FINAL REPORT

For

Development of Best Practices in Information Infrastructure Security Management

DEPARTMENT OF NEW MEDIA AND INFORMATION SECURITY
PLOT 423 AGUIYI IRONSI WAY
MAITAMA, ABUJA

Developed and Submitted
By

Modular Integrated Services Limited

Table of Content

Contents

Executive Summary

The telecommunications industry, meeting the needs of an increasingly global commerce environment, has contributed to better productivity and bridged communities globally in almost every industrial segment. That this communications infrastructure is so efficient is in no small part due to standards developed by organizations such as ITU-T. The standards that keep current networks efficient also lay the foundations for next generation networks. However, while standards have continued to meet end-user and industry needs, the increased use of open interfaces and protocols, the multiplicity of new actors, the sheer diversity of applications and platforms, and implementations not always tested enough have increased opportunities for malicious use of networks. In recent years, a surge in security violations (such as viruses and breach of confidentiality of stored data) has been observed throughout global networks, and often resulted in major cost impacts. The question then is, "in what ways can an open communication infrastructure be supported without compromising information exchanged?" The answer lies in efforts by standards groups to combat security threats at all areas of the telecommunications infrastructure. These provisions range from details in protocol specifications and in applications to the management of networks. The purpose of this document is to highlight and offer a bird's eye view of the numerous recommendations developed by ITU-T – sometimes in collaboration with other Standard Development Organizations – to secure the telecommunication infrastructure and associated services and applications. To address the multiple facets of security, it is necessary to establish a framework and architecture, in order to have a common vocabulary with which to discuss the concepts. To achieve this, NCC seek to develop Best Practices for Information Infrastructure Security Management in the Telecommunication Industry.

Chapter 1 – Introduction

The Nigerian Communications Commission was established to provide regulatory framework for the Nigerian telecommunications industry and to create an effective, impartial and independent regulatory authority. The commission is also vested with the responsibility to introduce innovative services and practices in the telecommunications sector in accordance with international best practices and trends and to ensure efficient management, monitoring and use of scarce national resources in the communications sub-sector.

The Nigerian Communications Commissions act 2003 clearly states in its third chapter -Technical Regulations- that the commission shall manage the frequency spectrum for the communications sector; all numbering and electronic addressing of network services and application services; and provide technical code and specifications in respect of communications equipment and facilities that may be used in Nigeria.[1]

In Nigeria today, daily activities such as shopping, entertainment, banking, manufacturing, office work, education, medical care, governance and even commuting have become increasingly dependent on information and communication networks. Indeed ICT networks are now making it possible for Nigeria to participate in the global economy in ways that simply were not possible in the past. This reality is reflected in the rapid growth in telecommunication that we have been experiencing in Nigeria.

The telecommunication sector is one with generic effect on almost all other sectors of the economy. Its function in any economy is a strategic one aimed at promoting economic growth and has linkages with other sectors. For Nigeria, a modern telecommunications infrastructure is not only essential for domestic economic growth, but a prerequisite for participation in increasingly competitive world markets and for attracting new investments.

There is no doubt that we are in the information age. The ever increasing volume of information generated daily in different formats and accessible from different electronic media gives credence to this assertion. Our world is gradually but steadily transforming into an information society; a world where information is the essential element of production and wealth creation. The World

[1] NCC Policies on NCC website

Summit on Information Society [1] described an information society as one in which there is equitable access to information and highly-developed Information and Communication Technologies (ICTs) that can improve the quality of life and opportunities for all people. Participating in the information society is however contingent upon access to information infrastructure.

With the foregoing it is not surprising that the Nigerian Communications Commission New Media and Information Security department has deemed it necessary to come up with a technical framework for best practices in information infrastructure security management in the telecommunication industry.

Telecommunication networks provide the pipelines through which information flows. The success of such flow is dependent upon many factors. Chief among them is availability, quality, affordability, and capacity of the telephone network. In particular, telephone services are either not available, or where available, the quality of the service is poor. The absence of basic telephone service, while denying the citizens basic voice and fax services, also restricts the availability of value added services such as the Internet. The Internet and basic e-mail services is only as good as the available telephone network.

It is clear that we have become more dependent upon information, and that this information will be exchanged through telephone networks. The security of information infrastructure in the telecommunication industry is essential since consumption of such information will increasingly rely on telecommunication networks.

It has been demonstrated that the telecommunication business is profitable and, with new technologies, all parts of the country can obtain adequate telephone services. It would benefit our government to create an enabling climate for the private sector to build sustainable networks. It is the belief of the NCC that sustainable information infrastructures can be constructed, efficiently managed and sustained.

1.1 Background

Infrastructure generally refers to the basic installations and facilities on which the continuance and growth of a community or state depends. Social facilities like roads, railways, telecommunication networks, electricity supply system and water supply system are all described as infrastructure. Infrastructural facilities have supporting and enabling functions and are shared by a large community of users. Recently, the term has also been used along with information to denote the information resources, networks, computers, software, developers, and producers which support the creation, transport, storage and use of information. Information infrastructure denotes socio-technical systems composed of hardware, software, information content, human experts and network standards that facilitate information creation and exchange. Each of these elements constitutes a critical component which can be easily misused if not properly managed hence, the need for best practices in information infrastructure security management.

Information infrastructures are an essential part of the overall infrastructures supporting modern society. These infrastructures and the services they support face increasing security threats. Ever more critical Information Technologies (IT) resources are supplied and operated in partnership between the public and private sectors and across national borders. In this way, IT and the marketplace for it, have become truly global, and thus have security risks. Unauthorized disclosure, corruption, theft, disruption, or denials of IT resources have the potential to impact the public and private sectors and society as a whole. One of the objectives of NCC is to promote the development of the culture of security across the society. A security-cultured society will help the telecommunication industry share good practices and develop consistent policies to ensure the security of information systems and networks. Among all information systems, some are critical because their disruption or destruction would have a serious impact on the health, safety, security, the economic wellbeing of citizens, or the effective functioning of government or the economy. These information systems constitute the critical information infrastructure; ensuring their resilience is one priority area for national policy which involves co-ordination with the private sector and co-operation across-borders. The overall objective of this report is to foster a better understanding of how to protect the critical information infrastructure and to increase international co-operation by enabling the sharing of knowledge and experience between the telecommunication industry. The report examines how risks to the critical information infrastructure are assessed and

managed in general terms, the emerging and existing models for public-private information sharing, and the national responses to the growing need for cross-border collaboration. It identifies similarities and differences in policies and highlights best practices for protecting the critical information infrastructure across the Telecommunication Industry.

The Nigerian Telecommunications Service Providers (TSPs) recognize the important role that they play in helping to "build a safer, more secure and more resilient Nigeria." TSPs realize that the communication services they provide place them in a unique position, for "the ability to communicate" is a key requirement for other critical sectors.

Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. TSPs are committed to ensuring the security of their infrastructure to reduce the risk of unplanned disruptions and help resolve problems.

This document defines common practices TSPs should follow to protect critical infrastructure. It also defines the common practices that TSPs should use to safeguard their networks. Protecting the availability of the underlying communications infrastructure on which their customers depend is critical for TSPs.

The best practices described in this framework focuses on information infrastructure security management in the telecommunication industry.

1.1.1 Overview of the Nigerian Telecommunication Industry

A modest development in the telecommunications industry in Nigeria started since the inception of Nigerian Telecommunications Limited (NITEL) in 1985. Out of the 700,000 public network lines capacity in Nigeria, 400,000 lines are connected. This indicates that Nigeria lags behind in the telecommunication industry. This led to the deregulation process and the establishment of the Nigerian Communications Commission (NCC) by Decree 75 of 1992. The objectives of the establishment of the NCC include:

1. To create a regulatory environment that facilitates the supply of telecommunications services and facilities,

2. To facilitate the entry of private entrepreneurs into the telecommunications market, and
3. To promote a fair competition and efficient market conduct among all players in the telecommunication industry.

Since the inauguration of NCC in July 1993, it has set out guidelines for private sector participation and issued licenses to a number of companies for the following telecommunications undertakings:

i. Installation and operation of public switched telephony;
ii. Installation of terminal or other equipment;
iii. Provision and operation of public payphones;
iv. Provision and operation of private network links employing cable, radio communications, or satellite within Nigeria;
v. Provision and operation of public mobile communications;
vi. Provision and operation of telephones;
vii. Provision and operation of value-added network services;
viii. Repair and maintenance of telecommunications facilities; and
ix. Cabling

Telecommunication infrastructure remains one of the major issues that affect technology deployment required for growth and development in Nigeria. Although, there has been massive improvement in infrastructure over the past few years. Nigeria has certainly left the telecomm state where there were only a few dial-up e-mail providers and Internet service providers (ISPs) and when Nigerian Telecommunications Limited (NITEL) was the only telecommunications operator. The NITEL era was characterized by slow Internet links, poor service, high cost, lack of infrastructure and an unprogressive telecoms monopoly.

Deregulation of the telecommunications sector led to the introduction of major Global System of Mobile Communications (GSM), mobile phone providers MTN Nigeria, V-Mobile, Globacom and Mtel (http://www.jidaw.com/telecomproviders.html).

NCC issues licenses to private telecoms companies to provide a variety of telecom services to the Nigerian populace.

According to NCC, deregulated telecommunications services include:

Sales and Installation of Terminal equipment (Mobile Cellular Phones, Satellite Communication and Switching equipment etc.), Public Payphone Services, Internet Services; Prepaid Calling Card Services Community Telephony with exchanges, Paging Service Trunk and 2-Way Radio Network Services, Fixed Telephony Services, employing cable and Radio, Satellite Network Services (e.g. Domestic VSAT networks), Repairs & Maintenance of telecommunications facilities, Cabling services, and Tele-Centers/Cyber Cafes.

1.1.2 The GSM Revolution

The GSM revolution began in August 2001 and changed the face of Information and Communications Technology in Nigeria. But note that the picture will not be complete without mentioning the Private Telephone Operators (PTOs) and other landmarks such as the licensing of Globacom as Nigeria's second national operator (SNO) as well as the licensing of 22 fixed wireless operators.

Though Globacom is presently more active in the mobile telephony sector (Glomobile), it has the same licenses as NITEL. Globacom's license constitutes a multi-service package of National Carrier, GSM, International Gateway and Fixed Wireless Access (FWA).

Since the GSM launch, mobile telephony has rapidly become the most popular method of voice communication in Nigeria. Growth has been so rapid that Nigeria has been rightly described as one of the fastest growing GSM markets in the world. These developments position Nigeria as having over five million mobile lines and about one million fixed lines, compared with only about 450,000 working lines from NITEL three years ago.

Telecommunications Services offered in Nigeria

There are a wide range of telecommunication services now available. They include:

- Telephony
- Telex
- Cellular Mobile Telephony
- Facsimile
- Radio/Television Carrier
- Extension of Telex Terminals to rural areas (Gentex)
- Voice Cast/Press Receipt
- Private Leased Circuit
- Alternate Leased Circuit
- Maritime Mobile Service, INMARSAT, Ship Shore, etc.
- Global Mobile Personal Communications Services (GMPCS)
- Data Communications
- High Speed Data Transmission
- Public Payphones
- Value Added Services
- Business Network Services
- Computer Networking
- Internet Service
- Telecommunications Consultancy Services
- Paging Services
- Mobile Radio Trunking Services

Table 1: List of Nigeria Telecom Operators

Nigeria Telecom Operators	Type of Services Provided	Primary Website
Airtel Mobile	GSM Service Provider	www.ng.airtel.com
Etisalat (EMTS) Mobile	Telephony Service Provider	www.etisalat.com.ng
Globacom Mobile	Second National Telecommunications Operator (Mobile GSM Telephone Services, Broadband Access, International Gateway, Online Telecommunication Services)	www.gloworld.com
Starcomms Mobile	Total Telecommunications Service Provider	www.starcomms.com
MTN Nigeria Mobile	Telecommunication Service Provider	www.mtnonline.com
Mtel (NITEL) Mobile	Local and International Telecommunications Services	www.mtelnigeria.com
Multilinks (Telkom) Mobile	Telecommunications Service Provider, Operator of Telecommunications Services	www.multilinks.com
Visafone Mobile	Telephony Service Operator, Telecommunication Service Provider	www.visafone.com.ng
Zoom Mobile	Advanced Digital Mobile Wireless Telephone Service Provider	www.zoomnigeria.com

Table 2: List of Fixed, Mobile, Internet service providers in Nigeria

Fixed, Mobile, Internet service providers in Nigeria	Website
21st Century Technologies Ltd	www.21ctl.com
Intercellular Nigeria Plc.	www.intercellular.com
Mobitel Limited	www.mobitel.com.ng
Monarch Comm. Limited	www.monarchng.com
Multi-Links Telkom	www.multilinks.com
Zoom Mobile	www.zoomnigeria.com
Peace Global Satellite Comms. Ltd	www.peaceglobal.net.ng

Table 3: List of Infrastructure Providers in Nigeria

Infrastructure Providers[2]	**Website**
Brand Direct Ltd	www.branddirectng.com
Dizengoff W. A. Nigeria	www.dizengoff.com
Flory Struct-Tech Ltd	www.florystruct.com
GTS -Infotel Nigeria Ltd	www.gts-infotel.com
Raeanna Nigeria Ltd	www.raeanna-nig.com
Watchers Telecoms Ltd	No website
VDT Communications Ltd	www.vdtcomms.com
Vodacom Business Nigeria (formerly Gateway)	www.vodacom.com
Voicewares Networks Ltd.	www.vnetnigeria.com
VPS Technologies Ltd	www.vpstechnologies.net
Phase3 Telecom Limited	www.phase3telecom.com
Vodacom Business Nigeria (formerly Gateway)	www.vodacom.com

[2] (VSAT, Trunking, paging, microwave Radio, Optic Fiber, Cabling, Interconnect, Long Distance Carrier)

Private Networks Nig. Ltd	www.pnngroup.net
Radial Circle Telecoms Ltd	www.radialcircle.com
Nera Microwave Nig. Ltd	www.nera.no
Lucratel Limited	www.lucratel.com
Layer3 Limited	www.layer3.cc
Main One Cable Company Ltd	www.mainonecable.com
Interchange Technologies(Nig) Ltd	www.interchange-technologies.com
Internet Solution Nigeria	www.nigeria.is.co.za
Helios Towers Nigeria	www.heliostowers.com
IHS Nigeria Plc.	www.ihsafrica.com
Disc Communications Ltd	www.discomtel.com
Comm Network Support Service	www.cnssl.net
Computer Warehouse Group	www.cwlgroup.com/dcc
Basnik Telecoms Limited	www.basniktelecoms.com
Backbone Connectivity Network Nigeria Ltd.	www.bcnnigeria.net
Telnet Networks Ltd	www.telnetng.com
Upland Consulting Nigeria Limited	www.uplandconsulting.com
Unotelos Limited	www.unotelos.com

Table 4: List of Internet Service Providers in Nigeria

ISP's (Internet Service Providers) in Nigeria	Websites
Best Communications Ltd	www.bestcomm.biz
Cobranet Limited	www.cobranet.org
Cyberspace Limited	www.cyberspace.net.ng
Geoid Telecoms Nig. Ltd.	www.geoidtelworld.com

IpNX Limited	www.ipnxnigeria.net
Iway Africa	www.iwayafrica.com.ng
Juniper Solutions Ltd	www.junisat.com
Kinten Telecom Ltd	www.kintentelecom.net
Linkserve Communications Ltd	www.linkserve.net
Pinet Informatics Ltd	www.pinet.com.ng
Pop Broadband Ltd.	www.popbroadbandng.com
Steam Broadcasting & Comm. Ltd	www.coollink.us
Swift Networks Ltd	www.swiftng.com
eStream Networks Limited	www.estreamnetworks.net

Table 5: List of Equipment Dealers in Nigeria

Equipment Dealers[3]	Websites
Accat Nigeria Ltd	www.accat.com.ng
Backup Networks Ltd.	www.backupnetworksng.com
Danimex Nig. Ltd	www.danimex.com
Briscoe Technologies Ltd	www.briscoetechnologies.com
CEBIT PARK LTD	www.cebitpark.com
Diyeem Global Concept Ltd	www.diyeemglobal.com
EIL Telecomm Ltd	www.eiltelecom.com
Globa Access Technologies Ltd	www.globalaccesstechng.com
ICT Convergence Ltd	www.ict-convergencelimited.com
Integrated System & Devices Ltd	www.isdlnig.com
Intertel Nig. Ltd.	www.intertel-ng.net
Jibson Dynamics Ltd	www.jibsondynamics.com

[3] (Sales, Supply, Installation & Maintenance of Mobile Phones, Two-Way Radios, Pagers, Telephone Handsets, Other Customer Premise Equipment, PABX and Major Network Installation, System Integrators)

KITS Technologies Ltd.	www.kittechnologies.com
Mikado Communications Ltd	www.mikadong.com
Mutimesh Communications Ltd	www.multimeshcom.com
P. A. Telecom Ltd	www.patelecoms.com
Ross Office Systems Nig Ltd	www.rossofficesystems.com
Sunborah Technology Ltd.	www.sunborahtech.com
Supadet Holdings Ltd.	www.supadet.com
SWAP Technologies & Telecomm Plc.	www.swap-ng.com
T3 Communications Ltd	www.t3comms.com
Teledom International Ltd	www.teledominternational.net
Telemobile Nigeria Ltd	www.telemobilenigeria.com
Total Telecom Solutions Ltd	www.totaltelecoms-ng.com
Web Inn Ltd	www.webinnsolutions.com

1.1.3 Major Threat to Telecommunication Information Infrastructure Management in Nigeria

Telecommunication infrastructure often times is confronted with certain threats that potentially lead to disruption of service and sometimes complete shut-down. We discuss some of the major threats in telecommunication information infrastructures and case studies on these threats with regards to NCC licensed telecommunication operators in Nigeria.

1. Case Studies on NCC Licensed Operators

Threat: *Telecom sites closure by government agents and Imposing myriads of taxes on licensed telecom operators.*

Recently some Telecom sites have been closed and several taxes imposed on licensed telecom operators in some states in Nigeria. According to the Association of Licensed Telecommunications

Operators of Nigeria (ALTON) [26], they have been affected in states such as Ogun, Ondo, Akwa Ibom, Ebonyi, Osun and Kaduna states.

In so many states, Telecom services providers have recorded cases of arbitrary site closure in an attempt to force them to pay local taxes and levies some of which are multiple in nature and most of which are only aimed toward telecom operators; Licensed operators believe that taxes and levies should be broad-based and fairly distributed across all sectors of the economy; there is therefore no justification for targeted and sometime very high taxes on telecom operations.

Effects of Site Closure and Imposed Arbitrary Taxes

i. Difficulty in the continued provision of uninterrupted services with the type of venerability of Licensed Operators and their infrastructure
ii. Reduced Quality of Service (QoS)

Expected Actions

i. First level of protection by Government
ii. Employing a cross-sector/multi-stakeholder approach to reduce growing burden of taxation on our industry
iii. A presidential declaration of telecommunication infrastructure as National Security and Economic Infrastructure as contained in the cybercrime law of 2015 as a way of guiding telecom infrastructure against vandalization as well as incessant government agency shutdown of cell sites.
iv. Following the best practices on this work with regards to physical security is also important

2. Bombing / Terrorist Attacks on Telecommunication Facilities

Attacks on telecoms installations do happen. For example, in 2012 alone, Boko Haram in Nigeria destroyed or damaged some 530 base stations and killed staff, causing an estimated $132.5 million in damage - capital that could have been used to further develop networks in Nigeria. [25]

This threat affected about 30 telecoms infrastructure in Yobe, Gombe, Kano and Borno. This can be a great setback for local and foreign direct investment inflows into the nation's

telecommunication sector and unprecedented in the history of telecoms sector. Affected operators according to Daily Sun, revealed that worst hit by the attack is MTN Nigeria, Etisalat, Airtel, Globacom, Multi-Links, Helios Towers, IHS and other ISPs.

According to MTN Nigeria's company's Corporate Services Executive, the attacks by unknown persons had caused service challenges in parts of the North as sensitive hub sites had also been affected. MTN confirm that like all the other major telecommunication operators, some of their installations in Northern Nigeria were damaged by unknown persons. Other destructions include base stations vandalism. Some of the telecoms towers destroyed are hub sites that connect to several other base stations and the impact in terms of service disruption.

MTN also claimed that they have experienced more than 70 cuts on its fiber network nationwide on a monthly basis, affected by violent attacks on some of its facilities before, and carried out by people intent on stealing.

According to the Executive Director, Commercial and Business Development, IHS, Gbenga Onakomaiya (whose company lost base stations), repairs could take six months to fix since some of the equipment need to be imported. The executive director claimed that the minimum time of recovery from an attack is two month if the affected piece of equipment is available in their warehouse.

Effects

i. Damage to telecom Infrastructures

ii. Scaring away and discouragement of Investors in the telecommunication Industry

iii. Lack of safety for Telecom Personnel who work on sites

iv. Serious security Concerns as people cannot communicate in real-time with one another especially during emergencies

v. Loss in Investment to telecom operators

vi. congestion or outright network failure

Expected Actions

i. Government to intensify the fight against insurgency

ii. Telecommunication Operators / Stakeholders to partner with the Federal Government to forestall future occurrence and improve the security situation in the country.

Other Threats include:

Cyber Attacks

Cyber-attack is now firmly established in the contours of conflict. This places both service continuity and key staff (with access to codes and passwords) at particular risk.

1.1.4 Regulator Sanctions on Licensed Telecom Operators

Sanctions can affect the ability of investors to further invest in the industry. The Regulator should device more ways of sanctioning licensed operators without impacting on the growth of the telecommunication industry.

Corruption

Corruption may also be a key driver of threat to telecommunication investors in weak or ungoverned areas, resulting in extortion attempts and obstacles to efficient, legal service provision and revenue collection.

1.1.5. Infrastructure Management by NCC Licensed Operators.

Before now, NCC operators had maintained the posture of jack of all trades and were trying to be master of all until the cookies began to crumble. With insecurity issues growing exponentially and service quality getting poorer as more and more Nigerians joined the mobile communications train, the reality of the need to secure infrastructure, expand service and install new base stations and infrastructure soon dawned on the operators. But to achieve this necessity, a number of obstacles are to be crossed, which perhaps the operators never envisaged at the beginning of the business.

First, they had to contend with series of application for approval from various government agencies and bodies, thereafter, they have to face threats from locals who also demand settlement before the operator bring its equipment for the installation of infrastructures and construction of base station. These are aside the challenge of how to secure the facilities against vandalism, theft and how to power it 24/7.

With all these challenges, the only option left for the operators is to embrace co-location that is, sharing of base stations and infrastructure. Tower sharing "entails operators collaborating to share either the active elements (the physical network) or the passive elements of their base stations – including the physical tower structure, security, power and diesel generators. Luckily at that period, independent infrastructure management companies began to show up at the Nigerian telecom scene and that brought a huge relief for the operators. Today, the likes of Helios Towers Nigeria (HTN), IHS and SWAP have become the burden bearer for telecom operators. As a matter of fact, they have become the major backbone of all telecom operators in the country as operators massively offload their infrastructures to those companies to manage.

By the end of 2014, over 70 per cent of towers, base stations and infrastructure in Nigeria were owned or operated by independent infrastructure companies. The massive shedding has continued with MTN, Airtel and Etisalat selling off their remaining towers in separate deals. And with these developments comes the greater expectations that the operators will be able to improve their service quality, having been set free of infrastructure management and left to focus on their core business of providing quality service.

Case study

As at the last count, the tower deals already sealed by three of the four GSM operators in the country, MTN, Airtel and Etisalat was in the region of $4 billion.

Incidentally, the tower and infrastructure sales frenzy began with troubled Code Division Multiple Access (CDMA) operators who were trying to remain afloat in the face of stiff competition from the GSM operators. By December 2010, STARCOMMS Plc. (now defunct) had finalized a sale and leaseback agreement with Swap Technologies and Telecomm Plc. relating to 407 of its 557 Base Station Towers. Under the terms of the transaction, Swap took over the operation, security

and maintenance of the passive aspects of the 407 towers. Those towers comprised the physical structures as well as the power components, while the core network and radio components remained under Starcomms' ownership and control. The lease agreement was for an initial duration of 15 years, and allowed Starcomms full access to the towers to operate its network.

