Asian Journal of Information Technology 10 (6): 240-248, 2011
ISSN: 1682-3915

The Use of FCAPS and ITIL in Managing the Network of a Medium to Large Public Sector Organisation

[1]U. Osigwelem Kenneth, [1]A.C. Akukwe,
[2]Agbakwuru O. Alphonsus and [2]Ukwandu Elochukwu
[1]Alvan Ikoku, Federal College of Education, Owerri, Nigeria
[2] Evan Enwerem University, Owerri, Nigeria

Abstract: Since, organisations depend increasingly on Information Technology (IT) for achieving business objective, it is expedient for network managers to be conversant with network management models that are capable of managing scalable networks to minimize downtime. However, the ability to identify potential problems and resolve same rapidly in an attempt to reduce Mean Time To Repair (MTTR) i.e., the time it takes to fix a faulty system or component is a hallmark of proactive network management initiative necessary for a sustained IT services to an organisation. This initiative is achieved by deploying good network management model. This study therefore, attempts to X-ray the operational structure of FCAPS (Fault, Configuration, Accounting, Performance, Security) network management model and ITIL service management framework and a mapping of their approaches and how they relate to each other in providing sustained IT service for organisation's business improvement.

Key words: Information Technology Infrastructure Library (ITIL), configuration management, service management, security, performance, Nigeria

INTRODUCTION

Network management can be described in terms of procedures, methods, tools and activities that relate to the day to day operation, administration, maintenance and of course preparing and equipping a network to enable it perform in such a manner as to meet the organisation's information need (Clemm, 2007). There are four units that make up network management (Subramanian, 2000), of the four sub units, the operations sub unit takes charge of day to day operations that provides network services, the network administration unit is concerned with ensuring that the goals, policies and procedures necessary for effective network management is implemented and administered.

The maintenance unit is responsible for IT facilities and equipment repairs and installation while the provisioning unit is involved in planning and design of the network. Suffice to say that network management as a service use a combination of tools, devices and applications in helping network managers to monitor, manage and maintain networks (Gupta, 2006).

This combination work together to achieve the network management goal of ensuring that the network end-users receive the IT service (s) expected from the network. The task and responsibility of managing a network has not been an easy one as network managers are faced with choice of network management model and framework to adopt given variety of alternative approaches and frameworks. Among other available models are Telecommunication Management Network (TMN), FCAPS, Information Technology Infrastructure Library (ITIL), IBM Tivoli, cfengine, Control Objectives for Information and related Technology (COBIT) etc. Any choice of network management model must take into consideration the various elements that constitute the network as well as the business.

Network management is comprised of the following integral aspects: Human, Methodology and Instrumentation (Hassan *et al*., 2009). The human aspect of network management is where managers define organisation's policy, goal and approach to realise the set goal.

The methodology aspect of network management attempts to define the architectural or technical framework as well as defining the functions to be carried out. The instrumentation aspect establishes the actual operational implementation of laid down algorithm (a step by step sequence of procedure to accomplish a given task), procedures and method as defined by the human aspect (manager) for data collection and processing, of reports, problem analysis and repairs to enhance performance improvement and predictability of service levels.

Corresponding Author: U. Osigwelem Kenneth, Alvan Ikoku, Federal College of Education, Owerri, Nigeria

TMN: The Telecommunication Management Network (TMN) is a reference model that was defined by the International Telecommunications Union-Telecommunication standardization sector (ITU-T) as a framework for heterogeneous telecommunication network management. TMN defines a standard interface for handling communication process in a network and it is by this interface that a single network management system can handle different network elements belonging to or coming from different manufacturers which otherwise would have been incompatible with each other due to vendor specific architectures.

TMN model came with stratification approach which stratify network management into five logical layers (Subramanian, 2000; Clark, 1997; Clemm, 2007; Burke, 2004) comprising of, Business Management Layer (BML), Service Management Layer (SML), Network Management Layer (NML), Element Management Layer and with Network Element Layer (NEL) at the base of the stratum as shown in Fig. 1.

