IT Strategic Plan 2016– 2020

Office of the Auditor General of Nepal

Auditor General
of Nepal

Babar Mahal
PO Box 13328
Kathmandu
NEPAL

Foreword

Information and Communication Technology (ICT) is of critical importance to any organization irrespective of whether it is private or public sector entities. As the SAI of Nepal, the main objective of the office of the Auditor General of Nepal (OAGN) is to provide reasonable assurance on the use of Public resources to the Parliament and various stakeholders.

Use of ICT helps to make the work easier and work can be completed in quickly and economic manner. Use of ICT helps in different factors like development of policies, planning, performance management of audit, processing if the results of Audit and preparation of audit reports.

To develop the ICT capabilities, the OAGN needs to develop its own ICT Strategic plan. This is the first ICT Strategic plan of the office of the Auditor General of Nepal (OAGN). We believe that this strategy will greatly help us our day to day work resulting in greater efficiency in our work.

Utmost care has been done to make this guide error free. However, we will be grateful if the user could inform any suggestion on this guideline to the concerned Directorate of the OAGN.

At last, I would like to appreciate team of OAG Nepal, SOAGP and stakeholders who gave their efforts in the preparation and development of this guide.

(Sukudev Kharty)

Acting Auditor General

Telephone: 977-1-4262958 Fax: 977-1-4262798/4268309 E-mail: oagnep@ntc.net.np/infoag@most.gov.np Web: www.oagnep.gov.np

TABLE OF CONTENTS

1 BACKGROUND

In today's world the ability to use information and communication technologies effectively is crucial to the success of any organisation whether in the private or public sectors. In particular, Information Technology (IT) is of critical importance to the Supreme Audit Institution (SAI) of a country. As the SAI of Nepal, the main objective of the Office of the Auditor General of Nepal (OAGN) is to provide audit assurance on the use of public resources to the National Parliament and to the various stakeholders.

Information technology impacts the work of an SAI in several ways. The main business of the SAI is to provide high quality audit services. It is a well-recognised fact that use of information technology can dramatically increase the efficiency of the audit process. Information technology also helps an SAI to improve the efficiencies of its internal processes in areas like office automation, internal and external communications, accounting and human resources management.

As the auditing profession becomes increasingly technology-driven and knowledge-based, the OAGN must ensure that its employees have the right information technology resources to perform their work and to gather and share information. The information technology Strategic Plan provides direction for making best use of the information and communication technologies (ICT) for fulfilling its vision and for achieving its organizational goals.

1.1 Need for IT Implementation

Use of ICTwill enable OAGN to enhance the efficiency and effectiveness of the processes that support the delivery of the audit services including (a) development of policies; (b) planning, performance and management of audits; (c) processing of the results of audit and (d) preparation of audit reports. To manage these activities successfully, the OAGN intends to make effective use of available information by organizing it appropriately and taking advantage of the latest developments in information and communication technologies.

The need to effectively manage its present and future information is critical for OAGN in order to achieve its corporate goals and objectives. It must treat its information processing needs as a strategic issue and properly plan the use of information and communications technologies (ICT).

As a first step towards developing its IT capabilities, the OAGN needs to develop its own IT Strategic Plan. This is the first IT Strategic Plan of the Office of the Auditor General of Nepal (OAGN). The Information Technology Strategic Plan aims to establish the appropriate direction and means for the management of information within the organisation and must be aligned with the OAGNsCorporate Plan. Effective use of ICT and development of an IT culture throughout the organisation is an important goal for an SAI. TheIT Strategic Plan must have formal approval of the OAGN top management and it should be widely circulated amongst its staff and stakeholders.

1.2 The IT Strategic Planning Process

An organisation's investment in information technology must be effectively managed if the organisation is to achieve its strategic business objectives and gain a competitive advantage. The rapid pace of technological change is providing the organisation with increasing opportunities

for:

- Development of new products and services;
- Enhancing the value of existing products and services; and
- More effective delivery of product and services to its customers.

This equally holds true for public sector organisations. In order to achieve the intended objectives, the investments in information technology must be leveraged by proper planning of IT, efficient delivery of IT services and top management oversight. The need to strategically manage future information requirements is critical if the organisation is to achieve its corporate goals and objectives. The organisation's IT Strategic Plan is a blueprint of how ICT would be utilized to achieve its corporate objectives which are detailed in the organisation's Corporate Plan. Failure to plan strategically for IT may entail exposure to the following risks:

- failing to exploit the benefits of information technology in meeting business needs;
- failing to explore the potential benefits offered by new and emerging technologies;
- committing resources to following technical fashions rather than satisfying business needs;
- developing or acquiring incompatible systems which, through lack of standardisation, make it difficultto interconnect different systems;
- failing to allocate appropriate resources which may lead to project failure due to poor quality IT infrastructure or lack of people with the necessary skills;
- failing to prioritise work correctly;
- overlooking essential tasks (e. g. not addressing skills and training needs; failure to document systems; failure to produce contingency plans);
- Lack of co-ordination resulting in poor data integrity and the duplication of effort in system development and data capture.

2 MANDATE, VISION AND MISSION

Public sector external audit is an essential component of the public accountability and governance framework which ensures financial discipline, compliance with authorities, and reliability of financial reporting in the government. It also acts as an aid to the administration by analyzing the causes of financial irregularities and mismanagement and recommending measures for improving financial discipline, for ensuring better use of resources and for reducing the risks fraud, inefficiency and waste. The Auditor General is the constitutionally appointed independent external auditor of Government. As the independent external auditor of Government, the Auditor General is mandated by the Constitution to assist the National Parliament in exercising its oversight over the public purse.

The Auditor General (AG) heads the Office of the Auditor General of Nepal (OAGN) and the audit department which currently employs nearly 400 staff. In the system of parliamentary democracy, OAGN is the Supreme Audit Institution (SAI) of Nepal and therefore has a key role in the matter of ensuring accountability in the use of public resources and protecting the interest of the taxpayer.

2.1 Core business

OAGN's core business can be summarised by the following points:

- oversight of operations for public sector agencies through performance of financial audit, compliance audit, performance audit and other types of audits to determine whether public funds are spent efficiently, effectively, and in accordance with applicable laws;
- attestation of financial accountability of the government administration as a whole and analysis of the financing of government activities;
- attestation of financial accountability of all government and public sector organizations, involving examination and evaluation of financial records and expression of opinions on financial statements;
- audit of financial systems and transactions including an evaluation of evaluating internal controls and governance;
- assuring whether government agencies are in compliance with applicable laws and regulations; rules and procedures;
- audit of revenue with a view to assuring that it is assessed correctly, and collected and deposited to consolidated funds promptly;
- conducting investigations to into alleged illegal or improper activities; and
- providing assistance to the Parliament in support of its oversight and decision-making responsibilities.

The overall desired outcome of OAGN's work is a more results-oriented and accountable Government.

2.2 Corporate Plan 2016-2020

OAGN has developed its Corporate Plan2016-2020 which enunciates its mission, vision, core value and strategic goals.

OAGN Vision: We strive to be a Credible Institution in Promoting Accountability, Transparency and Integrity for the benefit of the people

OAGN Mission: Provide Independent and Quality Audit Service to assure our stakeholders that the public funds are efficiently used

The core values which drive OAGN's service delivery are:

- Independence
- Integrity
- Professionalism
- Transparency
- Accountability

3 KEY ISSUES AND CONSIDERATIONS

For an SAI the IT strategy should be formulated to support the achievement of its organisational goals and objectives. The overarching concern for all SAIs is to enhance the efficiency and effectiveness of the audit process and audit support systems through optimum use of technology. An associated objective is empowering the employees with IT equipment and tools, as well as with IT skills and knowledge so that they perform their jobs better.

The main business of an SAI is to provide high quality audit services and produce high quality audit reports. High quality in the provision of audit services is achieved when the audits are performed systematically and professionally in accordance with the auditing standards and that the audits assignments are properly planned and performed so as to optimise the use of resources. The adjective "high quality", when applied in case of audit reports has several dimensions including (a) the information contained in the audit reports meets the needs of the users, (b) the reports fully reflect the SAIs' responsibilities regarding assuring financial discipline and utilisation of public resources and (c) the message is conveyed in a language that is logical, free of jargon and easily understood by all the users of the reports and by the stakeholders.

For achieving the above objectives, an SAI has an elaborate system of processing and using information. Such information includes information about the audited agencies, about the audit personnel, financial systems, the physical locations of the offices to be visited by the audit teams etc. The main information processing cycle comprises the planning of audits, processing the results; follow up of the audit issues with the management of the audited agencies, and consolidating the important results in the annual audit report.

3.1 Key Issues

An SAI would need an IT based audit information management and support system for planning the audit assignments, scheduling audit staff and for processing the results of the audit up to the preparation and timely submission of the audit reports. The IT system of an SAI must also support a well thought out communication plan to meet the needs of internal and external communication using formal and informal channels.

The main purpose of the OAGN's IT Strategic Plan is to take stock of the present and future information processing and communication needs and commit resources for acquiring IT solutions

to meet the these needs. Clearly IT Strategic Planning is not a one-off exercise but a rolling process which continuously reviews the needs of the organisation and takes cognisance of the emerging technologies and upgrades the information technologies systems and solutions on an ongoing basis

Already the major auditees of the OAGN have implemented advanced IT based financial management systems, the most notable of them being the TSA system of the FCGO, the National Tax Authority and the nationalised banks. Over time not only the existing systems will be upgraded, but the few remaining organisations which are yet to computerise will do so in near future. The implementation of IT systems in the ministries, districts and agencies all of which fall within the audit jurisdiction of the OAGN has important implications for the audit process and procedures and for the skills and knowledge of its staff.

As an SAI implements IT solutions and makes greater investments in IT, the issues relating to IT governance assumes greater importance. IT governance should be an essential component of the overall governance structure of any organisation because it is an essential process needed to provide the right direction for resourcing, acquisition, deployment and management of IT systems and solutions for the achievement of the desired corporate objectives and achieving the intended efficiencies. Managing the risks arising from the use of IT is an important responsibility of IT governance. The IT governance structure and processes for the OAGN should consider the risks to information integrity and confidentiality and establish policies regarding appropriate use of IT, IT security, safeguarding of logical and physical information systems assets and business continuity.

3.2 Auditing in IT Environments

In view of the rapidly changing audit environment in which it operates, OAGN must introduce new auditing techniques and upgrade the skills of its staff to discharge its mandate efficiently and effectively. OAGN urgently needs to develop in house skills and expertise in auditing in IT environments including skills for reviewing IT system controls, accessing electronic data from auditees systems, and use computerised assisted audit techniques to support their audit work.

Use of IT by Government agencies poses both a challenge and opportunity to OAGN auditors. The challenge is to acquire the capacities to conduct audits in a computerized environment where records of transactions and the processing of financial information takes place electronically and the usual hardcopy audit trail may not be available. Fortunately, there is the opportunity to acquire the capability to conduct audits by means of collecting information from electronic sources. The availability of the data in electronic format opens the possibility of testing vast quantities of data using computers. Use of Computer Assisted Audit Techniques (CAATs) may result in significant enhancements in audit efficiency and effectiveness.

3.3 Existing levels of IT knowledge and skills

There are indications that amongst OAGN staff IT knowledge and skills are at a much lower level than that required for conducting audits in computerized environments. However, there exists

a small group of professional staff who are familiar with IT and IT auditing, having previously attended training courses on this subject. They can potentially be organized into an IT core group to provide leadership and to act as change agents for developing capacity in information technology.

3.4 Automating Audit Support Processes

The main business of OAGN is to provide audit services, and the audit process must be supported by essential activities like audit planning, management of staff and resources. Currently most of these support activities are based on manual procedures. Relying solely on manual processes adversely affects the efficiency of audit operations. Lack of information is a hindrance to effective planning and performance of audits. To manage these activities successfully, OAGN must make full use of information technology to organise and process information efficiently.

3.5 Risks

As regards the use of computerised information systems by the auditee organizations, OAGN faces the following specific risks:

- inability to conduct audits in complex IT environments such as the FCGO TSA (GIFMIS) system;
- failure to take advantage of IT to enhance efficiency of audits and internal processes;
- failure to adhere to the International Standards on Auditing and ISSAIs[1] in conducting mandated audits;
- inability to assure integrity, security and confidentiality of information – a responsibility of the statutory external auditor;

Unless dealt with appropriately, exposures to the above risks may severely undermine OAGN's effectiveness as the Supreme Audit Institution of Nepal.

3.6 Strengths, Weaknesses, Opportunities and Threats (SWOT)

SWOT analysis a proven technique which facilitates strategic decision making. The analysis given in Table 1 below summarizes the strengths, weaknesses, threats and opportunities as far as the use of IT in OAGN is concerned.

[1]International Standards for SAIs prescribed by the INTOSAI (International Organisation of Supreme Audit Institutions).

