition [13:14]

AOC Functional Decomposition Version AOC-1.2 (88893) 15 Oct 2001

Sequence Number	Activity ID	Activity	Reference	Change Action	Thread
1.3.9.1	S1V120057	Translate air objectives into target sets	AFI 13-1v3 Operational Procedures - AOC, FM 90-36/AFJPAM 10-225		
1.3.9.1.1	S1V120058	Link Associated Category Codes With Objectives	AFI 13-1v3 Operational Procedures - AOC		
1.3.9.1.2	S1V120059	MIDB Target Search For Linked Category Codes	AFI 13-1v3 Operational Procedures - AOC		
1.3.9.2	S1V120060	Perform nodal analysis of target	AFI 13-1v3 Operational Procedures - AOC, FM 90-36/AFJPAM 10-225		
1.3.9.2.1	S1V120061	Analyze target systems to determine critical nodes to attack to achieve desired effects	13-1:7.4.2.5		
1.3.9.3	S1V120062	Prioritize targets within target sets	AFI 13-1v3 Operational Procedures - AOC, FM 90-36/AFJPAM 10-225		
1.3.9.4	S1V120063	Identify combat assessment criteria (including MoM)	AFI 13-1v3 Operational Procedures - AOC, FM 90-36/AFJPAM 10-225		
1.3.9.5	S1V120064	Develop JFACC's recommendations to the CINC's No Strike/Restricted Target List	AFPAM 14-210, p. 51		
1.3.10	S1V120065	Determine Phasing	JP 3-56.1, EAF C2 Process Manual: Chap 2		
1.4	S1V120066	Compare Aerospace Courses of Action (COA)	JP 3-56.1, EAF C2 Process Manual: Chap 2		
1.4.1	S1V120067	ID Standards of Comparison	JP 3-56.1, EAF C2 Process Manual: Chap 2		
1.4.2	S1V120068	Apply Standards to COAs	JP 3-56.1, EAF C2 Process Manual: Chap 2		
1.4.3	S1V120069	Analyze Results of Application	JP 3-56.1, EAF C2 Process Manual: Chap 2		

14

Fortunately, the USAF AOC processes, activities, requirements, and capabilities are well known. They are documented in products like the AOC Function Decomposition product in table 4.1. The ESC personnel have already begun identifying

AOC user requirements and linking them to AOC functionality. ESC uses a Requirements Traceability and Management (RTM) tool. The RTM tool is used to capture, track, and manage AOC requirements generated by the Government and DOD personnel. The system is integrated into several architecture and documentation databases to facilitate the rapid evaluation of the requirements into the AOC system.

Unfortunately the requirements are used to justify specific AOC component purchases instead of identifying IT services to resolve military capabilities. If an AOC customer requirement was the need to exchange SECRET information with coalition partners that requirement should drive the specification of a service. In this case, the service would break the requirement down into an SLA documenting the expectations of the customer. The delivery of a SECRET messaging service to the AOC customer is the focus of ITIL, not the physical IT solution.

4.3 AOC Service Delivery

Service Delivery includes: Capacity, Financial, Availability, Service Level, and Continuity Management. These ITIL areas define, create, document and improve IT *services* required to resolve IT-related military *requirements* and provide adequate *capabilities* to the users. They are concerned with the current health and future growth of the IT infrastructure. There is very little attention given to Service Delivery processes in the current AOC IT management organization.

4.3.1 AOC Financial Management

An ITIL-based Financial Management of the AOC is complicated by federal requirements. The AOC must project budgets years in advance without a clear

understanding of what resources will be available or the needs of the future warfighter. Many of the emerging technologies attractive to C2 systems like the AOC were not conceived when the budget process for the current year was created. This challenges IT managers to find legal and expeditious ways to pay for the technology going into the AOCs. Often the purchase of technology requires costly testing and accreditation efforts in addition to the component's purchase price.

ITIL AOC Financial Management will be complicated by a lack of control and influence over all AOC-related spending. AOC budgets are supplemented by other sources in the USAF. For example, a MAJCOM may decide to buy specific components for the AOCs within its theater. Other AOCs would not have access to that money or components. This dispersion of buying power within the USAF complicates AOC standardization and planning processes.

The USAF currently uses a centralized Sustainment Working Group to examine the initial and long-term support costs of various technologies. This group attempts to identify the overall cost of a *system*. Alternatively, the ITIL framework recommends an internal economy approach based on the costs associated with providing a specific *service*. The cost for a service is more useful than the costs of individual technology components used to create an infrastructure. Service costs allow customers to prioritize IT spending on processes, requirements and capabilities rather than constantly buying the latest technology.

An IT service orientation would help stabilize the USAF budgeting challenges as AOC IT services are identified and assigned a financial value. The services required would be based on documented AOC requirements. These requirements and their

resolving services should not change significantly from year to year. However, the technological solutions used to provide the AOC IT services will change. The job of translating the costs of the technology into a cost for the supported service is the job of ITIL Financial Management.