The TMN layers

Business Management Layer (BML): This layer performs business related functions like analysing trends in the network, Quality of Service (QoS), billings and financial reports.

Service Management Layer (SML): This layer is charged with the responsibility of managing the services offered by a service provider to customers or even to other (retail) network service providers. Under this layer we have services like billing, order processing, complaint handling and trouble ticketing. Trouble ticket also called trouble report is a mechanism used in an organisation to track the detection, reporting and resolution of problem in a network.

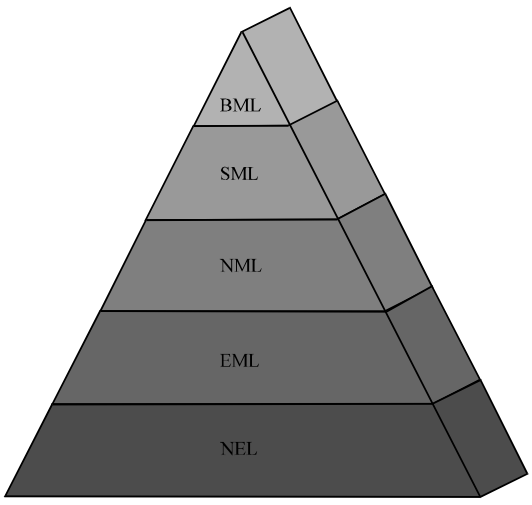

Fig. 1: A pyramidal view of TMN layers (Hassan *et al*., 2009)

Network Management Layer (NML): This layer helps to perform integrated fault management and network service provisioning functions like bandwidth control, performance control, network congestion control and quality of service control. It is worth noting that this layer is not vendor dependent (Subramanian, 2000).

Element Management Layer (EML): This layer contained functions handled by individual network elements. Such functions include network monitoring, inventory management, network provisioning and service assurance.

Network Element Layer (NEL): This is the layer where you find such devices like switches, routers, bridges and other transmission facilities.

FCAPS: FCAPS is a network management reference model which introduced the concept of function categorization. The model segments management functions into:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

Which forms the acronym FCAPS. This model originated from TMN. However, the functions of FCAPS might be thought of being equal but in real terms the model builds a foundation and overlay where all these functions interact with one another. From Fig. 2, security embraces and interacts with all other function for effective

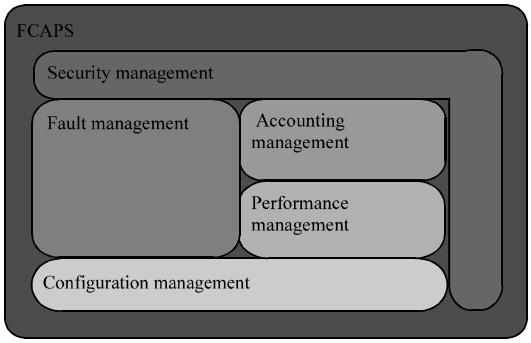

Fig. 2: Interactions of the FCAPS functions (Cisco, 2007)

security. Configuration management at the base makes available all vital data needed to support other functions. Each of these categories of management functions of FCAPS has its specified tasks as follows:

Fault management: This involves activities of fault monitoring, identification, diagnosis, elimination or correction and recovery procedure. Fault tolerant computing i.e., the ability of the system to perform specified tasks and conform to predictable results even in the event of program errors or hardware failure is the focus of FCAPS fault management.