Table 1: Strengths, weaknesses, opportunities and threats

Strengths	**OAGN possesses the following strengths which create conditions that are conducive to implementation of IT based solutions and IT based auditing techniques**
Visionary top management	OAGN boasts of a forward looking top management possessing a vision for effectively implementing IT for enhancing the quality of performance. The newly appointed Auditor General is a public financial management expert possessing long years of experience and fully supports adoption of technology in OAGN.
OAGNCorporate Plan	OAGNCorporate Plan 2016-2020 adequately emphasizes the role of IT in meeting OAGN's corporate goals and objectives.
Awareness	There is a high degree of awareness amongst OAGN management cadre regarding the issues concerning application of technology in a SAI. Many of the senior members of OAGN management have attended a number of professional audit training programmes abroad and have been exposed to the benefits of following the international auditing standards and the use of IT for auditing purpose.
Potential of the IT core group	There are a number of highly motivated OAGN senior level staff who possess relevant information technology and IT audit qualifications. These individuals can potentially form an IT core group which can provide strong leadership in implementing IT initiatives in OAGN.
	Under the SOAGN project funded by the World Bank a large number of IT initiatives are being funded.
Weaknesses	**The following existing weaknesses must be remedied for successfully implementing OAGN IT initiatives**
IT knowledge level	Currently the level of IT literacy amongst the majority of audit staff is at a generally low level. General lack of IT knowledge and skills amongst majority of audit staff is a potential barrier to successful implementation of IT initiatives.

Limited success of past capacity building programmes	For various reasons, the achievement of the past capacity building programmes has been quite limited. It is possible that the environment was not yet conducive for implementing IT audit techniques and CAATs. However, in the current audit environment especially with the implementation of large scale computerisations in the Government, this has become unavoidable
Lack of resources	Lack of adequate budgetary support has remained a significant constraint for OAGN in implementing IT initiatives and procurement of computer hardware and software for its staff. This may be one of the main factors why the level of IT skills and knowledge amongst OAGN staff has remained at a relatively low level.
Lack of awareness regarding latest developments in professional auditing	OAGNhas taken steps to update its audit methodologies to take align them with international auditing standards. However the new audit manual is yet to be tested and implemented. As such most of the SOAGN staff are yet not conversant with the updated audit methodology. This is a barrier to the implementation of the audit techniques and procedures that are required for auditing in IT environments.
Lack of sustained professional development programme	This can be an hindrance to the implementation of auditing in an IT environment.
Opportunities	**OAGN must take full advantage of the following opportunities**
Opportunity to use automated techniques in IFMS and other environments	OAGN has an audit environment in which most major auditees including the FCGO (which processes 90% of all government accounting information) use computer based financial management and accounting systems. As such there is a huge opportunity to use automated audit techniques such as the CAATs which promises to increase audit efficiency and effectiveness considerably.

Electronic working papers and other audit software tools	OAGN should introduce audit management and electronic work papers software which will result in better management of audit resources
Donor assistance	Many of the donor agencies are interested in supporting the strengthening of governance and accountability framework and intuitional strengthening of institutions such as OAGN. This opportunities may be fully utilized to obtain resources for IT capacity building.
International training resources	Training programmes offered by INTOSAI, ASOSAI etc. can be gainfully utilised to develop OAGN IT and IT audit capacity
Threats	**If OAGN is unable to implement the required IT initiatives effectively, it faces the following threats**
Rapid computerization of the environment	Unless the capacity to conduct audits in computerized environment is developed together with necessary upgrades to its financial and compliance audit methodology quickly, OAGN faces a serious threat of losing its credibility as an SAI. The failures to modernise its audit techniques may also imply lagging behind the SAIs of other countries.
An outdated workforce	Failure to train its staff in IT and updated the financial/ compliance audit methodologies will result in an outdated workforce and obsolete audit methodologies seriously threatening OAGN's effectiveness as a SAI.
Lack of motivation of staff	Lack of motivation on the part of general audit staff to change and adopt IT based audit techniques is a threat

4 IT STRATEGIC MISSION, VISION AND GUIDING PRINCIPLES

4.1 OAGN Information Technology Mission

The strategic mission of information technology in OAGN is to optimise the use of information and related technologies to enhance and sustain the efficiency, effectiveness and quality of the services with a view to meeting OAGN's corporate objectives.

4.2 OAGN Information Technology Vision

The vision of OAGN is "To be a visible organisations in effectively using information and related technologies to provide superior quality services to the stakeholders".

4.3 Information Technology guiding principles

The following guiding principles will underpin the use of information and related technologies in OAGN:

- Information technology is used to support OAGN's mission by providing appropriate IT based solutions in a professional, effective, and timely manner;
- Information technology is integrated with OAGN business processes to develop user friendly, secure and flexible solutions to meet OAGN's operational and audit related needs;
- AnIT based workplace culture is developed whereby increasingly OAGN staff use computers to perform their tasks;
- OAGN staff are given secure access to all information and documents that they need to perform their respective tasks, in a digital format;
- Audit and operations related information is collected, stored, processed and distributed with a high degree of accuracy to facilitate effective management decision making;
- The IT systems resources are available to the users with minimum disruption;
- It is ensured that all investments made in information technology are focussed on meeting specific needs of OAGN staff and are cost effective;
- OAGN users are made aware of their responsibility regarding maintenance of IT security and good practices for defences against malicious software;
- Information technology is used only for appropriate purposes and the users are aware of appropriate use policies;
- Intellectual property rights are respected and only licensed software is used in OAGN;
- Ensure that the IT systems are sustained and supported by technically qualified, competent and motivated IT personnel; and
- Information technology is properly governed in order to effectively manage OAGN'sIT investments by developing, implementing and monitoring appropriate policies, standards and processes.

4.4 Technological Considerations

The following guiding technological considerations will be followed in taking IT related decisions:

- Standardise IT infrastructure, network administration and monitoring software, hardware platforms, operating systems, and database and application development platforms and develop appropriate institutional technical knowledge to support the IT infrastructure through professionalization, knowledge transfer and cross training.

- Minimise technical support by standardising application the user interfaces faces by developing a common look and feel for the customised solutions and assist the end-users to become self-sufficient through training and awareness campaigns.
- Use technology that is available and supported by authorised vendors and dealers in Nepal and encourage local software developers for customised solutions.
- Adopt best practices standards and methodologies in IT governance and control like CobiT for planning, acquiring, support and monitoring of technologies.
- Provide for data sharing across OAGN including the audit directorate and between applications and encourage sharing of resources like printers though the use of the network.
- Adopt an appropriate IT security model and implement an IT security management system to protect information assets and resources.

5. Information Technology Strategic Plan

The purpose of the OAGN IT Strategic Plan is to spell out the medium- and long-term strategies for using information and communication technologies for meeting corporate objectives and fulfilling its mandate. OAGN IT Strategic Plan is aligned with OAGN's Corporate Plan and aims to establish the appropriate direction and means for the management of information as well as for building capacities for performing audits in IT environments.

Recognizing the fact that IT has become an essential component of modern auditing practice and that its auditors need to acquire knowledge, skills and abilities required for conducting audits in IT environments, OAGN IT Strategic Plan seeks to develop capacity in terms of skilled human resources, creating an appropriate IT infrastructure and installing an automated information management system to respond to the challenges posed by OAGN's rapidly changing audit environment.

5.1 Objectives of IT Strategic Plan

The major objectives of this IT Strategic Plan are as follows:

- To create an appropriate technology infrastructure consisting of adequate number of computers and a local area network;
- To update and modernize OAGN's audit methodologies and procedures;
- To create a sustainable capacity in OAGN in auditing in a computer environment and use of advanced computer assisted audit techniques; and
- To acquire and implement computerised solutions for audit management, automation of audit workflow and communications to facilitate better management of audit resources and enhance efficiency and productivity of OAGN staff.

5.2 IT Strategic Goals

In order to achieve the above-mentioned objectives, the IT Strategic Plan identifies five (5) goals. These IT strategic goals form the basis for IT decision making for the next five years.

IT STRATEGIC GOAL 1	Build an appropriate Information and communication systems (ICT) infrastructure and sustain it by properly managing technology
IT STRATEGIC GOAL 2	To create an enabling IT environment and foster a workplace IT culture
IT STRATEGIC GOAL 3	Establish capabilities in auditing in information technology environments and using IT based audit tools
IT STRATEGIC GOAL 4	Design and implement solutions for automating audit support systems for enhancing efficiency and effectiveness of the audit processes
IT STRATEGIC GOAL 5	Institutionalize effective IT Governance to provide overall direction and for effectively managing IT investments, roles and processes

Each goal is supported by a number of objectives as indicated in Table 2 and Figure 1 on the following pages. The ensuing sections describe the initiatives and activities that will be undertaken with a view to achieving these goals and objectives.

Table 2: Strategic Goals and Objectives

GOAL	OBJECTIVES
Î@ IT STRATEGIC GOAL 1 Î@ Build an appropriate Information and communication systems (ICT) infrastructure and sustain it by properly managing technology	Î@ Objective 1.1 Build and sustain the ICT infrastructure
	Î@ Objective 1.2 Strengthen IT management capabilities
Î@ IT STRATEGIC GOAL 2 Î@ Create an enabling IT environment and foster a workplace IT culture	Î@ Objective 2.1 Provide staff with secure access to technology
	Î@ Objective 2.2Create IT security awareness
	Î@ Objective 2.3 Optimise the use of ICT to enhance productivity and enhance communication

Î@ IT STRATEGIC GOAL 3 Î@ Establish capabilities in auditing in information technology environments and using IT based audit tools	Î@ Objective 3.1Build capacity in information technology auditing
	Î@ Objective 3.2 Implement CAATs
	Î@ Objective 3.3 Implement EWP software suite
	Î@ Objective 3.4 Develop IT skills and knowledge through regular training and professional development
Î@ IT STRATEGIC GOAL 4 Î@ Design and implement solutions for automating audit support systems for enhancing efficiency and effectiveness of the audit processes	Î@ Objective 4.1: Design, develop and Implement AMMS software
	Î@ Objective 4.2: Acquire and implement solution for other support systems
Î@ IT STRATEGIC GOAL 5 Î@ Institutionalize effective IT Governance to provide overall direction and for effectively managing IT investments, roles and processes	Î@ Objective 5.1 Establish IT governance structure and sustain IT governance processes
	Î@ Objective 5.2 Adopt and implement standard frameworks and best practices for IT controls and information security management

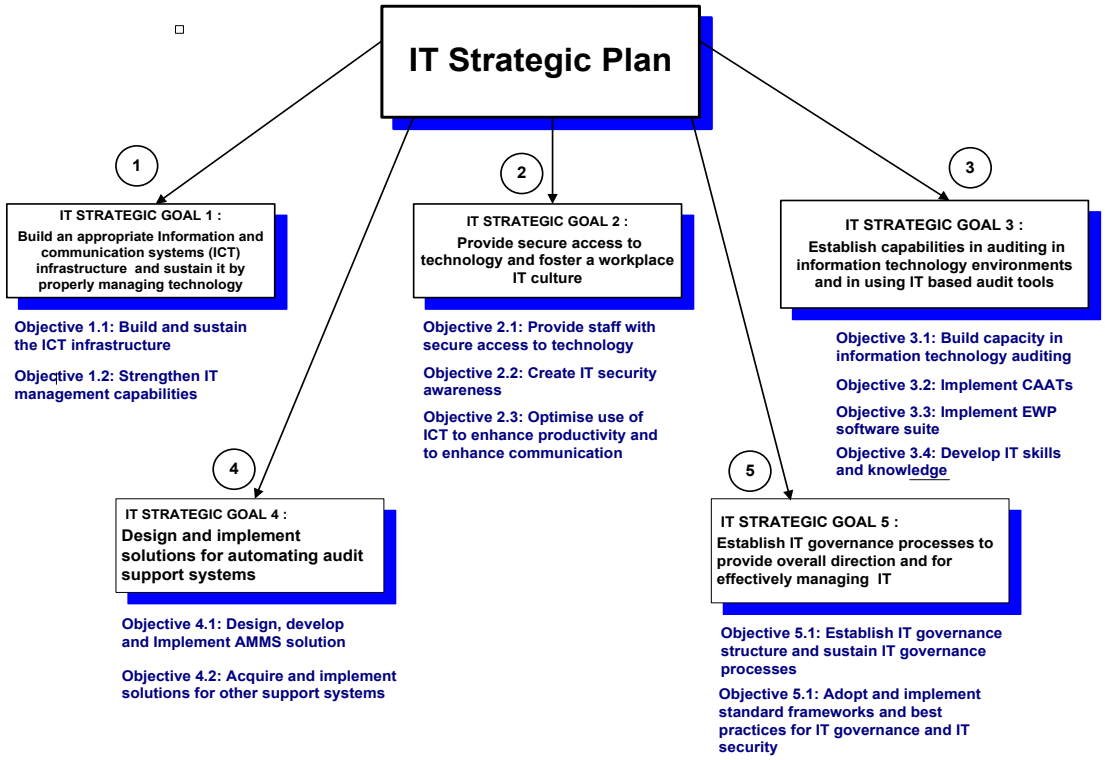

Figure 1: IT Strategic Plan, Goals and Objectives

IT Strategic Goal 1

Build an appropriate Information and communication systems (ICT) infrastructure and sustain it by properly managing technology

Installation of an appropriate ICT infrastructure is an essential pre-requisite for undertaking all IT related capacity building activities under the Strategic Plan. Therefore a major objective of OAGN IT Strategic Plan is to build ICT infrastructure appropriate to its needs.

