The 7th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 15th 2012

ITIL&FCAPS - NETWORK MANAGEMENT FUNDAMENTALS

Barbu Gheorghe

Air Forces

Abstract:
This paper briefly brings together the basics of two network management frameworks. The reader will understand that there are a lot of models used in network modeling and management processes, but only two of these all are essential in simplifying network representation, managing, preparing for the future and developing. Network management fundamentals frameworks as ITIL and FCAPS are the keys of success in these areas.

Key words: FCAPS, ITIL, Network management framework, information technology

1. Overview

Anecdotal evidence suggests that an operator's ability to manage a network decreases as the network becomes more complex. However, there is currently no way to systematically quantify how complex a network's design is nor how complexity may impact network management activities.

Network management is a large and complex topic. In nowadays diverse networking infrastructure, the network concept has to handle more instances of unified communications, video, and virtualization.

The role of the network management process includes not only monitoring for performance and security, but also anticipating and estimating future network problems and transcending technology to ensure everything runs well together, whether it's the network, the server, or the application.

Network management means different things to different people. As example, for the Chief Information Officer of an organization it would mean being able to ensure that the enterprise IT infrastructure (consisting of departments, locations and services) is performing optimally. On the other side, from the point of view of the network administrator, network management is defined as a set of activities where a variety of tools, applications, rules and devices are utilized by IT personnel to monitor and maintain information technology networks. To the network manager it would mean managing the details that constitute this high-level view.

As a general view, in the simplest terms, network management translates into managing fault and performance across applications, servers and networks.

2. Issues

In order to make an analysis with a more accuracy of what network management means, we need to find answers at the next questions:

2.1. What are the needs to be monitored?

First, we need to define the scope of the needs to be monitored and managed when we are dealing with networked applications.

Secondly, in order to provide satisfactory performance levels, we must be able to identify an array of problems that can have their source in the applications themselves, in the servers on which the applications run, or in the network. In the network, devices, applications, connections and configuration can all have an impact on the end-user service experience.

Finally, we have to determine how to resolve these problems. So, for assessing monitoring and management needs at a minimum level, we must plan to monitor:

2.1.1. End-user experience

We need to know whether there are response time problems before end users call the help desk or service desk to complain. We need to know whether a business application or service could fail or slow dramatically, threatening business revenues or institution image.

2.1.2. Servers at both ends and the devices in the network

We need to know if everything is configured correctly. Are servers performing correctly? Do performance level trends indicate an emerging problem? Is anything near a saturation point?

2.1.3. Traffic through the network

We need to identify which applications are consuming the most resources. Is the routing appropriate? Are there bottlenecks and when and why these could appear? Are some resources (hardware or software) over- or underutilized?

2.2. Which monitoring tools do we have?

Once we understand what we need to monitor, we can move to inventory and assess which tools and application resources we have available to do that task today. Then, to determine what data and information is currently collected. This information can provide insight into what is happening in the operational environment and how it will affect business service delivery and performance commitments. Knowing which tools and data we already have available that will allow determining the additional resources that we need in order to perform the overall management task.

3.Solutions

Nevertheless, we still have not achieved the expected results and in addition there are two frameworks which can use for understanding and taming network management: **FCAPS** and **ITIL**.

3.1. FCAPS

FCAPS (fault-management, configuration, accounting, performance, and security) is actually a network management device also called the ISO Telecommunications Management Network. It is an acronym for a categorical model of the working objectives of network management, part of the OSI Network Management model. This model helps the network and system administrators to understand the major functions of network management systems and to provide knowledge to understand and surpass different issues in order to protect its environment. Without it, many system downtimes would occur and the organization may suffer a large financial or/and image loss.