Users and customers indirectly determine service costs by specifying service level expectations in an SLA. ITIL IT providers buy technology to resolve those expectations. If the user increases the quality or quantity expectations of a service, the increased cost of the technology required to resolve that higher level of service is passed on to the customer as a service charge.

The use of ITIL Financial Management accounting, budgeting, and billing to create an internal AOC economy would help promote efficiency and an understanding of the value of IT services. Services would be paid for by the individual AOCs. Lapses in service levels result in financial penalties for the provider. That provider might be military or a contractor. The internal economy promotes the value of outstanding customer service.

4.3.2 AOC Continuity/Availability Management

The AOC availability and continuity requirements are rigorous. AOCs have been studied extensively to identify potential weaknesses in the infrastructure. AOC continuity refers to the ability to recover from a disaster. The USAF tests AOC systems and subsystems for integration problems or vulnerabilities that would result in loss of AOC capabilities. These are maintained at the individual sites and are tailored for each AOC. However, these continuity and availability plans are based on components of the

infrastructure instead of services.

The ITIL Continuity Management function is a service-based disaster response plan. Service-based redundancy, security, and recovery plans result in graceful degradation of AOC performance that can then be restored quickly. Service-based recovery plans are more intuitive for an AOC commander. He can prioritize AOC services more readily than the physical components and databases that make up his infrastructure.

ITIL Availability and Continuity Management issues must be addressed througout the planning and acquisition stages of IT management. Any proposed changes to the IT infrastructure would be examined by the ITIL Availability and Continuity Management teams to prevent IT component changes from introducing new vulnerabilities to the AOC IT services.

4.3.3 AOC Capacity Management

ITIL's Capacity Management predicts the infrastructure's ability to meet IT service requirements. It is the ability to measure the current service usage of infrastructure resources against maximum resource throughput. The ability to identify infrastructure bandwidth requirements with respect to services is very different than simply measuring the number of IP packets that can be transmitted over a link. Understanding IT service capacity needs and knowing the capacity of the IT infrastructure allows the IT staff to make smart decisions in the utilization of finite resources like bandwidth. An AOC commander can now prioritize certain services as more important than others. This allows for proactive resource utilization.

The elusive capacity metric is currently reactive in nature. The USAF must use a trial and error approach to establish bandwidth requirements. For example, an AOC can not predict whether a teleconference has to be rescheduled if there are three UAV missions currently utilizing the available bandwidth. This is because IT personnel typically think of capacity with respect to components not the services required for a teleconference or UAV mission. A focus on service capacity simplifies the visualization of infrastructure requirements.

ITIL Capacity Management is dedicated to the study of the IT infrastructure with a focus on service requirements as well as the capabilities of individual network components. [50] discusses ways to identify the network components used by specific services within a network. This technique combined with the idea of ITIL Capacity Management would help develop contingencies for the loss of specific services.

Matching infrastructure components to the services they support allows an AOC Commander to search his infrastructure for vulnerabilities to specific services. Knowledge of which network components are required for individual services allow the IT staff to make intelligent decisions concerning which component should be fixed first to restore the most important services.

4.3.4 AOC Service Level Management

One of the largest hurdles the USAF will have to overcome in the implementation of ITIL is the proper use of Service Level Agreements. Service Level Agreements are difficult to create and enforce because they require cooperation at an enterprise level. The effort to identify the large number of user requirements is an enormous task.

However, the establishment of Service Level Agreements is absolutely essential to implementing ITIL.

SLAs are extremely important in identifying and documenting user/customer requirement owner and the owners of the corresponding IT service solutions. They specify responsibilities with measurable criteria that serve as metrics of performance. These metrics are then used to identify short falls or breaches of service levels. The AOC SLAs should be supported by OLAs linking various external IT suppliers together in order to provide a service. The OLAs should have clear levels of performance specified with accompanying metrics. The OLAs should be enforceable and easy to modify.

The USAF has already tasked the SPO to create and maintain Service Level Agreements (SLAs) with peer organizations providing AOC components. [28] Unfortunately, the AOC SLAs very different from the SLAs described by ITIL and were created for a different function. The current AOC SLAs are more accurately viewed as Memorandums of Agreements that establish programmatic, engineering, and sustainment business relationships between the AOC SPO and other program offices. They communicate interface controls, test plans, and problem resolution strategies between agencies. These are not the SLAs referred to in ITIL because they do not specify services or levels of service.

The nature of the customer service culture in an organization is based on the efficacy of its SLAs. A complete collection of detailed and clear SLAs promotes cooperation and alignment within an organization. A history of enforcing the SLA service levels generates customer buy-in to the service culture. The implementation of SLAs will largely decide the success of an AOC ITIL Service Management

implementation.