GOAL	OBJECTIVES	ACTIVITIES
IT STRATEGIC GOAL 1 Build an appropriate Information and communication systems (ICT) infrastructure and sustain it by properly managing technology	Objective 1.1 Build and sustain the ICT infrastructure	1.11 OAGN network 1.12 Procure desktop, laptops and printers 1.13 Acquire software 1.14 Hardware inventory and media library
	Objective 1.2 Strengthen IT management capabilities	1.21 Strengthen MIS unit 1.22 Train IT support personnel 1.23 Establish IT help desk function

Objective 1.1:Build and sustain a state-of-the-art ICT infrastructure

The installation of a network has a visible impact by immediately improving internal communications through the use of email and by motivating OAGN staff to use computers. A network also enables the users to share information and resources such as heavy-duty multipurpose printers/scanners/photocopiers and back up important data files.

The completed network needs to be sustained through ongoing management of IT resources. It is necessary to regularly upgrade the information technology infrastructure to introduce newer versions of the operating system and scale the hardware to meet new demands on IT services. It is also necessary to plan for replacement of hardware components and computers.

This objective will be achieved by completing the following activities:

Activity 1.11 OAGN network phase 1

Under this activity an appropriate ICT infrastructure comprising a network (with the servers hostedat GIDC) will be built.

Activity 1.12 Procure desktop, laptops and printers

During the next five years OAGN will arrange for resources to procure additional computers with a view to providing access to computers to the maximum number of staff. Additional quantities of computer peripherals like network printers, scanners etc. will also be procured as required.

Activity 1.13 Acquire software

During the planning period the OAGN will additionally acquire various software tools necessary for increasing the productivity of audit staff such as communications software,

flowcharting software, statistical analysis packages, web publishing, report generator, etc. As a matter of policy use of licensed software will be strictly enforced.

Activity 1.14 Inventory of computer hardware assets inventory and media library

OAGN will provide topmost priority to maintaining and safeguarding its IT investments and its hardware and software assets. For this purpose a detailed inventory of the all information technology hardware and equipment will be made and a medial library of all software will be created. The assets will be maintained on an ongoing basis and there will be periodic review and stock verification to ensure physical security of the assets.

Objective 1.2: Strengthen IT management capabilities

In view of the importance of IT in OAGN, and the need to management technology properly, it is essential that OAGN has a permanent unit which will deal exclusively with IT issues, plans and implementation and to provide focus and direction to IT-related activities. For this purpose an IT Directorate will be established. The directorate will have two major functions:

a) Oversee the IT infrastructure and IT software applications; support the network, databases, website and intranet; and coordinate and equipping of all OAGN staff with adequate hardware and software tools.

b) Act as a central support group for IT audit, use of IT-based audit tools, such as CAATs (i. e. act as audit methods specialists/trainers in the IT area) and EWP[1].

The IT Directorate will include professionally trained IT technical staff (e. g. network administrators, maintenance staff and database administrators) who will be responsible for maintaining IT infrastructure and for ensuring the continued availability of the IT services.

This objective will be achieved by completing the following activities:

Activity 1.21 Strengthen MIS Unit

The scope of services of the IT Directorate will be expanded to enable it provide coverage to IT support functions as well as IT audit related functions. It will be positioned to provide leadership in “Auditing in IT environments”. In order to facilitate proper management of the MIS function, a formal charter has been developed. The charter spells out the objectives of the unit and provides the details of its duties and responsibilities. The charter is supported by the job descriptions of the MIS staff including the technical support staff. The charter and the job descriptions are attached to the UIT Strategic Plan as Annex A.

Activity 1.22 Train IT support personnel

The IT support personnel will undergo training on network administration and database

[1]Electronic working papers software

administration. It will be ensured that the personnel supporting the network upgrade their skills and knowledge through continuing professional training

Activity 1.23 - Establish IT help desk function

A help desk function will be established to provide user support and facilitate solutions to problems reported by the users. The help desk functions will be carried out in accordance with documented standard help desk procedures. In due course, in order to keep up with the expansion of the network and consequent increase in the number of users and applications automated help desk software will be procured.

IT Strategic Goal 2

Provide staff with secure access to technology and foster a workplace IT culture

Providing secure access to computing resources and fostering an "information technology culture" in the workplace is an important means for increasing the productivity of employees.

GOAL	OBJECTIVES	ACTIVITIES
IT STRATEGIC GOAL 2 To create an enabling IT environment and foster a workplace IT culture	Objective 2.1 Provide staff with secure access to technology	2.11 Provide secure access to the network 2.12 Provide universal email facility 2.13 Provide secure Internet access
	Objective 2.2 Create IT security awareness and implement IT security	2.21 Implement an organisation wide security awareness and training programme
	Objective 2.3 Optimise the use of ICT to enhance productivity and enhance communication	2.31 IT Human resources Development and training 2.32 Encourage use of IT in the workplace 2.33 Enhance OAGN website 2.34 Establish OAGN Intranet

Objective 2.1: Provide staff with secure access to technology

Providing OAGN employees with secure access to technology and computing resources is a primary focus of the IT Strategic Plan. The installation of OAGN network which can support up theusers is the first step towards achieving this objective.

This objective will be achieved by undertaking the following activities:

2.11 Provide secure access to the network

The procedure for allowing a user to logically access the system is commonly called the “log in procedures”. Login is a three-step process comprising (a) identification, (b) authentication and (c) authorization. The user goes through the first two steps by providing his identify to the system and providing a means of authentication whereas the authorization is performed by the system on the basis of predetermined rules. Use of password is the most common form of authentication. Certain best practices are followed to ensure that that the passwords of legitimate users are not compromised. People trying to guess others passwords and attempting to login with another ID – out of curiosity or with the intention to commit a wrong is unfortunately a common occurrence. The failed login attempts should be investigated by the IT security personnel and the legitimate users should be alerted. Procedures should be in place to address security incidents and remedy the control weaknesses.

Although in the initial phase, the number of workstations connected to the network will be limited and less than the total number of staff, all OAGN staff members will be created as users on the network. Employees who won’t have access to workstations of their own will be able to access the network from a common “cyber café” located in each audit directorate. In providing access to the network, security access controls will be implemented using the Active Directory. Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment.

2.12 Provide universal email facility

Email is one of the most commonly used applications on a network. Providing email accounts to maximum number of staff will not only improve intra-office communications but will also motivate the staff to use the network on a regular basis. Using Exchange Server 2010, email accounts using OAGN domain name will be provided to all employees. The email accounts will be accessible through OAGN network as well as through web-mail. The MIS unit will undertake capacity planning on a regular basis to ensure that sufficient memory is available to accommodate the archived emails.

2.13 Provide secure Internet access

Next to email, Internet is a major motivating factor for using the network. Internet is a valuable resource for the auditors for obtaining technical knowledge and to keep themselves up to date with the latest developments. Since the bandwidth available is always limited, it will be allocated amongst the various categories of users by means of a bandwidth management device appropriate to their respective needs. In providing access to the Internet, appropriate use policy for the Internet access will be developed and staff will be made aware of the policy in order to ensure proper use of the Internet resources.

Objective 2.2: Create IT security awareness & implement IT security

It is commonly acknowledged that information technology systems need to be adequately controlled because of the risks peculiar to computer environments. The objective of information security is "protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity."

There are three fundamental principles underpinning IT security:

- Confidentiality relates to avoiding unauthorised disclosure of information by taking measures such as encryption and access control;
- Integrity relates to preventingunauthorised modification of information throughmeasures such as input controls, logical access controls etc.; and
- Availability relates to ensuring continued service throughmeasures such as backup, disaster recovery controls etc.

Security controls are designed to collectively address all three of these core Information Securityprinciples. Security is very often compromised owing to lack of awareness amongst the end-users of IT systems.

This objective will be achieved by undertaking activity 2.21 Implement an organisation wide security awareness and training programme.

2.21 Implement an organisation wide security awareness and training programme

Information security awareness and training is critical to any organization's information security strategy and supporting security operations. IT security is the responsibility of not only the management or the MIS unit but it is a common responsibility of all employees.

OAGN will implement an IT security awareness and training programme to educate OAGN users about the importance maintaining IT security on an ongoing basis. Some of the indicative areas the awareness programme will educate OAGN users about are as follows –

IT security principles • Confidentiality • Integrity • Availability Security threats and risks • Unauthorised access • Damage to IT equipment • Theft and loss • Malicious software	IT security best practices • Secrecy of password • Password policies -Strong password. Periodic change of passwords, password version controls • Automatic logout • Logging of security events

The awareness programme will promote IT security best practices and will emphasise the need to behave responsibly and ethically. The programme will also provide instructions on appropriate responses to be taken on security incidents.

Objective 2.3 Optimise the use of ICT to enhance productivity and enhance communication

In order to achieve OAGN IT strategic goals and to develop an IT oriented workplace culture, it is necessary to raise the level of IT knowledge and skills through a massive training effort. Acquisition of basic IT skills and knowledge by OAGN employees is a pre-condition for implementation of other programmes under the IT Strategic Plan, i.e. implementation of CAATs, EWP and the audit management and monitoring system (AMMS) and building capacity to audit in IT environments.

It is also necessary to take effective measures to foster an IT culture in the workplace through encouraging communications using electronic media. Given the challenges required to make a transition from a situation characterised by limited use of computers to a highly digitalised paperless office system that is envisaged in the IT Strategic Plan, it is essential to encourageorganisation wide communication and to ensure that the motivation of OAGN staff to use IT on a day to day basis is sustained.

Communication patterns within an organization are largely influenced by the organizational structure. In any organization, communications flow in three directions—downward, upward, and horizontally. Downward communication consists of policies, rules, procedures, standards and administrative directives that flow from top administration to lower levels. Upward communication consists of the flow of performance reports, grievances, and other information from lower to higher levels. Horizontal communication is essentially coordinative and occurs between departments or divisions on the same level. Horizontal communication also comprises peer to peer information communication. External communication flows between the organization and a variety of stakeholders outside the organization.

For this purpose an internal communication plan will be developed which emphasizes upward and downward communication by means of using electronic media such as the email and the intranet.

2.31 IT Human Resources Development and Training

To achieve the goals of a high level of computer literacy amongst its staff, an organisation wide training programme on basic IT skills will be taken up. The curriculum of this training will be based the International Computer Driving License (ICDL) training programme for its staff. ICDL is an international accredited programme for developing basic computer literacy. The training areas covered by ICDL are:

Module 1: Concepts of Information Technology 1. General IT Concepts 2. Hardware 3. Software 4. Information Networks 5. Use of IT in Everyday Life 6. Safety and Security: Protecting Your Health, Data and Rights Module 2: Using the Computer and Managing Files 7. First Steps with the Computer 8. Working with Icons 9. Working with Windows 10. Working with Files and Folders 11. Viruses 12. Editing Text Files 13. Printing Module 3: Word Processing 14. First Steps with Word Processing 15. Basic Text Operations 16. Formatting 17. Tables, Graphics, and Other Objects 18. Word Processing Output	Module 4: Spreadsheets 19. Using the Spreadsheet Application 20. Cells 21. Worksheets 22. Formulas and Functions 23. Formatting Cells and Worksheets 24. Charts and Graphs 25. Preparing Outputs Module 5: Databases 26. An Introduction to Databases 27. Creating a Database 28. Retrieving Information Using Queries 29. Using Forms 30. Producing Reports Module 6: Presentation 31. Getting Started with Presentation Tools 32. Using Text and Images in PowerPoint 33. Slide Show Effects 34. Preparing PowerPoint Outputs Module 7: Information and Communication 35. The Internet 36. Web Navigation 37. Web Searching and Printing 38. Electronic Mail 39. E-mail Messaging

The training on basic IT skills will be continued in future internally by OAGN trained IT trainers

2.22 Encourage use of IT in the workplace

In accordance with the internal communication plan, OAGN management will make maximum use of the email and the intranet to send downward official communications to staff. OAGN staff will also be encouraged to make optimal use of email for official communications. The audit teams will be encouraged to write their reports using word processing software. The achieve the ultimate aim of a paperless audit environment,

audit software tools like electronic working papers software will be introduced (OAGN IT Strategic Objective 3.3).

2.33 Enhance OAGN website

A web site is an important tool for communicating with external stakeholders and making available information regarding the activities of the SAI. An important use of the SAI web site is to make available electronic copies of the published audit reports. The web site will be upgraded to contain information about SAI's objectives, legal mandate, profiles of key staff, FAQs, news-items, copies of audit reports, bulletin and so on

2.34 Establish OAGN Intranet

An intranet is an effective tool for improving internal communications and providing staff with access to important resources in a digital format. OAGN Intranet will be designed and developed. The intranet will contain a comprehensive collection of useful reference material such as audit manuals, guidance, training course, auditing standards and past audit reports and current audit files in electronic format. These can be accessed by the staff over the network. The intranet will also improve office-wide communication inasmuch as it will have an electronic notice board, staff contacts, information about training courses and meetings and so on.