Shortly after that, in 2011, Visafone Communications Limited, then the only surviving CDMA operator (now acquired by MTN), also sealed an infrastructure sharing deal with IHS Nigeria Plc., a leading telecoms infrastructure provider in sub Saharan Africa. The infrastructure sharing strategy, as revealed then, was a long-term partnership involving the sale and leaseback of the tower assets of Visafone, aimed at optimizing their operational efficiencies. The strategic partnership was expected to lead to significant benefits by enabling Visafone to focus on its core business of providing mobile services and solutions. It was also to provide IHS the platform of consolidating its telecom infrastructure business and industry leadership position with more than 800 owned sites under collocation in Nigeria and several thousands of sites under management.

Just recently, Etisalat Nigeria completed the transfer of 555 telecom towers to IHS Holding Ltd, leading Africa mobile tower provider, the second tranche of a sale and leaseback deal. Earlier, Etisalat Nigeria had sold 2,136 of its towers to IHS and leased them back as part of plans to expand its coverage. Etisalat said the partnership with IHS is designed to promote network sharing, ensure higher quality, sustain reliable mobile services, lower overall costs and also promote a cleaner environment through reduced diesel usage and increased investments in alternative energy solutions.

Likewise, Airtel, had sold more than 4,800 mobile phone masts in its Nigerian operation to American Tower Corp. Bharti Airtel agreed to be the anchor tenant on the masts it is selling to American Tower, initially for 10 years.

Similarly, MTN Nigeria has already sold more than 6,000 mobile towers to IHS which will be raised to 9,000 in due course. By selling towers to infrastructure groups such as IHS, MTN can offload the responsibility for the work needed in future, although they will incur the rental cost of continuing to use the towers. IHS, meanwhile, can open the towers up to rival groups to share, which generates additional revenues. Following the deals, IHS, the biggest tower company in Africa, will own and manage more than 15,500 of the installations in Nigeria and more than 23,100

in Africa as a whole. It will own and manage over 6,540 towers in Nigeria, all of which will be managed by the most advanced Network Operating Centre (NOC) in the country. The tower companies have installed a large number of alternative energy sites in Nigeria, investing state-of-the-art NOCs that ensure uptimes of over 99 per cent are achieved on their sites. They are also committing hundreds of millions of dollars in the towers acquired on advanced generators, efficient batteries and alternative energy solutions to reduce diesel consumption and improve efficiency of grid use. *(http://www.ittelecomdigest.com/qos-tower-operators-in-rescue-mission/)*

1.2 Significance of Study

The best practices defined in this document are intended as voluntary, and are designed to give guidance to Telecommunication Industry on how best to secure their information Infrastructures. They ensure that TSPs have a common understanding of what a secure, resilient, available communications service is and how to manage it.

1.3 Scope

As a product of the Nigerian Communications Commission (NCC), these best practices apply to TSPs that supply and support Nigeria's telecommunications critical infrastructure (CI). However, there is nothing contained in these best practices which prohibits other service providers from implementing these controls or from leveraging controls from a connected provider to meet the requirements.

The best practices apply to wire line communications, as well as to TSPs' wireless networks, such as (Code Division Multiple Access) CDMA, High Speed Packet Access or 4G (HSPA), and future generation phone networks.

The best practices identify the controls that any service provider should have in order to detect cyber security threats, thereby helping the service provider protect both its customers' interests and its own infrastructure.

The scope of this document includes basic controls that should be implemented for redundancy and availability, as well as other topics (such as vendor management) insofar as they relate to the objective of this document.

These best practices detail the features and practices that a TSP should have in its networks; however, the security resilience at the edge of the networks will vary according to the security service levels requested by customers. Nothing in these best practices limits a TSP's ability to restrict which features are available at which service levels, or to charge for those features. Many of the features listed in these best practices require a significant amount of investment and would have service levels based on customer requirements.

Throughout the best practices there are requirements to notify users if they appear to be infected with malware or if users need to take other actions. While these actions will have a benefit for customers, they are primarily intended to protect the service providers' infrastructure. TSPs are not responsible for removing infections on customers' computers.

1.4 Guiding Sources

These best practices leverage work done by other standards bodies, including:

i. International Organization for Standardization (ISO) 27001, 27002, 27011, 27032, and 27035;

ii. Communications Security Establishment Canada's (CSEC) Technology Supply Chain Guidelines for Telecommunication Equipment and Services;

iii. Australia's Internet Service Providers' Voluntary Code of Practice; and

iv. Internet Engineering Task Force Request For Comment (RFCs) as appropriate (such as Security RFCs, Security Considerations, Ingress Filtering for Multihomed Networks).

TSPs carry a mix of traffic over their networks, including internal service provider generated traffic and external customer generated traffic. Cyber security attacks can affect both types of traffic. These best practices take into account the differing privacy concerns as they relate to these

disparate networks and attempt to explain what can be monitored and addressed, and how to do so without violating customer privacy.

One of the key ways for TSPs to enhance customer safety and the stability of their portion of the Internet is to share cyber security threat information with one another. This cyber security threat information will be limited to threat characteristics and response information, and will not include individual customers. Mechanisms for sharing such threat information will be defined within NCC's mandate.

1.5 Understanding the Telecommunications Infrastructure Core

The telecommunications infrastructure of a network operator consists of a set of networks (transmission network, switching network, access network, signaling network, mobile network, intelligent network, management network), each performing a particular function towards the provision of the service to the customer. With the evolution towards IP-based network, the circuit switched network is migrating towards a new architecture called Next Generation Network (NGN) which emulates the behavior of circuit switching. With the advent of broadband access networks, the core network evolves towards IP Multimedia Subsystem (IMS) which provides IP-based multimedia services.

The objective of this section is to briefly introduce the telecommunication network structure to acquire the vocabulary of the field, understand the several types of networks involved in the operator's "Telecommunication Network", and gain knowledge on how these networks interface and interoperate. The various services supplied by each type of network are also emphasized. Another important objective of this section is to introduce the evolutions of these networks and services on the medium and long terms.

A Telecommunication network consists of two parts:

- The "network" (transmission, switching, access, signaling, mobile, intelligent network)
- The "business and technical information system" which consists of OSS (Operating Support System) and BSS (Business Support system).

Public Switched Telephone Network (PSTN)

PSTN is the fixed voice network. It consists of the transmission, switching, signaling and intelligent networks. The **transmission network** enables carrying all kinds of traffic (voice, video, and data). It consists of nodes called multiplexers and links among multiplexers. The goal of the multiplexer is to multiplex/demultiplex traffic onto/from the link. There exists three multiplexing technologies: PDH, SDH and D-WDM. The link technology is generally optic fiber but may also be coax, radio, etc. A transmission network generally consists of hundreds of multiplexers and tens of thousands of kilometers of optic fiber.

The **switching network** enables switching the traffic from the sender to the appropriate destination. A switching network consists of switches. All switches rely on the transmission network which provides digital trunks. A switch receives traffic from the transmission network at input ports, applies the switching function which forwards the traffic to output port. Then, the switch relies on the transmission network to send the traffic to an adjacent switch. The voice network is using the circuit switching technology which provides voice services.

A switching network operates in a connection oriented mode. That means that prior to enabling users exchanging their traffic, there is a need of reserving resources on the path between the sender/caller and the receiver/callee. To reserve resources, all switches on the path exchange signaling information. Signaling information is data. In the case of circuit switching, signaling data is carried over a separate network, i.e., a **signaling network** called Signaling System 7 (SS7). This is out-of-band signaling.

The **intelligent network** is used in the voice network for the provisioning of services such as free phone, premium rate, virtual private network, account card calling, etc. It consists of a set of application servers containing service logic and service data.

The **access network** is the network which enables attaching the user equipment to the switching/transmission network. The subscriber has a subscriber line, which may be an analog line, an ISDN line, a leased line, an ADSL line, etc., to connect to the PSTN.

EMSs (Element Management Systems) are sold with the equipment by the telecom vendor. EMSs enable operators to manage their equipment. The OSS (Operation Support System) is the

management of the network and the services. The BSS (Business Support System) is the interface to and the management of the customer.

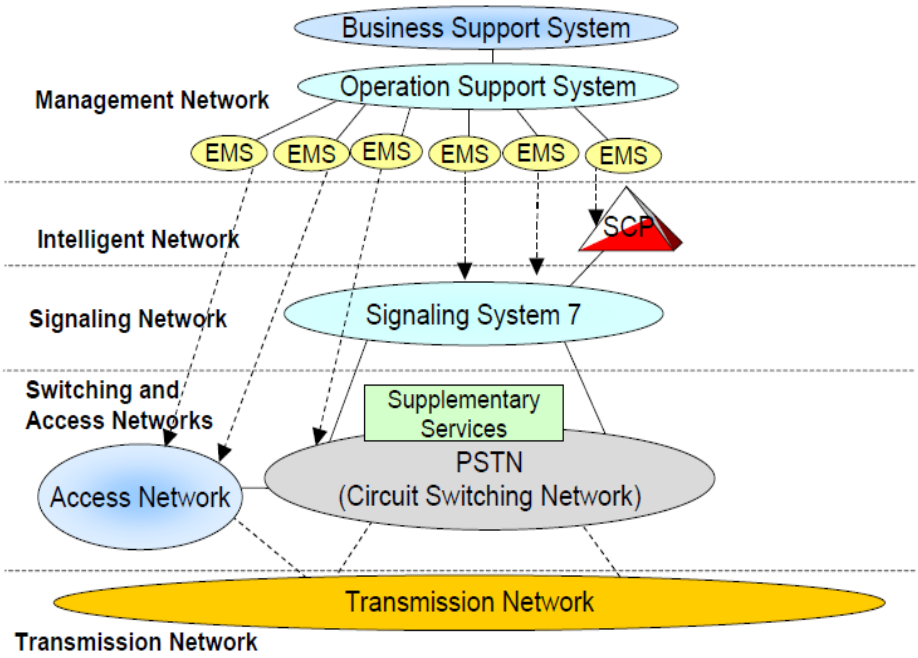

Figure 1.1: Fixed Voice Network – PSTN (Public Switched Telephone Network)

Global System for Mobile Communications (GSM)

The GSM network is a mobile voice network. It looks similar to PSTN but supports an additional service called terminal mobility. As for PSTN, it consists of a switching plane where Mobile Switching Centers (MSCs) may be found. The circuit switched network with MSCs is called NSS (Network Subsystem). The attachment of the mobile terminals to the network is handled by a Radio Access Network (RAN) called BSS (Base Station Subsystem) in case of 2G, and UTRAN (UMTS Terrestrial Radio Access Network) in case of 3G. The BSS/UTRAN consists of base stations and controllers of base stations.

The MSCs of the GSM network interface with the PSTN network to enable communication between mobile and fixed terminals. Since the GSM network is a voice network, SS7 is used for the transport of signaling information between BSS/UTRAN and NSS and between MSCs within NSS and between NSS and PSTN.

The Intelligent Network is called Customized Application Mobile Network Enhanced Logic (CAMEL). GSM provides terminal mobility and CAMEL provides service mobility. CAMEL provides services such as short numbers, VPN and Mobile prepaid. With CAMEL, the user may access to her/his services from visited networks; the home network has roaming agreements with.

The management of BSS/UTRAN is handled by OMC-R (OMC Radio). The management of the MSCs is handled by OMC-S (Switching). OMC-R and OMC-S are supplied by telecom vendors together with the equipment those OMCs have to manage. A mobile service provider builds its OSS and BSS that interface with these OMCs.

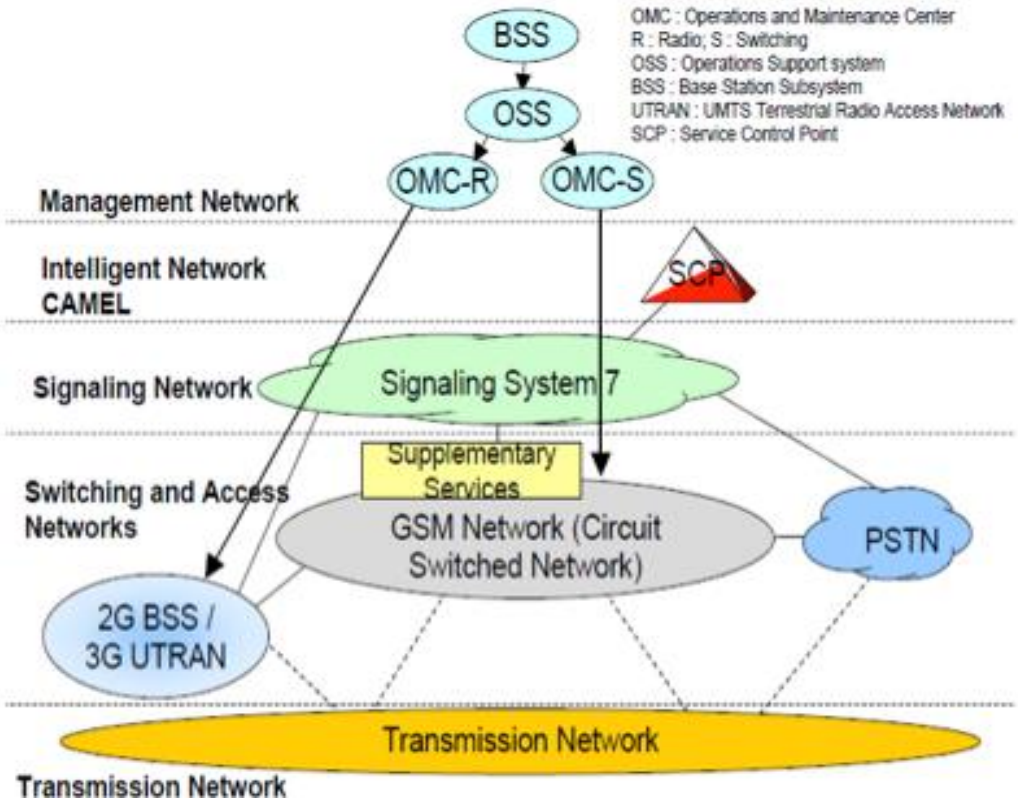

Figure 1.2: Mobile Voice Network: GSM (Global System for Mobile Communications)

General Packet Radio Service (GPRS)

GSM provides voice services. GPRS reuses the existing GSM infrastructure to provide end to- end packet-switched services, i.e., data services. While the mobile packet core network is called General Packet Radio **Service (**GPRS), the access technologies which may be considered to access to the GPRS network are GPRS (BSS), EDGE (BSS), W-CDMA (UTRAN), HSDPA/HSUPA (UTRAN).

While a voice communication requires 12 Kbit/s at the radio access, GPRS enables access to data services (for example, WAP) at a bitrate which is associated with the access technology, from 40 Kbit/s for GPRS access technology to 1 Mbit/s for HSDPA/HSUPA technologies.

Moreover, the cost of the data session is not related to the only duration of the session but related to several criteria including volume, duration, event, content, etc.

GPRS provides interfaces to Intranet and Internet networks. GPRS does not impact the GSM BSS (Base Station Subsystem) and 3G UTRAN. This is important because 65% of the cost of a mobile network is due to the access network while the remaining 35% is the cost of the core network. With the GPRS network, the user can have access to IP-based services, either those of Internet or those of the mobile service provider. Therefore, GPRS provides broad IP-based application support (E-mail, WAP, WEB, instant messaging, multimedia messaging, video streaming, mobile TV, broadband access to the Internet, etc.).

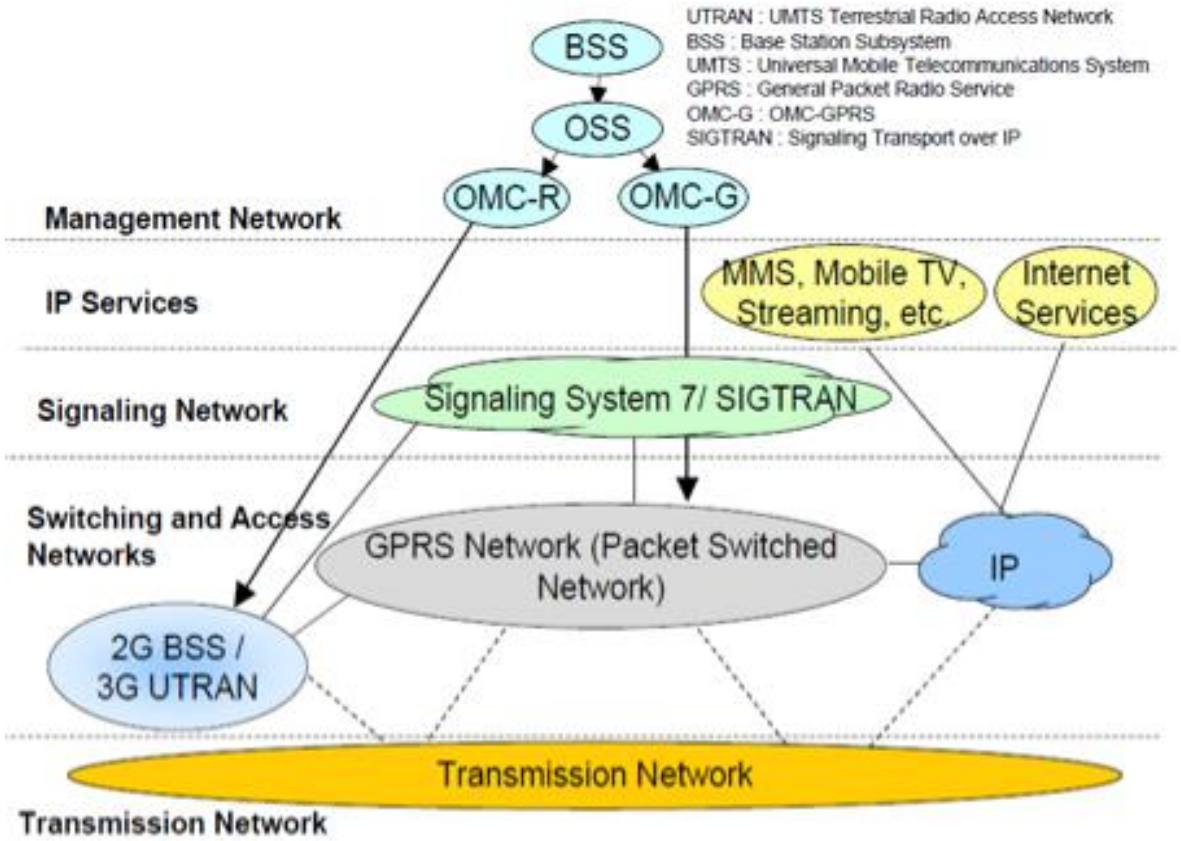

Figure 1.3: The Mobile Packet Network: General Packet Radio Service (GPRS)

Broadband access and broadband services

The trend is to propose broadband access to the customer and an associated bundle of broadband services including IP TV (broadcast TV, video on demand) and IP Telephony.

This is true for fixed and mobile accesses. Fixed accesses include FTTx, xDSL, cable, WiMAX technologies while mobile accesses include HSDPA/HSUPA, HSPA+ (3G+), EPS (4G), and EVDO (Evolution Data Only used for supplying high speed data access in CDMA2000-based networks).

The same IP network connects whatever broadband access technology and supports the IPbased service architecture. IMS (IP Multimedia Subsystem) s a standardized service architecture for multimedia services such as IP telephony, IP TV, presence, messaging, IP centrex, Conferencing, etc. Apart from the IP services supplied by the service provider, the user may access to any Internet services (Web, mail, file transfer, streaming, Internet telephony, etc.)

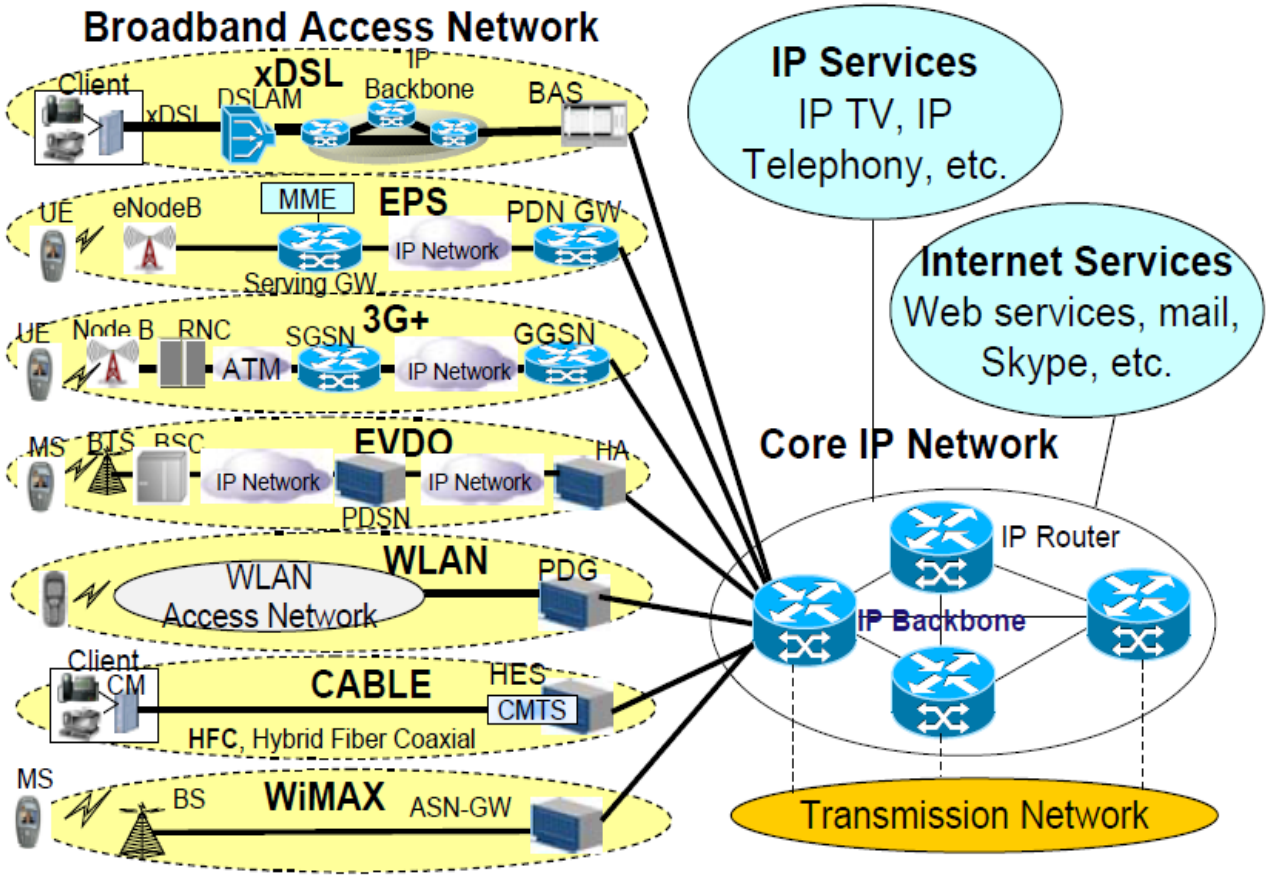

Figure 1.4: Broadband access networks and broadband services

From Circuit Switching to Next Generation Network (NGN)

From the fixed telecommunications circuit-switched network perspective a number of developments has occurred to give operator's greater flexibility in the deployment of networks. Distributed processing has enabled the separation of pure switch/routing functionality away from the control mechanisms. The separation of contemporary switch mechanisms into Media Gateways (MGWs) (containing switching, transcoding and user-plane transmission aspects) and Media Gateway Control functions (MGCs) (containing switch and service control functionality), connected via standard interfaces (e.g. H.248/Megaco, Media Gateway Control Protocol), enables operators to increase the service delivery and control parts of their networks in relative isolation to the growth of the user traffic parts of the network. The figure below illustrates the concept behind the distributed processing and switching mechanisms offered by H.248/Megaco. This

approach also enables procurement towards distributed networks with controller and gateway procured from separate suppliers, enabling a real progression towards call server 'farms' connected to 'pools' of resource control and switching.