Fault tolerance computing use redundant components to tolerate fault, examples include Redundant Array of Inexpensive Disk (RAID). In this way downtime is minimized and the network is kept operational. The major activities of fault management are:

- To predict when network equipment will likely fail
- To maintain error logs examine them regularly
- Carryout error detection and immediate response to error notifications and documenting same
- To track errors, carryout error diagnosis and identification and fault management performance measurement

Configuration management: Configuration is all about telling the network what it should do. This involves setting up the network and network devices in a working order so as to achieve organisation's policy. For the network to work, it needs to be told what things to do and perhaps how to do it and it could involve the task of initial configuration and modification of configuration parameters in order to accommodate updates in network devices and network function (Clemm, 2007). Configuration management keeps track of the devices like routers available to the network making sure that such devices are not unplugged, tampered with or physical repositioned elsewhere in the network. Configuration management forestalls unauthorised introduction of alien or strange device to the network. It therefore, follows that configuration management strives to make configuration identification functions available (Claise and Wolter, 2007), functions to collect configuration parameters, exercise control and provide information regarding configuration to network elements. Configuration management helps network providers to track changes to configuration setting by scheduling regular backup of configuration settings and copies kept. Other responsibilities of configuration management include:

- To install and configure physical equipments
- Plans for introduction of new services and decommissioning the undesirable services
- To control and determine the state of unit a unit i.e., when a unit is in service, out of service or standby
- To determine when there is need for growth in capacity of the network and introduce new technology

Accounting management: Accounting management is ultimately concerned with measuring the use of the network resources in order to ascertain metric, check quotas and determine costs on the part of the service provider to have a basis for billing the customer who is the consumer of the service (Burke, 2004). Accounting management helps the network provider in generating revenue and also to estimate cost/benefit ratio of running a network service which is vital for management decision making.

However, monitoring, measuring, billing and reporting are integral aspects of accounting management. Monitoring or surveillance involves knowing which unit or department for instances uses the server. Measuring which is effectively done by metering entails gathering data to establish duration of usage of the service. Billing uses established tariff policy to prepare bills working with the measured statistics and finally setting charges and generating summary for the period.

Data concerning billing is normally based on usage, capacity or destination i.e., volume, duration and quality (Clemm, 2007) e.g., megabytes (quantity/volume) of data, time (min) spend, type of service rendered, etc. in some other cases it could be a flat fee or a special fee depending on the nature and time of service such as peak and off-peak periods. The following applications are commonly used accounting management utility; RADIUS (Remote Authentication Dial In User Service) where server receives a start packet which describes the type and user of service initiated in a network. The RADIUS server sends back an acknowledgement to the user. At the end of the session stop packet is sent to the RADIUS server to terminate the session and generate statistical data relating to the service. TACACS+(Terminal Access Controller Access Control System) works in much the same way as RADIUS but it is more stringent in checking quota in the network.

Performance management: Performance management avails the function of evaluating and reporting on the behaviour and performance of the network and network elements and their characteristics. Performance management monitors the network to discover when there is congestion or overcrowding in the network, it predicts

trends and respond to changes in performance. The major activity here is to gather and analyse statistics data which in turn is used to monitor and correct network behaviour (network elements and other equipment inclusive). Network performance is measurable by the following attributes or characteristics:

Throughput: This is the number of units of work (in this case communication) per unit time. Such as number of bytes transmitted, number of packets routed per second, number of voice calls and call attempts per hour, etc.

Delay: By delay we mean per unit time taken for a transmitted byte to get to its destination, time taken for an IP packet to reach its destination, response time for request to get back to host and for voice call, time taken to receive a dial tone when receiver is lifted.

Quality: Quality is a measure of error rate in transmission, percentage of dropped packets, percentage of web request not serviced and abnormally terminated calls.

In large networks, performance data is obtainable using protocols like NetFlow or IP Flow Information Expert (IPFIX).

Security management: Because of the vulnerabilities of network resources, security management is geared towards preventing, detecting and containment of attack and threats as well as recovery from such vulnerabilities. Security administration by use of access control, authentication, encryption, authorization policies, intrusion detection (Burke, 2004) and firewall is commonplace in networks. Here security management is in two folds, firstly, security of management which ensures that access to management interfaces of devices in the network is authorized and forestalls unauthorized modification of network configuration by unauthorized personnel or intruder, secondly, management of security i.e., being in total control of the security situation of the network itself.