This framework includes five levels:

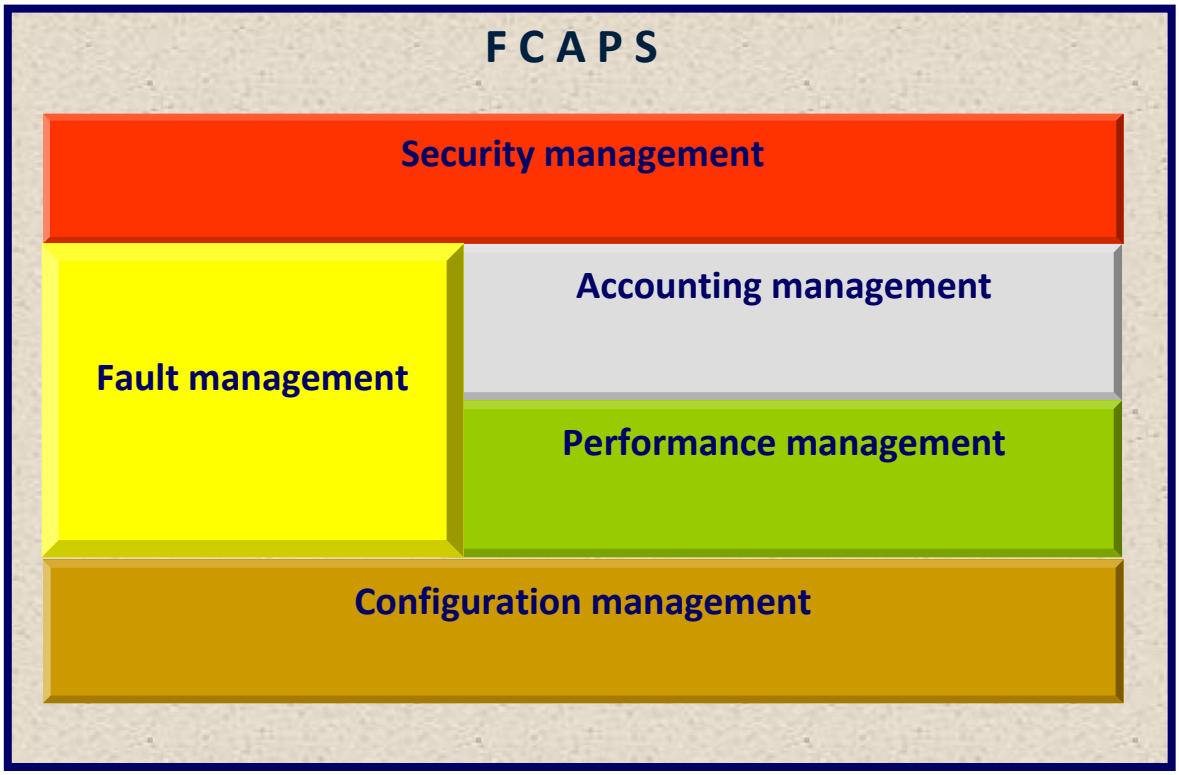


Fig. 1 FCAPS model levels

3.1.1. Level F—Fault management

At the F level, network problems are found and corrected. Potential future problems are identified, and steps are taken to prevent them from occurring or recurring. In this way, the network is kept operational, and downtime is minimized.

In Fault Management level, the aim is to recognize, isolate, correct, and log faults on the network. As a system and network administrator, it is your duty to put in right place efficient monitoring tools so you are alerted to when faults exist. For example, you want to be alerted when something (e.g. a critical service) goes down on the network. If there is a fault, you have to test, fix, update, and repair any faults that occur on the network.

A common fault management technique is to implement an SNMP-based network management system - such as HP Open View or Sun Solstice (formerly Net Manager) - to collect information about network devices.

3.1.2. Level C—Configuration management

At this level, network operations are monitored and controlled. Hardware and programming changes, including the addition of new equipment and programs, modification of existing systems, and removal of obsolete systems and programs, are coordinated. An inventory of equipment and programs is kept and updated regularly.

While it is possible to track these changes manually, a more common approach is to gather this information using configuration management software, such as Cisco Works 2000.

3.1.3. Level A—Accounting (allocation) management

The A level is for distributing resources optimally and fairly among network subscribers. This makes the most effective use of the systems available, minimizing the

cost of operation. This level is also responsible for ensuring that users are billed appropriately.

Accounting Management is concerned with aspects of the system users. It mainly focuses on charging and billing users for services, and regulating service use (printing services, Internet/bandwidth, disk space usage, application and software use, etc.).

While this may not be applicable to all companies, in many larger organizations the IT department is considered a cost center that accrues revenues according to resource utilization by individual departments or business units.