The architecture is called Next Generation Network (NGN). This intelligence now resides in

MGC also called Softswitch or Call Agent, which acts as the controlling element. Open interfaces towards Intelligent Network (IN) applications and new application servers facilitate rapid service provisioning and ensure a short time to market.

At the media layer, gateways are introduced to adapt voice and other media to the packet transport network (typically IP/Ethernet network).

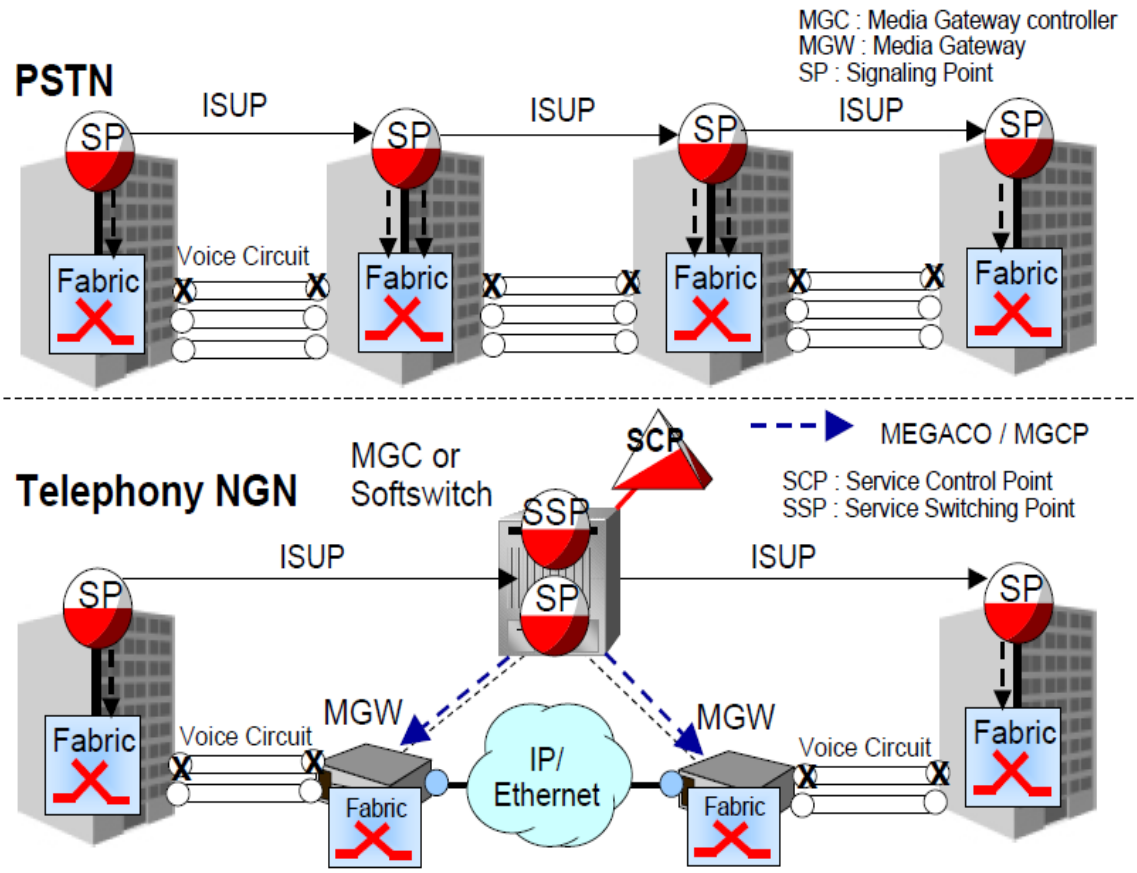

Figure 1.5: PSTN versus NFN

The mobile switches of a GSM network may also be replaced by an NGN architecture which is called R4 architecture.

Chapter 2 - Information Systems Infrastructures Management in Telecommunication

2.1 Framework for Information Systems Infrastructure

Our dependency on supporting infrastructures requires the interconnection of all basic facilities and service that enables them to function properly. The supporting infrastructures of a city, for example, includes components such as streets, power, telephone, water, and sewage lines, schools, retail stores, and law enforcement. Everyone depends on such infrastructures; cities with a good infrastructure, for example, are considered more livable than cities with poorer infrastructure and more likely to attract businesses and residents.

For telecommunication industries in Nigeria, managing a comprehensive and robust information system infrastructure can be a hard task. This is particularly true since Nigeria is a developing nation. For example, TSP's often cannot rely on an uninterrupted supply of electricity. Consequently, many of the large call centers and Telecommunication firms in Nigeria that support customers and companies such as the banking industry install heavy power generators to minimize the effects of frequent power outages. TSPs must continue to ensure that these and other supporting infrastructures are adequately managed, secured, and reliable. The framework for Information Systems Infrastructure can assist in achieving this goal.

2.1.1 The Need for an Information Systems Infrastructure

As people and companies rely on basic infrastructures to function, businesses also rely on an information systems infrastructure (hardware, software, networks, data, facilities, human resources, and services) to support their decision making, business processes, and competitive strategy. Business processes are the activities that organizations perform in order to reach their business goals and consist of core processes and supporting processes. The core processes make up the primary activities in the value chain; these include all the processes that are needed to manufacture goods, sell the products, and provide service, and so on. The supporting processes are all the processes that are needed to perform the value chain's supporting activities. These include an accounting system and human resources management. Figure 2.1 shows a generic value chain for core and supporting activities in an organization.

Most the business processes of an organization depend on the underlying information systems infrastructure. For example, an organization's management needs an infrastructure to support a variety of activities, including reliable communication networks to support collaboration between suppliers and customers, accurate and timely data and knowledge to gain business intelligence, and information systems to aid decision making and support business processes.

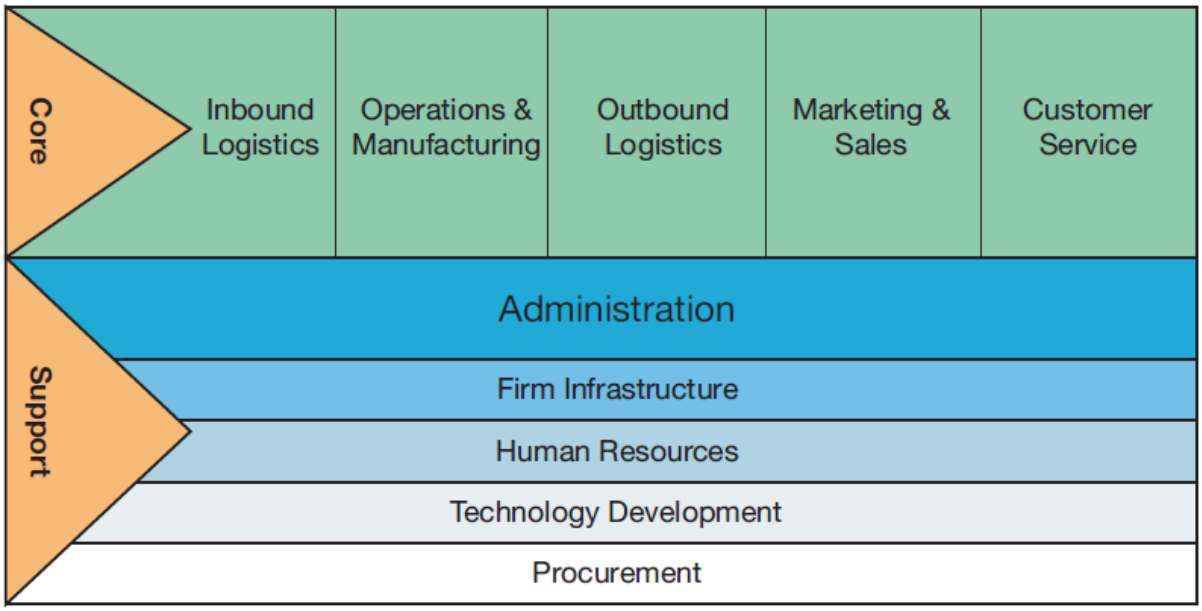

Figure 2.1: A generic value chain showing an organization's core and supporting activities.

2.1 Managing Hardware Infrastructure

The information systems hardware is an integral part of the Information System (IS) infrastructure. This hardware consists not only of the computers used in an organization but also of networking hardware. The computing hardware is part of an organization's IS infrastructure and is needed to store and process organizational data. Likewise, the networking hardware is needed to connect the different systems to allow for collaboration and information sharing.

Most Telecommunication firms often face difficult decisions regarding their hardware. Constant innovations within the information technology sector lead to ever-increasing processor speeds and

storage capacities but also to rapid obsolescence. Information systems executives within the firms therefore face countless complex questions, such as the following:

i. The choice of hardware technologies.
ii. The time interval that is required for the equipment be replaced.
iii. The best practice requirement to secure the information systems.
iv. The level of performance and storage that is required at the current time and in the future.
v. Best practice for assure reliability.

The following are different infrastructure solutions that address the above questions and can help to support an organization's competitive strategy, decision making, and business processes.

On-Demand Computing

The demand for individual IS resources is highly fluctuating in most organizations. For instance, there may be high-bandwidth applications, such as videoconferencing, that is needed only during certain times of the day, or some resource intensive data-mining applications that can only be used in irregular intervals. On-demand computing ensures that issues such as fluctuating computing needs are addressed. Available resources are allocated on the basis of users' needs (usually on a pay-per-use basis). For example, users engaging in videoconferencing may consume more bandwidth, while other users who do not need the bandwidth at that time receive less. In the same vein, a user running complex data mining algorithms would receive more processing power than a user carrying out some word processing task.

In deciding which hardware technologies to be chosen, some organizations prefer to "rent" resources from an external provider. This type of on-demand computing called "utility computing", is where the resources in terms of processing, data storage, or networking are rented on an as-needed basis and the organization receives a bill for the services used from the infrastructure provider at the end of each month. For many organizations, utility computing is an effective way for managing fluctuating demand as well as controlling costs; in essence, all tasks associated with managing, maintaining, and upgrading the infrastructure are left to the external provider and are typically bundled into the "utility" bill on a pay-per-use basis. Also, as with the

utility bill, customers are charged not only on overall usage but also on peak usage (i.e., different rates for different times of the day).

Grid Computing

Some tasks are beyond the capacity of a supercomputer, although today's supercomputers have tremendous computing power. Some complex simulations can take a year or longer to calculate even on a supercomputer. Sometimes, an organization that has need for a supercomputer but may not be able to afford one due to the extremely high cost. For example, the fastest supercomputers can cost more than $200 million, and this does not constitute the "total cost of ownership," which also includes all the other related costs for making the system operational. In addition, the organization may not be able to justify the cost because the supercomputer may be needed only occasionally to solve a few complex problems. This kind of situation leaves organizations with the choice to either rent time on a supercomputer or decide not to solve the problem.

However, with grid computing – a relatively recent infrastructure trend, organizations can save cost of computing infrastructures. Grid computing refers to combining the computing power of a large number of smaller, independent, networked computers (often regular desktop PCs) into a cohesive system in order to solve problems that only supercomputers were previously capable of solving. Unlike supercomputers are very specialized; grid computing allows organizations to solve both very large-scale problems as well as multiple (concurrent) smaller problems. For grid computing to work, large computing tasks must be broken into small chunks, each of which can then be completed by the individual computers.

While individual computers are also in regular use, calculations and processing are performed during the computers' idle time so as to maximize the use of existing resources. In Nigeria and around the world for example, many of the resources are idle during the night hours, often more than 12 hours per day. Because of time zone differences, grid computing helps utilize those resources constructively. One way to put these resources into use would be to join the Berkeley Open Infrastructure for Network Computing (BOINC), which lets individuals "donate" computing time for various research projects, such as searching for extraterrestrial intelligence or running climate change simulations.

However, as you can imagine, grid computing poses a number of demands in terms of the underlying network infrastructure or the software managing the distribution of the tasks. Additionally, many grids perform on the speed of the slowest computer, thus slowing down the entire grid. Telecommunication firms starting out with a grid computing infrastructure can attempt to overcome these problems by using a dedicated grid. In a dedicated grid, the individual computers, or nodes, are just there to perform the grid's computing tasks; in other words, the grid consists of a number of homogeneous computers and does not use unutilized resources. A dedicated grid is easier to set up and manage and is more cost effective for many organizations than purchasing a supercomputer. As the grid evolves and new nodes are added, dedicated grids become more heterogeneous over time.

One factor that adds to the popularity of using dedicated grids is the falling cost of computing hardware. However, the added complexity of managing heterogeneous grids poses a large cost factor so that today it is often more cost effective to set up a homogeneous, dedicated grid; in this case, the savings in terms of software and management by far offset the added costs for dedicated computing hardware in terms of both acquisition and maintenance.

Edge Computing

Another recent trend in IS hardware infrastructure management is edge computing. With the decrease in cost for processing and data storage, computing tasks are now often solved at the edge of a company's network. This means that, rather than have massive, centralized computers and databases; a multiple smaller servers are located closer to the individual users. This helps to save resources in terms of network bandwidth and access time. If there is need for a computer to compute a certain problem for several hours, then it is best to send the task over a network to a more powerful computer that might be able to solve that problem faster. However, as the costs for computing power have decreased tremendously over the past years, many problems can now be computed locally within a matter of seconds, so it is not economic to send such problems over a network to a remote computer. To save resources, organizations use edge computing for their online commerce sites. In such cases, customers interact with the servers of an edge-computing service provider. These servers, in turn, communicate with the business' computers. This form of edge computing reduces wait times for the consumers, as the e-commerce sites are replicated on

the providers' servers, while reducing the number of requests to the organization's own infrastructure. This process not only saves valuable resources such as bandwidth but also offers superior performance and reduces cost organizations.

Autonomic Computing

The increased complexity of IS infrastructures in general is one major drawback of these hardware infrastructure trends. The main reason for having this infrastructure is to fully utilize the resources, the time and money needed to manage them. However, these resources don't add value to the organization; in fact, some people believe that the costs of managing these systems undermine the benefits these systems provide, even if the organization decides to outsource its services. Autonomic computing systems are self-managing, meaning they need only minimal human intervention to operate. Figure 2.2 shows an autonomic computing systems. In this system, operators fine-tune the computer's configuration to efficiently solve a specific problem. In an autonomic computing environment, the main aim is to allow the system to do everything else on its own and remain transparent to the user. To achieve this objective, the autonomic computing system must know itself and be self-configuring, self-optimizing, self-healing, and self-protecting.

The different tasks in an autonomic system can be optimized. The first step in the autonomic system optimization is self-knowing or self-discovering. This includes knowing its configuration, capacity, what resource it requires. The second step is ability to use different resources based on different job execution requirements. This whole process constitutes of what is called self-configuring. This way the user does not have to take care of any configuration issues. Furthermore, when any parts of a system can malfunction, an autonomic system is must be self-healing so that any potential problems are detected and the system is reconfigured so as to enable the user to continue performing the tasks even if parts of the system are not operational. Finally, as almost any computer system can be the target for an attack, autonomic computing system must be aware of any potential dangers and must be able to protect itself from any malicious attacks (e.g., by automatically quarantining infected parts of a system).

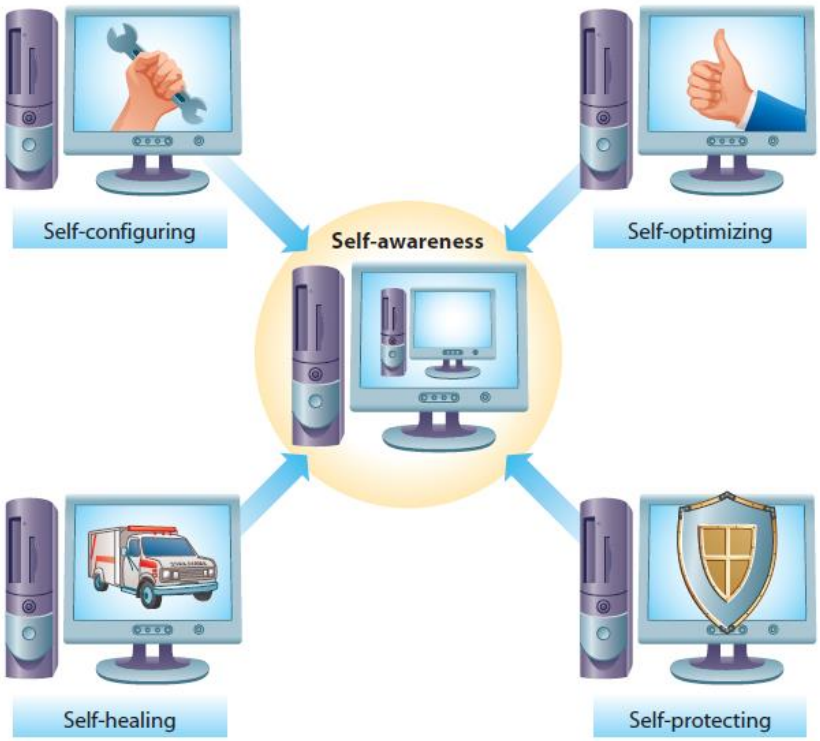

Figure 2.2: A diagram of autonomic computing systems has self-awareness and are self-configuring, self-optimizing, self-healing, and self-protecting.

Generally, these are formidable tasks the telecommunication industry has to address in order to manage their information systems. However, considering the time and money that is currently spent on managing and maintaining IT infrastructures, autonomic computing systems are promising for the future.

2.2 Managing Software Infrastructure

Information systems software enables companies to utilize their information systems hardware and networks. This software allows organizations to execute business processes and in their competitive strategy. Due to the increased reliance on information systems for managing organizations effective utilization of software resources has become increasingly critical and complex. For instance, organizations have to manage the software installed on all computers used, including managing updates, fixing bugs, and managing issues related to software licenses. In addition, they also have to decide when to perform upgrades for their software and the right time to perform the upgrades.

Clearly, software is an intangible asset protected by copyright and contract law. Due to its intangible nature, software poses unique challenges in terms of asset management. This challenge is further compounded when it comes to the management of software assets for an entity as large and complex as the telecommunication industry. Focus on this section will be on how software assets can be effectively and efficiently managed in the telecommunication sector.

2.2.1 Issues and Challenges

The way we communicate, deliver services, access/store/transmit information, conduct businesses and undertake daily online transactions has fundamentally be changed by Information Technology.

Managing IT assets has become more challenging as the telecommunication industry provides services that empower government to undertake critical and widespread e-Governance projects and transacts with citizens and entities, through computers and network, powered by software applications.

Some key trends/challenges being faced by organizations including telecommunication firms today include:

i. Management of all strategic IT assets
ii. Licenses
iii. Upgrades
iv. Documentation
v. Software versions

vi. More client machines (PC/Laptops) and Mobile Devices connected to unsecured networks.
vii. Increasing frequency of virus and security attacks.
viii. Increasing frequency of client security patch releases.
ix. Wider usage of open source and licensed software with differing licensing agreements.
x. Many License agreements require mandatory periodic independent audits

An effective Software Asset Management (SAM) framework will ensure that the Telecommunications industry is ready to deal with these challenges posed above and at the same time complies with the regulatory, legal, and security requirements of the Software being used.

In order to establish a Software Asset Management Framework, there is need to provide guideline assurance that:

i. A clear management policy for projects for open source, licensed and customized software is established.
ii. Project based software assets are integrated with existing software assets.
iii. A clear software asset ownership policy covering the entire asset life-cycle of the assets and project is established.
iv. To prevent use of illegal software.
v. To comply with software license conditions is adequately monitored.
vi. There is appropriate number of licenses for each item of software in use.
vii. There are effective controls in place for the physical security of software media.

Recognizing that various TSP's differ in their goals, operations and their composition, the guiding principles should be designed to serve as the common denominator allowing TSP's sufficient space and time to create specific plans while providing a unifying platform for all their asset management efforts.

2.2.2 Software Asset Management (SAM)

According to the Information Technology Infrastructure Library (ITIL), Software Asset Management (SAM) comprises of all the infrastructure and processes necessary for the effective management, control and protection of the software assets throughout all stages of their lifecycle. Figure 2.3 shows the software life cycle.

SAM is a business practice designed to reduce information technology costs, limit risks related to the ownership and use of software, and increase IT and end-user efficiencies. ISO 19770 Standard is the international standard on Software Asset Management (SAM) – (See Annexure A).

2.2.2.1 Key Procedures for Implementation

A number of key issues should guide the initial planning and implementation of a SAM framework and these issues should be addressed before developing an implementation plan. These include, but are not limited to:

i. Gaining senior management support;
ii. An assessment of the risks involved in not implementing a framework such as over-licensing, under-licensing, increased expenditure, security breaches, software compatibility issues, lost time and lack of technical support and product upgrades;
iii. An assessment of benefits of implementing a framework such as savings through purchasing only what is needed when it is needed, employees being able to work more efficiently, assists with the compilation of an accurate budget, ability to manage and monitor usage to link with ICT planning;
iv. The development of a business case to demonstrate the effectiveness of the framework
v. Consideration of what functions may be centralized: for example, license management, procurement and software asset registers;
vi. Long term management including continuous improvement, upgrades, compliance and audits.

Software needs to be controlled throughout its entire lifecycle, form the initial request to de-installation from a machine. The Lifecycle diagram below (Figure 2.3) outlines all the key procedures that should be established to support and maintain a successful framework.