Internal communication must provide mechanisms that recognize that employees not only have needs related to the workplace but also needs related to family, health, religious faith, community relations and gender-related needs. Therefore the Intranet will provide means for facilitating social interaction communicating and exchanging informal information amongst members of the staff through use of social events calendar, blogs, chat rooms and newsletters. Such channels will also enable OAGN management to receive feedback from employees on their concerns and problems related to their workplace as well as those they face in their family, health, religious and community environments and addressing these concerns.

Annex B provides an indicative list of the features and the content of OAGN intranet.

IT Strategic Goal 3

Establish capabilities in "Auditing in information technology environments" and using IT based audit tools

Creating capacities for "*Auditing in information technology environments*" is a key focus area of OAGN Corporate Plan 2016-2020 and is one of the major goals of the IT Strategic Plan. OAGN now faces a major challenge from the increased use of computer based financial management and accounting systems by its audit clients e. g. the FCGO's TSA system, the Nepal Rashtra Bank, the major nationalized banks and many of the state owned enterprises. In such systems much of the information and audit evidence are held in electronic format inside computer systems and therefore poses major challenges for the auditor to access this information and assess its reliability.

According to the international auditing standards for SAIs (ISSAIs), public sector auditors should possess the capacity to access electronic data from auditee's computer systems and analyzing the data using computer assisted audit techniques(CAATs). CAATs are used for both audit planning and audit examination purposes. The International Organization of Supreme Audit Institutions (INTOSAI) has also strongly advocated development of capacity in auditing in IT environments for its members. Absence of the capacity to conduct audits in IT environments may severely limit OAGN's effectiveness as a Supreme Audit Institution.

The introduction of automated financial management and accounting systems has a major impact on the way an audit organisation like OAGN performs its work. The impact can be summarised under four main categories:

- Changes in the audit trail and audit evidence:Collecting reliable audit evidence in a computerized system is more complex than in manual systems. Traditional paper based auditing techniques are not applicable in the online real-time environments where paper based audit evidence is mostly absent and the intermediate processes take place inside the system. Therefore the auditors should possess knowledge about functionalities of computer based systems and collectively possess the skills to access and analyse digital information from such systems.

- Changes in the type and nature of internal controls: A computerised financial management system must ensure integrity, confidentiality and availability of data and programmes and produce relevant and reliable information enabling the management to take informed decisions. In computerized environments the internal controls are generally more complex and technology based. The vulnerability of computers systems to errors, system failures, fraud and computer crime is an important consideration for the auditors. The ISSAIs prescribed by the INTOSAI make assessment of IT risks and evaluation of IT systems controls an integral part of the financial audit process.

- New audit techniques: In a computerised environment the auditor will need to adopt different audit approaches to gain sufficient audit evidence. The changes in the audit trail and in the nature of the audit evidence imply that the auditor may have to obtain and use specialised audit tools and techniques which allow the data to be converted and interrogated for the purpose of gathering audit evidence. The

new audit processes and procedures will invariably include the use of computer assisted audit techniques (CAATs).

- VFM review of IT investments**:** In view of the significance of the investments made in acquiring and operating computer systems, the public sector auditor needs to assure value for money from such investments.

The international auditing standards require that the auditors obtain an understanding of the auditee system functionalities and collectively possess the skills and knowledge required for conducting their audit in the complex IT environments.

Use of IT based audit tools like CAATs. can significantly enhance the effectiveness and efficiency of the auditors. However this cannot be achieved solely by providing training on the functionalities of the software. Procedures which make use of CAATs must be integrated into OAGN financial/compliance audit methodology.

Because of the highly technical nature of the functionalities of IT based audit tools and the nature of the issues, the in-house expertise in these areas will have to be developed amongst a relatively small group of people who will provide support to the general audit staff. For this purpose, a core group of knowledgeable and motivated individuals will be selected and developed as IT audit and CAATs specialists through intensive training and knowledge transfer. Because of the close link between IT audit techniques and financial audit procedures, the IT and financial audit core groups will have some common members.

Building capacity to conduct audits in IT environments has several dimensions:

- Build capacity to use of IT based audit tools and techniques like CAATs and integrate these into the financial/compliance audit methodology.
- OAGN staff must be given access to information maintained in electronic format inside the auditee system. It is a generally accepted principle that an SAI should have unfettered access to Government's financial information - whether held in paper-based or electronic formats.
- Develop capacity to conduct "IT systems audit",i.e. assess the risk arising from the use of IT and evaluate the information systems controls.
- The audit staffshould be empowered with IT based productivity and quality assurance tools like the electronic working papers (EWP) software.

Strategic Goal 3 is supported by four objectives as follows:

GOAL	OBJECTIVES	ACTIVITIES
IT STRATEGIC GOAL 3 Establish capabilities in auditing in information technologyenvironments and using IT basedaudit tools	Objective 3.1 Build capacity in information technology auditing	3.11 Establish IT audit core group 3.12 Develop IT audit manual and training course 3.13 Train core group 3.14 Integrate IT audit into financial/ compliance audit 3.15 Conduct pilot IT audits 3.16 Rollout IT audit training 3.17 Organise and manage IT audit
	Objective 3.2 Implement CAATs	3.21 Select CAATs software 3.22 Train core group 3.23 Establish data link with CGA systems 3.24 Track PFM developments 3.25 Data downloads from other important auditees 3.26 Integrate CAATs into audit cycle planning 3.27 Integrate CAATs into financial/ compliance audit procedures
	Objective 3.3 Implement EWP software suite	3.31 Acquire EWP software 3.32 Establish EWP champion group 3.33 Develop risk-based financial audit methodology and update the financial audit manual 3.34 Customise EWP solution and develop programme library 3.35 Conduct pilot audits using EWP and EWP library 3.36 Develop training material and EWP manual 3.37 Implement a EWP roll-out programme
	Objective 3.4 Develop IT skills and knowledge through regular training and professional development	3.41 Undertake an IT training needs analysis 3.42 Prepare training strategy and plan for IT capacity building

Objective 3.1: Build capacity in information technology auditing

Increasingly, government and public sector agencies in Nepalare using computerized financial management and accounting systems. Because of the risk and vulnerabilities of computer systems, the reliability of computerized data and of the systems that process, maintain and report these data are a major concern to audit. The international auditing standards make it mandatory for all auditors to assess the reliability of computer generated data and to evaluate IT systems controls. Therefore building capacity to perform IT audit (assessing IT risks, evaluating and testing IT system controls) is imperative for OAGN.

With the computerization of government accounts, IT has become inextricably linked to the "regular" financial/compliance audit process. It no longer becomes possible, for example, during a financial audit to make separate and distinct assessments of computer controls and manual internal controls – they are both part of one overall system of internal controls. OAGN auditor will need to evaluate the overall system of controls including IT controls.

In order to create an effective capacity in IT auditing the following activities will be carried out:

3.11 Establish IT audit core group

When auditing in an IT environment, the audit team should collectively possess the necessary skills and knowledge to evaluate IT systems controls and to use IT based audit tools like CAATs. All auditors should possess a certain basic level of knowledge of IT and information systems audit. However in view of the specialised nature of the knowledge and skills involved in the audit of complex IT systems, it is more efficient to establish a IT audit specialist group. Therefore as the first step towards building in-house capacity in IT auditing OAGN an IT audit core group will be established. The IT audit core group members will spearhead the initiative and provide leadership in IT audit capacity building on OAGN. In view of the close relation between IT audit and financial/ compliance audit, the respective core groups for IT audit and financial audit will have some members in common.

3.12 Develop IT audit manual and training course

An IT audit manual which provided comprehensive guidance on information systems auditing and a training course on IT audit will be developed. The IT audit training course will be developed for two levels of audiences. The IT audit fundamentals training course will be developed for the general auditors whereas the advanced IT audit course will aim at developing the IT audit skills and knowledge of the specialist IT auditors. The audit manual and the IT audit training courses will incorporate the guidelines provided by the INTOSAI IT audit committee. The manual will be tested through conducting pilot IT audits of systems such as FCGO TSA system.

3.13 Train core group

The members of the core group will first receive training in IT audit methodologies and in the use of IT based audit tools like CAATs. They will also be developed as trained trainers on this subject so that they are able to deliver training to the general audit staff

and members of OAGN management on the IT audit basics.

For capacity development in IT audit, it is necessary to create an IT audit/CAATs core group of champions. This group would be developed as subject matter specialists and trained trainers for sustaining the IT audit and CAATs activities in the OAGN. The various training this group would attend is as follows:

- IT awareness and IT systems used by auditees. Especially these group would receive training on functionalities of the CGA computerised accounting system;
- Fundamentals of IT audit;
- Basic and intermediate CAATs training; and
- Advanced IT audit.

3.14 Integrate IT audit into financial/compliance audit methodology

In accordance with the ISSAIs, assessment of risks arising from IT and evaluation of IT controls should be an integral component of the financial/compliance audit process. Clearlyit is not useful to conduct isolated IT audits but these audits should be linked to the financial audit process or conducted as part of the financial audit processes.

It is therefore necessary to upgrade OAGN's existing financial/compliance audit methodology in order toincorporate IT audit procedures into the standard financial audit methodology. The financial audit manual will be revised to provide clear guidance on (a)gaining an understanding of the auditee computer systems and associated risks, evaluate the IT controls andtest the IT controls respectively

3.15 Conduct pilot IT audits

The IT audit manual and the related audit methodologies (e.g. use of CAATs in audit planning and performance of financial/compliance audits) will be tested by means of conducting of pilot IT audit by the members of the IT audit core group. The lessons learnt from the pilot audits will be used to modify and upgrade the IT audit manual.

3.16 Rollout IT audit training

After the completion of the pilot audits the ITaudit training material will be finalised and the training will be rolled out to all audit staff of OAGN by the trained IT audit trainers.

3.17 Organise and manage IT audit

In order to properly organise and manage the crucially important IT audit function, a centralIT audit specialist group will be established within the IT Directorate. While all OAGN auditors should possess the capability to understand auditee computer systems and carry out a high level review of the IT controls, for evaluation complex network based IT infrastructure and advanced applications, specialised expertise will be necessary. This will be provided by the IT audit specialist group. When needed the general auditor will seek the assistance of IT specialist auditors. The IT specialist auditors will provide support to the audit efforts of the various audit directorates in the following areas

- Documenting complex IT systems in use by the auditees

- Evaluation and testing of controls of complex system
- Providing CAATs support
- The function of the IT specialist auditors will have been indicated at Annex –I.

3.18 Performance audit of IT

Performance audit of IT although a new and emerging audit area will be introduced in the long run to assess the economy of IT investments, efficiency and effectiveness of large and critical IT projects.

Objective 3.2: Acquire and Implement CAATs

Use of audit software and computer-based audit techniques allow the auditors perform complex tests and interrogations which would not be possible to be performed relying solely on manual procedures. The specialized techniques and software which the auditors nowadays use for this purpose are collectively known as Computer Assisted Audit Techniques (CAATs) or data analysis software. Computer assisted audit techniques enable the auditor to perform many of the previously manually intensive tasks both quickly and efficiently allowing savings in time and cost for the auditing a computerized accounting environment. The use of audit software tools enable the auditor to access financial data held inside auditee computer systems and perform a wide variety of tests for achieving the audit objectives.

CAATs may be used by public sector auditors for conducting financial audits and systems audits. In particular, CAATs is an important tool for conducting risk-based financial audits because it enables the auditor to identify high risk account areas and transactions through spotting of unusual patterns and exceptions by analysing large quantities of financial and operational data. CAATs also enable performance of tests of control and substantive procedures where there are no input documents or a visible audit trail, or where population and sample sizes are very large. Additionally, CAATs may also be used for other types of audit work like performance audits, compliance audits and forensic audits. CAATs are also used by IT security professional for IT security management and IT audit purposes such as analysis of security logs. Use of CAATs (Computer Assisted Audit Techniques) software can potentially enhance the efficiency and effectiveness of audit planning and performance process because it enables the auditor to interrogate entire populations of digital data, choose audit samples more scientifically and perform a wide variety of analyses.

The International Standards for Supreme Audit Institutions (ISSAIs) emphasise the benefits of using CAATs and strongly recommends their use when conducting financial/ compliance audits in computerised environments.

There are some essential conditions must be fulfilled for successful implementation of automated audit techniques like CAATs:

- First,since CAATs is basically adata analysis software, the auditor should have the ability to access the financial and operational data held in digital format inside

auditee computer systems

- Second, because CAATs is a tool used by the auditor to enhance the efficiency and effectiveness of the audit process, the use of CAATs must be integrated into the regular financial/compliance audit procedures.
- Third, the financial/compliance methodology must be aligned with the international auditing standards i. e. the ISSAIs.

In order to effectively implement CAATs across OAGN the following activities will be carried out under the IT Strategic Plan:

3.21 Select CAATs software

IDEA, a popular CAATs software package, has already been in use in OAGN. However during the planning period OAGN will also explore the possibility for introducing other CAATs software if considered necessary.

3.22 Train core groups

Because of the highly technical nature of the tasks involved in downloading of data from different types of computer systems, planning and operating the CAATS, an SAI should have a group of CAATs specialists. The CAAT specialists will have a very important role to establish procedures for downloading data from different platforms, developing CAATs procedures and supporting the audit directorates in applying CAATs in various situations.