Security breaches have been known to emanate from both within and outside the organisation; it is a good security culture to employ audit trails like syslog server for internal security since, it is envisaged that 2/3rd of security breaches are from internal. Audit trails (Clemm, 2007) keep record of all attempted and actual operations that within the network. With audit trails, any operation on the network can be traced to source (user) in the network and it also enhances recovery from such security breach. Possible security threats in a network include modification of information, denial of service, message stream modification, masquerade, disclosure, virus attack, spam among others. Management of security should include:

- Intrusion detection which detects suspicious traffic patterns that portend attack
- Honey pots-honey pots play the role of trap, they are camouflaged as device in the network to deceive attackers who sees the honey pot as part of the network and unleashes attack. The honey pot then gathers this attack information in order to defend against such attack in the network
- Black list-ports and network addresses that are flagged with suspicious traffic patterns are blacklisted and put under severe security surveillance

Any network management framework acceptable for implementation must have features that cater for all these required tasks. In order to defend against the myriad of attacks, the following security practices should be respected:

- Setup procedures that will ensure orderly operations in the network
- Access privileges should be assigned for immediate job function to only the people that have genuine need of it
- Passwords should be made up of letters, numbers and special characters in a combination of upper and lower cases. Such type of passwords are not easily cracked
- Intermittent change of passwords should be practiced
- Well practiced audit trail should be used
- Critical management data should have backup and restore facilities in place

What is ITIL: Information Technology Infrastructure Library (ITIL) is a service management framework (Concepts and policies) that is hinged around experience and research proven reliable techniques or methodology (called best practices) for IT service management (Potter, 2007). ITIL defines a service as the IT system (s) that enable customers and users to implement business processes. Online banking, travel reservation systems, payroll systems for instance are examples of services. Each of these services can be made up of other services. Taking online banking for instance, this service can have other services like balance checking, deposit and withdrawal. TIL was developed by the British government through Central Computer and Telecommunication

Agency (CCTA) (now known as the Office of Government Commerce (OGC)) with industrial cooperation of some experts from the industry in the late 1980's. ITIL has evolved over time culminating into three versions.

The first version of ITIL addresses issues like cabling infrastructure strategy, computer installation acceptance and network service management. While this version was more of technical, the second version of ITIL incorporated service delivery and service support components of service management framework into the earlier version. In May 2007 the third version was introduced (Korn, 2007). The third version which is the most recent and current took yet a higher-level view by integrating IT and business process with core components which includes service strategy, service design, service transition, service operation and continuous service improvement.

ITIL is now the fastest growing tool for business optimization initiative and has equally gained wide acceptance in North America and some other part of the globe. However, the secret behind ITIL's general acceptability could be traced to its design flexibility resulting from best practices collection hence, it can be adapted and adopted in various ways with respect to the needs of individual organisations (Parker, 2005) because ITIL took into consideration that different organisations have different peculiarities in terms of procedure, size, strengths, etc. (Potter, 2007). ITIL only describes what things that should be done and not the methodology (Gucer *et al*., 2009) i.e., it does not give the guidance on how to implement the process because of varied individual organisational requirement that may be peculiar to a particular organisation.

The structure of ITIL framework: ITIL as a service management framework classified service management roles in an organisation into two-chambered generic standard based on either tactical function or strategic function (Burgess and Schaaf, 2008; McNaughton *et al*., 2010) which culminated into service delivery and service support with each of the chambers concerned with different management functions as discussed on the next page below. Service delivery deals with details of how ITIL can be implemented while service support deals with the application.