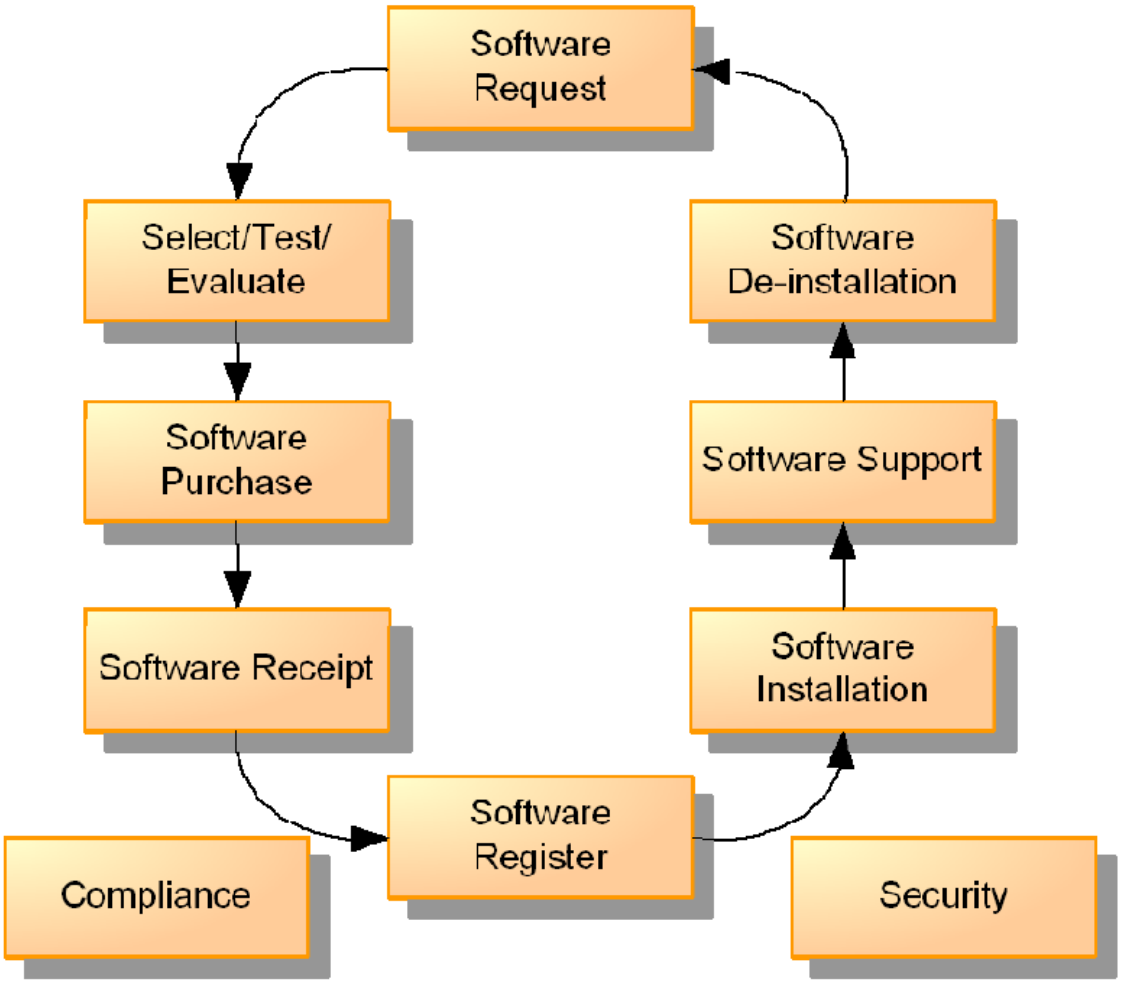

Figure 2.3: Software Life-cycle Diagram showing procedures that should be established to support and maintain a successful framework

2.2.2.2 Implementation Details

The implementation of SAM involves four stages:

i. Initiation
ii. Assessment
iii. Prioritization
iv. Implementation

Initiation:

i. Commitment and support of senior management
ii. Formulation and formalizing the SAM strategy
iii. Defining policies and initial procedures

Assessment:

i. Manual inventory of software
ii. Automatic inventory using software inventory tools
iii. Mapping of licenses

Prioritization:

i. IT strategy
ii. IT budget
iii. Usage pattern
iv. Legal/Regulatory considerations

Implementation:

i. Implement technology
ii. Implement people processes
iii. Implement processes and procedures

Below is a flowchart to practically implement the four stages:

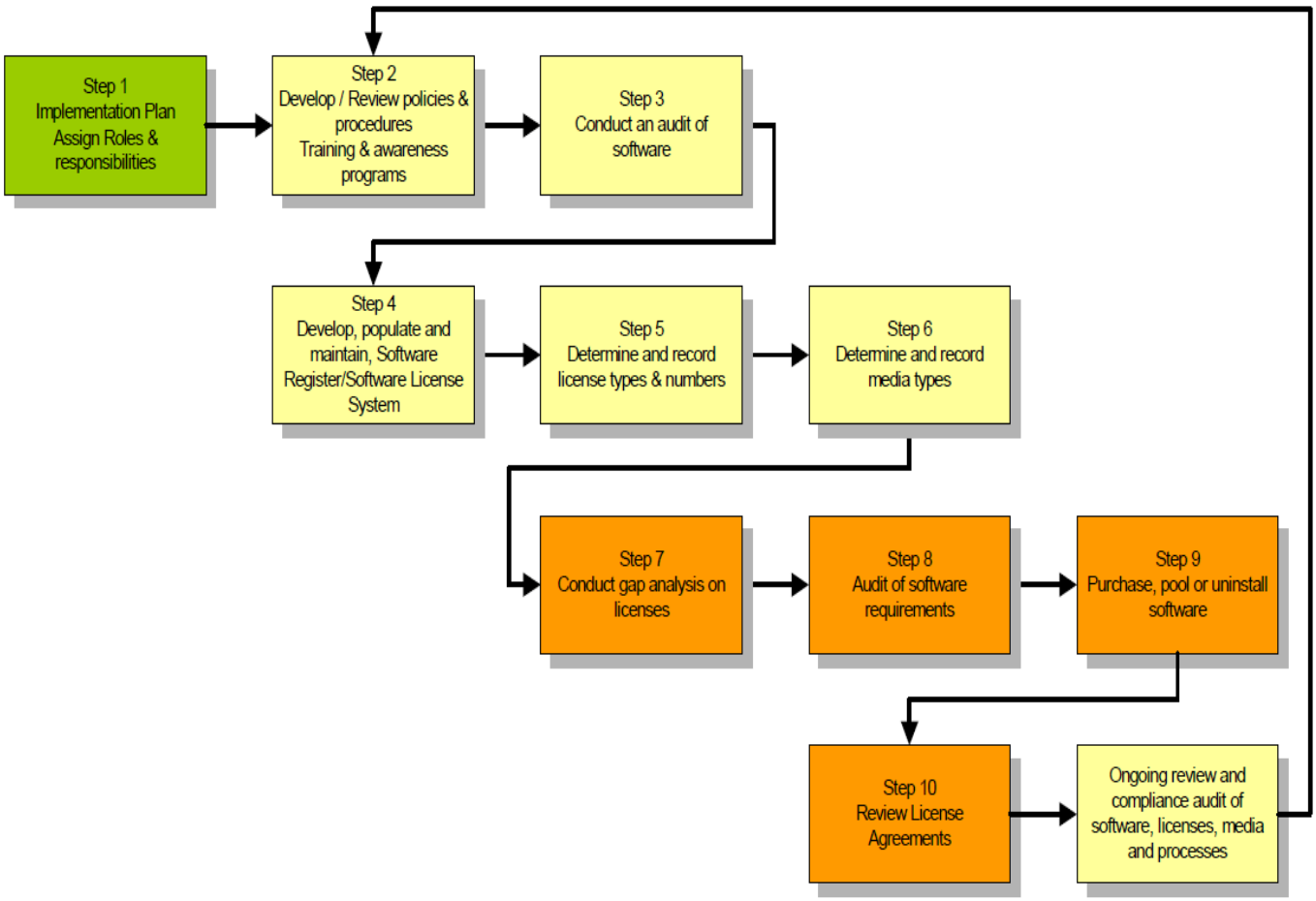

Figure 2.4: A flowchart for the implementation of SAM

2.2.2.3 Security

Security features helps to prevent theft or the unauthorized use of a system.

Security features generally available with SAM include:

i. Passwords, power-on passwords, set-up passwords;
ii. Smart cards or biometrics technology for access protection;
iii. Security locks, which can be activated remotely;
iv. Central and remote activation and deactivation of the system, its components (diskette drive, hard disk, ports and so on) or both;

v. Disabling of interfaces (serial, parallel, Universal Serial Bus [USB]) locally and remotely.

2.2.2.4 Audit and Compliance

An audit of the organization's deployed software should be undertaken to ascertain what software is installed on its computer networks and devices. The initial audit should provide an accurate report of the quantities of software products deployed within the organization.

Once the key information is collected, they should then be entered into a Software Asset Register (SAR) to assist in matching software in use with the organizations license details.

Audit

Software audit at its basic level involves the following:

i. Identification of Software Assets;
ii. Verifying that the Software Assets includes licenses, usage, and rights;
iii. Identifying gaps that may exist between what exists on the installations, and the licenses possessed, and the rights of usage;
iv. Taking action to close any gaps;
v. Recording and storing the results in a centralized location with Proof of Purchase records;
vi. Compliance to notified standards.

Compliance

An effective SAM framework would ensure that:

i. Business practices are in line with applicable laws;
ii. Adequate safeguards have been taken to cover the legal risks at appropriate software lifecycle stages (Contracting, Procurement);
iii. Policies and procedures are in tune with legal requirements;
iv. Personnel are aware of the legal risks posed by unauthorized/pirated software;
v. Regular monitoring is done to assess compliance.

Benefits of Compliance:

i. Reduced risk and liability for intentional or unintentional copyright infringements;
ii. Better software license management with reduced incidence of over or under licensing.

2.2.2.5 SAM Tools

Finding the right software licensing systems and tools can be a big challenge primarily owing to the immaturity of the software asset management tool and license management software solution market and the types of system available either of the database (simple) or workflow database (advanced) variety, and compatibility with existing network and software/hardware infrastructure of the organization. In such a scenario, it is important to have a detailed categorization of the SAM tools available.

SAM tools concentrate on five key functions:

i. inventory and asset management;
ii. security;
iii. system settings configuration, deployment and software updating;
iv. fault and performance management;
v. integration with enterprise management tools.

Various categories of tools which could be used are given in the Table 2.1

Table 2.1: Categories of Tools for SAM

Tool Category	Features Offered
Asset Inventory Tools	i. Allows management of inventory of software assets and licenses ii. Offers simple tools (Excel) to complex systems
Asset Discovery Tools	i. Identifies hardware and software installed in the company ii. Checks software on all platforms iii. Cannot work on stand-alone PCs

	iv. Does not work for new applications/internally developed applications v. One server application may be used by many users, since the tools looks at application instances
Metering Tools	i. Checks use of software on workstations ii. Can be Passive (check usage) or Active (check licenses) iii. Sends exception reports (exceeding license limits) iv. Cannot be used for stand-alone PCs
License Management Tools	i. Allows for management of license information. ii. Periodically determines a need for each type of software license used iii. Traces the license requests with license's effective use iv. Identifies unused licenses
Contract Management Tools	i. Manages all the issues related to software purchase contracts and their installation ii. Checks for terms of contract, their possible automatic renewal or expiry dates
Deployment Management Tools	i. Monitors software during the deployment stage ii. Allows installation with related authorizations
Security Tools	i. Prevents the installation of unauthorized software ii. Prevents changes in the released and authorized configurations
Procurement Tools	i. Allows for purchase of new licenses
Vendor License Management Technology	i. Uses Licensing keys i. Makes use of hardware dongles ii. Allows for online license management iii. Performs Software Metering

2.3 Managing the Communication and Collaboration Infrastructure

The communication and collaboration needs of an organization are a major infrastructure component. As with the hardware and software infrastructure, changes in the organizations' needs have taken place over the past years; for example, e-mail has become the communications medium of choice for many people. However, other forms of communication such as telephone, instant messaging, meetings, or videoconferences are more suited. One recent trend to satisfy such diverse communication and collaboration needs is the growing convergence of computing and telecommunications.

2.3.1 Convergence of Computing and Telecommunications

There is an increasing convergence of functionality of devices in the computing industry. A few years ago there were great differences between a cell phone and a Personal Digital Assistant (PDA) in terms of their capacities and robustness. However, such devices are now converging such that the boundaries between devices are becoming increasingly narrowed by their robustness and functionalities. Many devices offer a variety of different functionalities which formerly were only available on separate dedicated devices. These functionalities address differing needs of knowledge workers and consumers alike (e.g., phones, PDAs, cameras, and music players).

In addition to a convergence of capabilities of devices, there is also increasing convergence within the underlying infrastructures [2]. For example, in the past, the backbone networks for the telephone and Internet were distinct. However, currently, most voice and data traffic shares a common network infrastructure. To facilitate this convergence, the use of Internet Protocol (IP) for transporting voice, video, fax, and data traffic (also termed IP convergence), has allowed enterprises to make use of new forms of communication and collaboration (e.g., instant messaging and online whiteboard collaboration) as well as traditional forms of communication (such as phone and fax) at much lower costs. Two uses of IP for communication are voice over IP and videoconferencing over IP.

2.3.1 Voice Over IP

Voice over IP (VoIP) (or IP telephony) refers to the use of Internet technologies for placing telephone calls. Whereas just a few years ago the quality of VoIP calls was substandard, recent technological advances now allow the quality of calls to equal or even surpass the quality of traditional calls over (wired) telephone lines. In addition to the quality, VoIP offers a number of other benefits; for example, users can receive calls from almost anywhere they connect to the Internet. In other words, knowledge workers are not bound to their desk to receive VoIP calls; instead, using IP routing, their telephone number "follows" them to wherever they connect to the Internet. Organizations can also benefit from tremendous cost savings, as often as there is almost no cost incurred over and above the costs for a broadband Internet connection (VoIP software such as Skype allows home users to make free PC-to-PC calls).

2.3.2 Videoconferencing Over IP

In voice communications, IP can also be used to transmit video data. Traditionally, videoconferences were held via traditional phone lines, which were not made to handle the transfer of data needed for high-quality videoconferencing.

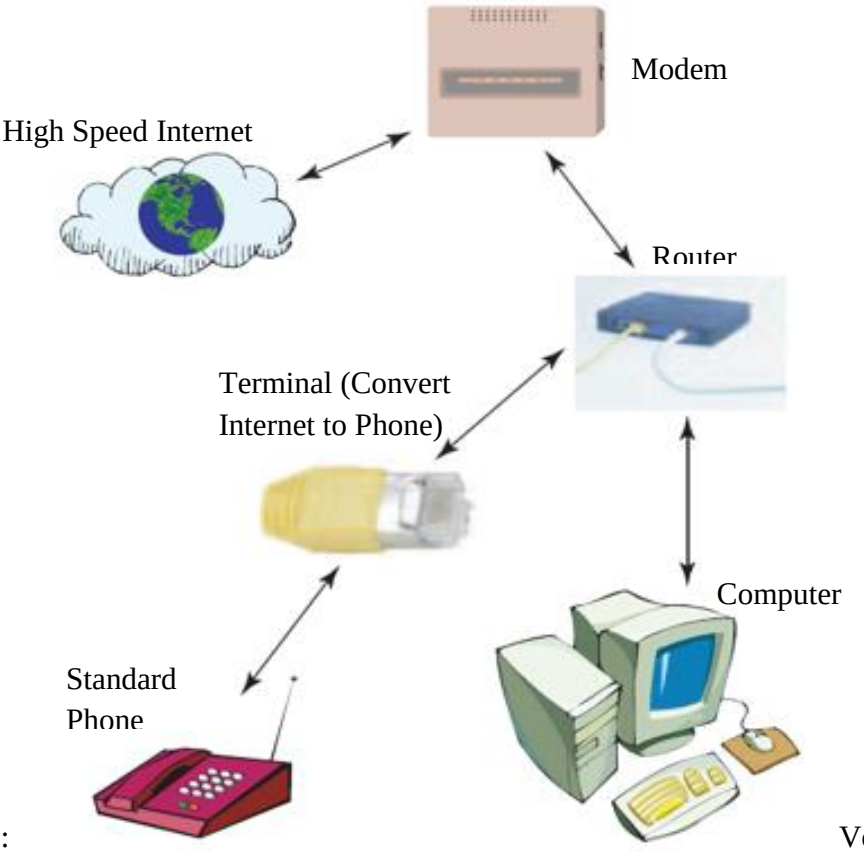

Figure 2.7: VoIP Technology Enables Organizations and Individuals to Reduce their Telecommunications Costs

Increasing Mobility Changes in communication media such as the growth of e-mail or instant messaging has led to changes in the way we communicate. In today's digital world, knowledge workers are connected, whenever and wherever they are, so that they are able to quickly respond to any communication or use any spare minute to clean up their e-mail in-box. One infrastructure component supporting this need for connectivity is the provision of a wireless infrastructure.

2.3.3 Wireless Infrastructures

There are two primary categories of wireless devices used for communications; (1) communication devices (such as cell phones) that use the public telephone infrastructure and (2) wireless devices capable of connecting to an organization's internal network. The convergence of devices and infrastructures allows the sending and receiving of e-mails using a cell phone. Thus, they no longer need a laptop computer, nor do they need to be connected to an organization's network to get useful tasks completed. Similarly, Web-enabled cell phones or PDA's, can be used to access an

organization’s networks and informational resources. However, for many applications, having access to an organization’s network can offer many advantages in terms of speed, ease of use, and so on. Thus, organizations are increasingly using wireless infrastructures.

When deciding on installing wireless infrastructures, organizations have to take great care to address issues such as the standards being used as well as the security of the network. For example, wireless networks based on the 802.11 family of standards are common. However, with the widespread use, misuse also abounds; as most current devices are equipped with the necessary hardware to connect to 802.11 networks, people often try to surf the Internet for free while on the road or even try to (illegally) access organization’s networks (also called drive-by hacking or “war driving”.

Chapter 3 – Information Security Landscape in the Telecommunication Industry

3.1 Telecommunications Network Components

The Public Switched Telephone Network (PSTN) has been the dominant type of public telecommunications (also referred to as "telecom" in this work) network worldwide, and is made up of telephone lines, fiber optic cables, microwave transmission links, communication satellites and undersea telephone cables.

The advent of cellular technologies has also led to the interconnection of the mobile phone (cellular) networks with PSTN. The PSTN was based on circuit-switched technology, which had been primarily developed for voice traffic. Technologies developed for data transmission like PSDN, ISDN, Dial-up, DSL and others also leverage the existing PSTN infrastructure.

Due to the growing demand for data and video services and the limitations of the circuit-switched technology, telecom operators find it economically prohibitive to expand their circuit-switched networks to meet demand. This has led to a gradual move towards the adoption of packet-based switching technology.

Newer 2G and 3G mobile phone systems like GPRS, EDGE and HSPA that are designed for data transmissions are also based on packet-based switching technology.

The term, Next Generation Network (NGN), is generally used to refer to these packet-based networks that transport all information and services – data, voice and media like videos. NGNs are most commonly based on the Internet Protocol (IP). NGN is expected to reshape the current structure of the telecommunication system and access to the Internet.

Today's telecom networks are a combination of several technologies – PSTN, 2G, 3G – that have evolved over a period of time. Generally speaking, the current telecom network comprises the following parts:

i. Access Network – This is the part of the network that connects the telecommunication equipment – fixed or mobile – to the core network for provision of services. This includes the local loop (telephone cables/fiber optic) of the fixed networks and the radio links in a mobile network, the radio towers, base stations and controllers;

ii. Core Network – This consists of the network elements responsible for service delivery and setting up of the end-to-end connection and handovers, and may be classified into circuit-switched and packet-switched domains. The core network includes components such as switches, the Mobile Switching Centre (MSC), the Host Location Register (HLR), the Visitor Location Register, and the Authentication Centre;

iii. Application and Management Network – This consists of end-user application servers, and systems and services that support the operation, administration and maintenance functions of the network. Internal Network – This is the telecom operator's internal network. This includes systems used by the operator's employees;

iv. External Network – This is the externally visible network, typically deployed in the De-Militarized Zone (DMZ). This includes the Web servers, application servers and mail servers that are hosted by the telecom operator.

3.2 Need for Security Management in Telecommunication Networks

The import of telecom equipment from other countries that are antagonistic to our national strategic interests may lead to supply chain contamination by means of embedded logic bombs and malware. The dependence on telecommunication networks and the critical role that they play in our economic growth has led to government regulations in the telecom industry through NCC, which include requirements for ensuring the security of the telecom equipment and networks.

The interconnection of the PSTN networks of fixed and mobile phone systems and the next generation network has increased the attack surface of the telecom networks. The wide range of end-user devices that can now connect to the telecom networks has added to the complexity of the networks, thereby increasing the risks and vulnerabilities as well.

Several international standard development organizations like ITU, ISO/IEC, 3GPP, 3GPP2 and ETSI have prescribed standards that are applicable to telecom networks. Some of the most prominent standards that include requirements/guidelines for the security of telecom networks are listed in Table 3.1 below. Also, there must be legislations and regulations that the telecom operators must comply with, which may require the adoption of specific security standards.

Telecom operators should adopt a robust, managed security programme to ensure that their networks are protected against malicious attacks, both external and internal, while also ensuring compliance to the regulatory environment. This requires a holistic approach to implementing security measures, based on globally accepted security standards and best practices.

Table 3.1: Security standards for the telecommunication industry

Organization	**Standard/ Specifications**	**Description**
ISO/IEC	27001:2005	Specifies requirements for an information Security Management System.
	27002:2005	Specifies a code of practice for information security management based on ISO 27001.
	27011: 2008	ISO 27002 tailored specifically for applications to telecommunications organizations, developed as a joint effort with ITU-T.
	15408 (The Common Criteria)	A common set of security requirements for evaluation of computer security products and systems, including telecom network components
3GPP	33-Series	Provides specifications for security standards for GSM (including GPRS and EDGE), W-CDMA and LTE (including advanced LTE) mobile systems.
3GPP2	S.S0086 and others	Provides specifications for security standards for GSM (including advanced LTE) mobile systems.
ITU-T	E.408	Provides an overview of security requirements, threat identification frameworks and guidelines for risk mitigation.

	E.409	Incident organization and security incident handling.
	X.805	Security architecture for systems providing end-to-end communications.
	X.1051	ISMS guidelines for telecommunications, which is also referred to as ISO 27011:2008.

3.3 Vulnerability of Telecommunications Information Infrastructures

With a large number of vulnerabilities and an increasing number of attacks exploiting them being reported across technology platforms, it is becoming difficult to ensure that the critical elements of a telecommunications network are not vulnerable to these attacks [3].

Vulnerability assessment can be used to:

i. Identify vulnerabilities;
ii. Report and assess the vulnerability and its overall consequence;
iii. Recommend mitigation strategies (safeguards or workarounds)
iv. Ensure that organizational security policies are met by auditing the system configurations;
v. Provide input into the incident handling process.

A five-phase approach to vulnerability assessment is explained below:

3.3.1 Fuzz Testing

The fuzz testing is a software testing technique used to discover coding errors in networks. This schemes inputs massive amount of random data called fuzz to the system in an attempt to crash it. The fuzz testing test for reliability and how vulnerable a system is. While vulnerability assessments can help identify and mitigate known vulnerabilities, it cannot be used to protect against exploitation of unknown vulnerabilities that are likely in complex networks like telecom networks.

A methodology that is now being used to address these unknown vulnerabilities is Fuzz Testing, which is a form of attack simulation where abnormal inputs are used to trigger vulnerabilities. One approach is model-based fuzzing, which uses protocol specifications to target tests at protocol areas most susceptible to vulnerabilities. Another approach, traffic capture fuzzing, uses traffic captures to create the fuzzers used for testing.

3.3.2 Radio Access Path Security Testing

An aspect of security testing that is unique to a telecommunications network is the testing of the radio access network. By and large, the approach to testing radio nodes is based on custom test scenarios that are in turn based on the characteristics of individual radio nodes. The primary tools in use are a modified Mobile Station (MS) and the custom radio traffic injection scripts. In order to protect the privacy of subscribers' information during the security tests, it is recommended that a second test device (an unmodified MS) is used as the primary target for the attacks where possible. The tests should be designed to prevent legitimate subscribers from associating with the modified equipment being used, and also to ensure that there is no service disruption.

3.3.3 Penetration Testing

Penetration testing supplements the vulnerability assessment activities by taking "the last step" and actually exploiting these vulnerabilities to compromise and gain access to the target systems, and not just report potential vulnerabilities. Penetration testing provides the "hacker's" perspective inside and outside the network perimeter. Security testing specialists attempt to infiltrate the client's network, systems and applications using not only common technologies and techniques, but also specialized tools and some unexpected methods, such as combined techniques ("multi-vector" attacks). The result is a detailed report identifying key vulnerabilities and suggested protection tactics – an action plan to improve the organization's security posture.

3.3.4 Conducting Security Testing

Maintaining a consistent security posture across an organization's network in the face of the ever changing nature of IT security is a complex and time consuming task. Periodic security testing plays a vital role in assessing and enhancing the security of networks.

Telecommunication networks are likely to have a heterogeneous mix of equipment from various suppliers. A highly credible, trusted third party certification programme must be in place to conduct an assessment to identify and evaluate security weaknesses and vulnerabilities contained in equipment software, firmware and hardware implementations. Certification of the supplier products against the Common Criteria Specifications (ISO 15408) ensures this at the component level.

3.4 Conducting Network Security Audits

Network security audits can be conducted to discover, assess, test and report the existing security infrastructure implementations. Network security audits should be based on internationally accepted standards and frameworks like ISO 27001 and COBIT.