The IT audit core group will provide leadership in implementing CAATs in OAGN and will act as in-house CAATs experts. As such at first the members of this group will receive training on CAATs and its application in audit. However since use of CAATs is closely linked to the financial/compliance audit process, the members of the financial audit core group and members of OAGN management will also need to undergo training in order to understand the applications of CAATs in the financial/compliance audit process and to acquire basic skills.

3.23 Establish data link with FCGO systems

One of the essential conditions for using CAATs is that the auditors must be given access to financial and accounting data held inside the audited agency's computer systems. Before CAATs software can be used, the auditors need to download relevant data from the auditee computer systems to their own computers. The best practice in this regard is to provide the auditors with online access to the computer system by treating them as valid users with login IDs and passwords. However the user profile of the auditors should provide for read only access to records for the purposes of checking and verification only and they should not be given the privilege to alter the records.

Auditors as valid users of the government's information technology systems, auditors should have logical access and privileges to view, examine and download digital records albeit on a read only basis. Auditors cannot do their jobs solely on the basis of standard reports printed from the computerized system because limited reliance can be placed on printed reports. Furthermore reports are not amenable to CAATs analysis. Direct access to the data in digital format provides the best assurance to the auditor that the data has not been changed or altered in any way to represent a misleading picture of the state of affairs.

In order to provide better oversight of public expenditure by the Auditor General, it essential that OAGN network is connected to the FCGO systems and OAGN is given unfettered access to the FCGO systems. For this purpose an optical fibre link has been established between OAGN and the FCGO. Under the SOAGN project the techniques for downloading data from the TSA system and its analysis using IDEA will be developed and selected OAGN staff will be trained in using these techniques.

3.24 Track PFM developments

Under the various development and capacity building initiatives, the public financial management (PFM) systems and supporting accounting applications for the Government of Nepalare being upgraded. As the external auditor of the Government, the AG would need to be kept informed about the changes in the PFM systems and the upgrades made to the information technology systems. In particular it will be necessary for OAGN to ensure that the new systems are auditable[2.]

In a computerized system, a visible audit trail is not present as the records are maintained electronically and the processes by which initial transactions get summarized in the financial statements are not immediately transparent. Therefore it is necessary to build a usable electronic audit trail into the computerized system during the system development stage itself otherwise it may be prohibitively expensive and impractical to build the audit trail after the system has become operational. The computerized financial management application packages that are commonly used nowadays can provide an electronic audit trail (this needs to be specially activated) and also provide other facilities for the auditors to examine the records and produce standard and ad hoc reports from the system. It is a valid expectation that OAGN auditors should be given the opportunity to use such facilities and be trained in using these advanced computer based audit techniques.

In view of the above considerations, OAGN will maintain ongoing communication with FCGO and Ministry of Finance regarding the PFM reforms to ensure new IT based system contain adequate audit trails and IT system controls.

---

[2]Auditability is largely dependent on the existence of an audit trail in the system. Audit trail refers the paper or 'electronic' trail that enables the auditor to drill down from an account balance and trace financial data to the source transactions. Existence of an audit trail is a precondition for conducting audits. In a non-IT system a hardcopy paper based audit trail is available in the manually maintained accounting books and records which provide for easy tracing of a transaction to its final summarization in the financial statement and vice-versa.

3.25 Access to other auditee systems

As with the CGA system, it will be essential to establish standard procedures for data access and data downloads the IT based financial systems of major audit clients. However, it needs to be emphasized that the auditors should be given access to financial records for the purposes of checking and verification only and they should not possess the right or the capability to alter the records. Accordingly, in an electronic environment, the auditors should be given access to the system on a read only basis and it should be ensured that the auditor's activities should not interfere with the normal functioning of the system. In modern computerized systems such facilities can be easily provided through giving theauditors restricted logical access, thus providing assurance to the system owners, custodians and end-users,that auditor's activities willin no way interfere with their duties and will not affect system performance or data integrity.

Early in the IT Strategic Plan period, the IT Audit directorate will work together with the concerned Directors General of audit and the auditee institutions to establish standardised agreed upon procedures to obtain secure access to auditee computer systems and to download digital information for audit purposes.

3.26 Integrate CAATs into audit cycle planning

Use of CAATs can result in significant improvements in the annual audit cycle planning process in the Audit Directorates. Analysis of digital records of transactions obtained from the FCGOsystems can help identify risky and high value transactions which can be used to determine the frequency of the audit of the various units and for providing the audit teams with prior information.

For this purpose the use of analysis of TSA systems data and CAATs must be integrated into the annual audit cycle planning process in the respective directorates. The following necessary activities will carried out accordingly under the IT Strategic Plan:

- Create awareness about the usefulness of CAATs in annual audit cycle planning amongst the senior officers in the Directorates and amongst those responsible for planning by holding CAATs training; and
- The IT audit core group will work with the senior managers in the Audit Directorates to introduce the necessary changes in the audit cycle planning process and document the same.

3.27 Upgrade financial/compliance methodology and Integrate CAATs

In order to effectively conduct audits in an increasingly computerised audit environment, the OAGN must institutionalise related audit techniques such as IT audit (*IT risk assessment and testing of IT controls*) and CAATs by fully integrating these techniques into its financial/compliance audit methodology. For this purpose the OAGN will upgrade

the existing financial/compliance audit methodology to align it with the international auditing standards. In the public sector context, “Auditing in an IT environment” is not a separate variety of audit but signifies using methods and IT based tools to conduct “Financial/Regularity audits” when the audited body is using information technology systems. Therefore upgrading of the financial/compliance audit methodology is an essential prerequisite before the IT based techniques can be fully integrated in the audit methodology to obtain the intended benefits.

The existing financial/compliance audit methodology of the OAGN needs to be upgraded in order to ensure adherence to international standards on auditing and for assuring quality of the audits. An audit methodology is a step-by-step structured approach to conducting an audit. The audit methodology provides the overarching structure for developing the detailed audit procedures and audit programmes. One of the benefits of developing a structured financial audit methodology will be that it will facilitate migration of the audit steps and programmes to an electronic working papers software platform with relative ease.

OAGN financial audit and IT audit core groups will work together with the Audit Directorates to upgrade and implement a risk-based financial/compliance audit methodology and audit programme which incorporate use of CAATs in audit planning and audit testing. The new methodology will be tested in field through conducting pilot audits.

3.28 Roll out CAATs training

According to the ISSAIs, it is desirable that the general auditors should possess basic knowledge of IT audit and CAATs. After the procedures for using CAATs for financial/ compliance audit planning and testing have been developed, basic level CAATs training will be rolled out to the majority of OAGN officers and staff by trained trainers.

Objective 3.3: Implement EWP solution

Increasingly auditors are using a variety of software tools for automating the audit related business processes of maintenance of audit working paper files, quality assurance and review, preparation of audit reports, audit planning, audit issues management, time and cost management etc. Use of audit software tools like the electronic working paper (EWP) is known to significantly increase the efficiency and quality of audits. It takes out the drudgery out of the audit documentation process enabling the auditors to concentrate more on performing the audit proceduresOne of the important benefits of using an electronic work papers solution is the need to have a fresh look at the audit methodology and upgrade the audit programmes and work-paper templates used during an audit.

The EWP software contains functionalities which enable the auditors to perform their work in accordance with a standard audit methodology, record their findings electronically and enable an audit team to work in a distributed fashion. It is a generic software containing various functionalities like recording of audit work done, rising of audit observations, replication, online review of audit working papers by the audit supervisor and so on.

Implementation of the electronic working papers implies migration of the audit process, recording of work and review of working papers from a manual environment to a paperless environment. Use of standardised templates, the ability of the EWP software to generate reports from the observations recorded electronically and the facility to share work and review the audit working papers electronically, significantly enhances the efficiency the audit work and quality of the output.

Because of the structured approach and use of technology, use of EWPs significantly enhances audit efficiency and effectiveness. It also helps adherence to the auditing standards and therefore it is an effective tool for audit quality assurance.

In order to effectively implement a EWP solution in OAGN the following activities will be carried out under the IT Strategic Plan:

3.31 Acquire EWP software

An appropriate EWP software solution will be acquired after evaluating the various COTS[3] packages which are available commercially.

3.32 Establish EWP champion group

The best practice for implementation of EWP software is to establish a champion group which will provide leadership in developing the audit methodology and audit programmes and test out methodology together with the customised software in the field. Typically it is the members of the EWP champion group who first receive training on the functionalities of the software and eventually become in-house trainers. Having in in-house expert group facilitates that significant change management effort that is required for gradually moving to a paperless audit environment.

3.33 Develop risk-based financial audit methodology and Update financial audit manual

In order to use the EWP software, the software must be customised and an electronic manual containing the standard audit procedures, audit programmes, risk assessment tools, working paper templates, audit checklists, ICQs, etc. must be created and integrated into software. The first step towards implementing an EWP solution is to develop an appropriate "*audit methodology*".

An audit methodology is a step-by-step approach to conducting an audit with well-defined phases e. g. audit planning and risk assessment, testing, reporting and so on. Typically the "Financial/Regularity audit" is more amenable to be implemented using TeamMate, because a structured methodology can be developed in accordance with the international standards on auditing. Upgrading the existing financial audit methodology to risk-based methodology aligned with the international auditing standards and the revision of the financial audit manual is an essential condition for implementing a EWP solution as it is for implementing the techniques for auditing in IT environments.

[3]Commercial Off The Shelf (COTS)

In order to implement the EWP solution, the existing financial/compliance audit methodology will be upgraded to align it with the international auditing standards (ISSAIs) and the audit manual will be revised.

3.34 Customise EWP and develop library

In order to use EWP, the software must be customised and the standard audit procedures and audit programmes must be inserted into the software. As mentioned, the first step towards implementing TeamMate is to develop an appropriate "*audit methodology*". The various phases of the financial/regularity audit methodology are further decomposed into audit procedures and audit steps. For each of the audit steps it is necessary to develop the detailed procedures and guidance. It is also necessary to design and develop document templates and tools like ICQs etc. , which are attached at appropriate places for recording the results of audit. Collectively all these are put together to form a "EWP library".

The EWP software will be customised and audit procedures libraries will be developed. Initially in the implementation process, a very significant amount of effort goes into developing an appropriate audit methodology and the electronic work procedures and working paper templates library. However once the library of procedures has been developed, it facilitates the audit process by providing structured guidance on performing various the audit procedures

3.35 Conduct pilot audits using EWP and EWP library

The EWP library will be tested by conducting pilot audits by the EWP champions. The lessons learnt from the pilot audits will used to modify and upgrade the EWP library.

3.36 Develop training material and EWP manual

The risk-based audit methodology and EWP library will be pilot tested in the field by the EWP champions. After pilot testing, the training material on the software and the manual will be developed. The training on the EWP solution will include the training on the navigation and functionalities of the EWP software and that on the use of the financial/regularity audit library.

3.37 Implement a TeamMate roll-out programme

Successful implementation of a EWP solution, which may involve radical modifications in the audit processes and work practices resulting from a changeover from a manual audit environment to a paperless, generally entails a massive change management effort. For this purpose active involvement of the SAI top management to provide effective leadership and direction to bring about the changes and manage the risks, is an essential condition. .

The training on the EWP solution and the EWP library will be rolled out to the audit staff of OAGN. The objective of the EWP roll-out programme will be to ensure that larger number of audit staff use the EWP solution and the risk-based financial/compliance audit methodology in performance of their mandated audit work.

Objective 3.4 Develop IT skills and knowledge

The training requirements for OAGN staff in connection with development of capacity in IT auditing are extensive and diverse. For example the IT audit specialists of OAGN not only should possess a good understanding of not only ofthe processes and functional modules of the auditee computer systems (e. g. TSA system of FCGO), but also of the underlying ICT infrastructure comprising the network, hardware, system software, database and network components, and the facilities, the policies and IT organization and the risks, to be able to review the entire range of IT general and application controls as prescribed by the international standards on auditing. The general audit staff should possess basic knowledge about IT based financial management systems, IT risks and controls, risk based financial audit methodology and CAATs.

Keeping the above considerations in mind, a number of different but interlinked training course modules will be designed, developedand delivered.

Under this objective the following activities will be carried out:

3.41 Undertake an IT training needs analysis

As the first step towards planning and delivering training, a training needs analysis (TNA to identify the gaps in the IT skills and knowledge will be undertaken. Results obtained from any previously held TNA will be updated.

3.42 Prepare training strategy and implement plan for IT capacity building

To be able to conduct the regular annual financial and regularity audits of Ministries and Local Authorities covered by the FCGO TSAsystem and to be able to conduct an evaluation of the information systems controls, OAGN auditors need to acquire collectively a fairly wide range of skills and knowledge. Therefore training will be planned and delivered in the following areas:

- Developments in information and communication technologies, IT processes IT risk, control and security issues. IT governance and quality assurance
- Operation of the auditee financial management and accounting systems
- Review of IT general controls relating tosecurity, data integrity, confidentiality, availability, IT organization, system development and change controls, business continuity, facilities and network controls
- Review of application controls over completeness, accuracy and validity of data input and control over data files
- Ability to use the system interfaces to query and download information
- Use CAATs to test and analysis data, use audit sampling techniques
- Use automated audit management tools like TeamMate to perform the audits

Considering the fact that the exposure to OAGN staff to these types of advanced auditing techniques has been rather limited in the past, capacity building in IT and ITauditing will require a sustained training effort over the entire period covered by the IT Strategic Plan. The training will be given delivered at two levels

(a) Basic IT audit/CAATs. EWP courses for OAGN management and general

audit staff and

(b) Advanced courses for the members of the IT specialist groups

The training will also have to be delivered in a phased manner. In the first phase of the training programme, the members of the IT specialist groups and members of OAGN management cadre will attend awareness workshops, which will sensitize them on the impact of the IT on auditing and the impact of public financial management (PFM) reforms on OAGN auditing processes. They will also undertake training on the functionalities of the major auditee computer system like the IBAS. Additionally,

Training of OAGN general audit staff on basics of IT audit and CAATswill be organisedon an on-going basis.