4.4 AOC Service Support

Service Support includes the areas: Change Management, Configuration Management, Incident and Problem Management. Service Support focuses on maintaining an infrastructure capable of supporting the services needed by an organization. Some of the ITIL Service Support best practices are already being accomplished in the current USAF AOC IT management processes. For example, the USAF is already using its version of a federated Service Desk to improve its incident management capabilities.

4.4.1 AOC Incident Management

Incident Management represents one of the fastest returns on an ITIL investment. The USAF has implemented a distributed Help Desk system for the AOCs around the world. The Help Desk operates a three-tier system of customer service. The Tier-0 level of the Help Desk service utilizes a local help desk manned by technicians on site at the individual AOCs. These technicians include AOC communications personnel, System Administrators, System Managers and local Wing Network Control Center personnel. They defer the problem to the Tier-1 centralized Help Desk if they are unable to solve the problem within a specified amount of time.

Tier-1 support is provided by a Help Desk maintained by the 83rd Communications Squadron located at Langley AFB, VA. The main functions of the 83rd Help Desk (HD) are event management, internal infrastructure management, and configuration control. They are tasked to provide a single focal point for reporting,

tracking, and resolving problems encountered in an AOC. If Tier-1 cannot resolve the problem, it is sent to Tier-2. [15:5]

Tier-2 is composed of individual engineers from companies that wrote the original software or built the hardware that is used in the AOC WS but not managed by the AOC SPO. Currently, there are more than thirty major systems managed outside the influence of the AOC SPO. These 'external' systems have their own support staff and sometimes their own help desk structure to support events involving their components.

Unfortunately, there is no way to provide 24/7 Tier-1 or Tier-2 support at this time. Tier-1 support is currently limited by manning and funding. This is an issue that will soon be resolved. Lack of complete Tier-2 coverage is a much more difficult problem to solve. Tier-2 response times vary from system to system. Many Tier-2 systems do not schedule staff during the evenings or weekends. This can lead to uncomfortably long wait times if an AOC system goes down during the Thanksgiving holidays, for example. The AOC SPO has no leverage or funding to increase Tier-2 coverage.

Another problem involves Tier-2 system employees working at the local AOC site supporting the software or hardware as part of a contract with the USAF. Often these engineers will contact their respective company directly instead of going through Tier-1 first. This practice is efficient but excludes the USAF HD system and prevents the capture of valuable metric and resolution information.

ITIL recommends the use of an integrated database to expedite the documentation and resolution of incidents. The 83rd HD uses a modified Remedy electronic trouble ticket system known as the AOC Service Support System (AS3) to track and resolve

events (i.e. incidents). The AS3 system will eventually become a central repository of resolution information and metrics that should provide information to administrators and managers throughout the AOC IT system.

Currently, the 83rd HD is the sole user of the system and some AOC events are resolved without interacting with the AS3 system. Additionally, the AS3 is not integrated with the Configuration Management process and cannot provide accurate metrics to identify systemic problems within the AOC WS. These shortcomings limit the synergy of the Incident Management potential in the current implementation of AS3.

It is evident that the USAF has invested in improving its ability to provide technical support to the AOCs in the field. However, an ITIL Incident Management would require a dedicated Help Desk committed to outstanding customer service and accountable to a single management authority. The USAF needs to abandon the 83rd Communications Squadron temporary fix in favor of a dedicated facility with the personnel and resources to provide 24/7 resolution of infrastructure incidents. The Remedy AS3 software system used by the Help Desk is adequate, but it is not integrated with an AOC CMDB. Any changes made to the AOC infrastructure as a result of a Remedy tracked solution must be manually entered into the Configuration Management database. This makes it challenging to control the system configuration, look for trends associated with specific component failures, or track maintenance costs associated with software products. An integrated version of AS3 will aid the USAF in implementing an ITIL solution.

4.4.2 AOC Problem Management

The USAF does not currently have a ITIL Problem Management process for the AOC. The lack of Problem Management reduces the Incident Management function to a reactionary approach for maintaining required levels of service. Problem Management looks for root causes to related incidents in an effort to reduce the number of service level breaches in the future. The Problem Management function should be linked to the Help Desk, Configuration and Change Management to facilitate the prompt investigation of an AOC problem. An AS3 trouble ticket system integrated with the CMDB systems would allow Problem Management investigators access to comprehensive information about the AOC infrastructure. The integrated CMDB would also document any changes made to the infrastructure during the solution of a problem.

4.4.3 AOC Change Management

Change is inevitable. There will always be new requirements and capabilities within the AOC Weapon System. However, a technology-centric approach to managing that change is impractical and destined to fail. Change Management within the USAF AOC IT organization emphasizes a service-based approach to managing the integration of new technology into an infrastructure.