Figure 3.1 illustrates a methodology for network security audits, consisting of four distinct phases:

i. Scope and Plan - This involves defining the audit objective, determining the audit scope, understanding the business risks and defining the project plan;
ii. Information Gathering – This is gathering the information about the security policies, processes and security controls that have been implemented, and also the industry best practices, standards and guidelines that are applicable;
iii. Assessment – This is performed to discover the vulnerabilities existing in the system. The impact of any discovered vulnerability on the telecom operator business is used to determine a risk rating;
iv. Documentation – This includes the analysis and reporting of data and test results. The report documents the results and findings of the security assessment and includes a discussion of the risk analysis arising from the assessment, implications to the telecom operator's systems and networks and recommendations for improving the security position of the operator's applications, systems and networks;

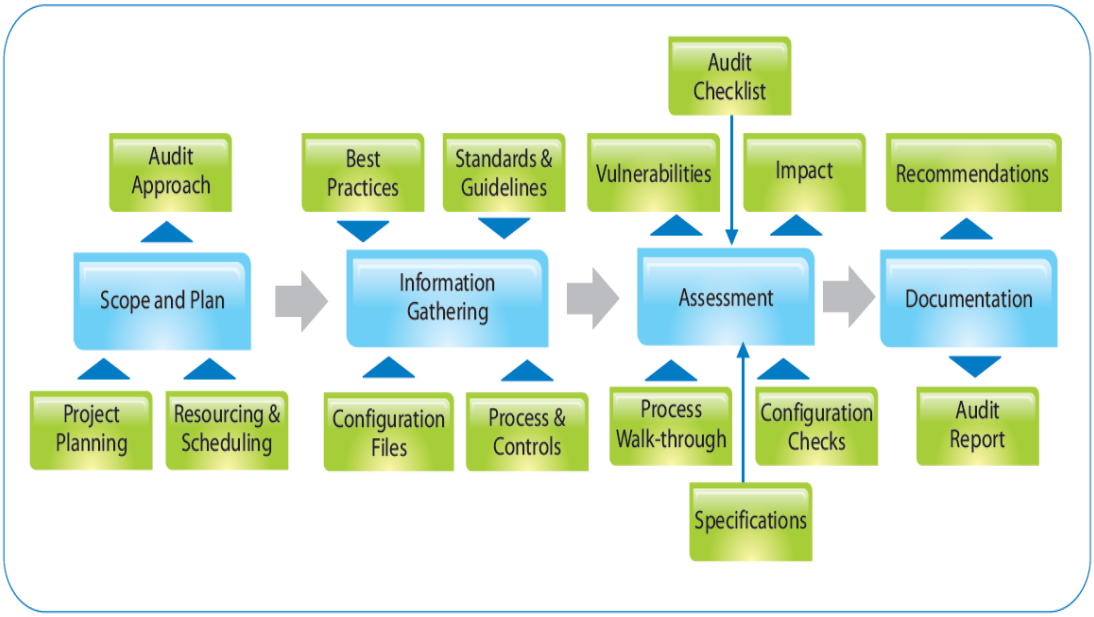

Figure 3.1: Security Audit Methodology

3.5 Threats and Risks to core National Telecommunication Infrastructure

The structure and functioning of circuit-switched PSTN networks, traditionally controlled by the telecom operators, ensured fewer possibilities for misuse of the network, as compared to a packet-switched network based on an open protocol like the Internet Protocol (IP). However, the PSTN networks are increasingly being controlled and are dependent on software and on the operations networks. As a result, users now have greater access to functions that were previously restricted to telecom employees. This exposes the network to intruders and increases the potential for attacks caused by virus, worms and malicious software.

GSM, which is a widely used mobile phone system, implements several security mechanisms designed to protect confidentiality over radio interfaces, subscriber authentication, subscriber anonymity to external parties, and prevent the use of stolen terminals. However, a speech call made between two GSM operator networks or between a GSM phone and a fixed phone traverses the fixed network, and is subject to the same security considerations in speech and signaling as for a fixed network. CDMA mobile networks are also exposed to the same threats and attack vectors as a GSM network.

Packet-based switching technology used in Next Generation Networks is usually implemented through the use of the Internet Protocol (IP) suite. The IP was based on open standards and not originally designed for security implementations. The weaknesses in the IP have been exploited since long, and add to the risks of adopting an IP-based network.

Both the traditional circuit-switched networks and the packet-based next generation networks are exposed to different threats and attacks – both from external and internal sources – that target the various parts of the telecommunications network. These attacks may be targeted at any part of the telecom network, including the radio path of the access network. Attacks on one telecom operator's network could also spread to multiple networks over the interconnection interfaces. Some of the threats to the telecom networks are listed in Table 3.2 below.

Table 3.2: Threats to Telecom Networks

Threat	**Likely Consequences**
Unauthorized physical access to switching infrastructure, underground and local loop cable infrastructure and other critical telecom network equipment, for example, AuC, HLR and VLR.	Tempering, destruction or theft of information and equipment. Illegal tapping and interception of the network traffic.
Interception of voice traffic or signaling system in PSTN networks due to absence of encryption for speech channels and inadequate authentication, integrity and confidentiality for the messages transmitted over the signaling system (which is based on the ITU-T SS& specification).	Unauthorized access to telecom network traffic.

Threat	Likely Consequences
Use of modified mobile stations to exploit weaknesses in the authentication of messages received over the radio interface.	Spoofing of user de-registration and location update requests, leading to unreliable service/disruption.
Use of modified base stations to entice users to attach to it.	Denial of service, interception of traffic.
Misuse of the lawful interception mechanism.	Illegal tapping/interception of telecom network traffic.
Compromise of the AuC or SIM used for storing the shared secret for the challenge-response mechanism.	Identity theft (intruders masquerading as legitimate users).
Deployment of malicious applications on devices with always-on capabilities like smart phones and tablets.	Use of these compromised devices target the operators' network (for example, by setting up botnets to carry out DDoS attacks).
Intrusions into the operations networks.	Unauthorized changes to the user's service profiles, billing and routing systems, resulting in toll fraud and unreliable service.
Compromises of network databases containing customer information.	Unauthorized access to personal and confidential data.
Masquerading as authorized users, by gaining access to their credentials by means of malware, hacking tools, social engineering tools or other means.	Gain unauthorized access or greater privileges to the network systems, which can be used to launch other attacks.

Threat	Likely Consequences
Traffic analysis – observing the calling and called numbers, and the frequency and length of the calls.	Inference of activities that can be used against.
Social engineering attacks on operator employees.	Unauthorized access to confidential information.

Consequences for operators who fail to adequately protect their networks include:

i. Financial loss;
ii. Loss of reputation for the operators in the industry;
iii. Loss of customer confidence;
iv. Legal action and fines from regulatory bodies for failure to provide secure services.

Apart from these, the weaknesses in the telecommunication networks may also be exploited by anti-national and terrorist organizations for their own benefit by intercepting communications, causing denial of service during terror strikes and also using it as a platform to launch attacks.

3.5.1 Telecom Infrastructure risk management process

A multi-pronged approach to security should be adopted by telecom operators to address the current and future security risks. Industry-recognized standards, best practices and technologies must be adopted to build a robust security programme. In addition, all applicable legal and regulatory requirements should also be considered.

3.5.1.1 Adopting a Security Framework

Organizations develop and implement security policies and procedures to address the security requirements for their environment [4]. However, to be effective, these policies and procedures should be tightly coupled, and supported by industry-accepted guidelines, standards and best

practices. There also should be a risk-based approach while developing these policies to ensure that the security measures are adequate to the address the perceived business risks.

Several IT Frameworks available today, like COSO, COBIT, ITIL, ISO27001 and others can be adopted to formulate a security programme. The ISO 27001:2005 standard is one of the most widely accepted security standards across industries. This provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). For the telecom industry, this is further supported by ISO 27011:2008, which provides guidelines on information security management for telecommunication networks (jointly developed along with ITU-T).

The ISO 27001 standard is based on the Plan-Do-Check-Act (PDCA) model, which is applied to all ISMS processes, as illustrated in Figure 3.2 below. This PDCA model ensures that there is a continued focus on the security programme, and that it is not a one-time activity.

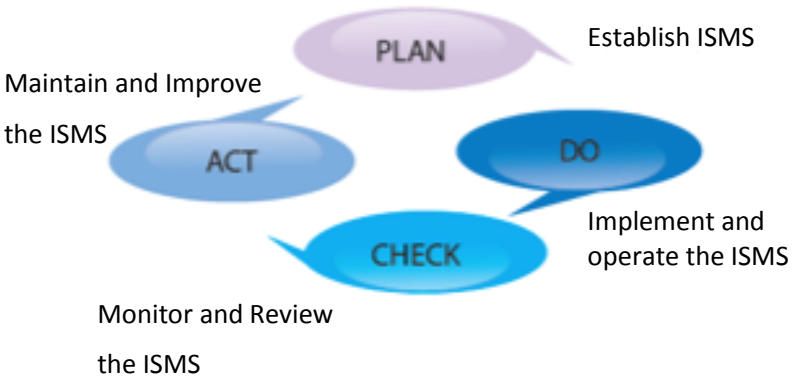

Figure 3.2: The PDCA Model

The ISO standard spans 11 security domains, and prescribes a total of 133 controls across these domains. Among others, this covers areas of Security Governance, Physical Security, System and Network Security, Business Continuity, Incident Management and Compliance, all of which are critical for the security of the telecommunication networks.

Managing telecommunication security without cognizance of risk exposure creates the possibility of inappropriate or inadequate security measures, the consequences of which include resource wastage and unchecked exposure to harm. So, risk assessments play a vital role in any information

security programme, ensuring that resources are being allocated in the most effective way to support the business. The ISMS framework requires that controls be identified on the basis of a thorough risk assessment, and documented as the Statement of Applicability (SoA). Figure 3.3 illustrates a possible risk management process for telecom networks.

The ISMS framework also provides flexibility in adopting controls so as to meet the regulatory and legal requirements of the telecom operator. Post-implementation, the ISMS is reviewed on a periodic basis by means of internal audits to check the effectiveness of the implementation. The standard also requires organizations to continuously improve their ISMS based on inputs from monitoring and maintenance activities, internal audits, reviews and industry best practices.

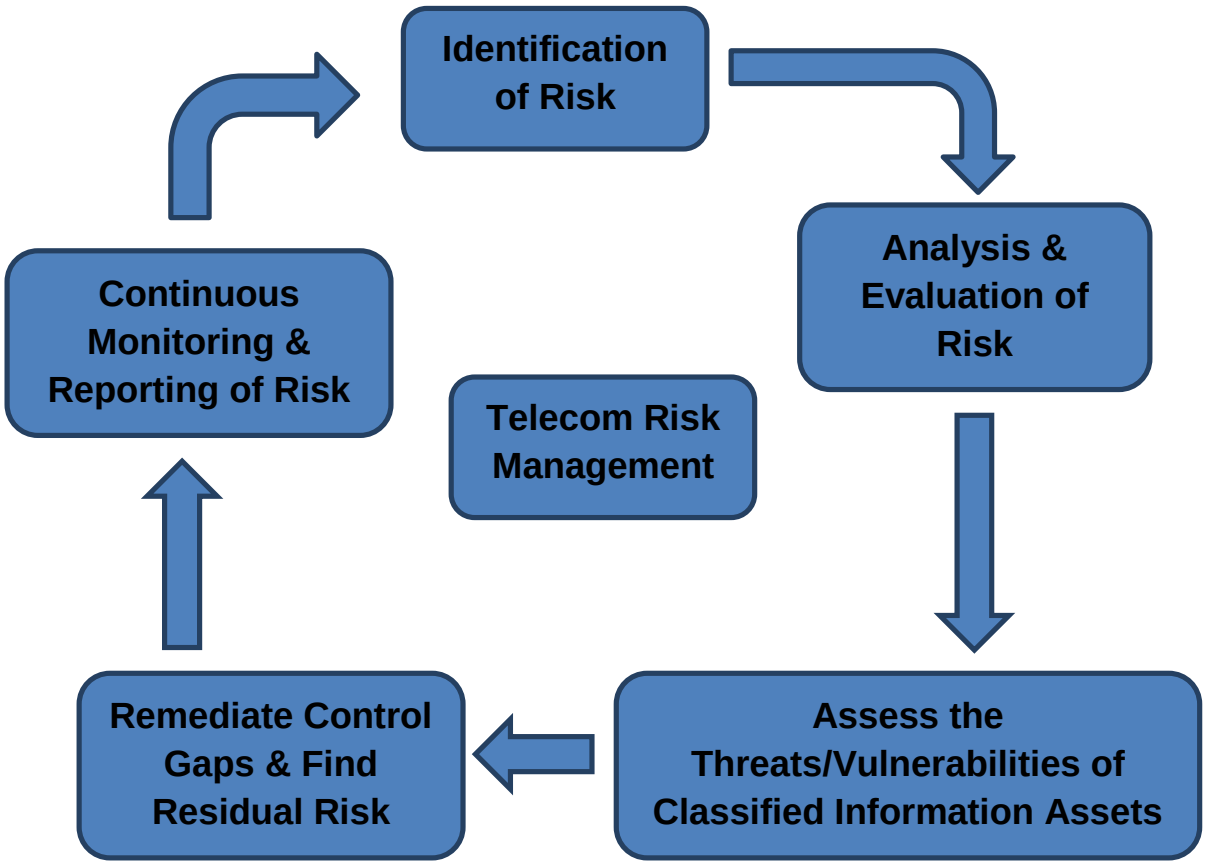

Figure 3.3: Telecommunication Risk Management Process

Organizations' can also choose to undertake ISO 27001 certification based on assessments by external independent certified bodies. The certification will not only validate the implementation on a periodic basis, but also underscore management's commitment towards a strong security programme.

3.6 Implementing a Security Infrastructure

The implementation of ISMS policies and processes should be supported by a security infrastructure that includes multiple security layers. This "Defense in Depth" approach as depicted in Figure 3.4 below ensures that the compromise of one security layer alone does not expose the network to attacks.

Some of the security measures that can be deployed across the various layers are:

i. Interference and tamper-proof cabling infrastructure;
ii. Security guards and CCTV monitoring for operator premise perimeters;
iii. Physical access control mechanisms like smartcard and biometric readers;
iv. Firewalls at the network perimeter and DMZ for publicly accessible systems
v. Host- and network-based Intrusion Detection/Protection Systems;
vi. Security Information and Event Management (SIEM) systems to handle security events and logs generated by multiple systems;
vii. Malware management by deployment of antivirus, antispyware technologies on internal systems and mail servers;
viii. Secure application development practices;
ix. Security testing of the telecom equipment, perimeters, critical network components and applications;
x. Encryption and data masking techniques for both data at rest and transit;
xi. Security awareness.

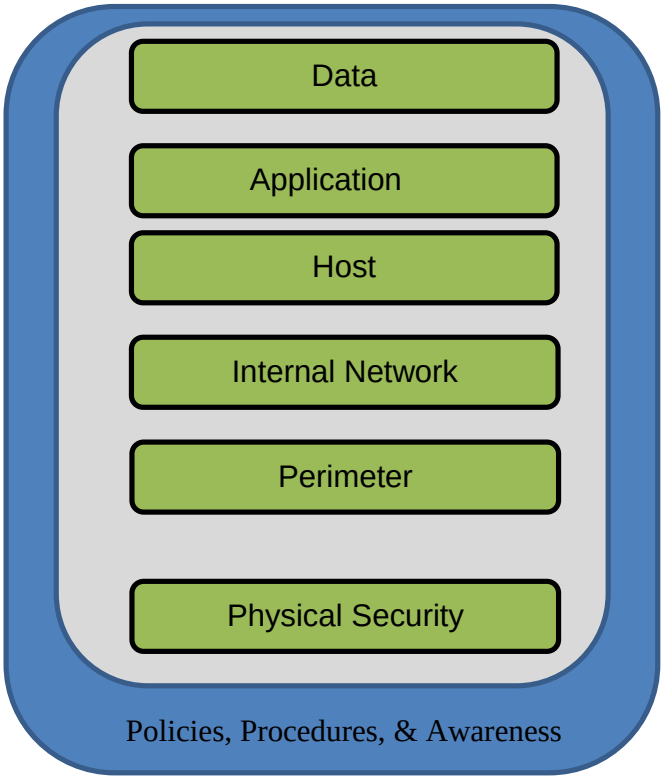

Figure 3.4: Defense in Depth

Chapter 4 - Best Practices and Principles in the Information Infrastructure Security Management

4.1 Security of Telecom Network Infrastructures

Conceptually speaking, TSPs' networks are composed of three different layers or "planes" with different types of traffic associated with each plane. The management plane is used for communications-related to network traffic management and operations. The control plane is used for routing and signaling of network traffic. The user plane or data plane carries the network users' traffic (data communications).

Each of these planes interconnects various systems or devices and allows them to communicate. Because of the different nature of the communications across each plane, the communications of one plane are separated from those of the other planes.

4.1.1 Network Segmentation

Objective:

To ensure that service provider networks work securely and that traffic from one plane does not affect other planes, it is important to implement basic architectural features in the TSPs' networks.

The controls listed below pertain to each TSP's core network. They are not intended to be implemented on every single network component, as this may not be feasible in all network types and architectures.

Controls:

The TSPs should have the capability to:

1. Ensure that the management, control and user planes are, at a minimum, logically separated and preferably physically separated as well;
2. Provide diagrams demonstrating plane separation within their network infrastructures.

4.1.2 Management Plane

Objective:

The network management plane is the set of network segments over which both the network and associated infrastructure components are managed. This plane includes remote access to systems, as well as management functions such as backup, patch delivery and log extraction. The management plane also carries provisioning traffic, and is the network interface over which communications with back-end billing and customer care systems take place.

If the management plane is not properly protected, then the network components connected to the management plane will be compromised and exposed to attacks. Therefore, it is essential to protect the management plane components.

Controls:

The TSPs should have the capability to:

1. Isolate management functions;
2. Restrict access, allowing access to only known and approved hosts and services;
3. Filter management access to devices;
4. Use secure management protocols whenever possible;
5. Log critical events for network elements;
6. Identify the sources of malicious events.

4.1.3 Control Plane

Objective:

The Control Plane is defined as the networks over which call setup is done and management signaling is passed. These networks must be protected in order to ensure proper operation of the TSP's network.

Controls:

The TSPs should have the capability to:

1. Validate all signaling partners;
2. Validate all external input from signaling partners;
3. Drop/filter signaling outside of defined and allowed adjacencies;
4. Prevent signaling points from being addressable from the either the Data Plane or being accessible from outside of the Control Plane layer;
5. Maintain separation between the data plane and the control plane traffic;
6. Implement mechanisms to protect wireless control channels and signaling traffic;
7. Implement mechanisms to validate the end devices on their networks to ensure that no unauthorized devices are able to connect;
8. Implement egress filtering controls.

4.1.4 Data Plane

Objective:

The data plane is the routing path by which network communications arrive to the end customer. Efforts must be taken to prevent this path from delivering malicious data to the end-user and from being used as an attack path on Canadian critical infrastructure.

Controls:

The TSPs should have the capability to:

1. Validate the integrity of external traffic entering their network wherever possible;
2. Prevent traffic from spoofed (false originator) devices or sources from entering their network;
3. Prevent malicious or inappropriate traffic from entering their network. These measures include protocol, address or volume filters;
4. Prevent volumetric attacks (i.e. attacks that attempt to exceed network or device bandwidth) from affecting their infrastructure;
5. Ensure that management resources and infrastructure networks cannot be targeted by data plane traffic;

6. Use traffic restrictions based on a "blacklist" approach, where all traffic is allowed by default, but the TSP has the ability to block (or blacklist) malicious or inappropriate traffic as necessary;
7. Track malicious traffic to the originating source on their network, or to the point of entry to their network;
8. Correlate traffic sourced on their network to individual customers;
9. Ensure the integrity of traffic leaving their networks;
10. Implement mechanisms to prevent traffic with invalid characteristics;
11. Behave as responsible network citizens and take steps to avoid harm to other networks;
12. Respond to reasonable external complaints from their networks about cases of abuse that have not been prevented.

4.2 Security Controls for Core Equipment

TSP networks are made up of a variety of components, including telephone switches, home location registers, voicemail platforms and value-added service platforms, which provide services to more traditional components such as routers, switches, and other systems-based information technology (IT) components, as well as core IT services, e.g. Domain Name System (DNS) resolution, mail services via Simple Mail Transfer Protocol (SMTP), and network time syncing via Network Time Protocol (NTP).

It is necessary to ensure that these systems be designed and configured in a manner which minimizes the exposure to threat exploitation.

4.2.1 System and Component Hardening

Objective:

TSPs' networks and their components can only function securely if all components are appropriately protected. The following recommended controls facilitate appropriate configuration of a TSP's infrastructure components. This list is not intended as an exhaustive or mandatory list given that necessary controls are to be based on the individual components.

Controls:

Basic device hardening should be employed according to vendor guides and industry-recognized best practices, which are not listed in full here but include the following.

The TSPs should have the capability to:

1. Refer to system and device hardening guides published by reputable organizations for more detailed recommendations on the hardening of various types of systems and devices;
2. Choose an industry-recognized hardening standard, or develop in-house standards that meet the same level of effectiveness as recognized public standards and mandate the use of these standards within their organizations;
3. Mandate hardening requirements for third party service providers through contractual obligations relating to the provision and maintenance of services.

4.2.2 Domain Name System *(DNS)* Hardening and Security

Objective:

The DNS is a fundamental control protocol in Internet Protocol (IP) networks that is essential for connectivity to the Internet. DNS servers provided by TSPs must be secure and resilient to security events and must provide accurate data.

Controls:

The TSPs should have the capability to:

1. Ensure that they are deploying, configuring, and securing DNS infrastructure and services according to industry-recognized standards;
2. Ensure that they protect their own domain, as well as all other domains for which they are responsible;
3. As an authoritative source, ensure that they provide valid contact information;
4. Monitor DNS activity to detect and respond to abuse that could affect customers or other service providers;
5. Respond to abuse queries in a timely fashion;

6. Ensure that authoritative and resolving DNS servers are geographically diverse.

4.3 Security Testing

4.3.1 Vulnerability Assessments

Objective:

TSP environments consist of many interconnected components that make up the management, control, and data network planes. Equipment and services must be tested in a lab prior to deployment in order to ensure that they meet the vendor security specifications and to validate that the security configuration applied by the TSP does not compromise network security.

Controls:

The TSPs should have the capability to:

1. Include security testing in all system development test plans;
2. Test devices against the hardening security standards adopted;
3. Perform security testing prior to systems being granted approval to move into production;
4. Ensure that network planes are secure by conducting regular risk assessments on each plane to identify and respond to unacceptable risks.

4.3.2 Ongoing Compliance Monitoring and Audit

Objective:

After a service or technology is implemented, it must be maintained in a secure fashion. At the core of this is a program of compliance monitoring and audits to ensure that security standards have not degraded over time in the production environment, and that systems adapt to new security standards as they are updated.

Controls:

The TSPs should have the capability to:

1. Establish a Vulnerability Management Program (VMP) containing processes and tools to scan production systems and network equipment for vulnerabilities;
2. Document processes and procedures for addressing discovered vulnerabilities;
3. Detect when new equipment has been added to networks.

4.4 Change Control Procedures

Objective:

A comprehensive Change Management Program will help to ensure that changes to production environments are managed to meet business needs. Good change management will ensure that changes are assessed for risk, approved and implemented in a controlled, consistent manner and that only authorized changes enter into production.

Controls:

The TSPs should have the capability to:

iii. Maintain a Change Management Program to ensure that changes to production environments and systems are introduced in a controlled manner to help to mitigate risk and ensure that all changes comply with security requirements;

iv. Ensure that the Change Management Program includes a Change Advisory Board (CAB) that has representatives from all impacted areas to ensure that changes are properly reviewed;

v. Ensure that changes are approved by management with direct responsibility for the operations of the components being changed;

vi. Ensure that the change control procedures define the testing that is required to validate changes;

vii. Ensure that post-change testing is conducted to validate the integrity of all pre-change security controls.

4.5 Network Security Monitoring and Detection Capabilities

In addition to securing the TSPs' infrastructure, it is also necessary to perform security monitoring and incident detection within the environment; even the most secure environment is still susceptible to incidents and attacks.

4.5.1 Requirements for TSPs to Monitor Network Infrastructure

Objective:

Service providers should be able to monitor network traffic in order to detect malicious or potentially malicious behaviors on their networks. TSPs should also work toward having the capability to search through cyber security-relevant event logs and monitoring systems for trending in order to detect anomalous behaviors for further investigation.

Controls:

The TSPs should have the capability to:

1. Monitor the infrastructure used for the provision of key services to customers;
2. Monitor critical assets from both external and internal threats;
3. Operate a security information and event management system that collects and correlates information from a variety of systems and devices;
4. Monitor multiple connections;
5. Provide volumetric monitoring of traffic;
6. Monitor for ad hoc threat indicators provided from public, private, and third party sources where feasible;
7. Monitor flows within their networks to detect anomalies;
8. Define their response plans for traffic identified as suspicious by their monitoring activities.