3.1.4. Level P—Performance Management

The P level is involved with managing the overall performance of the network in order to meet the users and organizations desires. Performance management is focused on ensuring that network performance remains at acceptable levels (the network and systems services must be available, the speed must be efficient, their must not be bottlenecks and the network should never be used to its maximum capacity for prolonged period of times and potential problems are identified). System and network administrators must actively monitor the network performance to ensure problems do not occur.

A major part of the effort is to identify which improvements will yield the greatest overall performance enhancement.

But Performance Management involves network analyze too in order to gather information so that you can prepare it for the future (because performance criteria of a network varies all the time).

3.1.5. Level S—Security Management

At the S level, the network is protected against hackers, unauthorized users, and physical or electronic sabotage. Confidentiality of user information is maintained where necessary or warranted. The security systems (controls overall activities and ensure data security through authentication and encryption) also allow network administrators to control what each individual authorized user can (and cannot) do with the system.

As a network and system administrator, we are to address network authentication and security auditing to detect and prevent network sabotage, abuse and to prevent unauthorized access thereby:

- Record logs
- Firewall setup
- Control Spam
- Prevent Viruses, Trojans, Spyware
- Upgrade software, install OS patches
- Implement authorization techniques and password control (which is linked to accounting and configuration management)

3.2. ITIL - Information Technology Infrastructure Library

While the FCAPS framework is a great model for defining the objectives of network management, another best practices approach for service delivery was designed to align itself with current IT organizational structures and expand upon the FCAPS model.

ITIL - ISO/IEC 20000 (previously BS15000) standard - is a set of practices for IT service management that focuses on aligning IT services with the needs of business.

ITIL describes procedures, tasks and checklists (that are not organization-specific) used by an organization for establishing a minimum level of competency. It allows the

organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

ITIL procedures are widely implemented in a lot of organizations all over the world (such as NASA, the UK National Health Service -NHS, HSBC bank and Disney™, etc). ITIL is also supported by quality services from a wide range of providers including examination institutes, accredited training providers and consultancies, software and tool vendors and well known service providers (IBM, HP and British Telecom, etc.).

ITIL is not a theoretical set of information and process descriptions. ITIL tries to adapt working processes in IT Infrastructure and the aims are:

- to reduce costs
- to provide high quality IT services
- to create a basis for quality management
- to have satisfied customers
- to have a better communication between customers and IT staff