In the second phase of the training programme, members of the IT specialist groups will attend advanced level training courses on IT audit, CAATs and on using data link with CGA IBAS system.

In the third phase of the training the focus will beon advanced techniques like statistical sampling for audit, audit management software suite and advanced IT auditing. Table 3 provides an indicative list of training courses that will be delivered.

Table 3: IT Capacity Building Training Courses

Description of Training Course	Duration in Days	Number of Courses to Be Delivered	Number of Trainees
Auditing in IT environments – CAATs/ IT audit training for members of the core groups	5	3	24
Basic IT audit/CAATs/auditing in IT environments for BCS officers	5	4	20
Basic IT audit/CAATs/auditing in IT environments for BCS probationers	10	1	20
Basic IT audit/CAATs/auditing in IT environments for AAOs & Superintendents	5	10	20
Training for expert core trainer group -Statistical sampling & audit testing	5	2	20
Training for trainer (TOT) course for OAGN expert core trainer group	3	2	20
Advanced IT audit for specialist IT auditors	10	2	20

Description of Training Course	Duration in Days	Number of Courses to Be Delivered	Number of Trainees
Advanced CAATs training for specialist IT auditors	10	2	20
Training on EWP and Risk based financial/compliance audit for core groups	10	2	20
Training on EWP and Risk based financial/compliance audit for BCS cadre officers with emphasis on using EWP for audit supervision	5	2	**20**
Training on EWP and Risk based financial/compliance audit for AAOs & Superintendents	5	10	**20**

3.43 Professional development

It is essential that OAGN audit staff especially the members of the IT audit, financial audit and EWP core group are encouraged to acquire relevant professional qualifications. A policy for professional development and certification will be developed. In accordance with this policy OAGN staff will be encouraged to obtain and sponsored for professional certification programmes.

IT Strategic Goal 4

Design and implement solutions for automating audit support systems

A number of applications will be implemented over OAGN network for enhancing efficiency and effectiveness of the audit processes. This goal is supported by two objectives:

GOAL	OBJECTIVES	ACTIVITIES
IT STRATEGIC GOAL 4 Design and implement solutions for automating audit support systems for enhancing efficiency and effectiveness of the audit processes	Objective 4.1: Design, develop and Implement AMMS software	4.11 Develop user requirement specs and design 4.12 Acquire and implement the AMMS solution
	Objective 4.2: Acquire and implement solution for other support systems	4.21 Acquire and implement a document management system 4.22 Acquire and implement audit support solutions

Objective 4.1: Design, develop and Implement AMMS software

One of the main applications to be implemented will be the automated audit follow up and monitoring system (AMS)The AMS is be a computerized database application that will help the audit directorates to monitor and track disposition of the large number of audit observations. The AMMS will enhance the efficiency and effectiveness of the audit management process and will facilitate production of better quality audit reports.

4.11 Develop user requirement specs and design

In the design, development and implementation of the AMS a system development life cycle methodology (SDLC) will be followed. As per the SDLC approach, at first the user requirement specifications for the AMMS will be captured and a solution design will be developed.

4.12 Acquire and implement the AMMS solution

The AMMS solution will be acquired by awarding the work to a competent local software developer through competitive bidding process. It will be a bespoke system using the following platform.

1. Solution development - ASP. NET with C#
2. Web based user interface - Internet Explorer or Mozilla Firefox
3. Database - SQL Server 2008
4. Report generation - Crystal Report for Reporting, exporting facility to Microsoft Word, Excel, etc.

After the AMS solution is developed, it will be subjected to user acceptance testing. The AMS user manuals will be developed and the users will be trained in its use. The AMS will be necessarily implemented after OAGN staff have acquired basic computing skills otherwise there is a risk that the new solution won't be embraced and used by them.

Objective 4.2: Implement solutions for other support systems

4.21 Acquire and implement a document management system

A electronic document management system (EDMS) is a software solution that helps an organization capture, store andtrack important documents whether electronic or scanned copies of paper-based documents. Given the nature of work of OAGN, it is essential that an EDMS is deployed over the network to capture, store and archive the different types of documents generated by OAGN during the course of its business. The document management system will enable OAGN to systematically file the documents and enable OAGN staff to locate documents through a full search capabilities including searching document by title or by text search capabilities. By planning the format, content and flow of documents in the EDMS OAGN organization can take effective steps towards the implementation of a paperless office.

An appropriate EDMS software solution will be chosen and implemented in OAGN. The various categories of documents generated by OAGN which can be stored and searched using an EDMS are as follows:

Document generated by the audit process

- Annual audit cycle plan by the various audit directorates
- Audit Inspection Files Local Audit Report (LAR)
- TeamMate project files generated by the field audit teams
- Individual audit observations
- Audit queries issues to the auditee and replies received
- Serious Financial Irregularities (SFIs)
- Advanced paras
- Minutes of tri-partite discussions
- Audit reports

Documents relating to the administrative processes

- Office orders
- Notifications
- Sanctions of leave documents
- Departmental budgets
- Periodic reports submitted by the Audit Directorates to the Office of the CAG

4.22 Acquire and implement solutions for support systems

After carrying out user needs surveys, OAGN will acquire IT based solutions for other support systems such as accounting and budgeting, human resources management etc.

IT Strategic Goal 5

Institutionalize effective IT Governance to provide overall direction and for effectively managing IT investments, roles and processes

IT Governance has been defined as "*an integrated part of Corporate Governance. It is the responsibility of the board of directors and executive management and consists of the leadership and organisational structures and process that ensures that the organisation's IT sustains and extends the organisation's strategy and objectives*. "[5]

[5]Definition given by IT Governance Institute (part of ISACA

In today's world, ability to use information and related technologies effectively is a key success factor for almost all types of organizations. IT governance seeks to integrate IT related issues in the standard governance framework. Generally speaking IT governance is the process by which the top management and those in charge of governance of an organization ensure that ICT is optimally used to achieve the organizations business objectives and at the same time the risks arising from the use of IT are also properly managed.

Given the importance of information systems for most organisations, the increased dependence on such systems to deliver business results and the size of investments made in IT, effective IT governance is an essential condition that must be fulfilled for an organisation to achieve its corporate objectives.

GOAL	OBJECTIVES	ACTIVITIES
IT STRATEGIC GOAL 5 Institutionalize effective IT Governance to provide overall direction and for effectively managingIT investments, roles and processes	Objective 5.1 Establish IT governance structure and sustain IT governance processes	5.11 Establish IT steering committee 5.12 Establish IT Technical Committee 5.13 Sustain IT governance
	Objective 5.2 Adopt and implement standard frameworks and best practices for IT controlsand information security management	5.21 Develop and implement IT policies 5.22 Adopt a standard IT control framework 5.23 Standardise IT hardware, software and IT methods 5.24 Implement information security management system

Objective 5.1: Establish IT governance structure and sustain IT governance processes

IT governance is an important issue for a Supreme Audit Institution. The active support and involvement of the top management is the key feature of the IT governance structure. An IT governance structure helps ensure proper oversight and monitoring of the IT initiatives by the top management. It is an important element of an SAI's strategic development and risk management framework. The IT Governance structure ofOAGN will have the following components

- IT steering committee
- IT Technical Committee
- IT Directorate
- IT Audit/CAATs/Audit Methodology Expert Group

To achieve this objective the following activities will carried out:

5.11 Establish IT steering committee

The IT Steering Committee is at the apex of the IT governance structure. The IT steering committee will be established. Chaired by the CAG, the IT Steering Committee will periodically review the progress of the implementation of OAGN's IT Strategic Plan and take strategic decisions relating to the use of information technologies. Director MIS will be the de facto secretary of the IT steering committee

5.12 Establish IT Technical Committee

Consisting of officers representing different audit directorates, the Technical Committee will be responsible for implementing the new IT-based auditing techniques in the respective audit directorates and in general provide coordination amongst the IT Directorate and the various audit directorates.

The respective roles of the IT Directorate and the IT Audit/CAATs/Methodology Expert Group have been described under Objective 1.2 Strengthen IT management capabilities. The expert group will have the responsibility of providing central support to the users in the audit directorates in applying the newly developed advanced IT-based audit techniques. It will also be responsible for upgrading and maintaining audit methodologies, procedures and audit programmes.

5.13 Sustain IT governance and monitoring

Throughout the IT Strategic Plan period, there will be periodic and regular meetings of the IT Steering committee and the Technical Committees in order to review and monitor the progress of the IT related components and to facilitate coordination with other components of SCOPE. Ideally the IT steering committee should meet every two months and the IT Technical Committee should meet every fortnight. Before each meeting the MIS unit will prepare a report on the progress of the implementation of the IT Strategic Plan, issues relating to IT operations and an agenda for the meeting. The minutes of the meeting will be recorded and the decisions taken in the meetings will be implemented by responsible persons who have been assigned the tasks. The MIS unit will prepare and submit periodic report on the progress of the implementation of the IT Strategic Plan based on the performance metrics identified in section 7.

Objective 5.2: Adopt and implement standard frameworks and best practices for IT controls and information security management

IT is should be governed by good (or best practices), to ensure that the organisation's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. To achieve these objectives Management implements controls over information technology at three levels: Policies, IT Standards; and Processes.

The policies, standards and processes cover the following areas:

- using IT to improve organizational efficiency and effectiveness;
- leveraging IT to create new business opportunities and to enhance competitiveness;
- managing the IT risks;
- obtaining value for money from investments made in IT; and
- empowering personnel with appropriate hardware and software tools and new work techniques.

To implement a standard IT control and governance framework in OAGN the following activities will be carried out:

5.21 Develop and implement IT policies

Policies provide the overall framework for the operation of information technology within the organisation. The IT polices will broadly cover the following areas:

- Strategic Planning
- System Development
- Data Security
- Data Custodianship
- Internet, Intranet and Extranet
- Risk Management
- Change Management
- Project Management
- Quality Assurance
- Back-Up
- Service Level Agreements

5.22 Adopt a standard IT control framework

To derive maximum benefit from information technology, OAGN must ensure that the applications, technology and infrastructure, are appropriate to the needs of the users. Acquiring or installing IT infrastructure and solutions by itself does not guarantee success in achieving objectives. It is necessary to exercise proper control, supervision and monitoring of IT processes to ensure that the information systems actually meet the expectations of the users and help them to perform their tasks more efficiently and effectively. Processes are the procedures and guidelines that assist in the implementation, execution and monitoring of compliance with the Policies and Standards. For this purpose the management must adopt best practices in IT management and control and implement a standard IT governance and control framework.

CobiT (Control objectives of Information Technology) is an IT Governance and control framework developed by the Information Systems Audit and Control Association (ISACA) that has gained worldwide acceptance. CobiT combines the principles embedded in existing reference models in three broad categories: quality, fiduciary responsibility and security. From these broad requirements, the framework divides IT management into four areas

- **Plan and Organise (PO)—**Provides direction to solution delivery (AI) and service delivery (DS)
- **Acquire and Implement (AI)**—Provides the solutions and passes them to be turned into services
- **Deliver and Support (DS)**—Receives the solutions and makes them usable for end users
- **Monitor and Evaluate (ME)—**Monitors all processes to ensure that the direction provided is followed

For each of these areas, the CobiT framework provides detailed guidelines on the processes, control objectives and control best practices. By adopting widely accepted IT governance framework like CobiTthe OAGN will not only achieve better control over its own IT processes but will also set an example for other public sector agencies in Nepalin implementing best practices.

5.23 Standardise hardware, software and IT methods

Standardisation of IT hardware and software refer to defining the minimum requirement to be complied with in the use of IT. Ensuring that hardware and software purchases follow a common standard can lead to cost savings and increased staff productivity. Generally, standardization results in greater connectivity, compatibility, and ensures that expenditures for IT are efficient and effective because of the discounts that can be obtained from bulk purchase of hardware and software. Standardisation also reduces training costs and increase transferability of computer skills.

Standardisation is also applied to IT methods and processes like system development, software acquisition, IT security etc. as an organisation attempts to implement the best practices in these areas. However it is necessary to take a balanced approach to standardisation so as not to sacrifice flexibility and becoming too dependent of particular products. As such it is necessary to periodically review the standardsand upgrade the requirement as necessary.