4.5.2 Types of Traffic to Monitor

4.5.2.1 Malware

Objective:

Malware traffic cannot always be detected on the computer that is infected because malware writers take steps to avoid detection. Mechanisms such as separate TCP/IP stacks or kernel hooks that hide malware applications in listings can defeat computer detection. There are times when a TSP can detect the signs of malware but the customer cannot. If, in the course of its monitoring duties, a TSP becomes aware of a customer who is affected by malware in this manner, the TSP should take immediate steps to inform the customer.

TSPs are not intended to be a replacement for anti-virus (AV) or other computer security tools that are normally loaded on customers' systems. TSPs are expected to be able to deal with malware traffic if it becomes excessive or is reported to them by a reputable third party.

Controls:

The TSPs should have the capability to:

1. Identify the source of malicious traffic on their network;
2. Respond to valid reports of malicious activity on their networks;
3. Monitor for different types of malicious traffic;
4. Detect malware by signature and volume characteristics.

4.5.2.2 Network Service Abuse

Objective:

Compromised customer systems may not individually pose a threat to the reliability or performance of critical network services and protocols such as DNS or Dynamic Host Configuration Protocol (DHCP); however, left unchecked in large numbers, these systems can negatively impact the service of other customers and/or inflate capital costs (e.g. through higher TSP capacity provisioning costs).

Controls:

The TSPs should have the capability to:

1. Monitor traffic flows from internal customers to the provider's critical infrastructure-related network services;
2. Refer detected anomalies to Incident Response procedures to address the issue.

4.5.2.3 Message Abuse

Objective:

Abuse of email messaging services can often result in services being blocked externally and may result in loss of reputation. It is, therefore, important for responsible TSPs to monitor email services in order to ensure that the services are being used as intended.

Controls:

The TSPs should have the capability to:

1. Monitor for misuse, including specific monitoring of outbound message volumes and high numbers of intended message recipients, if they are providing email services;
2. Ensure that customers that exceed message volume and high-number thresholds are identified and follow-up action is taken;
3. Ensure that third party service agreements for outsourced message services include controls and processes for monitoring and responding to message abuse;

4.5.2.4 Outbound Spam

Objective:

Email-related services should be monitored for outbound spam messages from individual customer IP addresses. The indicators used for detection can be drawn from trusted third parties, such as Sender base, which tracks counts on outbound spam messaging.

Controls:

The TSPs should have the capability to:

1. Monitor for high volumes of spam-related traffic coming from individual customer IP addresses in order to notify those customers of a potential infection, or take other actions to stop such traffic.

4.6 Security Incident Response Capabilities

4.6.1 TSPs' Incident Response Capabilities

Objective:

To ensure that TSPs have the capacity to deal with security incidents, both internal and external to the service provider, the TSPs need to have defined and repeatable processes. The TSP must also have a team of individuals who are capable of handling security incidents as they occur. This team could be a highly distributed functional team or a centralized security incident response team (e.g. security operations center).

Controls:

The TSPs should have the capability to:

1. Manage cyber security incidents via a defined, tested, and repeatable program;
2. Implement a governance structure for their cyber security incident management program;
3. Respond to operational security incidents occurring during normal and off-hour times;
4. Engage with defined contacts for reporting abusive behavior, which is monitored and responded to appropriately.

4.6.2 Response Procedures for Issues Affecting Customers

4.6.2.1 Incidents Involving Customers' Information Technology (IT) or Home Computers

Objective:

There will be times when a TSP becomes aware of a security breach or malware that is affecting a customer's computer, whether as a victim of an attack or as the perpetrator of an attack (either knowingly or unknowingly). When a TSP becomes aware of such a breach in a customer's system or data, the TSP should notify all affected customers or partners immediately in order to protect the customer from further damage.

Additionally, TSPs should, where technically feasible, contain the impact of the attack by whatever means possible. This could include remediating and mitigating the malicious traffic or suspending the customer until such time as the threat is remediated.

Controls:

The TSPs should have the capability to:

1. Define their process for customer notifications;
2. Track customer notifications, including methods and frequency of notifications issued;
3. Validate third party incident information before acting on it;
4. Protect the information source in customer notifications when the source is a confidential third party;
5. Identify and respond to known breaches or potential loss situations affecting customers.

4.6.2.2 Breach of Customer Information

Objective:

When a TSP becomes aware of an incident that has caused a breach of customer's personal information or information regarding the network configuration, the TSP should notify all affected customers or partners immediately in order to protect those customers and partners from subsequent fraud.

Controls:

The TSPs should have the capability to:

1. Define notification procedures that can be implemented in a short period of time (a maximum of two days) in order to protect their customers and partners;
2. Document and communicate internally who is responsible for contact with customers, partners and the general public;
3. Establish a trusted prearranged method for communicating incident or breach of information with customers;
4. Establish security mechanisms to ensure that customers and partners can authenticate communications coming from the TSP;

4.6.3 Remediation and Mitigation of Malicious or Inappropriate Traffic

Objective:

There are certain circumstances where some types of traffic might be damaging to customers and/or the TSP. For example, a Denial of Service (DoS) attack against one customer could impact the service provider or other customers. Some types of malware can cause excessive network traffic and have a similar effect as a Distributed Denial of Service (DDoS) attack. In order to protect the TSP's infrastructure, its customers, and the Canadian telecommunications critical infrastructure, TSPs need to have the capacity to filter or to drop traffic that is causing significant damage to others.

Note:

This section concerns traffic that the TSP deems to be malicious or harmful to its network, and is intended for the mitigation and remediation of such traffic. It does not oblige TSPs to block content that a third party finds objectionable or that harms a third party, but merely states the controls that should be in place, should the TSP decide to take action.

Controls:

The TSPs should have the capability to:

1. Determine what categories of malicious traffic that they would be willing to throttle, filter, or block, and ensure that they have the capability to take these actions;
2. Identify the conditions under which throttle, filter, or blocking actions will be taken on malicious traffic, and which of their networks these actions will protect;
3. Consider traffic filtering and blocking as a last resort when protecting critical networks to prevent the possibility of affecting legitimate traffic;
4. Identify the authoritative intelligence sources on malicious traffic;
5. Issue a publicly stated policy on malicious traffic remediation and mitigation;
6. State their policies on malicious traffic remediation and mitigation within their customer Service Level Agreements (SLAs).

4.7 Information Sharing and Reporting

Information sharing and reporting are crucial components of protecting critical infrastructure. The extent, the breadth, and the complexity of today's threats are such that cooperation among TSPs is necessary to protect the Canadian critical infrastructure.

In addition to direct information sharing with other Canadian TSPs and government, TSPs should participate in third party working groups and trust groups relevant to their business needs and security responsibilities. These groups offer collaboration and information-sharing opportunities that significantly enhance an organization's ability to prepare and to respond to cyber security events.

Examples of some currently established working groups and trust groups include:

1. Messaging Anti-Abuse Working Group (MAAWG);
2. Forum for Incident Response and Security Teams (FIRST);
3. Microsoft Security Response Alliance (MSRA);
4. Canadian Telecommunications Cyber Protection (CTCP); and
5. North American Network Operators' Group (NANOG).

Additionally, there are a number of established individual based trust groups in which TSPs should actively encourage their staff to participate.

Membership requirements for these groups vary, including fee-based (e.g. MAAWG and FIRST) and contributory participation (e.g. MSRA and CTCP). Regular face-to-face participation is a requirement of all these groups.

Information sharing communities (formal or informal, open or private) may have their own restrictions, including but not limited to Non-Disclosure Agreements (NDAs), vetting and web-of-trust requirements (e.g. withdrawal of attestations of trustworthiness).

Information-sharing between service providers, federal departments and agencies and other relevant entities must respect information classification levels set by information owners, adhere to relevant legislation and guidelines on information sharing.

4.7.1 Sharing of Information for Telecommunications Critical Infrastructure Protection

Objective:

To ensure that TSPs are actively engaged in cyber security information sharing for the protection of both their customers and the Canadian critical infrastructure.

The TSPs should have the capability to:

Controls:

1. Both receive and take action on threat information from other network operators and incident response organizations;
2. Document and implement information-sharing practices for sharing threat information with other third parties;
3. Participate in the Canadian Telecommunication Cyber Protection (CTCP) Working Group, if they are responsible for telecommunications critical infrastructure, as defined by Industry Canada.

4.7.2 Establishment of Mechanisms for Information Sharing

Objective:

All TSPs should have a set of common capabilities to support secure information sharing. These capabilities are minimum requirements in order to securely exchange threat and incident information. While there are more advanced mechanisms, not all organizations will have access to these; hence, a base level of capabilities is necessary. In addition to securing the data, the mechanisms used should also provide for authenticating the sender to the recipient of the information in order to avoid phishing or other impersonation attacks.

Controls:

The TSPs should have the capability to:

1. Support appropriate security mechanisms designed for the secure exchange of information as dictated by the forums in which the information is being shared;
2. Establish and enforce internal policies on classification, privacy and distribution of information, which include requirements for the collection, use, disclosure, retention, and disposal of information;
3. Establish and enforce an acceptable use policy and/or terms of service policies for customers, especially for abuse management;
4. Limit the information shared to only that required to resolve issues, and avoid sharing of personal information.

4.8 Vendor Management

4.8.1 Equipment Supply Chain

TSPs act as vendors to their customers. However, they are also customers themselves, as they procure systems and technology from vendors in order to build the infrastructure that provides service to Nigerians.

Objective:

In order to reduce threats to their infrastructure and customers, TSPs should make reasonable efforts to ensure that network equipment is secure.

Controls:

The TSPs should have the capability to:

1. Define security standards for procurement of systems, devices, and software;
2. Ensure that relevant security standards are included in purchase agreements, Requests for Proposals (RFPs), and contracts;
3. Require third parties to test and verify all equipment, systems, and software in accordance with well-known best practices (e.g. Common Criteria);
4. Avoid doing business with vendors who do not meet security standards unless the vendors are willing to address the issues or mitigating controls can be introduced;
5. Define procedures to ensure that vendors are following the standards defined by the TSP;
6. Support a compliance verification program to ensure that vendors are following the standards defined by the TSP;
7. Ensure that hardening requirements are passed to suppliers.

4.8.2 Vendor Security Management

Objective:

Telecommunications vendors often provide significant levels of support to TSPs. TSPs should, therefore, implement security controls on vendors accessing their equipment.

Controls:

The TSPs should have the capability to:

1. Limit vendor access to only those systems for which vendors provide support;
2. Demonstrate that the practices of their telecommunications vendors do not impact or degrade the level of security of the TSPs' infrastructures;

3. Monitor vendor activity to ensure the integrity and security of their networks;
4. Ensure that security hardening requirements are included in Service Level Agreement (SLA) clauses with third party providers.

4.9 Privacy

Objective:

The privacy rights of Nigerians are protected by the Constitution (Chapter 4 Section 37), as well as privacy regulations [4]. These legal requirements take full precedence over the guidelines listed in these best practices. TSPs that follow these best practices are also expected to maintain the same level of commitment concerning privacy toward their customers.

Specifically, sharing of personal information is rarely needed for abuse or trouble resolution. The TSP serving a customer must be able to identify the user who is infected or performing abuse activities, but this information should not be shared with other entities unless disclosure is done in accordance with the requirements of the provider's Privacy Policies and Terms of Service.

While the relevant legislation outlines the privacy rights of citizens, along with the responsibilities that TSPs have in protecting citizens' rights, there are additional best practices that should also be applied.

Controls:

The TSPs should have the capability to:

1. Ensure that the solutions and services that they provide adhere to all applicable privacy legislation;
2. Ensure that they deal with privacy concerns promptly and transparently;
3. Evaluate any actions that they take to protect the security of their network against the privacy trade-offs to their customers.

Chapter 5 – Security of Information Infrastructure in Telecommunication

5.1 Prevention and Early Warning

Prevention and early warning are indispensable components Critical Information Infrastructure Protection (CIIP). They aim to reduce the number of information security breaches. However, since threats to CIIP are diverse, interdependent, and complex, it is less likely that incidents can be altogether prevented [5]. A more realistic goal is to ensure that critical information infrastructures "are less vulnerable to disruptions, any impairment is short in duration and limited in scale, and services are readily restored when disruptions occur [6]. The main function of prevention is to ensure that the telecom industry is prepared to cope with incidents as they occur.

We define prevention to consist of activities that raise the general preparedness of the telecommunication industry. This involves the dissemination of recommendations and guidelines on best practices, timely and credible warning of specific threats, and the implementation of training and exercises. It is worth noting that prevention and early warning cannot be approached on a purely technical level – potential dangers have to be weighed up constantly in a trade-off against risk situations.

The CIIP unit should enforce preventive measures which include hosting workshops to discuss protection measures and best practices and disseminating warnings and advice. However, although these tasks are essential, the CIIP unit is not the only source of support and guidance in information security. The telecommunication operators and TSP's know their business better and there are other sources of warnings and advice. Therefore, the CIIP unit should focus its services on types of support that are not readily available elsewhere. In consequence, the workshops, warnings and advisories should be designed to reflect the specific needs of operators and TSPs, with exclusive information.

The CIIP unit should also provide exclusive information because of its exceptional position. For example, as a government body, it may be perceived as neutral and free from commercial interests. The CIPP workshops, warnings and advice may be seen as more credible than the products of private information security consultants. In addition, a well-designed CIIP unit has a large network of contacts available at its disposal with access to exclusive information. The CIIP unit can foster

information-sharing among the telecommunication industry and raise their awareness of their interdependency. In this respect, it can act as a neutral and safe platform where experiences and knowledge can be shared among the different operators and TSPs.

The task of the prevention of telecommunication infrastructures can be accomplished selectively and without incurring immense operating expenses. Apart from this, however, new forms of attacks (for example, Distributed Denial of Service (DDoS) attacks) involve the use of a large number of compromised computers to attack systems. This indicates that measures to protect telecommunication infrastructures should not be limited solely to the operators and TSPs. Every connected computer that is not sufficiently protected threatens the security of all other connected systems. The CIIP unit must therefore focus on prevention measures for the benefit of the broader public. However, since this task is time-consuming and cost-intensive, the CIIP unit needs supporting partners. Supporting partners may be found in private-sector associations (for example, industry associations), among IT manufacturers and software producers, among other governmental organizations (for example, data protection agencies), in the academia or in the media. Preventive measures aimed at the broader public are only successful when they are supported by different actors.

Telecommunication systems robustness and preventive measures of the telecommunications systems are keys for their effective utilization during disaster. TSPs are required to implement the following measures in order to increase the robustness and prevent failures of their networks during disasters and emergencies.

a) Physical Infrastructure Safety

TSPs should follow apply the standards for building their physical infrastructure. In addition, the following best practices are recommended for safety of the primary network elements and infrastructure:

i. Telecommunication equipment should be installed at suitable locations in disaster prone areas to be able to withstand impacts of any disaster. For example, in flood prone areas location of exchanges/ critical equipment to be preferably at higher altitude area to avoid inundation of water. The base should be kept high in coastal and flood prone areas;

ii. Wherever it is feasible, the critical equipment for telecommunication infrastructure should not be concentrated in one building;
iii. All the buildings, towers, and equipment sites should be equipped with adequate fire protection measures like detection and extinguishing systems;
iv. All buildings, towers, and equipment site structure should comply with building bylaws prescribed for earthquake resistant building depending upon the prevailing seismic zones;
v. As far as possible, communication cables should be buried underground in ducts to reduce their vulnerability (it is also advisable to have all disaster management centers connected through underground cables).

b) Redundancy

Redundancy in traffic management is critical to the integrity and robustness of the telecommunication networks. Sufficient redundancy prevents total network failure due to a single point of failure. As a result, the TSPs must ensure that transmission links between main network elements and switching equipment are redundant through two distinct geographical paths. Some of the key aspects of a robust and resilient telecommunication network are:

i. Alternative telecommunications links (such as SDH ring on optical fiber) between primary switches;
ii. Connection of main switches and Network Elements through mesh and ring transmission networks;
iii. Redundant microwave, aerial or underground links and other network elements such as switches etc. should be secured in alternative locations;
iv. Remote area satellite connectivity should be used in areas of undulating topology;
v. Hazard profiling of the area must be done as a first stage following the TSPs identification of vulnerability of their respective telecommunication infrastructure. This will facilitate adequate planning and reparation for emergency situations. All the vulnerable critical network components should have sufficient redundancy including transmission links and power backups in terms of battery storage capacity or any other source of energy;

vi. Low power consumption equipment should be preferred at all vulnerable / critical locations.

c) Backup of network elements

Provision of sufficient power banks of network elements (standby generators, batteries, and fuel) can prevent total failures from minor equipment damage. The TSPs should also ensure sufficient fuel, power and essential equipment backups. Some of the key actions recommended include:

i. Provision of an Uninterrupted Power Supply (UPS) along with sufficient external battery support to ensure that the power supply is not interrupted to the key equipment in the event of a main power supply failure;
ii. Ensure supply of fuel for back-up generators;
iii. Ensure availability of spares on site during emergency;
iv. Ensure enough spares in air conditioning equipment to serve the peak hours' load;
v. Store backup spares and fuel in an accessible and secured area;
vi. Use alternate means of power such as solar energy wherever possible.

d) Overload Prevention Measures

Emergency situation often triggers overload of the network due to high traffic, anxiety calls and repeated call attempts. The TSPs should ensure provision of an effective solution to prevent the crash of the network in such cases and develop effective congestion management processes which should be reviewed and tested periodically. The public is also required to use alternate mode of communications such as SMS or internet media whenever congestion in the voice calling in mobile network is experienced.

5.2 Protection: Protecting information infrastructures adequately

Security risks can be reduced by spreading knowledge about threats and possibilities for protection, clearly assigning responsibilities for security matters, implementing security measures, and using reliable telecommunication products and processes.

Goal1: Raise awareness of risks related to Information Infrastructure

The Nigerian Communication Commission (NCC) continues to trust in raising the awareness of

the general public and the telecommunication sector about the risks to their information infrastructure. To this effect, initiatives are being launched that are directed to people at all levels, from corporate management and high-level public administration to ordinary employees and private individuals in the telecommunication industry.

Goal 2: Use of safe telecommunication products and secure IT systems

The NCC supports the use of reliable telecommunication products and systems and trusted IT security applications in the industry in Nigeria. This indicates that NCC is extending and improving its capacity to examine and evaluate telecommunication products/equipment and systems under security aspects and issue relevant certificates by establishing an online portal for type approval. This will enable NCC to easily publish product recommendations, issues technical guidelines for the use of these products and lists products that were issued a Nigerian security evaluation certificate.

Goal 3: Respect confidentiality

Unprotected digital communications are extremely vulnerable, easy to intercept and manipulate. Therefore, the security of the Nigerian information society and Nigeria as a place to do business depend on the availability of reliable, innovative and trusted encryption products that guarantee confidential communication. NCC is promoting the development and the Nigerian manufacturers of adequate products and will use encryption and security applications for its own communications.

When awarding Information Technology security contracts, the telecommunication service providers and operators must pay greater attention to national security interests on the one hand and the reliability and trustworthiness of bidders on the other. The business sector is made particularly aware of the risks associated with information theft (for example, caused by economic espionage) and the possibilities and benefits of preventing such theft by using reliable encryption products.

Goal 4: Putting safeguards in place

It is necessary to put coordinated technical, physical, organizational, and structural safeguards in

place. Responsibilities, duties and roles for all tasks related to IT protection must be clearly defined. Adequate IT security measures should be implemented in the telecommunication industry. The NCC will ensure that IT security strategies for TSPs are kept up to date and are implemented effectively. NCC is improving IT security management coordination within the communication industry to ensure uniform and generally comparable, efficient, and transparent processes and workflows from the highest level down to every single authority within the remit of the industry. All businesses and organizations are firmly called up on to make adequate arrangements for protecting their IT systems.

Goal 5: Creating framework conditions and guidelines

NCC undertakes to create adequate framework conditions and guidelines, taking account of international norms and standards, in order to ensure full protection in all security-relevant areas. Each telecommunication operator and TSP will make sure that standards and guidelines are implemented in accordance with the NCC plan and put the necessary structures in place (for example, CSIO for IT security issues; reporting; role and responsibilities of the management, etc.).

Appropriate guidance will be given where special requirements apply to IT security. Other areas of concern will be provided with recommendations and guidelines on IT security.

Goal 6: Coordinated security strategies

Since security systems are only as robust as the weakest link in the chain, it is crucial to harmonize security-relevant processes and mechanisms. Therefore, NCC advocates defining joint standards and coordinated application concepts, among other things, in order to optimize systems with regard to their security, technical, economic, and data protection properties.

Goal7: Shaping policy at national and international level

NCC will intensify its efforts to actively shape policy with regard to existing and new forms of cooperation for protecting information infrastructures. In addition, it will strengthen national and international cooperation in order to bring Nigerian security interests to bear when formulating guidelines, directives and other legal instruments. To be able to respond comprehensively to threats, given the global character of networks, NCC and other federal authorities will increase

their cooperation with their counterparts abroad. Together with its partners, for example in the EU, NATO, UN, G8 and at international level in general, the Federal Government will raise the awareness of the vulnerability of information infrastructures and support the provision of technical solutions.

5.3 Detection

To promote security and to avoid particularly vulnerable technologies, it is crucial that new threats be discovered as quickly as possible. In order to recognize emerging threats on a timely basis, there is need to depend on a broad national and international network. In close collaboration with technical experts from Computer Emergency and Response Teams (CERTs), the CIIP unit should identify new technical forms of attacks as soon as possible. Furthermore, non-technical analyses of the general risk situation such as information about the emergence of criminal organizations are needed. Thus, the CIIP unit should have restricted access to certain relevant information provided by intelligence services. In addition, technical as well as non-technical information may need to be shared with international partners, since the threats to information security are not limited to geographic borders.

However, the network of contacts that belongs to CERTs and the intelligence services is of only limited use without the close cooperation of the operators of CI. Since the CI operators are the first to be affected by new attacks, they report incidents, detection and early warnings of the telecommunication infrastructures. The importance of information-sharing with the private sector was highlighted in the US federal government's 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP) [7]. Nevertheless, information-sharing is generally the only limited and many initiatives for information-sharing have proved only partly successful [8]. This is because companies share information only under conditions of strictest confidence. Building trust is a major task for any CIIP unit to obtain information about incidents directly from the firms. We discuss the procedure for achieving these tasks as follows:

5.4 Reaction

Reaction includes the identification and correction of the causes of a disruption. Initially, the CIIP unit should provide technical help and support to the targeted company. However, the CIIP unit

cannot take on the management of incident response for these companies. The activities of the CIIP unit should complement the efforts of companies by providing advice and guidance on how to tackle an incident. The CIIP will not offer complete solutions.

A major requirement for accomplishing this task is that the CIIP unit must have a 24-hour incident reporting service. Attackers often prefer to execute their attacks on the information infrastructure of companies at times when they expect to face few immediate countermeasures. To a large extent, the damage caused by an attack depends on how long it takes to counteract it. Therefore, incident response must start as quickly as possible. The support provided by the CIIP unit is most helpful, if it is always available.

However, similar to the prevention and detection of attacks, incident response is not restricted to technical measures. In particular, prosecution of attackers is a vital part of reaction. The law enforcement may not be able to help targets directly, but it can help protect others by increasing the risk of capture, prosecution, and wider deterrent [9]. Since many attacks are carried out by international actors, companies often do not know how to secure appropriate law enforcement responses abroad. The CIIP unit should support targeted companies by referring them to the responsible authorities.

Finally, adequate reaction also includes analysis of incidents. In cooperation with the target, the CIIP unit must draw up a final report on the incident. The lessons learned should be made available to other operators of CI. The private industry tends to focus mainly on lessons learned to improve their internal systems, however, the government can take a broader approach. Lessons learned should be exchanged with all critical players in order to improve crisis planning and to streamline information-sharing in crisis situations. Companies and government sectors that were not affected by the attack can compare emergency plans and take steps to avoid mistakes. This concludes the cycle of prevention, detection, reaction, and crisis management.

5.5 Crisis Management and Restoration

Crisis management has been part of CIIP since its inception. Minimizing the effects of any disruptions on society and the state has always been a major task of protection, so the CIIP unit must be embedded in the national crisis management structure. Depending on the organizational

structure and management administration of a nation's crisis that is available, the CIIP unit can be positioned in several different ways. It should be well-positioned in order to have direct access to decision-makers, because a key function of the CIIP unit is to alert the responsible people and organizations. In case of a national crisis, the CIIP unit must be able to offer advice directly to the government.