The Fig. 3 shows a high level diagram of the structure of ITIL framework. From the Fig. 3:

- The business perspective maintains a close relationship or alignment to the organisation's business while technology on one end maintains an aligned relationship to information technology

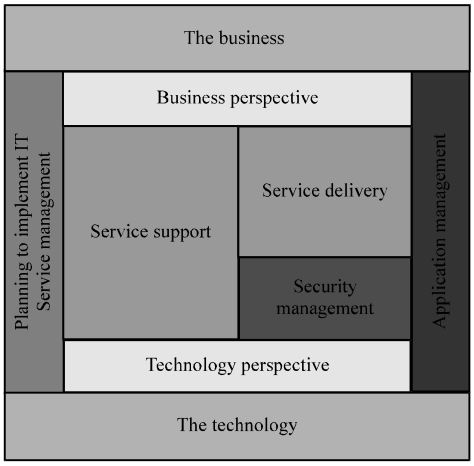

Fig. 3: Showing the structure of ITIL framework (Watt, 2005)

- The planning to implement service management handles matters ranging from planning and implementation to improving IT management service and all its associated processes
- The service delivery component covers all aspects of planning IT services and delivering of IT services. It involves several management practices that ensures that the service provider provides services in consonance with Service Level Agreement (SLA) reached with the customer
- The service support component defines and describes processes necessary to support and maintain IT services daily i.e., those discipline that help for effective provision of IT service
- The application management component of ITIL describes in detail all the processes for application management within the life cycle of the application
- The security management though under service delivery is very fundamental in this framework cuts across the core components of ITIL which includes service support, service delivery, application management and technology perspective. All these components require interaction with security management for effectiveness of operation

Service delivery

Service Level Management (SLM): Service level management involves the activity planning, coordinating and managing business service within budgeted cost. SLM engages customers in negotiating service delivery agreement also called Service Level Agreement (SLA), determining the customer's need, sets performance target according to the need of the customer. The focal point of

the SLA is network service provisioning. It is the responsibility of the Service Level Manager (SLM) to prepare the contract agreement making sure that the agreement takes of finance, security, capacity plans, availability plans and continuity plans. The service level management team needs to work with all the units under service delivery in order to accommodate their input in the service contract.

Finance management: The finance management prepares bill for charges of IT service rendered to the customer, prepares cost account and budget for IT service furnishing the SLM with cost statistics of the customer's desired service. Finance management determines the prices of network services, prepares bills based on financial data collected and applies policies and methods for billing.

Capacity management: The capacity management unit of service support endeavours to provide needed IT infrastructure as at when needed within budgetary allocation and also ensuring efficient use of infrastructure. It carries out routine monitoring of the usage of the network in order to ascertain the capacity usage level of the network. It takes note of free and used capacity and performs trend analysis needed to enable projections for future capacity provision. Projection ensures that capacity is not under-subscribed or under-utilized.

Continuity management: Continuity management ensures sustained service and minimizes service outage by trimming down the impact of incidents and disasters. Continuity management takes steps towards alleviating the risks to which the network environment is susceptible to and makes contingency planning to cater for all predictable disasters that may occur in the future. The continuity manager draws up his network recovery plan continuity strategy in the event of any disaster occurring in the network. The continuity manager carries out simulation tests to guarantee that his set out recovery plans and strategy will meet the desired requirements.

Availability management: The availability management makes plan to ensure overall availability of service to the customer. The availability manager takes charge of making network service available and also manages the quality of service by minimizing Mean Time Between Failures (MTBF) i.e., the predicted elapse time between inherent failures of a system during operation. The availability management restores failed service and failed component with minimal Mean Time To Restore (MTTR) and also incorporate fault tolerant technology into the system using redundancy. By redundancy we mean keeping copies of a hardware or software components of a system in order to tolerate fault. With fault tolerance the system will continue to execute specified operations even in the face of fault.

IT security management: Central in the responsibility of the security management is to ensure and maintain uninterrupted network operations. The security manager ensures sustained network operations through controls, monitoring, audit and good incident handling process. Auditing here involves finding and detecting vulnerabilities in the network using audit trail.