USAF attempts to manage change by enforcing baselines and exercising configuration control on the numerous AOC infrastructures within the USAF have been unsuccessful. The individual AOC Commanders and their staff continue to modify and evolve their AOC to suit their needs because they focus on the flexibility offered by the quick fix. The AOC management authority requires stability in order to provide safe

technology integration into the AOC Weapon System. The need for stability and flexibility compete against each other. The identification of IT services and the requirement to provide those services gives both the AOC management and the AOC customer a common reference to balance the two needs.

Stability and standardization are needed to centrally manage services within the AOC infrastructure. The centralized management and standardization of the AOC IT services lead to greater specialization, economies of scale, consistency, and standardized controls. [47:10] Stable IT services provide a synergy of trained personnel and capable systems through a standardized baseline of manpower, equipment, applications, training, and processes. This ensures a consistent and clearly understood capability presented to a JFACC. Stability allows for certification that assures the USAF that the AOC Weapon System is properly trained, organized, and equipped. [25:10]

The AOCs are used to flexibility. They have become accustomed to running their own operations. They have a long history exercising business ownership of their IT problems and corresponding solutions. Flexibility is required to allow an AOC to adapt to its environment. AOCs must support the full spectrum of operations from conflict to peace keeping to disaster response. Flexibility allows the rapid integration of technology into the AOC system. AOC Commanders demand responsive integration of the latest technology into their AOC to help them achieve their operational objectives. Rapid integration requires a short response time to emerging technology and a way to quickly test and field new capabilities. Local AOCs do not want to surrender their independence to a central management function because they will lose flexibility.

Change Management can work as a thermostat to balance the need for centralized

management stability and distributed operational flexibility using a federated approach. It places the IT decision making authority and policy enforcement at the central management level. It provides clear guidelines concerning the IT services to be provided to the AOC users and customers. The local AOC sites would have the flexibility to make adjustments to local operations within the service guidelines provided by the centralized management authority. The local AOC sites remain responsible for the safe operation of their systems and are held accountable by the central authority.

ITIL Change Management must employ a service-centric view of AOC IT management to be effective. Military requirements and their resolving IT Services are more stable and persistent than the IT technology that supports them. Identifying requirements, services, and capabilities allow the competing concepts of stability and flexibility to be aligned with organization goals and strategies.

Johnson and Johnson faced a similar conflict between stability and flexibility as it tried to achieve IT Governance over its global business. Johnson and Johnson struggled with distributed and diverse organizations that were used to a decentralized management style. However, the need to reduce costs and improve services required them to centralize the IT infrastructure management. Early attempts by Johnson and Johnson to centralize IT failed due to "cultural barriers and business resistance to change"

They found success with the federated approach. Johnson and Johnson "challenged local business managers to surrender business-specific IT domains for the good of the enterprise and to establish business-to-corporate and business-to-IT partnerships. The federated approach allowed local IT staff personnel to solve problems at the lowest level as long as central management policies were followed. Johnson and

Johnson was able to centralize the IT decision process without removing responsibility for IT decisions from the individual business managers. [47:12]

4.4.4 AOC Release Management

The ITIL Release Management principles address changes required to improve established services. It is the integration of numerous authorized IT service-related changes into a single 'release'. The USAF is currently using a concept called spiral evolutionary development. It is a similar idea, except that it focuses on components and systems rather than services.

The biggest challenge facing an AOC central management authority is responsiveness. Identifying user/customer requirements and resolving them safely requires time to validate, test, and deploy the solution. This cycle represents a bottleneck in the throughput of authorized changes to the AOC Weapon System. That bottleneck is perceived by AOC users/customers as a lack of responsiveness and accountability.

The perceived lack of responsiveness is due to inadequate manning and facilities to meet the demands of a complex system like the AOC. The USAF tasked the Air Force C2 Test Center (AFC2TC) to help expedite testing and the integration of new C2 technology. The AFC2TC manages the primary test bed for the AOC (CAOC-X at Langley AFB, VA). Other AOC facilities at Nellis AFB, NV, and the FTU at Hulbert Field, FL have been used for testing as well. These facilities have significant simulation limitations. These test facilities cannot accurately simulate the Falconer AOCs due to the large number of authorized and unauthorized variations among the real world AOCs.

AOC system engineers and testers have become swamped with requests from

individual AOCs to install new hardware or update software products. Attempts to integrate new technology become bogged down in testing and budget bureaucracy. Unauthorized variations will continue to plague the AOC system due to delays associated with inadequate testing facilities and long response times.

Users experience frustration as their requirements for the upgraded systems seem to go unheeded. The users/customers sense a lack of accountability at the AOC IT management level because their requirements never seem to materialize into IT solutions. Often customers/users utilize drive-by fieldings to create their own IT solutions. These solutions provide quick fixes but create long-term problems associated with undocumented variances from the base lines. [27:18]

While, a service-orientation in the AOC would help slow down the onslaught of technology specific requests; it will not solve the testing bottleneck experienced by the AOC management organization. The USAF must invest heavily in flexible test facilities capable of simulating any AOC configuration currently in use. The number of test personnel must be increased to open up the bottleneck and allow a more agile response to the need for change in the AOC infrastructure.