Within the administration, the CIIP unit should act as the center of competence for all questions that relates to information security. Since many agencies have to deal with issues of information security, the CIIP unit needs to cooperate with various partners within the government. Hence, requirements for security management in an organization must be reviewed for updates at regular intervals. One of these core requirements is a well-designed crisis management plan to handle emergencies. The CIIP unit should conduct exercises with other governmental crisis organizations and CI operators repeatedly. All crucial actors must be familiar with their responsibilities, duties, and risks in times of crisis.

The CIIP unit should raise awareness of the various existing interdependencies. Operators of CI are dependent on each other in many respects. For instance, energy supply is crucial for the communication sector and vice versa. Since companies may tend to focus on their own business, they may often lack awareness of these interdependencies. The government in turn may also forgot that they dependent on the functioning of these critical infrastructures. A key task for the CIIP unit is to reinforce understanding of these dependencies among different actors: for example, through workshops and exercises. CIIP can only succeed if all stakeholders work together, with the same goals.

Procedures and best practices in restoration and recovery of information Infrastructure

a) Preparedness for Handling Disasters

i. All TSPs shall prepare their Disaster Management Plan and submit the same to NCC.
ii. The preparedness measures taken by TSPs will be reviewed every six months.

b) Nodal Officers

TSPs shall identify Main and alternate Nodal officers at central level and at every telecom circle level and publicize their full contact details for coordination related to disaster management

prominently on their website. Same shall also be informed to NCC Nodal officer and respective TERM cell head.

c) Disaster Response Task Force (DRTF)

TSPs shall have a Disaster Response Task Force (DRTF) at the State level. DRTF teams will be responsible for the provision of emergency communication and restoration of telecommunication services in disaster affected areas. DRTF shall consist of teams of experts in the following areas:

i. Transmission Team;
ii. Switching Team;
iii. Infrastructure Team;
iv. Mobile Service Team;
v. Telecom relief Team (for opening PCOs, helpline response etc.)

The self-contained minimum infrastructure which the teams must have include satellite terminal, system related spares and stores, tools and testers, portable generator set, vehicles, arrangements for logistics support like food, water, tents, and beds blankets. Additional resource requirements shall be augmented by TSPs upon request.

d) Rapid Damage Assessment Team (RDAT)

If the disaster affected area is a larger area or a more remote area, the TSPs shall involve the Rapid Damage Assessment Team (RDAT). The RDAT shall work to determine the precise nature and extent of damage so that the planning for restoration of telecommunication services can be done in the efficient and effective manner. The initial focus of the RDAT will be to identify:

i. The operational telecommunications assets available for use within the affected area;
ii. Any damaged communication facilities;
iii. Telecommunications assets that are not within the affected area that may be brought physically or employed electronically to support the affected area. Preliminary assessment shall be carried out immediately within 24 hours for planning the response. RDAT shall consist of members from various telecom fields such as mobile communication, switching, transmission, civil, electrical experts etc. This team shall also be well equipped with tools for quick assessment. The RDAT must be a self-contained team having arrangements for

logistic support like water, food (at least 2 days), blankets, bed, satellite phone, mobile phone etc.

e) Resource center

i. Locations of the designated resource centers shall be identified at the organization's head office and at the various branch offices for purpose of inventory. The inventory should include following:
   - Satellite terminal (for example, DSPT);
   - Satellite based emergency communication terminals;
   - Portable/air-transportable BTSs and satellite equipment for connecting to BSC/MSC;
   - OFC cable with restoration kit;
   - Portable power generator sets or batteries. At the resource center locations, concerned responsible officers are required to be identified with participation of nodal officer from the TSPs.

ii. To restore the mobile services disrupted due to damaged BTSs, TSPs should keep, as inventory, certain minimum number of portable BTSs and satellite equipment for connecting to BSC/MSC in case of disaster. Suggested number could be around 10 per TSP so that collectively sufficient numbers of portable BTSs with VSAT connectivity are available.

f) Memoranda of Understanding amongst TSPs

For restoration of Telecommunication services in emergencies and disaster conditions, TSPs enters enter into Memoranda of Understanding (MoU) among themselves for sharing specialized resources and intra-circle roaming for provisioning of services. Priority user groups are to be identified, who might be involved in rescue, relief and restoration activities. These include different government agencies, police, paramedics, Firefighting division, medicals, civil defense, the Red Cross, the Army, financial institutions, NGOs, and all the officers and staff engaged in restoration of telecommunication services. Priority is given to these groups for provisioning of additional communication facilities and restoration of telecommunication services.

g) Training and Drill

A quick and efficient response to disaster depends on availability of trained staff and inventory in immediate deployable condition. Periodic training and drills ensure a continuous awareness of the additional demands which each individual might be confronted with in case of disaster. Similarly, it is important that the equipment meant for restoration should be periodically inspected for reliance and to ensure that they are in working condition. TSPs are required to conduct periodic mock-drills within their network and in coordination with other support agencies.

h) Directory

A directory of nodal officers that is responsible for telecommunication services during disaster at various levels of the organization shall be prepared to handle incidents. Data such as names, addresses, telephone numbers, mobile numbers, email address, fax numbers shall be obtained from the created directory and updated.

5.5.1 Control Room

5.5.1.1 Emergency Control rooms will be set up at the organization with requisite facilities. If control rooms already in existence at the organization, they must be upgraded to meet requirements and be rescue ready.

5.5.1.2 Objectives of the Control Room

The Control Rooms are setup as nerve centers for coordination and management of disasters. The objectives of the control rooms shall be to provide centralized direction and control of any or all of the following functions:

i. Receive and process disaster alerts and warnings from nodal agencies and other sources and communicate the same to all designated authorities;
ii. Monitor emergency operations;
iii. Facilitate coordination among ministries, departments, and Agencies;
iv. Requisitioning additional resources during the disaster phase;
v. Issuing disaster/incident specific information and instructions to all concerned;
vi. Consolidation, analysis, and dissemination of damage, loss and assessment data;

vii. Forwarding of consolidated reports to all designated authorities.

5.5.1.4 Location of Control Room

The control room will be set up at a suitable location and the building should be disaster resistant so as to withstand the impact of disasters and remain functional during the emergency phase.

5.5.2 Trigger Mechanism

The Trigger Mechanism prescribes the manner in which the disaster response system shall be automatically activated after receiving early warning signals of a disaster happening or likely to happen or on receipt of information of an incident. The activities envisaged in this SOP under the response phase shall be initiated simultaneously without loss of time to minimize the loss and damage and mitigate the impact of disaster.

The objective of having a trigger mechanism for natural disasters is to have a suo-motto activation mechanism for spontaneous response to set in motion command, control and management of the situation. There shall be two types of situation with different trigger mechanisms for natural disasters; (a) situation I – when disaster occurs and there are early warning signals and (b) situation II – when disaster occurs and there are no early warning signals.

A. Where early warning signals are available

i. Organizational agencies have been designated by National Emergency Management Agency (NEMA) for generating/forecasting of events of natural disasters. Onset of disaster shall be indicated through forecasting by the organization and her agencies;

ii. TSPs shall inform their customers via SMS or cell broadcast or recorded voice messages with respect to rescue instructions;

iii. TSPs shall keep all the required inventory and personnel in readiness.

B. Where Disaster occurs without early warning

In disaster situations where no early warning signals are available, the primary objective of the trigger mechanism shall be to mount immediate rescue and relief operations and set the process in as quickly as possible. The following procedure shall be followed in such situations:

i. Organization control room shall be fully activated for managing the incident.
ii. DRTF and RDAT teams shall be deployed by TSPs.

The following shall be the sequence of action:

i. Where disaster strikes with or without early warning signals, the TSPs shall immediately assess damage to their network and deploy Rapid Damage Assessment Team (RDAT) and Disaster Response Task Force Teams (DRTF) with required inventory to provide emergency communication to priority callers such as the police, fire, medical, civil defense, Red Cross, army, and financial institutions;
ii. Upon request, portable or vehicle mounted or air-transportable BTSs / BSCs with backhaul on satellite media may be installed by TSPs;
iii. Officer of TSPs of affected telecommunication circle level shall report to concerned official (TERM), NCC (Chairman of Swept-Time Delay Cross Correlation (STDCC)) in that circle, for sharing information and coordination related matters;
iv. TERM units of NCC shall be the single nodal point in the disaster region where representatives of TSPs shall also be present to coordinate and oversee communication restoration efforts;
v. The official head of concerned TERM cell shall act as interface between all TSPs and other support agencies including State Government for any coordination related issues;
vi. Meeting of STDCC shall be convened to review situations;
vii. TSPs shall make helpline numbers operational where the last location of the survivors or missing persons can be intimated to the relatives;
viii. Information about the last location details or sharing of CDRs of the subscribers, in the disaster affected areas shall be provided through helpline numbers. This is achieved under the special regulatory permission. In the case of extreme and adverse

case of disaster, permissions would be deemed automatically permitted for duration of two weeks;

ix. TSPs shall share specialized resources and allow intra-circle roaming with respect to MoU for the provisioning of services to priority user groups and general public during disaster period;

x. To have wider coverage from a single Base Transceiver Station (BTS), TSPs may radiate more radio power from the BTSs located in the disaster affected areas beyond the Electromagnetic Radiations (EMR) limits prescribed for two weeks;

xi. TSPs shall broadcast messages at regular intervals, in consultation with STDCC to all the subscribers in the affected areas through SMSs / Cell broadcast giving details about; (i) details of TSPs helpline numbers. (ii) Details about rescue and relief activities such as tentative schedule of full recovery;

xii. TSPs shall open sufficient number of PCOs, preferably free of cost, for use of general public in affected area. The TSPs shall also ensure that in the disaster affected areas, no subscriber shall be denied access to voice or SMS communication due to any commercial consideration, whatsoever, including non-payment / insufficient balance/recharge – offer of toll free access to all networks. This services shall continue for at least two weeks;

xiii. TERM Cell shall submit the status report in respect of overall telecommunication facilities in affected area to NCC, Head Quarter (HQ) on daily basis or as sought by NCC, HQ;

xiv. The control room under respective TERM cell shall remain operational till the telecom services are restored to normal or as per instructions from NCC, HQ.

Chapter 6 – Adoption of the Best Practices in Information Infrastructure Security Management in the Telecommunication Industry

The Best Practices for Information Infrastructure Security Management Framework in the telecommunication industry does not constitute a foolproof formula for security. However, the benefits of its adoption may be missed if overlooked or if the implementation of its voluntary guidelines are postponed in part or in whole. The reasons are simple; (a) the implementation framework comprises of leading practices from various standard bodies that have proved to be successful and (b) there is a guaranteed delivery of regulatory and legal advantages which extend well beyond improved security for telecommunication organizations that adopt it early.

It is on this basis that we develop a risk-based compilation of guidelines that will help the telecommunication industry to identify, implement, and improve information infrastructure security best practices, and create a common language for internal and external communication of security issues. This framework is a reiterative process/concept which is evolving and it will synchronize with changes in emerging security threats, processes, and technologies in the telecommunication industry.

The framework for adoption can be revised periodically to incorporate lessons learned and feedback from the industry. In effect, the framework envisions effective information infrastructure security as a dynamic, continuous loop of responses to both threats and solutions. The framework also provides an assessment mechanism that will enable the Nigerian Communication Commission to determine its current security capabilities, setup individual goals for a target state of infrastructure security management, and establish a future plan for improving and maintaining information infrastructure security programs.

6.2.The Benefits of Adoption

The effective adoption of the best practices in this document can provide many benefits to the telecommunication industry. These include:

i. Avoiding re-inventing the wheel;
ii. A reduction of dependency on information infrastructure on the security experts;
iii. An increase in the potential to utilize less-experienced staff if properly trained;

iv. An easy to leverage external assistance;
v. A reduction in risks and errors;
vi. Quality improvement;
vii. Capacity to manage and monitor productivity;
viii. Cost reduction which can increase standardization;
ix. Trust and confidence improvement from regulators, other telecommunication industry and partners.

A Road Map to Adopting the Information Infrastructure Security Management in the Telecommunication Industry

We now present a clear roadmap to adopting the information infrastructure security management in the telecommunication industry and maintaining an effective compliance of best practices in information infrastructure security. The roadmap begins with establishing clear goals and objectives in order to align effort with the real needs of the telecommunication sector, to manage expectations, and to ensure continual focus. The roadmap then consists of activities to get started, followed by the key implementation tasks with suggested roles and responsibilities. This adoption path is only the initial phase of what is required in order to guarantee an iterative sustainable approach.

Adopting these best practices will mean major changes for telecommunication organizations. Therefore, it is important to have a high-level of sponsorship and active involvement of key stakeholders. The roadmap begins with an initial phase to define overall goals and to gain the support and commitment of top management which then leads to the ongoing effective governance and implementation.

6.3.Typical objectives of the initial implementation phase

i. To define the meaning and need for information infrastructure security management best practices;
ii. To identify any organizational/environmental/cultural constraints and enablers;
iii. To achieve a broad understanding of security issues and benefits across all stakeholders;

iv. To agree, publish and gain acceptance of initial developed framework, tools and processes;
v. To complete an initial gap analysis against the developed best practices (demonstrate where if any of the best practice is already in place and to highlight areas of focus);
vi. To identify and sign-off of key performance indicators and critical success factors;
vii. To document and estimate timescales and resource implications;
viii. To align initiative with business objectives/strategy;

The following are the notable success criteria for the initial implementation phase:

i. The key stakeholders must be identified, they must be engaged and involved actively;
ii. The identified key stakeholders should be made to contribute towards achieving the goals and be able to explain and support the business case;
iii. The key stakeholders should have an understanding of the expectations;
iv. Those responsible for the implementation of the published framework should accept the adoption as a first priority;
v. There should be a formal and effective communication plan. The plan should clearly provide and explain the key aspects of who to overcome any barriers and to motivate change, what to overcome any barriers and to motivate change, and when to overcome any barriers and to motivate change;
vi. The changes must be sustainable and institutionalized such that they become "business as usual practices".

6.4.Important Key Activities to get started

After setting the goals and gaining the support from stakeholders, the adoption process must be activated. Activation consists of two steps. Planning, based on analysis of the current environment (telecommunication infrastructures in place) and the implementation.

(a) Planning: These are recommended implementation planning activities together with some critical success factors:

Activities	Critical Success Factors
i. Identify champions - stakeholders (including partners), input providers, Best Practices Strategy Committee (BPSC) members ii. Identify skill set and capabilities required from telecommunication organizations involved iii. Identify existing good practice or successes that could be built on or shared iv. Identify cost/benefit arguments – that is why is it important that do we must do v. Identify inconsistencies in process or practice vi. Identify potential opportunities for "rest of organization" i.e. the whole telecommunication industry to get involved in Information Infrastructure security management vii. Utilize external influences viii. Create a measurement approach for an area or activity to expose actual evidence of problems ix. Carry out some gap analysis against the developed industry best practice	i. Authorize and articulate champions ii. Available skills and capabilities iii. Well prepared business cases approved by stakeholders iv. Real opportunities for the sector to see the benefit of participating v. Practical and useful implementation approaches vi. Effective and useful measures to ensure compliance vii. Expose the truth /whole picture, warts and all, about best practice success or failure – show how adherence and compliance can be helpful.

(b) Implementation: We recommend these activities to start up the implementation roadmap, together with some critical success factors:

Activities	Critical Success Factors
i. Create a sound implementation structure • This must define scope (what is included/excluded) and the deliverables • It must agree on success criteria/quality criteria • It should set realistic timeframes and allocate suitable resources and roles • The implementation structure must identify risks and a risk mitigation strategy ii. Gain approval from senior management (the higher the better within the organization) iii. Find reference site, or external examples to learn from. iv. Build communication plan to gain buy-in, and break down barriers - Who/what/how frequent/purpose v. Do a pilot activity (demonstrate the business case) to show how it would work and demonstrate potential benefits. vi. Follow a phased introduction, e.g. - focus on critical but easier to address areas • Assess Best Practices first • Build up operational performance improvement progressively based on prioritizing maximum return for lowest cost. • Consider one business area first, others later - Aim to establish some successes while learning how to be effective	i. Good compliance management (set the governance tone) ii. Expectations set correctly iii. Approved business case iv. Manage compliance like you manage the rest of the business v. Convincing reference sites vi. Successful pilot vii. Address quick wins first to demonstrate results and realize benefits before attempting any major changes

6.5.Participants: Their Roles and Responsibilities?

All three generic groups of stakeholders (the top management, the providers – the telecommunication firms, and the controllers – the monitoring committee), and their interests, should be involved in the implementation initiative. A key characteristic of any successful implementation initiative is the establishment of an organizational-wide approach that clearly sets

out roles and responsibilities. The roles and their responsibility specification should emphasize that everyone has a part to play to enable a successful outcome.

It may also be helpful to include an external, or internal, facilitator to provide an objective and neutral position. Table 6.3 below provides the suggested generic roles and responsibilities of the three main groups. Figure 6.1 in this chapter below suggests the proposed timeline for the adoption guideline.

Table 6.3: The suggested generic roles and responsibilities of the three main groups

Top Management	**Providers (Telecommunication Firms)**	**Controllers (Monitoring Committee)**
• Management board (authority to make things happen) • Give direction backed up with adequate support and sponsorship • Balance requirements with available resources, making available additional resources if required • Insist on and seek measurable benefit realization • Coordinate overseas/satellite parts of the enterprise to ensure their interests and constraints have been considered • Create organization and structure to ensure board involvement in the governance process – by forming	• IT management (internal and external), with support from business management • Take ownership and set direction of Information Infrastructure Security activities • Build and achieve a pilot business case for applicable best practices • Set infrastructure security objectives • Define governance and control framework • Identify critical IT processes • Assess risks, identify concerns • Assess IT capability, identify gaps • Initiate a continuous improvement programme • Develop business cases for improvements	• Internal and External Audit • Scope audits in coordination with governance strategy • Provide assurance on the control over the best practices developed • Provide assurance on the control over the information infrastructure security performance management system Risk Management • Ensure that new risks are timely identified, provide advice for Compliance officers • Ensure that Best practice complies with policy, laws and regulations Finance

Top Management	Providers (Telecommunication Firms)	Controllers (Monitoring Committee)
committees, establishing reporting processes • Monitor performance, monitor risks, correct deviations, Business and IT senior managers, business partners and project sponsors • Implement organization and necessary infrastructure • Take ownership of requirements • Champion and collaborate in governance activities • Ensure business strategy and objectives are set and communicated and aligned with IT • Assess business risks and impacts • Establish reporting processes meaningful to stakeholders • Communicate any business concerns in a balanced and reasoned way • Provide project champions, creating the seeds of change User representatives	• Design and implement Best practice solutions as it relates to Information Infrastructure security • Commit skilled resources • Establish performance measurement system • Report to regulator (NCC) • Respond to Q&A feedback from customers' suppliers/business partners • Integrate any own existing or planned practices with customer's • Support and contribute to customer's governance approach • Agree service definitions, incentives, measures and contracts/agreements • Ensure adequate education and communication • Incorporate information infrastructure security principles and best practices into induction and performance measurement process • Define plan and deliverables • Organize team and roles (architects, senior responsible	• Advise on and monitor Best Practice costs and benefits • Provide support for management information reporting • Incorporate best practice requirements into purchasing/contract process

Top Management	Providers (Telecommunication Firms)	Controllers (Monitoring Committee)
• Take responsibility for Quality Assurance programme (design and output) • Regularly check actual results against original (or changed) goals • Provide service feedback to providers	officer, facilitator, project manager, process owners) • Undertake core tasks • Report progress to plan	

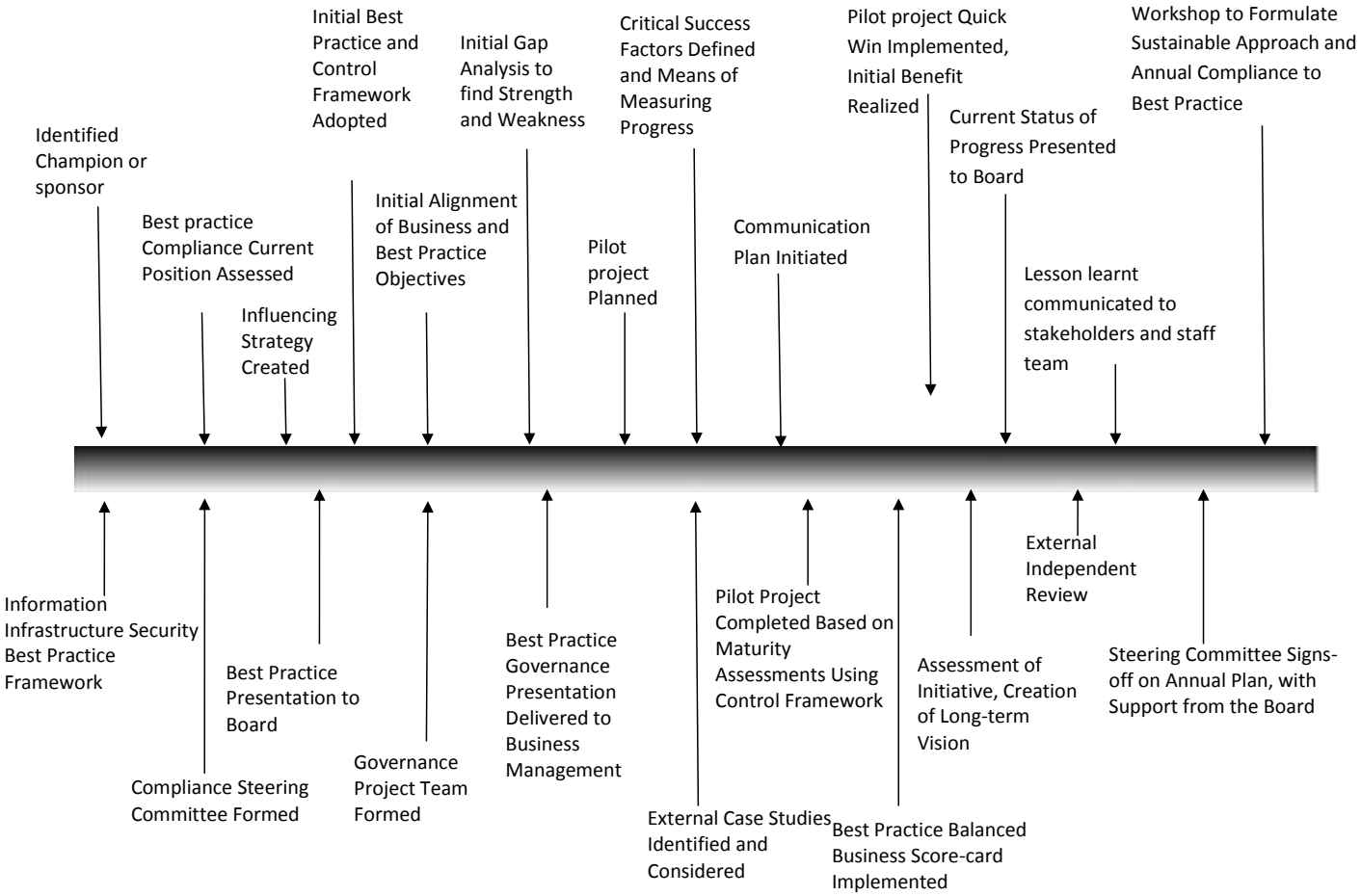

Figure 6.1. Timeline for the Adotion of the Best Practices in Information Infrastructure Security Management in the Telecommunication Industry

Chapter 7 – Conclusion and Recommendations

Organizations today must deal with a multitude of information security risks. Terrorist attacks, fires, floods, earthquakes, and other disasters that can destroy information processing facilities and critical documents. Theft of trade secrets and the loss of information due to unexpected computer shutdowns can cause businesses to lose their commercial advantage.

A number of best practices have been identified in this work that can help organizations assess their security risks, implement appropriate security controls, and comply with governance requirements as well as privacy and information security regulations.