Standardisation in an IT environment generally covers the following resources:

• IT facilities like the data centres • Hardware • Software • System Development methodology • Project Management	• Programming • Change Management • Quality Assurance • Risk Management • Service Level Agreements

The following is an indicative list of the standards that will be adopted by OAGN:

Software standards	
Network operating system Email Solution development framework Database management system Security software Virtualization Workstation OS Office automation	Windows 2008 Enterprise Server R2 Microsoft Exchange 2010 server Enterprise Edition Microsoft. Net 4.0. 30319. 1 (4.0) Microsoft SQL Server 2008 R2 Enterprise Edition Forefront Security for Client/Forefront Security for Exchange Server VM ware Windows 2007 Microsoft Office Professional suite 2010
Audit Software	
CAATs EWP suite Flowcharting Document publishing	IDEA Version 8. 0 TeamMate Microsoft VISIO Adobe Acrobat
Hardware	
Server Network equipment Firewall Internet traffic management	2 Quad Core Intel® Xeon® processor E5520 CISCO products CISCO Bandwidth Manager
IT Methods	
IT governance and control System Development IT Security management Project management	CobiT/Risk IT/Val IT SDLC/PRINCE2 ISO 27001 and CobiT PRINCE 2/Project management standards of PMI[1]

5.24 Implement information security management system

Security of IT systems is a critically important issue, which must be given a very high priority by the management of all organisations. An organization-wide security policy and

programme plan is the foundation of an effective security framework. In the absence of an IT security policy there will be no clear direction to security related activities. As a result the security control and procedures would be unsystematic and arbitrary leading to insufficient protection of sensitive information resources. Furthermore theprocedures for implementing security and monitoring the security procedureson a day to day basis should bedocumented and the employees at all levels must be made aware of the policies and procedures. Unless this is done the security policies even if formalized in a document may not be actually implemented in practice. Finally, the security policies and procedures must be reviewed and updated on a regular basis to take into account the changed conditions.

For an SAI the need to maintain information security and confidentiality must be given the highest propriety because of the highly sensitive nature of information handles by the SAI and the risk of unauthorised disclosure of such information which may threaten national security and result in embarrassment of the SAI.

The six major activities involved in information security are:

- Policy Development—Using the security objective and core principles as a framework around which to develop the security policy
- Design—Developing a security and control framework that consists of standards, measures, practices and procedures
- Roles and Responsibilities—Ensuring that individual roles, responsibilities and authority are clearly communicated and understood by all
- Awareness, Training and Education—Creating awareness of the need to protect information, providing training in the skills needed to operate information systems securely, and offering education in security measures and practices
- Implementation—Implementing the solution on a timely basis, then maintaining it
- Monitoring—Establishing monitoring measures to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices.

The Director ITwill work with the audit directorates to develop and implement a comprehensive information systems security management system (ISMS) and a security awareness programme to improve and maintain information security. The security programme should follow a risk-based approach to focus on areas possess the highest security risks and implementing initiatives that address these risks in a cost effective way. The ISMS will be based on a standard IT security framework like the ISO 27001.

6 TIMELINE FOR OAGN IT STRATEGIC PLAN ACTIVITIES

Activities	Start	Finish
IT STRATEGIC GOAL 1 -ICT Infrastructure		
Objective 1.1: Build & sustainICT infrastructure		
1.11 OAGN network phase		
1.12 Procure desktop, laptops & printers		
1.13 Acquire software		
1.14 Hardware inventory &media library		
Objective 1.2: Strengthen IT management		
1.21 Strengthen MIS unit		
1.22 Train IT support personnel		
1.23 Regularise IT Support personnel		
1.24 Establish IT help desk function		
IT STRATEGIC GOAL 2 - Enabling IT environment & IT culture		
Objective 2.1 Provide secure access to technology		
2.11 Provide secure network access		
2.12 Provide universal email facility		
2.13 Provide secure Internet access		
Objective 2.2 Create IT security awareness		
2.21 Implement security awareness and training programme		
Objective 2.3 Optimise ICT to enhance productivity		
2.31 IT Human resources & training		
2.32 Encourage use of IT in the workplace		
2.33 Enhance OAGN website		
2.34 Establish OAGN Intranet		
IT STRATEGIC GOAL 3 - Auditing in IT environments		

Activities	Start	Finish
Objective 3.1 Capacity in information technology auditing		
3.11 Establish IT audit core group		
3.12 Develop IT audit manual and training course		
3.13 Train core group		
3.14 Integrate IT audit into financial/compliance audit		
3.15 Conduct pilot IT audits		
3.16 Rollout IT audit training		
3.17 Organise and manage IT audit		
Objective 3.2 Implement CAATs		
3.21 Select CAATs software		
3.22 Train core group		
3.23 Data link with CGA systems		
3.24 Track PFM developments		
3.25 Data downloads from other auditees		
3.26 Integrate CAATs into audit cycle planning		
3.27 Integrate CAATs into financial/compliance audit procedures		
Objective 3.3 Implement EWP software suite		
3.31 Acquire EWP software		
3.32 Establish EWP champion group		
3.33 Develop risk-based audit methodology & update manual		
3.34 Customise EWP and develop library		
3.35 Conduct pilot audits using EWP and EWP library		
3.36 Develop EWP manual		
3.37 Implement EWP roll-out programme		

Activities	Start	Finish
Objective 3.4 Develop IT skills and knowledge		
3.41 Undertake an IT training needs analysis		
3.42 Prepare training strategy and plan for IT capacity building		
IT STRATEGIC GOAL 4 Implementaudit support systems		
Objective 4.1: Design, develop and Implement AMMS software		
4.11 Develop user requirement specs and design		
4.12 Acquire and implement the AMMS solution		
Objective 4.2: Implement solutions for other support systems		
4.21 Acquire and implement a document management System		
4.22 Acquire and implement audit support solutions		
IT STRATEGIC GOAL 5 - Institutionalize effective IT Governance		
Objective 5.1: Establish IT governance structure and sustain IT governance processes		
5.11 Establish IT steering committee		
5.12 Establish IT Technical Committee		
5.13 Sustain IT governance		
Objective 5.2: Adopt and implement standard frameworks and best practices for IT controls and information security management		
5.21 Develop and implement IT policies		
5.22 Adopt a standard IT control framework		
5.23 Standardise IT hardware, software and IT methods		
5.24 Implement IT security management system		

7 PERFORMANCE METRICS

This section of the plan indicates the output-based performance metrics for measuring the successful completion of the various activities scheduled in the IT Strategic Plan. It is expected that the IT directorate willuse these metrics to measure the progress of the IT plan on an ongoing basis and submit reports thereon to the IT Steering committee.

Objective 1.1: Build and sustain the ICT infrastructure

OAGN network	• Date of commissioning of the network vis-à-vis the planned date

Procurement of computers and peripherals	• Number of workstations configured and connected to the network
	• Number of the following items as against targeted number of procurements
	  ○ Desktops
	  ○ Laptops
	  ○ Printers

Acquisition of software	• Number of software licenses procured as against planned numbers
Inventory of It equipment	Date of completion of the IT equipment inventory

Objective 1.2: Strengthen IT management capabilities

Strengthen IT Directorate	• Creation of the IT directorate • Number of additional staff posted to IT Directporate • Date of approval of the MIS unit charter and job descriptions
Training of IT support personnel	• Number and description of professional training courses completed by IT support staff
Regularisation of IT Support personnel	• Date of the matter referred to Ministry of Personnel • Date of regularisation of IT support staff
IT help desk function	• Number of issues and problems referred to help desk • Number of issues escalated to appropriate authorities • No. of problems resolved • Number of complaints and problems remaining unresolved for more than a certain period

Objective 2.1: Provide staff with secure access to technology

Secure access to the network	• Number of network users created using Active Directory • Percentage increase in the number of users accessing the network
Email accounts	• Number of email accounts created • Percentage increase in the number of users using email
Internet access	• Bandwidth allocated and used
Security awareness and training programme	• Management approval of training material and policy on IT security awareness • Number of training programmes and workshops organised • Number of people attended IT security workshops and training • Number of employees expressing satisfaction with the IT security awareness training
IT Human resources Development and training	• Number of training courses courses held • Number of people completed courses
Use of IT in the workplace	• Number of office circulars and administrative orders circulated through email • Number of audit reportsprepared using MS Word
OAGN website	• Number of audit reports placed in OAGN website • Number of people accessing OAGN website
OAGN Intranet	• Number of OAGN staff accessing the Intranet • Number of audit reports and management accessible in the Intranet • Number of officer orders and notifications circulated over the Intranet • Number of training courses reported • Number of newsletters published over the Intranet

Objective 3.1: Build capacity in information technology auditing

IT audit core group	• Number of people appointed to the IT audit/ CAATs core group
IT audit manual and training course	• Date of management approval of the IT audit manual and training course
Training of core group	• Number of IT audit training courses delivered • Number of people attended IT audit training
Integration of IT audit into financial/compliance audit methodology	• Number of financial/compliance audits which included review of IT controls
Pilot IT audits	• Number of pilot IT audits conducted • Number of IT audit specialist participated in pilot IT audits • Number of IT audit related observations raised.
Rollout IT audit training	• Number of roll out IT audit courses delivered • Number of people attended IT audit roll-out training
Management of IT audit	• Number of audits in which IT audit support is provided by IT audit specialists • Number of audits of complex IT audit systems completed by OAGN IT audit specialists • Number of audit observations and recommendations made

Objective 3.2: Acquire and Implement CAATs

CAATs software	• Number of CAATs software licences procured
Training of core groups	• Number of CAATs training courses held for IT/ financial audit core group members • Number of CAATs training courses held for OAGN management cadre officers • Number of people attended CAATs training
Data link with CGA systems	• Approval of CGA data link • Number of OAGN staff trained in using the data link • Number of transactions and reports downloaded using the data link

PFM developments	• Number of meetings held with PFM reform agencies/projects (e. g. SPEMP A) • Number of OAGN suggestions made regarding IT controls and Auditability of new systems • Number of recommendations accepted
Access to other auditee systems	• Number of meetings held with other agencies regarding access to data • Number of transactions and volume of data downloaded
Integration of CAATs into audit cycle planning	• Number of annual audit plans prepared using CAATs in different audit directorates
Upgrade financial/ compliance methodology with CAATs	• Number of workshops held on this subject • Number of financial/compliance audit conducted in which CAATs was used
Roll out CAATs training	• Number of roll out CAATs courses delivered • Number of people attended CAATs roll-out training

Objective 3.3: Implement EWP solution

Acquire EWP software	• Number of licenses of EWP suite procured
EWP champion group	• Number of staff appointed as EWP champions
Risk-based financial audit methodology and Update financial audit manual	• Approval of the risk-based financial audit methodology and revised financial/ compliance audit manual • Number of training courses and workshops delivered on the new risk-based financial audit methodology • Number of people attended training on new financial audit methodology • Number of copies of revised financial/ compliance audit manual printed and circulated
EWP library	• Number EWP libraries developed • Number of procedures created in the library • Number of working paper templates in the library

Pilot audits using EWP	• Number of pilot audit conducted using EWP • Number of people participated in pilot audits • Percentage increase in audit efficiency
EWP training material and manual	• Approval of the EWP training material and manual • Number of copies of the manual prepared and circulated
EWP roll-out programme	• Number of training courses held on EWP and risk-based audit methodology • Number of people attended EWP training • Number of audits conducted using EWP

Objective 3.4: Develop IT skills and knowledge through regular training and professional development

IT training needs analysis	• Number of people surveyed in the TNA • Approval of the TNA report by management
Implementation of training plan for IT capacity building	• Number of various categories of IT training courses delivered • Number of people attended the training courses • Feedback received from the trainees • Number of trained persons performing audits using the acquired IT skills

Objective 4.1: Design, develop and Implement AMMS software

AMMS user requirement specs and design	• Number of workshops and discussions held with OAGN management and staff regarding design of AMMS • Date of approval of the AMMS design
Implementation of AMMS	• Number of users trained on AMMS • Number of annual audit plans prepared using the AMMS • Number of audit observations processed using AMMS

Objective 4.2: Acquire and implement solution for other support systems

Document management system	• The date of acquisition of the document management software
Solutions for support systems	• Number of additional systems automated

Objective 5.1: Establish IT governance structure and sustain IT governance processes

IT steering committee	• Date of establishment of the IT steering committee
IT Technical Committee	• Date of establishment of the IT Technical Committee
IT governance and monitoring	• Number of meetings of the IT Steering committee • Number of meetings of the IT Technical Committee

Objective 5.2: Adopt and implement standard frameworks and best practices for IT controls and information security management

IT policies	• Number of IT related policies prepared and approved
Standard IT control framework	• Number of standards adopted and implemented
Standardisation of hardware, software and IT methods	• Description and number of items standardised
Information security management system	• Date of approval of the ISMS

8 CRITICAL SUCCESS FACTORS

The successful implementation of OAGN's IT Strategic Plan depends on the following critical success factors:

- Active involvement of OAGN top management in directing and monitoring the IT function
- Effective IT governance
- Immediate strengthening of the MIS unit
- Availability of appropriate resources for implementing the strategy
- Sustainability and establishment of an IT corporate culture
- Access to the CGA databases and system logs through an online data link

9 CONCLUSION

Implementing OAGN's IT Strategic Plan is an urgent and vital requirement to ensure its continued effectiveness and relevance as the supreme audit institution of Nepal. The IT Strategic Plan provides the guidance on effective implementation of the various initiatives and activities for achieving the intended goals and objectives. The expected outcome of the implementation of the IT Strategic Plan is attainment of higher levels of efficiencies, a more productive and knowledgeable workforce, and heightened respect of OAGN as a public sector institution that has taken effective steps in achieving the goal of digital Nepal.