4.4.5 AOC Configuration Management

The Configuration Management function must be executed in a uniform manner if it is to be effective. There must be a clear understanding of Configuration Management policy. Those responsible for executing it must be held accountable for its proper execution.

Currently there is little enforcement of AOC Configuration Management authority

or policies. Numerous examples of work arounds and drive-by fieldings attest to a lack of understanding of the importance of Configuration Management. [27:18] Clear enforceable policies must be put in place to both educate and facilitate the implementation of this important ITIL Service Management principle.

The Configuration Management process is currently split between personnel on site in the AOC and the ESC personnel at Langley AFB. Configuration Management personnel at Langley are tasked with maintaining a reference baseline CMDB that represents the ideal AOC configuration. There are also autonomous Configuration Management staffs at each AOC that maintain an independent, site-specific CMDB for their AOC Commander. In addition, they maintain a separate media and documentation library as well. Each AOC site runs an independent Configuration Control Board (CCB) to determine the changes that will be implemented at that specific AOC. [23:10]

This division of the configuration management function causes problems because the AOC Configuration Management personnel work directly for the AOC commander instead of ESC. The local AOC Configuration Management personnel can and will continue to alter the AOC configuration without coordinating or even communicating that event to the ESC Configuration Management personnel at Langley AFB, VA.

This disparity introduces undocumented inaccuracies between the baseline and the actual AOC infrastructure at each location. The inaccurate baseline is used to make planning, testing and implementation decisions that affect all AOCs. Therefore, ESC has had to conduct an annual audit of each AOC to reestablish each AOC's official configuration.

An integrated CMDB is fundamental to the ITIL framework. The CMDB should

contain complete configuration data for all of the AOCs. This data must be accurate and dynamically represent the actual configurations of AOCs in the field. This is not possible with the current management implementation of Configuration Management.

The USAF currently uses several independent databases to manage the AOC IT technology. USAF and DOD guidance require the AOC personnel to maintain the independent databases to track AOC equipment. All hardware purchased for the AOC must be tracked in a Logistic Support Plan/Program Support Management Plan database IAW AFI 33-112 *Computer Systems Management*. Commercial computer equipment must be accounted for in the Information Technology Asset Management System (ITAMS) database. And certain high-value equipment with national stock numbers are tracked the in the Air Force Equipment Management System (AFEMS) database IAW AFMAN 23-110 USAF Supply Manual. [15:16] These parallel databases create drag and confusion in managing change in the AOC WS.

An integrated CMDB is required to track the IT service solutions from implementation through the retirement phase. An integrated CMDB provides continuity and collaboration between the AOC management organizations. While there are a number of commercial CMDB products available, the federated middleware solution appears to offer the best solution at this time. A federated CMDB is a middleware solution that will integrate legacy stovepipe databases to provide a seamless view of the stored data. In any case, the integrated CMDB is necessary for the USAF to properly implement an ITIL Service Management framework.

4.5 Summary

This chapter established arguments for the creation of an empowered centralized organization using a service-based framework to manage AOC IT. AOC resistance to traditional management controls was linked to its complex nature. And the ITIL Service Management functions Service Delivery and Service Support were applied to specific AOC functions.

The adoption of a service-centric framework is necessary to move towards IT Governance. The current AOC IT management organization will continue to struggle as it seeks to find a balance between stability and flexibility. The lack of USAF empowerment will prevent the enforcement of necessary AOC IT configuration control. The warfighter perception of a lack of AOC management accountability and responsiveness to their requests will continue to frustrate configuration control attempts.

While the AOC IT management focus remains on technology components, there will always be an overwhelming demand for newer systems and software. Expectations of AOC IT quality, innovation and value continue to increase while budgets for IT are scrutinized. To achieve mastery over AOC IT the USAF's technology-centric paradigm must evolve into a business/service-centric view. [40:2]

The use of an ITIL Service Management framework to shift the focus of the AOC organization to a customer service paradigm is necessary to achieve alignment between AOC IT management and the warfighter. That alignment will effect the transformation of the current AOC IT management organization into the agile IT organization needed to provide safe, integrated C2 capabilities to the JFACC and his staff.

V. Conclusions and Recommendations

5.1 Summary

AOC IT management has evolved significantly over the past forty years. The early individualized evolution of the AOCs has been difficult to manage and control through traditional system engineering methods. Managing rapid technological changes in a complex AOC weapon system is not possible using the Darwinian decentralized management style of the past or the current semi-centralized distributed management practices in place today.