Of the various best practice frameworks available, the most comprehensive approach is based on the implementation of the international information security management standard, ISO/IEC 17799, and subsequent certification against the British standard for information security, BS 7799. This ISO 17799/BS 7799 frame work is the only one that allows organizations to undergo a third-party audit.

Some of the best practices that facilitate the implementation of security controls that have been identified in this work include Control Objectives for Information and Related Technology (COBIT), ISO/IEC 17799/BS 7799, Information Technology Infrastructure Library (ITIL), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE).

Focus on the ISO/IEC 17799 standard is warranted, given that it provides the most comprehensive approach to information security management. The other best practices focus more on IT governance, in general, or on the technical aspects of information security (See Table 3.). Moreover, ISO 17799/BS 7799 is the only best practice framework that allows organizations to undergo a third-party audit and become certified. Implementing an overarching compliance framework using ISO/IEC 17799 and BS 7799 requires a methodical information security management system that facilitates the planning, implementation, and documentation of security controls and ensures a constant process review.

7.1 Certification Process

Telecommunication firms can apply to become certified on information security management systems (ISMS) on BS 7799 specifications. An organization that obtains certification is said to be ISO/IEC 17799 compliant and BS 7799 certified. Development, implementation, maintenance, and continual improvement of documented ISMS are fundamental to certification. To guide organizations through this process, BS 7799 uses the Plan-Do-Check-Act (PDCA) model that is common to other management systems. Table 2 provides an overview of PDCA cycle phases as they relate to an ISMS.

Once an organization has developed, implemented, and documented its ISMS, an accredited certification body carries out a third-party audit. The BS 7799 audit includes both a documentation audit and an implementation audit. Security auditors assess whether an organization's ISMS scope covers all aspects of operations. They also ensure that the risk assessment reflects the organization's business activities and that the assessment's results are reflected in the risk treatment plan. Finally, the implementation audit verifies that the organization has effectively implemented its security policies and controls and that processes have been set in place to ensure the ISMS's review and improvement.

A number of critical factors can affect success or failure in the certification process. Key success factors include adopting an implementation approach that is consistent with the organization's culture. Below are some of the factors to consider:

Table 7.1: Uses of the ISO/IEC 17799 Standard

Type of Company	Size	Primary Objective	Use of the Standard
Small Enterprise or Organization	Fewer than 200 employees	Raise the awareness of the management regarding information security	ISO 17799 contains security topics that should be dealt with as a foundation for information security management

Type of Company	Size	Primary Objective	Use of the Standard
Medium Enterprise (centralized or decentralized)	Fewer than 2,000 employees	Create a corporate culture of compliance	The standard contains the practices required to put together an information security policy
Large Enterprise	More than 2,000 employees	Obtain security certification at the end of the process	Use BS 7799-2 to implement, maintain review, and improve an information security management system (ISMS)

Table 7.2: Information Security Management Systems and the PDCA Model

PDCA Phase	Description
Plan (Establish the ISMS)	• Define the ISMS scope and the organization's security policies • Identify and assess risks • Select control objectives and controls that will help manage risks • Prepare the Statement of Applicability (SoA) documenting the controls selected and justifying any decisions not to implement, or to only partially implement, certain controls
Do (Implement and operate the ISMS)	• Formulate and implement a risk mitigation plan

PDCA Phase	Description
	• Implement the previously selected controls to meet the control objectives
Check (monitor and review the ISMS)	• Conduct periodic reviews to verify the effectiveness of the ISMS • Review the levels of acceptable and residual risk • Periodically conduct internal ISMS audit
Act (maintain and improve the ISMS)	• Implement identified ISMS improvements • Take appropriate corrective and preventive action • Maintain communication with all stakeholders • Validate improvements

Below is a quick comparison of the Best Practices discussed in this document:

Table 7.3: Quick Comparison of Security Best Practices

Best Practices and Compliance Frameworks	Description / Scope	Offers Certification?	Comparison with ISO/IEC 17799
CERT Security Practices	A set of recommended best practices for improving security of computer network system.	No	ISO/IEC 17799 addresses a more comprehensive set of

			information security issues.
Common Criteria for Information Technology Security Evaluation ISO 15408	A technical standard that certifies the levels of defense conferred by the security measures implemented in information systems	Yes	ISO/IEC 17799 focuses on the organizational and administrative aspects of information systems. Therefore, they are complementary
Control Objectives for Information and (Related) Technology (COBIT)	COBIT is an international standard for IT governance that seeks to bring together business control models and IT control models	No	COBIT and ISO/IEC 17799 are mutually complementary, with COBIT providing a broader coverage of IT governance in general and ISO/IEC 17799 focusing more specifically on security and providing certification.
Guidelines for the management of IT Security (GMITS) (ISO 13335)	GMIS is an international standard that lays out guidelines for information security management and consists of a number of technical reports covering information security management concepts and	No	The two standards are complementary. While GMITS describes high-level concepts for IT security management, ISO/IEC 17799

	models, techniques, IT security management and planning, and selection of safeguards		specifies controls that can be used to develop and implement an information security management system (ISMS).
Information Technology Infrastructure Library (ITIL)	A supplement to Committee of Sponsoring Organizations of the Treadway Commission (COSO) and COBIT that proposes best practices for IT service management	No	ITIL and ISO/IEC 17799 are complementary and can be used together. ITIL can be used to improve general IT processes and controls and ISO/IEC 17799 can be used to improve security controls and processes.
Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	An assessment and planning framework for security that enables companies to identify and analyze risks and develop a plan to mitigate those risks. The OCTAVE approach can be implemented using two assessment methods: one for large companies (OCTAVE Method) and one for small businesses (OCTAVE –S).	No	OCTAVE is an evaluation activity, not a continuous process. BS 7799, on the other hand, implements a continuous process for risk management and compliance based on the PDCA model. As such, an

			OCTAVE method could be created and incorporated into the planning segment of the PDCA cycle used in BS 7799
System Security Engineering Capability Maturity Model (SSE-CMM)	A model for assessing the security maturity level of an organization. Five security levels exist, from 1 (performed informally) to 5 (continuously improving). SSE-CMM does not describe a way of doing things but rather reports widespread practice.	No	Bs 7799 provides a process for the continuous improvement of information security. As such, SSE-CMM and BS 7799-certified organizations may seek to be recognized as SSE-CMM Level 5 organizations

7.2 Recommendations

We recommend that NCC sets up "Focus Groups". The purpose of these Focus Groups should be to meet periodically, analyze current problems facing manufacturers and service providers, and create recommendations to industry on what best practices can be implemented for improving the mission of that Focus Group. The result is methodical, and independently conceived, expert solutions that each Focus Group documents at NCC website, and publicizes through various public awareness and education campaigns. Focus Groups should publish best practice recommendations on improving the physical security of national Telecom and Datacom infrastructure. With the support of NCC, several best practice recommendations should be voted on for adoption and implementation by the telecommunication industry. Members can be made up of fifty-six senior representatives from Telecom, cable, Internet and satellite industries.

Focus Groups can include:

- Focus Group 1 – National Security
    - 1A – Physical Security
    - 1B – Cyber Security
    - 1C – Public Safety
    - 1D – Disaster Recovery & Mutual Aid
- Focus Group 2 – Network Reliability
- Focus Group 3 – Network Interoperability
- Focus Group 4 – Broadband

7.3 Recommended Specific Best Practices for the Telecommunication Industry

Table 7.4 Recommended Best Practices

Best Practice (BP) Number	Best Practice
6-0001	In areas of critical infrastructure, Service Providers, Network Operators and Equipment Suppliers should alarm and continuously monitor all means of

Best Practice (BP) Number	Best Practice
	facility access (e.g., perimeter doors, windows) to detect intrusion or unsecured access (e.g., doors being propped open).
6-0002	Service Providers, Network Operators and Equipment Suppliers should establish corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.
6-0003	Service Providers, Network Operators and Equipment Suppliers should consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.
6-0004	Service Providers, Network Operators and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.
6-0005	The electronic equipment area environments for Service Providers and Network Operators should be continuously monitored, controlled and alarmed to detect operating parameters that are outside operating specifications (e.g., equipment temperature, humidity).
6-0006	Service Providers, Network Operators and Equipment Suppliers should adopt a comprehensive physical security plan and design that focuses on providing an integrated approach that seamlessly incorporates diverse layers of security (e.g., access control and appropriate life safety systems, CCTV and recording, sensor technology, administrative procedures, personnel policy and procedures and audit trails).

Best Practice (BP) Number	Best Practice
6-0007	Service Providers and Network Operators should ensure outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) has adequate protection against tampering, and should consider monitoring certain locations against intrusion or tampering.
6-0008	Service Providers, Network Operators and Equipment Suppliers should establish additional access control measures that provide positive identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.
6-0009	Service Providers, Network Operators and Equipment Suppliers should periodically audit all physical security procedures and records (e.g., access control, key control, property control, video surveillance, ID administration, sign-in procedures, and guard compliance). Audits should include review of logs and records as well as testing of procedures through activities such as penetration exercises.
6-0010	Service Providers, Network Operators and Equipment Suppliers should periodically audit all data collection, software management and database management systems related to physical security including response plans.
6-0011	Service Providers, Network Operators and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points to include monitoring and recording for incident analysis. Where appropriate, consider providing near-real-time remote monitoring and archiving.
6-0012	Service Providers, Network Operators and Equipment Suppliers should establish access control procedures that: 1) Confirm identity of individuals, 2)

Best Practice (BP) Number	Best Practice
	Confirm authorization to access facility, and 3) Create record of access (e.g., written log, access control system log).
6-0013	Service Providers, Network Operators and Equipment Suppliers should provide audit trails on their electronic access control systems.
6-0014	Service Providers, Network Operators and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate property and invalidating access to all corporate resources (physical and logical) at the time of separation for employees, contractors and vendors.
6-0015	Service Providers, Network Operators and Equipment Suppliers should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing and proper displaying of ID badges, and the sign-in and escorting procedures where appropriate.
6-0016	Service Providers, Network Operators and Equipment Suppliers should include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility (e.g., facility location selection, security system design, configuration of lobby, location of mailroom, compartmentalization of loading docks, design of parking setbacks). Consider sign off authority for security and safety on all construction projects.
6-0017	Service Providers, Network Operators and Equipment Suppliers should establish policy and procedures related to access control to provide pre-notification of visits and exception access (e.g., emergency repair or response) to critical facilities.

Best Practice (BP) Number	Best Practice
6-0018	Service Providers, Network Operators and Equipment Suppliers should establish a procedure governing the assignments of facility access levels to ensure adequate levels of protection and the accountability of local responsible management for individual access based on risk and need for access.
6-0019	Service Providers, Network Operators and Equipment Suppliers should install environmental emergency response equipment (e.g., fire extinguisher, high rate automatically activated pumps) where appropriate, and periodically test environmental emergency response equipment (e.g., fire extinguisher, high rate automatically activated pumps).
6-0020	Service Providers, Network Operators and Equipment Suppliers should establish and implement policies and procedures to secure and restrict access to power and environmental control systems (e.g., air conditioning, air filtration, standby emergency power, generators, UPS) against theft, tampering, sabotage, unauthorized access, etc.
6-0021	Service Providers and Network Operators should establish and implement policies and procedures to secure and restrict access to fuel supplies against theft, tampering, sabotage, ignition, detonation, contamination, unauthorized access, etc.
6-0022	Service Providers and Network Operators should ensure critical infrastructure utility vaults (e.g., fiber vault) are secured from unauthorized access.
6-0023	Service Providers, Network Operators and Equipment Suppliers should consider ensuring that critical infrastructure utility vaults (e.g., fiber vault) are equipped to detect unauthorized access (such as the use of proximity and intrusion detection alarms). This might require coordination with local utilities.

Best Practice (BP) Number	Best Practice
6-0024	When guard services are utilized by Service Providers, Network Operators and Equipment Suppliers, a process should be developed to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.
6-0025	Service Providers and Network Operators should establish standards, policies and procedures to ensure that 1) the equipment and personnel from collocated Inter-connectors are restricted to defined collocation space and designated pathways, 2) Collocated Inter-connectors' access and equipment moves, adds, and changes (MACs) are actively coordinated by the host.
6-0026	For Service Providers and Network Operators collocation sites, the host should require all tenants to adhere to the security standards set for that site.
6-0027	Service Providers and Network Operators should consider establishing and ensuring dual transmission of all sensitive alarms and reliability of all communications links between the areas of critical infrastructure and monitoring stations in order to prepare for possible communication failures during emergency or disaster situations.
6-0028	Service Providers, Network Operators and Equipment Suppliers should base building designs for new construction, major modification and alteration for security should include consideration for the protection of and accessibility to air handling systems, air intakes and air returns.
6-0029	Service Providers, Network Operators and Equipment Suppliers should establish incident reporting and investigations program to ensure that all events are recorded, tracked and investigated. Reported information should be analyzed to identify potential trends.

Best Practice (BP) Number	Best Practice
6-0030	Service Providers, Network Operators and Equipment Suppliers should implement a tiered physical security response plan for telecommunications facilities that recognizes the threat levels identified in the National Security's Physical Security Alert Status Program.
6-0031	Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.
6-0032	A Service Provider and Network Operator tenant within a telecom hotel should meet with the facility provider regarding security matters and include the facility provider in the overall security and safety notification procedures, as appropriate.
6-0033	Network Operators should maintain the ability to detect the location of break-ins along optical and electrical transmission facilities.
6-0034	Service Providers, Network Operators and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.
6-0035	Service Providers, Network Operators and Equipment Suppliers should develop and implement procedures for video recordings and equipment that cover tape rotation, storage and replacement, assurance of accurate time/ date stamping, and regular operational performance checks of recording and playback equipment.
6-0036	Service Providers, Network Operators and Equipment Suppliers should consider compartmentalizing loading dock activities from other operations. As

Best Practice (BP) Number	Best Practice
	appropriate, the following should be considered: enhanced lighting, remote CCTV monitoring and recording, remote dock door closing capabilities and remote communications capabilities.
6-0037	Access to critical areas within Telecom Hotels where Service Providers and Network Operators share common space should be restricted to personnel with a jointly agreed upon need for access.
6-0038	The facility provider of a telecom hotel utilizing an electronic perimeter access control system should operate such systems with an up-to-date list of all personnel with authorized access to the facility and require periodic updates to this list from the tenants. Each Service Providers and Network Operators tenant of the telecom hotel should provide a current list of all persons authorized for access to the facility and provide periodic updates to this list.
6-0039	Service Providers and Network Operators should ensure availability of emergency/ backup power generators to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.
6-0040	Service Providers and Network Operators should periodically test fuel reserves for emergency/backup power generators for contamination.
6-0041	Service Providers and Network Operators should maintain sufficient fuel supplies for emergency/backup power generators running at full load for a minimum of 8 hours.

Best Practice (BP) Number	Best Practice
6-0042	Service Providers and Network Operators should tightly control access to the AC transfer switch housing area, and ensure that scheduled maintenance of the transfer switch is performed and spare parts are available.
6-0043	Where feasible, Service Providers and Network Operators should place fuel tanks underground. Access to fill pipes, vents, man ways, etc. should be restricted (e.g., containment by fencing, walls, buildings) to reduce the possibility of unauthorized access. Where feasible, fuel lines should be completely buried to reduce accessibility.

NCC should focus on National Security by ensuring the security and sustainability of public Telecom networks in the event of a terrorist attack or national disaster. The specific best practices recommendations above is clear and specific to industry for increased physical security at Telecom and Datacom sites, such as Data Centers, Mobile Switching Centers, and Outside Plant. The purpose of systematically identifying these Best Practices is to protect the nation's communications infrastructure against attack and to prepare for service continuation and disaster recovery should an attack occur. For these Best Practices to be implemented, Service Providers, Network Operators, and Equipment Suppliers must ensure that their current operations and security practices follow these Best Practices. And take action where there are deficiencies.

References

[1] UN World Summit on the Information Society Declaration of Principles and Plan of Action: www.itu.int/WSIS/

[2] Convergence and Next Generation Networks, Ministerial Background Report (OECD), 2007

[3] Unknown Vulnerability Management for Telecommunications, Anna-Maija Juuso and Ari Takanen,Codenomicon, February 2011

[4] Security in Telecommunications and Information Technology, An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications, ITUT, June 2006

[5] Holderegger, Thomas (2006): The Aspect of Early Warning in Critical Information Infrastructure Protection (CIIP), in: Dunn, Myriam and Victor Mauer (eds.): International CIIP Handbook 2006 Vol. II: Analyzing Issues, Challenges, and Prospects (Zurich: Center for Security Studies), p. 112.

[6] Juster Kenneth I. and John S. Tritak (2002): Critical Infrastructure Assurance: A Conceptual Overview, in: Joint Economic Committee, United States Congress: Security in the Information Age – New Challenges, New Strategies (Washington, DC: White House), p. 12.

[7] United States Government Accountability Office (GAO) (2004): Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors (Washington, DC: White House), p. 8.

[8] Poulsen, Kevin (2005): U.S. Info-sharing Called a Flop, in Security Focus, 11 February 2005. Available at: http://www.securityfocus.com/news/10481.

[9] Schechter, Stuart E. and Michael D. Smith (2004): How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks (Cambridge, Cambridge University Press).

[10] Alberts, Christopher et. al., "Introduction to the OCTAVE Approach." CERT Coordination Center.Available at *www.cert.org/octave/approach_intro.pdf* (Accessed 3 June 2005).

[11] BSI. “Information and Communication Technology: Frequently Asked Questions.”

Available at www.bsi-global.com/ICT/Security/faqs.xalter (Accessed 3 June 2005).

[12] BSI. Information security management systems—specification with guidance for use. 2002. Computer Security Institute. “2004 CSI/FBI Computer Crime and Security Survey.” Available at *www.gocsi.com* (Accessed 3 June 2005).

[13] Information Systems Audit and Control Association (ISACA). “COBIT Mapping: Mapping ISO/IEC 17799: 2000 with COBIT.” Available at *www.isaca.org/Template.cfm?Section=Research2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15056#cobitiso* (Accessed 3 June 2005).

[14] ISO/IEC. ISO/IEC 17799: Information Technology–Code of Practice for Information Security Management. 2000.

[15] META Group. “Unraveling Security and Risk Regulation,” white paper. January 2005.

[16] National Institute of Standards and Technology (NIST). “International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management – Frequently Asked Questions.”November2002.Available at *csrc.nist.gov/publications/secpubs/otherpubs/revisofaq.pdf* (Accessed 3 November 2015).

[17] Passori, Al. META Group. “CIO Primer for Three Standard Deviations,” 6 January 2005. Available at *www.metagroup.com/us/resCenter/displayResourceCenter.do?areaPrefix=ITLVM* (Accessed 12 December 2015).

[18] Rasmussen, Michael. Giga Information Group, Inc. “IT Trends 2003: Information Security Standards, Regulations and Legislation.” 5 December 2002. Available at *images.telos.com/files/external/Giga_IT_Trends_2003.pdf* (Accessed 15 September 2015).

[19] Roger L Freeman, Fundamentals of Telecommunications, 2nd Edition, Wiley 2005.

[20] Tarmo Anttalainen, Introduction to Telecommunications, Network Engineering, 2nd Edition, Artech House, 2003.

[21] Rogier Noldus, CAMEL, Wiley Editions, 2006.

[22] Regis J. Bates, GPRS: General Packet Radio Service, McGraw-Hill Professional, December 2001. Pierre Lescuyer and Thierry Lucidarm, « Evolved Packet System: LTE and SAE Evolution of 3G UMTS », Wiley 2008.

[23] Miikka Poikselkä, Georg Mayer, Hisham Khartabil, Aki Niemi, "IP Multimedia Concepts and Services in the Mobile Domain", 3rd Edition, Wiley, 2008.

[24] Alberts, Christopher et. al., "Introduction to the OCTAVE Approach." CERT Coordination Center.Available at *www.cert.org/octave/approach_intro.pdf* (Accessed 12 September 2015).

[25] Threats to Telecommunications Operators in Fragile and Conflict Landscapes. Availaboe at http://blog.willis.com/2014/10/threats-to-telecommunications-operators-in-fragile-and-conflict-landscapes/#sthash.ycmKjHMr.dpuf (Accessed 21 March 2016)

[26] Association of Telecommunication Companies of Nigeria (ATCON)

Annexure A: International Standard on SAM

The development of the International Standard on SAM is a global project led by Swedish

Standards Institute (SIS). The International Standard on SAM is unique as it combines process descriptions and software adaptations without the two parts being dependent on each other. When performing inventories of installed software, everything is scanned and the result is often difficult to understand due to the volume and complexity of information reported. The definitions in part two of the standard will enable identification to be simpler therefore making the inventory process more efficient and effective.

8.1 ISO 19770 Standard is the international standard on SAM. It is a two part standard, covering:

- Business issues (ISO 19770- 1): was developed to enable an organization to prove that it is performing SAM to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. It covers the processes and procedures for SAM planning, inventory control and software lifecycle management.
- Technical issues (ISO 19770- 2): technical specifications and metrics (under development) IS Governance framework entails SAM and is based on the following standards:
- ISO 27001 Information Security Management System.
- BS 15000 IT service management.

These standards mandate compliance with regulatory requirements for restricting copying of software in organizations.

8.2 ISO 19770 has six main sections:

- Control environment, which deals with processes, procedures, roles and responsibilities;
- Planning and implementation, which deals with resource required, reporting structure, measurement and verification;
- Inventory, which deals with selection and confirmation of assets, monitoring of existence, usage and storage;
- Verification and compliance, which deals with processes to identify and match inventory to licenses;

- Operations management, which deals with documentary evidence of implementation, and management of relationships with vendors;
- Lifecycle, which deals with software lifecycle management.

Abbreviations and meaning

Terms	Meaning
ITU-T	ITU Telecommunication Standardization Sector
NCC	Nigeria Communications Commission
IT	Information Technology
TSP	Telecommunication Service Provider
CDMA	Code-Division Multiple Access
HSPA	High Speed Packet Access
NGN	Next Generation Network
IMS	IP Multimedia Subsystem
OSS	Operating Support System
PSTN	Public Switched Telephone Network
PDH	Plesiochronous Digital Hierarchy
SDH	Synchronous Digital Hierarchy
D-WDM	Dense Wavelength Division Multiplexing
SS7	Signaling System 7
ISDN	Integrated Services Digital Network
ADSL	*Asymmetric Digital Subscriber Line*
EMSs	Element Management Systems
BSS	Business Support System
GSM	Global System for Mobile Communications
NSS	Network Subsystem
MSCs	Mobile Switching Centers
RAN	Radio Access Network
2G	Second-Generation Wireless Telephone Technology
UTRAN	UMTS Terrestrial Radio Access Network
CAMEL	Customized Application Mobile Network Enhanced Logic
VPN	Virtual Private Network
GPRS	General Packet Radio Service
WAP	Wireless Application Protocol
WEB	World Wide Web

FTTx	Fiber to the x
xDSL	High-Data-Rate DSL
Wimax	Worldwide Interoperability for Microwave Access
EPS (4G)	Evolved Packet System (Fourth-Generation)
EVDO	Evolution Data Only/Evolution Data Optimized
MGWs	Media Gateways
MGCs	Media Gateway Control functions
IS	Information System
ITIL	Information Technology Infrastructure Library
SAM	Software Asset Management
ISO	International Standard Organization
PDA	Personal Digital Assistant
IP	Internet Protocol
VoIP	Voice over IP
MSC	Mobile Switching Centre
HLC	Host Location Register
DMZ	De-Militarized Zone
ITU	International Telecommunication Union
VLR	Visitor Location Register
SIM	Subscriber Identity Module
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COBIT	Control Objectives for Information and related Technology
ISMS	Information Security Management System
PDCA	Plan-Do-Check-Act
SoA	Statement of Applicability
CCTV	Closed Circuit Television
SIEM	Security Information and Event Management
CCB	Closed customer base CERT Computer Emergency Response Team
CI	Critical infrastructures
CII	Critical information infrastructures
CIIP	Critical information infrastructure protection

CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response and Security Teams
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Center
IT	Information Technology
ITU	International Telecommunication Union
ITAA	Information Technology Association of America
WARP	Warning Advice and Reporting Point
OCB	Open customer base
PPP	Public-Private Partnership
SME	Small and Medium-sized Enterprise