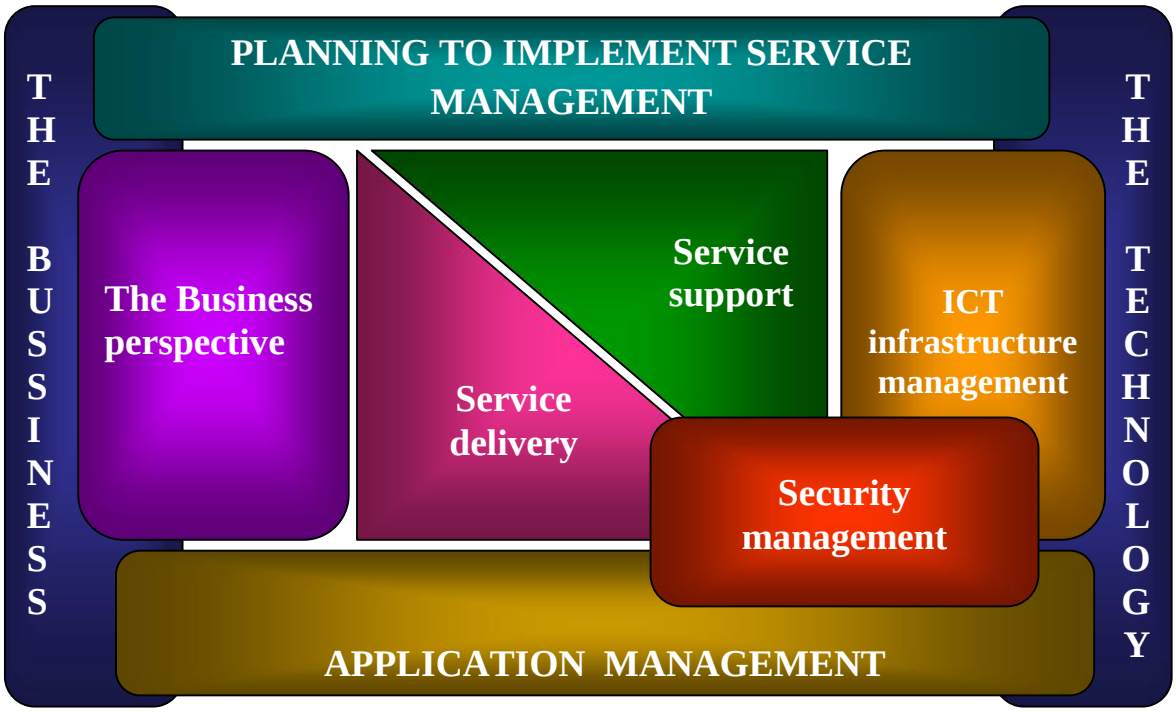


Fig. 2 – ITIL framework levels

ITIL was designed to provide a better framework to deliver high-quality, consistent application delivery over a network infrastructure.

To reach the above described aims, the ITIL framework is defined by the next levels:

3.2.1. Business Management

According to the 2011 edition of ITIL, business service management (BSM) is "*the management of business services delivered to business customers. Business service management is performed by business units*."

Business Management can be used to understand the impact of business needs on IT services and infrastructure, helping in the process of planning to ensure the portfolio of Business Services and IT Services aim to support these changing needs and objectives.

This approach also helps to understand how technology, including incidents, changes and new developments, impact the business and customers.

3.2.2. Application Management

Application management is designed with the sole purpose of ensuring that an application has the right configuration and design to be implemented in the network environment. This discipline can cover many various aspects of network management, from number of application dependencies to delay timers for satellite links. Application management is designed to ensure that the application, end-to-end, is fully enabled to provide the service and delivery to the end users.

3.2.3. Service delivery

For many organizations, this is typically for network operations center (NOC). The service delivery process begins by defining the services to be delivered, the target consumers of the service, the business requirements and motivators for the services, and other high-level business issues.

The service delivery level is focused to ensuring to the end users the applications that they require. This area focuses on aspects of troubleshooting, help desk, and supporting new applications over the network. Problems management would track the number of incidents and facilitate troubleshooting of faults or performance problems that occur in the environment.

To troubleshoot a network environment, a good understanding of what devices are on the network and their configuration is handled by the configuration management (often referred to as configuration management database (CMDB)). Change management also involves both aspects of problem management and configuration management as the change board would approve planned changes for the infrastructure, update the CMDB, and record any problems encountered during the change.

3.2.4. Service Support

IT Service Management (ITSM) is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organization. ITIL is fast becoming an international de facto standard, providing a comprehensive, consistent and coherent set of best practices for IT Service Management, promoting a quality approach to achieving business effectiveness and efficiency in the use of information systems.Service Support focuses on ensuring that the customer has access to appropriate services to support business functions. Issues covered include Service Desk, Incident Management, Problem Management, Configuration Management, Change Management and Release Management.

3.2.5. Security Management

A basic concept of security management is the information security and the primary goal of information security is to guarantee safety of information (the confidentiality, integrity and availability). The goal of the Security Management is split up in two parts:

- The realization of the security requirements defined in the service level agreement (SLA) and other external requirements which are specified in underpinning contracts, legislation and possible internal or external imposed policies;
- The realization of a basic level of security. This is necessary to guarantee the continuity of the management organization. This is also necessary in order to reach a simplified service-level management for the information security, as

it happens to be easier to manage a limited number of SLAs than it is to manage a large number of SLAs.

Security Management involves protecting a network from all kinds of unauthorized access. This includes many sub functions like collecting and reporting security related information, proactively detecting and preventing intrusions, etc.