ANNEX A: IT DIRECTORATE CHARTER AND JOB DESCRIPTIONS

Charter of the IT Directorate

The objective of the IT Directorate is to provide support to OAGN in implementing the ICT and IT audit related activities with a view to enhancing efficiency and effectiveness and professionalism in the delivery of audit services. The IT Directorate has two major functions:

a) Overseeing the IT infrastructure and IT software application; support the network, databases, website and intranet; and coordinate and oversee the equipping of all OAGN staff with adequate hardware and software tools.

b) Act as a central support group for IT-based audit tools, such as CAATs (i. e. act as audit methods specialists/trainers in the IT area).

Responsibilities: The MIS will provide the following services

ICT support services

- Manage and support OAGN ICT infrastructure including the data centre, networks, computers and peripherals
- Administer and support the applications
- Provide user support and under take desk functions
- Implement IT related policies and educate end-users about IT security and best practices
- Implement the IT Strategic Plan and develop short term IT operational plans. Review and update the IT Strategic Plan and other plans on an ongoing basis by taking into account the needs of the office and the latest developments in technology

IT Audit support services

- Undertake audits of complex IT systems of OAGN auditees. Examples of such systems are the CGA IBAS system and its future upgrades, Customs ASYCUDA++ systems, nationalized banks IT systems etc. These IT audits may be in support of the financial audits of the concerned entities or may be standalone audits to provide assurance regarding security, integrity and reliability of auditee IT systems to the concerned stakeholders
- Providing support in the use of computer assisted audits techniques including downloading data from auditee computer systems and performing data analysis using software IDEA
- Providing help and support to the users of theTeam Mate audit management software and OAGN risk-based audit methodology/TeamMate library

- Help in improving the professional skills and knowledge of OAGN staff in the field of IT, IT audits, CAATs and TeamMate and other related areas through plans for professional development and training.
- Make recommendations to the IT Steering Committee and OAGN top management in IT and IT audit related matters

Scope of IT audit services

- Continuously update the knowledge about auditee existing computer ICT systems of auditees and ICT projects under development or planned though carrying out general review of IT (GRIT) surveys
- Plan, leading, perform, and report on IT systems controls covering the full range of general and application controls of major existing computer systems in order to assure security, reliability and integrity of information
- Review and audit major IT system acquisitions and systems under development. Work with the project management team of major government IT systems under development to ensure that
- adequate audit trails are created in the new systems
- OAGN is given appropriate access to the data and downloading facilities data access and audit trail development
- proper internal controls and security measures are implemented
- Review and audit web based systems in use in the Government
- Devise and document methods of accessing and downloading data from the different hardware and software platforms in use in the auditees and data analysis using CAATs software
- Provide IT audit support to OAGN financial and performance auditors
- To act as repository of knowledge and best practices in the field of IT system risk, security and controls;

IT Directorate Job Descriptions

Director MIS

- Assist in developing strategic and annual plans for OAGN Information System applications and ICT infrastructure in close consultation with the IT Steering committee
- Help implement the IT Strategic Plan
- Monitor ICT service delivery and manage acquisitions

- Develop and justify, financial and human resources plans for the IT Directorate by considering OAGN' stechnology environment and IT Strategic Plans
- establish goals and objectives for staff develop performance management plans for each auditor which incorporates training and development plans to enable them to effectively carry out their duties and under take performance reviews
- Direct and manage through the IT audit group the implementation of the annual information systems audit plan covering multiple auditees in consultation with the IT audit core group the respective Directors General of Audit
- Report regularly on the plan's status and provide operating and senior management with an independent, objective and timely appraisal of each system audited
- by conducting general review of IT (GRIT)surveys and research and by reviewingthe results of previous IT audit plans assure OAGN senior management that the IT audit coverage is appropriate and meets the appropriate part of OAGN's audit responsibilities
- Direct and approve the audit planning memorandum for each IS audit and provide effective leadership through advice and direction as needed,
- Participate as a project leader on major audits and act as a resource/advisor to OAGN top management through the Director of Audit (Central Government) on the reliability and integrity of OAGN's internal and auditee Information Systems, their internal controls, significant control weaknesses and issues with current policies/guidelines, procedures and programs.
- Provide leadership in the design and delivery of training programmes on TeamMate/Risk-based audit methodology/CAATs/IT audit/General IT skills

Audit Officer MIS

- Keep abreast of changes and major developments in technology, ICT concepts, auditing and accounting standards, and relevant developments in auditing and Information Systems by maintaining professional competency through training, development and inquiry
- Maintain communication linkages with professional organizations like the INTOSAI Development Initiative (IDI), AFROSAI-E, Information Systems Audit and Control Association, Institute of Internal Auditors,
- Be aware of latest trends in Information Systems technology, auditing and accounting standards
- Assess the risks in the auditee computer environments following an appropriate methodology and develop a program of Information Systems audit. coverage for the major auditee IT systems

- Develops and implement variousanalytical and auditing techniques designed to assure the adequacy and effectiveness of the internal control structure in major audit IT systems
- Provide sophisticated computer support to the general audit staff in the areas of IT audit, CAATs, data access and download and use of other computer based audit tools as and when required.
- Provide support in the use of TeamMate EWP software and other computer based audit tools as and when required.
- Lead IT audits as team leader and effective plan, perform and monitor the progress and quality of OAGN's IT audit projects
- Impart training both classroom and on-the-job training to IT audit staff and OAGN general staff on theory and practice of IT audits

IT Audit and CAATs Specialists

- Undertake IT audit work relating to IT audit projects under the guidance of the Director MIS and Audit officer MIS (IT Audit)
- Assist in risk assessment of auditee ICT systems and planning for IT audits
- Undertake survey of auditee ICT systems using the GRIT template
- Keep abreast of changes and major developments in technology, ICT concepts, auditing and accounting standards, and relevant developments in auditing and Information Systems by maintaining professional competency through training, development and inquiry
- In the course of performing IT audit work, develop, write and present audit findings and policy and procedural recommendations to Director MIS and OAGN top management
- Assist in the development of an audit work schedule that includes what activities are to be audited, when they will be audited, and the estimated time required
- Assist in design and delivery of IT and IT audit related training including training on CAATs and EWP
- Provide support to TeamMate/Risk-based audit methodology users

Data centre manager/Systems analyst

- plan, install, configure, troubleshoot, maintain and upgrade operating systems and associated subsystems
- provide system-level support of multi-user operating systems, hardware and software tools, including installation, configuration, maintenance, and support of these systems,

- Install, configure, troubleshoot, maintain and upgrade hardware and software interfaces with the operating system,
- resolve hardware, software, and connectivity problems, including user access and component configuration
- Record and maintain hardware and software inventories, site and/or server licensing, and user access,
- maintain system security and confidentiality of information,
- Install, configure, and upgrade desktop hardware and peripherals to include; network cards, printers, modems, and add-in boards,
- analyze and evaluate present or proposed business procedures or problems to define data processing needs Prepare detailed flow charts and diagrams outlining systems capabilities and processes, (j) recommend hardware and software development, purchase, and use,
- implement and support application systems

Network administrator

Implementation of OAGN network in conformance with appropriatenet work standards and maintaining the network management framework,

- overall management of OAGN network,
- provide guidance to the expansion and growth of OAGN networkin terms of the messaging, intranet, internet and other functionality in the interest of OAGN and be responsible for all technical upgrades and
- assist in managing the inventory of all IT equipment including components of OAGN network, software, licences etc.

Database administratort

- maintaining and upgrade of database systems
- ensuring data integrity and backup and business continuity
- install application software
- user creation and maintenance
- maintaining application security
- support application users with report generation
- database Performance tuning
- establish database usage and security policies and procedures for staff
- train users in security and password management

ANNEX B: CONTENTS OF OAGN INTRANET

The main purpose of the Intranet is to provide online real-time access by OAGN staff to the reference information and technical guidance. The core business of OAGN is auditing. Therefore the primary focus of the intranet will be to provide OAGN staff with the information and tools they need to perform their audit work. The other benefits are efficient information dissemination and exchange to facilitate better communication amongst staff and facilitate audit support activities and administrative matters. Intranet will provide means for facilitating social communication and exchanging informal information amongst members of the staff relating to family, health, religious faith, community relations and gender-related needs.

OAGN Intranet will have the following components:

1.Knowledge library	**7. Staff calendar**
2.Technical Guidance	**8. Training**
3.Audit Reports/management letters	**9. Help desk**
4.Administrative area	**10. OAGN development projects**
5.Procurement	**11.Staff library**
6. Staff database/directory	**12.Social Area**

Each of the above will appear as a link in the Intranet web interface/home page. The details of each of the areas are indicated below.

Facilities

- Search facility
- Text messaging
- External links
- Content management system

1. Knowledge library

The knowledge library will be the digital repository of reference material as indicated below -

- Corporate Plan OAGN
- IT Strategic Plan

- The auditing standards (ISSAIs, ISAs)
- Accounting standards –IPSAs, IFRSs
- IT standards – CobiT, ISO 27000 series, ITIL
- Best practices – Internal controls, IT, audit committees
- Nepalfinancial acts and regulations, public procurement act and regulations
- Regulations – TRAI, FR
- StandingOrders
- Circulars and standing instructions

2. Technical Guidance

This area will contain the guidance developed internally for use by OAGN staff

Audit manuals

- Financial audit manual and risk-based audit methodology
- Performance audit manual
- Guidance on audit testing and sampling
- IT audit manual (basic and advanced0
- Guidance on using the IFMS audit interface
- Guidance on using CAATs (IDEA) in CGA IBASenvironment and for other OAGN auditees including methods of accessing and downloading data
- EWP manual
- Administrative manual

Templates – standards documents to be used in the financial/IT audits i. e. audit notification letter, request for documents, risk assessment, materiality, ICQs and audit programmes.

3. Archive of audit reports and management letters

This section will be repository of all published audit reports and management letters for quick access by OAGN management and staff through file search and text search

The structure of the database maintained for this purpose will be as follows

Type of report	Directorate	Unit audited	Year/Period	Remarks
Annual audited accounts/ management letter				
IT audit reports				
Special audit reports				
Investigations				
Audit reports of projects				

4. Administrative area

The purpose of this section is to disseminate and capture information for the purpose enhancing efficiency of administrative actions. The following contents are indicated

- Notice board – making available electronic copies of all general officer orders and notices
- Engagements – notices about meetings to participants and booking of meeting halls
- Leave applications/travel approvals – the staff will be able to submit leave applications and travel approval requests online and receive authorizations
- Administrative instructions
- Travel approvals
- Registry/file user index/staff appraisals
- Correspondence tracking
- Stores Requisitions e. g. stationery/computerconsumables
- Stores management system
- Transport/fleet management/servicing and maintenance

Administrative Forms

This section will provide the staff to download or complete electronically various forms relating to their work e. g.

- Travel applications
- Claims
- Staff appraisal
- Leave applications

5. Procurement

This section will contain information relating to procurement. Access to this section will be restricted to authorised users only.

- Procurement requisitions
- Prequalified list of suppliers
- Status of procurements
- Minutes of the meetings of the Contracts committee/tender boards

6. Staff database/directory

This will contain a comprehensive database on OAGN staff including personal and service details, qualifications, experience and contact details. There will be various levels of access. For example, the top management and the AAG (Administration) will be able to see all information, but the general staff will see only the contact details.

7. Staff calendar

This section will provide the information about the whereabouts of important OAGN officers and staff. This will maintain by the concerned individuals themselves or their personal assistants indicating details about their location, travel details, availability etc.

8. Training

This section will contain details of training courses and facility for entering training related information

- Training calendar
- Details of participants and facilitators
- Training evaluation forms
- Trainingfollow up
- Training data base
- Reference – Training course material

9. Help desk

- IT help desk
- TeamMate/financial audit methodology help desk

10. OAGN development projects

This section will provide information relating to the various donor-funded projects being

implemented in OAGN.

- Details of projects – project plans
- Status and progress reports
- Minutes of project management committee meetings

11. Staff library

This section will provide information about OAGN library and will enable staff to reserve books for lending and track the borrowings. It will contain the following features

- A complete indexed list of books available in OAGN staff library
- New additions
- Keeps track of borrowings and returns

12. Social area

The purpose of the section is to provide and information not strictly relating official business

- News items: information regarding marriages, births, other matters of common interest etc.
- Blog – provided facility for maintaining blogs and for text chatting amongst OAGN staff
- News Letter
- OAGN in press – clippings from newspapers concerning OAGN

Facilities

- Search facility There will be search facility which will enable the users to search the entire database of documents by name or by keywords
- Text messaging – the employees will be able to send text messages from their mobile telephones to the Intranet
- External links – links to useful websites
- Content management system – this will be used by the Intranet administrator to manage and update the contents

Technical requirements

The system must be fully compatible with Microsoft Active Directory infrastructure so that all authentication to the Intranet and privileges are managed from OAGN's existing active directory

(Footnotes)

1 Project Management Institute (PMI)