Service support

Incident management: Incident management maintains a stable service level by making sure that services are restored to their normal service level within the shortest possible time after an incident has occurred. It keeps record of incident occurrence, interruption in service, dwindling service quality and their causes. Incident management monitors incident and carry out investigation with the aim of tracing the incident to its source. Restoration of service is the priority of incident management.

Problem management: Problem management arranges resources in the network according to priority in order to meet business need and resolve or address problems causing incident in the network. It also keeps statistics of problem resolution which helps in SLM. Finding the root cause of a problem and resolving same is the principal responsibility of problem management.

Change management: Change management controls and coordinates every change to IT service so as to minimize the impact of such changes on service. It tries to ascertain the effect of change in organisation, hardware and software on network service and determines to what extent such impact can have on service performance.

Release management: Release management implements changes in IT services considering technology, people and process. It acts as the custodian of the organisations definitive software library (software repository) and services change request from change management, installs and setup software components for network service. It keeps record of deployment details for the SLM.

Configuration management: Configuration management establishes Configuration Management Database (CMDB) that contains all the details of hardware, software, documentation and people used in providing network service and network management. Configuration service involves a four major step task of configuration identification, configuration control, status accounting and verification. Configuration identification task identifies all the configuration structures and items (IT components), control task determines and specifies who has the authorization to change a configuration item (s), configuration status task keeps record of the status of all configuration component in the CMDB while verification task carries out review and auditing of the information content of CMDB for accuracy. Configuration management in ITIL is vested with the task of assisting in giving account of IT assets, providing accurate and reliable information needed to support service management activities like release, change, problem and incident managements (Cisco, 2007).

Given the fact that the main focus of ITIL is service management, it ensures continuity and availability of IT service through suitable and effective incident management. Incident has been defined by Forte (2007) as any event that does not constitute part of the standard operation of a service and which causes or is capable of causing an interruption in quality of service or compromise in quality of that service. The paramount objective of incident management is to minimize interruptions in business activities and ensure availability of service at all times in the network.

ITIL version 3 (ITIL v3): ITIL v2 outlined what things to be done in order to improve IT service while ITIL v3 describes how to do it. ITIL v3 used by about 42% of network users (Blum, 2009) employs lifecycle approach which is a magnification of service management. It sets its focus on customers need and expectations from the service organisation and its impact on business. ITIL v3 further broke down the 11 component processes of ITIL v2 into 27 collapsed into 5 core components namely service strategy, service design, service transition, service operation and continual service improvement in an attempt to describe the how of ITIL v2 (Anderson, 2009) (Table 1 and Fig. 4).

Of these components, service design, service transition and service operation represents day to day transformations in the business. Service strategy contains policy and objectives of the organisation required for improvement. Continual service improvement is centred on adaptation to the environment and improvement in service.

Service strategy: Service strategy is the nucleus of the lifecycle approach. It strives to improve the service

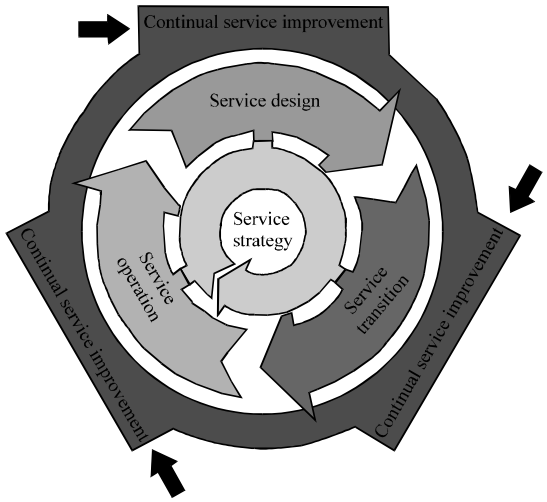

Fig. 4: Structure of ITIL v3 (Korn, 2007)