Current centralized management efforts have not been effective because they were diluted across numerous stakeholders who lacked empowerment to enforce policies. Additionally, the USAF has approached the AOC IT management problem by concentrating on the management of infrastructure components and their capabilities rather than services. They assembled a loosely coordinated team of technicians and engineers to maintain numerous legacy network infrastructures and then asked them to solve the ensuing IT problems.

The AOC management organization was given little or no authority to enforce IT management configuration control. The individual AOCs purchase IT solutions without consulting with the IT personnel that will maintain it. This results in excessive expenditures on equipment that may not meet the expectations or needs of a distributed and complex organization. This research proposes an ITIL Service Management framework that changes the AOC IT management focus from technology components to

user service requirements.

The USAF needs to exert more control over the AOC to increase its efficiency while lowering operational costs. MGen Tommy Crawford, Commander of the AFC2ISRC, captured the USAF's vision of the future AOC when he said "The USAF believes a true network-centric command and control environment will enable dominance of the air/space/info battle space and lead to seamless integration into joint command and control. … It [the AOC] will have 4D instant deconfliction of airspace and be able to digest and fuse full spectrum ISR in an instant. It will be capable of interoperability with any foreign partner through true multi-level security at the data level." [10]

The current semi-centralized AOC IT management organization lacks the empowerment and vector required to deliver the capabilities demanded by AOC commanders. In order to provide the AOC of the future, the USAF needs to change the way it manages AOC information technology. It will require a break lock from the technology fixation and the adoption of an agile service-centric paradigm.

The use of ITIL in the AOC IT management process will enable greater agility and control over the technology used in the AOC. It will help the AOC integrate new technology faster and help position the AOC for the future. The incorporation of service-centric best practices is necessary to enable IT governance in the AOC IT enterprise.

5.2 Conclusions of Research

The proposed transformation of the AOC infrastructure into a responsive and valuable contributor to the warfighting capabilities of the USAF will require the adoption and adaptation of AOC ITIL management framework and functions. The three factors

required to achieve AOC IT governance transformation are:

1) Focused USAF leadership *empowerment.*

2) The establishment of a *single centralized enforcement authority*.

3) The adoption of an *IT service management* orientation.

The AOCs need ITIL's customer-centric approach to providing IT services designed to resolve business IT process requirements and provide capabilities. ITIL Service Management principles applied across an empowered centralized AOC management organization will achieve necessary progress towards IT governance.

The USAF and the AOC management personnel need immersion in ITIL principles and applications. A USAF leadership and AOC customer/user buy-in is required to establish the necessary customer service culture within the AOC infrastructure. The paradigm shift from technology to services is difficult. However, it has been done by several large organizations facing similar challenges and must be accomplished to achieve an IT Governance transformation.

The AOC management function must be completely restructured into an all-powerful centralized management body with the empowerment necessary to establish and enforce ITIL service-based policies. This empowered central management function will provide the agility necessary to balance flexibility and stability in light of rapidly changing technology.

5.3 Significance of Research

Many of the ITIL best practices are already incorporated in the management of the AOC Weapon System. However, the integration of a service-centric management framework is noticeably missing. The USAF is currently seeking the aid of a Weapon System Integrator to transform the AOC into a lean, agile, integrated system with a small footprint and a wide field of view. ITIL expertise and experience should be a requirement for the job. The establishment and empowerment of a central AOC IT management body with the authority to implement and enforce a service-centric framework on AOC IT infrastructure enterprise is necessary to achieve the transformation to IT Governance the USAF seeks.

5.4 Recommendations for Action

Educate AOC management personnel on ITIL principles and applications

Reorganize AOC management function into a single all-powerful organization

Pursue WSI contract with an emphasis on ITIL based methods of IT management

5.5 Recommendations for Future Research

Application Management: ITIL's Application Management functions are designed to help large companies control the dynamics associated with developing software. The AOC is attempting to evolve its legacy TBMCS collection of software tools into a leaner, more integrated application (i.e. TBONE). The use of ITIL Application Management could be useful in the transition.

Security Management: ITIL provides a Security Management set of best practices that would be applicable to the multi-level security requirements of the AOC. Research into specific Joint/Coalition applications would be useful.

Quality Tools: There are several tools currently used to compliment ITIL management implementation in achieving IT Governance within an organization.

These tools include: Control Objectives for Information and Related Technologies (CORBIT) tools, PRINCE2 (project management methodology for a rapidly evolving operational environment), Six Sigma (techniques to measure quality of changes and services), and Capability Maturity Models (used to measure software quality). [40:11] These tools help assure quality and security requirements are met in the provision of IT services.

Proprietary Solutions: While ITIL is vendor independent, several companies offer ITIL in a box. These solutions set up a scalable CMDB and integrate it with all aspects of ITIL Service and infrastructure management. A thorough investigation of the strengths, weaknesses, and applicability of these products to the AOC IT management problem would be useful to USAF officials.