Security Management covers the following aspects:

- Intrusion Detection (Network and Host) –(Eg. OSSEC, Prelude Hybrid IDS, Snort or Suricata, Nessus)
- Configuration Management of remote nodes (Mercurial, Rancid(routers), CVS, Subversion, git)
- Analysis of data collected at the remote nodes (Cacti*, Hyperic, Munin, Nagios, OpenNMS, Sysmon, Zabbix)
- Taking action based on analyzed data
- Real- time response to certain types of intrusions

3.2.6. Information and Communication Technology (ITC) Infrastructure Management

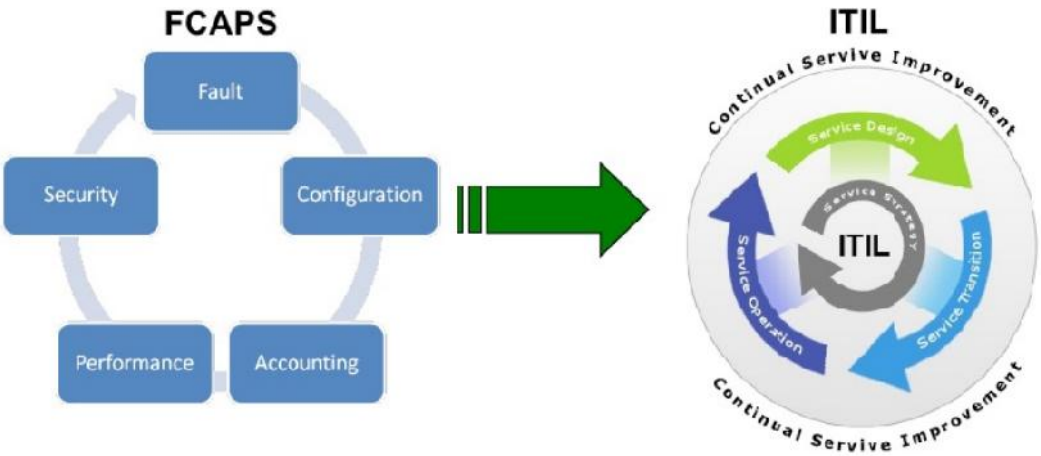
In larger organizations, the teams that design and troubleshoot the systems are separate entities than the team that installs the equipments. This is why an accurate configuration management is essential to the success of IT organizations. Infrastructure management is responsible for the installation and physical configuration of all network devices in the organization. When changes are approved by the configuration management team, infrastructure teams are the army that enforces these changes based on the designs by other architects and engineers.

Software asset management is often considered a vital aspect of managing an organization. Software licenses and products are expensive commodities. Software asset management is designed to be partially configuration management as it provides essential information about the software installed on each device, its revision or platform level, and how many instances are required. Accounting for proper licensing and software maintenance is a big business with many larger IT organizations.

4. Conclusions

A simply review of these standards shows that ITIL and FCAPS overlap in terms of concept that they address. It is true that they do speak some of the same concept but they do so at completely different levels of abstraction. While FCAPS is primarily focused on the concept of technology management (starts with a technology centric view), ITIL is all about the process for how to run an efficient IT organization (ITIL focuses on process and workflow).

FCAPS has proven to be a logical and low risk starting point. As a recommendation, start with FCAPS concepts and put a plan in place to optimize the organization by developing ITIL best practices.



We can start with FCAPS and implement ITIL across our corporate !

References

[1] Greenfield N., *FCAPS Management for the Smart Grid High-level Summary* -- May 6, 2009
[2] Midgley F., Williamson N., Lacy S., *ITIL® Managing Digital Information Assets*, White Paper January 2011
[3] Arraj V., *ITIL: The Basics*-- White Paper, May 2010
[4] Clinch J. *ITIL V3 and Information Security*-- White, Paper, May 2009
[5] Gkantsidis C., Ballani H., *Network Management as a Service*
[6] England R., *Review of recent ITIL® studies For APMG*, White Paper, November 2011
[7] Benson T., *Unraveling the Complexity of Network Management* --
[8] Parker J., *FCAPS, TMN and ITIL –Three key ingredients to effective IT management*, May 6, 2005
[9] Faber M., Faber R., *ITIL and Corporate Risk Alignment Guide. An introduction to corporate risk and ITIL, and how ITIL supports and is assisted by Management of Risk* --, March 2010
[10] Whittleston S., *ITIL® is ITIL* - University of Northampton, March 2012
[11] *Everything you wanted to know about ITIL® in less than one thousand words!*- - White Paper,October 2007
[12] Cartlidge A. and others, *An Introductory Overview of ITIL® V3* -- 2007