Table 1: Integrating functions of ITIL v2 into ITIL v3

Service strategy processes	Service design processes	Service transition processes	Service operations processes	Continual service improvement processes
Service portfolio management	Availability management (V2)	Change management (V2)	Service desk management	CSI service level management
Demand management	Capacity management (V2)	Service asset and configuration management (V2)	Technical management	Service measurement and reporting
Finance management (V2)	IT service continuity management (V2)	Knowledge management	IT operations management	CSI improvement process
	Service level management (V2)	Release and deployment management (V2)	Applications management processes	
	Information security management	Service validation and testing	Event management	
	Supplier management		Incident management (V2)	
	Service catalog management		Problem management (V2)	
			Request fulfillment	
			Access management	

organisation over time by setting investment priority for the service provider and carrying out market based analysis.

Service design: Service design must take cognisance of service strategy by designing a service that will meet customers' desire and results that meets their expectations which is specified in the service strategy.

Service transition: Service transition is about change management and configuration management. When service has been designed to conform to service strategy, the next thing is to make the designed service available. Service transition is concerned with introducing the new service making it operational at the least cost and least risk.

Service operation: Service operation is concerned with operational capabilities of the service organisation. Service strategy design must take into consideration the operational capability and the organisation's drawback (s) to avoid coming up with strategy that can't be matched with capability.

When service design, service transition and service operation work in harmony with service strategy then customer satisfaction is met and the business continually improves resulting in improved revenue for the service provider.

Advantages of ITIL: Advantages of ITIL model include:

- **Flexibility:** ITIL is designed for flexible implementation with respect to organisation's peculiar need
- ITIL offers improvement of customer satisfaction through IT service
- There is improved quality of service through operational efficiency
- There is cost justification and reduction because ITIL considers budget in SLA

FCAPS vs ITIL: FCAPS was introduced in April 1997 by ITU-T with emphasis on telecommunication network management. It simply splits management function into five categories consisting of fault, configuration, accounting, performance and security from where it derived its acronym. However, these five categories describe only the five different types of information which management system handles and not roles with respect to business.

ITIL on the other hand introduce around 1980 by the British government places focus on IT service management which is based on best practices. ITIL attempts to split both tactical and operational processes into 11 areas of interest grouped into either service delivery or service support with ITIL v3 collapsing the eleven areas of ITIL v2 into service strategy, service design, service transition, service operation and continual service improvement using lifecycle approach which implies a closer alignment to service than technology.

This is to say that ITIL implementation is with respect to organisational business need peculiar to the organisation. Both FCAPS and ITIL overlap in their individual concepts, i.e., they altogether preach the same concepts but with different approach and abstraction. While FCAPS places greater emphasis on technology, ITIL has its focal point on business service (Table 2 and 3).

Table 2: Comparison of ITIL and FCAPS

	A comparison of FCAPS and ITIL
FCAPS	ITIL
Management functions categorized into 5	Management functions categorized into 11 of service delivery and service support for ITIL v2 and five for ITIL v3
FCAPS emphasises on technology (Network) management	ITIL emphasises on service management
Performance management activities	Performance management activities of FCAPS are taken care of by ITIL's capacity management, availability management, continuity management and service level management
Accounting management activities	Accounting management activities of FCAPS are taken care of by ITIL's financial management
Configuration management operations	Configuration management activities of FCAPS are taken care of by ITIL's configuration management change management, and release management
Fault management operations	Fault management activities of FCAPS are taken care of by ITIL's incident management and problem management
Security management operations	Security management activities of FCAPS are taken care of by ITIL's IT security management
FCAPS has its origin from TMN, ISO and ITU-T	ITIL has its origin from OGC and British government

Table 3: Showing mapping of ITIL functions to FCAPS model; tick (√) connotes correspondence (Burgess and Schaaf, 2008)