Bibliography

1. Alexander, Christopher. *The Timeless Way of Building.* Oxford Press, 1979

2. Bartolini, Claudio and Salle Mathias. *Business Driven Prioritization of Service Incidents*. Trusted Systems Laboratory, Oct 2004

3. Bartonili, Claudio and others. *Management by Contract: IT Management driven by Business Objectives.* Hewlett Packard Company, 2004

4. Bartonili, Claudio and Salle Mathias. *Business Driven Prioritization of Service Incidents*. Hewlett Packard Company, 2004

5. Bar-Yam, Y. and M.L. Kuras. *Complex Systems and Evolutionary Engineering.* AOC WS Contracting Office, Sept 2003

6. Bar-Yam, Y. *Complex Systems and Evolutionary Engineering* AOC WS LSI Concept Paper, Sep 03

7. Behler, Robert. *Perseverance with a 'big picture look' is key to integration* intercom – Journal of the Air Force C4 Community. Langley AFB VA, September 2002

8. Betz, Charles. *The Convergence of Metadata and IT Service Management,* 2003

9. Center for Information Technology at the National Institutes of Health. *Information Technology Management Reform Act Summary*. 5 Jul 2005 http://irm.cit.nih.gov/itmra/itmrasum.html

10. Crawford, Thomas. *AFC2ISRC's Vision of the Future AOC.* https: AOC website. Accessed 12 July 2005.

11. Dare, Rob and Allen Knoff. *AOC Weapon System Infrastructure Technical Requirements Document* (DRAFT). 18 Mar 2005

12. Deming, N. *TBONE on the menu.* C4ISR Journal, November/December 2004

13. Department of the Air Force. *Aerospace Operations Center (AOC) Functional Decomposition* Version AOC-1.2. Aerospace Command and Control & Intelligence Serveillance and Reconnaissance (C2&ISR) Center. Langley AFB, VA, 15 October 2001

14. Department of the Air Force. *Air and Space Operations Center AN/USQ-163 Weapon System Configuration Control Board Charter*. Electronic Systems Center. Hanscom AFB, MA Dec 2004

15. Department of the Air Force. *Air and Space Operations Center Weapon System Help Desk (AOC WS HD) Enabling Concept* (Draft). Air Combat Command Langley AFB, VA. 30 Mar 05

16. Department of the Air Force. *Air and Space Operations Center Weapon System Integrated Product Team Charter.* AFC2ISRC/DO, Langley AFB, VA, 30 June 05

17. Department of the Air Force. *Air and Space Operations Center Weapon System AN/USQ163 Falconer Modernization Program* (Revision 1). Electronic Systems Center. Hanscom AFB, MA, May 2004

18. Department of the Air Force. *Air Force Glossary*, AFDD 1-2. HQ AFDC/DR, Washington D.C. 6 September 2005

19. Department of the Air Force. *Air Operations Center Combined Test Force.* AFMC Eglin AFB, FL. 25 Jan 2002

20. Department of the Air Force. *Air Operations Center Road Map* (DRAFT). 10 February 2004

21. Department of the Air Force. *AOC Weapon System Acquisition Strategy.* AOC SPO Langley AFB VA, 22 April 2005

22. Department of the Air Force. *Charter for the Command and Control General Officer Steering Group (C2 GOSG)* (DRAFT), May 2005

23. Department of the Air Force. *Configuration Management Plan (CMP) for the Korea Air and Space Operations Center (KAOC) AN/USQ-163 Weapon System* Version 1.0. 607th AOG, 18 June 2004

24. Department of the Air Force. *Memorandum of Agreement between Commander, Air Force Command And Control & Intelligence, Surveillance, and Reconnaissance Center, and Vice Commander, Electronic Systems Center, and Commander, Air Warfare Center, and Commander, Air Armament Center, and Commander, Air Force Research Laboratory, and Commander, Air Force Operational Test and Evaluation Center for Test and Assessment Activity and the Air Force Command And Control Transformation Center*. March 2004

25. Department of the Air Force. *Operational Procedures – Aerospace Operations Center* AFI 13-1 AOC Vol 3, HQ USAF/XOO, 1 July 2002

26. Department of the Air Force. *Program Management Directive 2440 PE# 27410F –The Air and Space Operations Center (AOC) Weapon System (WS) Program , Director, Information Dominance Programs*. Secretary of the Air Force (Acquisitions), 30 Sep 2004

27. Department of the Air Force. *PSAB CAOC Tiger Team-Enabling the full potential of the CAOC Weapon System for CENTAF CC and the USAF Interim Report and Recommendations*, USAF Chief of Staff. 31 May 2002

28. Department of the Air Force. *Service Level/Sustainment Agreement Between Air and Space Operations Center Weapons System System Program Office and Theater Management Core System Program Office.* Hanscom AFB, MA, 28 Jan 05