	FCAPS Functions Category				
ITIL functions category	Fault	Configuration	Accounting	Performance	Security
Incident management	√	-	-	-	-
Problem management	√	-	-	-	-
Configuration management	-	√	-	-	-
Change management	-	√	-	-	-
Release management	-	√	-	-	-
Financial management	-	-	√	-	-
Capacity management	-	-	-	√	-
Continuity management	-	-	-	√	-
Availability management	-	-	-	√	-
Service level management	-	-	-	√	-
IT security management	-	-	-	-	√

CONCLUSION

Both ITIL and FCAPS help in evaluating and defining network management tasks. ITIL as a service management framework engenders alliance between IT department and organisation's business. ITIL's definition of configuration management offers immense support to CMDB, change, incident, problem and capacity management culminating into formidable coordination of network management. It therefore follows that if FCAPS is administered on ITIL platform, user satisfaction and expectation will be met and continual improvement in business growth will be accomplished since, ITIL has provision for all FCAPS processes though in different theoretical perspectives.

REFERENCES

Anderson, C., 2009. The difference between ITIL v2 and v3. Bizmanualz, http://www.bizmanualz.com/blog/business-improvement-services/the-difference-between-itil-v2-and-v3.html.

Blum, R., 2009. BT IT industry survey: IT information library. British Telecommunications Plc Reports.

Burgess, M. and T. Schaaf, 2008. Integrating cfengine, ITIL and enterprise processes. http://cfengine.com/files/cfengineEnterprise.pdf.

Burke, R., 2004. Network Management: Concepts and Practice: A Hands-on Approach. Pearson Education Inc., New Jersey.

Cisco, 2007. Network configuration management. Cisco Systems Inc., USA., http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.pdf.

Claise, B. and R. Wolter, 2007. Network Management: Accounting and Performance Strategies. Cisco Press, Indianapolis, USA.

Clark, M., 1997. Networks and Telecommunications: Design and Operation. 2nd Edn., John Wiley and Sons Ltd., Chichester, England.

Clemm, A., 2007. Network Management Fundamentals: A Guide to Understanding how Network Management Technology Really Works. Cisco Press, Indianapolis, USA.

Forte, D., 2007. Security standardization in incident management: The ITIL approach. Network Security, 2007: 14-16.

Gucer, V., L. Balestrazzi, E. Chan, M. Hooker, M. Luccas, N. Pearson, S. Pillay and P. Wozniak, 2009. End-to-end service management using IBM service management portfolio. IBM Redbook, http://www.redbooks.ibm.com/redbooks/pdfs/sg247677.pdf.

Gupta, A., 2006. Network management: Current trends and future perspectives. J. Network Syst. Manage., 14: 483-491.

Hassan, R., R. Razali, S. Mohseni, O. Mohamad and Z. Ismail, 2009. Architecture of network management tools for heterogeneous system. Int. J. Comput. Sci. Inform. Secur., 6: 31-40.

Korn, E., 2007. Best practices insights Focus on: ITIL service strategy. BMC Software Inc., http://media.cms.bmc.com/documents/USA-Promotions-attachments-ITIL-Service-Strategy-85216.pdf.

McNaughton, B., P. Ray and L. Lewis, 2010. Designing an evaluation framework for IT service management. Inform. Manage., 47: 219-225.

Parker, J., 2005. FCAPS, TMN & ITIL three key ingredients to effective IT management. Openwater Solutions, LLC, Enterprise Management System White Paper, http://netcourses.tech.purdue.edu/cit443/Data/lectures/FCAPS_TMN_ITIL.pdf.

Potter, R., 2007. ITIL: What network managers need to know. http://searchnetworking.techtarget.com/tip/ITIL-What-network-managers-need-to-know.

Subramanian, M., 2000. Network Management: Principles and Practice. Addison-Wesley, Reading, Massachusetts, ISBN: 9780201357424, Pages: 644.

Watt, S., 2005. Enhance IT infrastructure library service management capabilities. IBM, https://www.ibm.com/developerworks/webservices/library/ws-itil/.