29. Department of the Air Force. *U.S. Air Force Concept of Operations for the Aerospace Operations Center (AOC).* AC2ISRC/CC, Langley AFB, VA. 9 Mar 2001

30. Department of the Air Force. *U.S. Air Force Policy Letter Digest.* USAFHQ/PA, Washington D.C. Apr 2002

31. Department of the Air Force. *U.S. Air Force Transformation Flight Plan.* HQ USAF/XPXC, Washington D.C. November 2003

32. Dubie, Denise. *Reaping the Rewards of Best Practices.* Network World Inc. Vol 19 Iss. 39, 30 Sep 2002.

33. Fogelman, Ronald R. *Command and Control Weapon System* Memorandum for ALMAJCOM/CC, 1995

34. *Framework for Service Quality Agreement*. ITU-T Rec E.801, October 1996

35. Information Technology Service Management Forum (itSMF). *IT Service Management: An Introduction.* Van Haren Publishing, May 2002

36. Jumper, John P., USAF Chief of Staff. *CSAF Seeks Improvements in Warfighting.* Address during the Air Warfare Symposium, Lake Buena Vista FL, February 2004

37. Jumper, John P., USAF Chief of Staff. *Future Force: Joint Operations.* Address during the Air Armaments Summit VI, Sandestin FL, 17 March 2004

38. Mendel, Thomas. *Centralized CMDBs: Don't Buy Into The Hype.* Forrester Research http://www.forrester.com/Research/Document /Excerpt/0,7211,36584,00.html accessed 11 November 2005

39. Meyer, Dean. *Beneath the Buzz: ITIL.* 31 March 2005

40. *Microsoft Operations Framework.* Microsoft Corporation, August 2004

41. Norman, Douglas. *Engineering a Complex System: A Study of the AOC.* MITRE Corp

42. Norman, Douglas. *Risk Reduction for Selecting the AOC WS Lead System Integrator*. MITRE Corp, 23 August 2003

43. Office of Government Commerce (OGC). *IT Infrastructure Management.* The Stationary Office, 2005

44. Office of Government Commerce (OGC). *Planning to implement Service Management.* The Stationary Office, 2005

45. Office of Government Commerce (OGC). *Service Delivery.* The Stationary Office, 2005

46. Office of Government Commerce (OGC). *Service Support.* The Stationary Office, 2005

47. Peterson, Ryan. *Crafting Information Technology Governance Information Systems Management.* Fall 2004

48. Rudd, Colin. *An Introductory Overview of ITIL*. itSMF, 2004

49. Salle, Mathias. *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing*. Hewlett Packard Company, 2004

50. Stanley, Jeff. *Enabling Network Centric Warfare Through Operational Impact Analysis Automation.* Air Force Institute of Technology, March 2005

51. Stevens, Renee. *Systems Engineering in the Information AGE: The Challenge of Mega-Systems*. MITRE Corp

52. Violino, Bob. *IT frameworks demystified; ITIL, COBIT, CMMi, ISO 17799 – best practices abound for managing the new data center.* Network World; Feb 21 2005

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
22-12-2005	Master's Thesis	June 2004 – December 2005

4. TITLE AND SUBTITLE

Leveraging ITIL to Govern AOC Information Technology

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

1. AUTHOR(S)

Weaver, Robert V. III, Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIA/ENG/06-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Lt Col Robert Dare OC2SG/KQ
11 Barksdale St, Bldg 1614
Hanscom AF Base, MA 01731 [Robert.Dare@hanscom.af.mil]

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Air Operations Center (AOC) is a complex system of systems that is resistant to traditional engineering controls and management strategies. The US Air Force (USAF) seeks to transform its antiquated AOC Information Technology (IT) management function into an agile enterprise capable of leveraging cutting-edge technology by aligning the AOC's infrastructure with its organizational strategies and vision. The USAF calls this effort a transformation. Private industry calls it IT Governance.

To achieve AOC IT Governance, the USAF must stop managing infrastructure *components* and start managing IT *services*. IT Service Management abstracts business processes from the technology supporting them by creating IT services. Those services resolve business process requirements and provide IT capabilities. Effective IT Service Management requires an all-powerful, centralized IT management organization focused on providing value to the enterprise through the monitoring and improvement of IT services aligned with enterprise goals and strategies.

This research will focus on the potential benefit of a service-centric collection of industry best practices known as the Information Technology Infrastructure Library (ITIL). The ITIL best practices are designed to enable the implementation of IT Service Management. The ITIL framework is a necessary step forward in the USAF's quest for IT Governance.

15. SUBJECT TERMS

*Management Information Systems, *Military Procurement, Configuration Management, Infrastructure, Resource Management, Management Planning and Control, Systems Management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert F. Mills, (ENG)
U	U	U	UU	114	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4527 (Robert.Mills@afit.edu)