Funded by
the European Union

Information Technology (IT) Audit Guidelines

[For Internal use of OCAG Bangladesh]

Office of the Comptroller & Auditor General of Bangladesh

24 November 2025

[Amended Draft based on OCAG Task Team Inputs]

Technical Assistance to Support the Implementation of the PFM Reform Strategic Plan in Bangladesh

(Funded by the European Union)

Table of Contents

List of Figures 5
Appendices 5
Abbreviations and Acronyms 7
FOREWORD 9
PREFACE 10
INTRODUCTION 11
Users of the IT Audit Guidelines 11
Content and Structure of the Guidelines 12
Scope of the Guidelines 12
Revisions to the Guidelines 12
1. CHAPTER 1 - PRINCIPLES OF IT AUDITING 13
1.1. Effect of IT on Audit Procedures 13
1.2. Key Definitions in IT Audit 13
1.3. Auditing in IT Environments 14
1.4 IT Audit Objectives 15
1.5 Scope of IT Audit 15
1.6 IT Auditing Standards and Audit Criteria 16
1.7 IT Controls Framework 20
1.8 IT General Controls 21
1.9 Application Controls 21
1.10 An Overview of IT Audit Methodology (Three Level Approach) 21
1.10.1 Planning for IT Audits 21
1.10.2 Audit Risk 22
1.10.3 Materiality 23
1.10.4 IT Audit Engagement Process 23
CHAPTER 2 IT AUDIT STRATEGIC PLAN AND ANNUAL AUDIT PLAN 25
2.1 Overview of IT Audit Planning 25
2.2 General IT Survey and the Audit Universe 25
2.3 IT Audit Strategic Plan and Annual Audit Plans 26
2.4 Risk-Based Audit Planning Process 26
2.5 Obtain Knowledge of Responsible Party IT Systems 27
2.6 The Audit Universe 27
2.7 Consideration of Risk Factors 27

2.8 Risk Assessment of Auditable IT Systems 28
2.9 Preparing the Strategic IT Audit Plan 28
2.10 Developing the Annual Audit Plan 28
CHAPTER 3 THE IT AUDIT ENGAGEMENT PROCESS 29
3.1 Types of IT Audit Engagement 29
3.2 Audit Commencement 30
3.2.1 Audit Objective 30
3.2.2 Audit Scope 30
3.2.3 Audit Notification 30
3.2.4 Entry Meeting 30
3.3 Understanding the Entity and IT Environment 31
3.3.1 Knowledge of Organisational Function 31
3.3.2 Documenting IT Systems and Control Frameworks 31
3.4 Risk Assessment Engagement Strategy and Audit Plan 32
3.4.1 Risk Assessment 32
3.5 Review and Test IT Controls 36
3.5.1 Review of IT General and Application Controls 36
3.5.2 Control Objective 37
3.5.3. Testing and Evaluation of Controls 37
3.5.4 Evidence Collection and Forensic Analysis 37
3.6 Audit Reporting and Quality Assurance 39
3.6.1 Audit Findings 39
3.6.2 Exit Meeting 39
3.6.3 Audit Quality Control and Quality Assurance 40
3.6.4 IT Audit Report 40
3.6.5 Audit Follow Up 41
CHAPTER 4 REVIEW OF IT GENERAL CONTROLS 42
4.1 IT General Control Domains 42
4.2 OM: IT Organisation & Management 43
OM.1 IT Governance & Strategic Planning 43
OM.2 Risk Management 44
OM.3 IT Organisational Structure 44
4.3 PE: Physical & Environmental Controls 44
PE.1 Physical Access Controls 44
PE.2 Environmental Controls 45

4.4 SD: Segregation of Duties 45
4.5 SM: IT Security Management 46
SM.1 Security Policies & Procedures 46
SM.2 Incident and Problem Management 46
4.6 AC: Access Control 48
AC.1 Logical Access Controls 49
AC.2 Password Management 49
AC.3 User Account Administration 49
4.7 CC: Service/System Acquisition, Development & Change Control 49
4.8 BC: Business Continuity Planning 52
4.9 NC: Network Controls 53
4.10 DC: Data Management Controls 53
CHAPTER 5: REVIEW OF CYBER SECURITY CONTROLS 55
5.1 Types of Cyber Attack 55
5.2 Cyber Security Control Areas 56
5.3 GRC: Governance, Risk & Compliance 57
5.4 IAM: Identity & Access Management 57
5.5 NWC: Network Security Controls 58
5.6 DSC: Data Security & Protection 58
5.7 APP: Application Security 59
CHAPTER 6 REVIEW OF APPLICATION CONTROLS 60
6.1 Major GoB IS/IT Systems 60
6.2 Application Control Domains 61
6.3 IAC: Input Authorisation & Controls 62
6.4 PAC: Processing Accuracy Controls 62
6.5 OAC: Output Accuracy Controls 63
6.6 UAC: User Access & Authentication 63
6.7 CDC: Change & Development Controls 64
6.8 LGC: Logging & Monitoring Controls 64
6.9 BAC: Backup & Recovery Controls 65
CHAPTER 7 IT AUDIT IN SUPPORT OF BUDGETARY CENTRAL GOVERNMENT ACCOUNTS 66
7.1 IT Audit and Government Financial Statements 66
7.2 Budgetary Central Government Finance Accounts 66
7.3 IT Auditing Approach and Process 67

7.4 Understanding the IT environment, Information System and System Controls 68
7.5 Assessment of Risks and the Control Environment 69
7.6 Assessment of IT Controls 69
7.7 Substantive Tests 72
7.8 Reporting 73

List of Tables

Table 1: Outline of Chapters 12
Table 2: IT Standards and Regulatory Frameworks 17
Table 3: IT Audit Engagement Stages....23
Table 4: Three Level Approach to IT Audit Planning 26
Table 5: Impact Risk Factors....28
Table 6: Probability Risk Factors....28
Table 7: Knowledge of IT Systems....31
Table 8: Audit Planning Memorandum 33
Table 9: IT General Controls....36
Table 10: Cyber Security Controls (CS) 36
Table 11: Application Controls (AC) 36
Table 12: IT General Control Domains....42
Table 13: Type of Cyber Attack....55
Table 14: Cybersecurity controls....56
Table 15: Application Control Domains 61
Table 16: Input Controls, Processing Controls and Output Controls....70

List of Figures

Figure 1: IT Controls Framework....20
Figure 2: Levels of IT Audit Planning....25
Figure 3: IT Audit Engagement Process....29
Figure 4: Engagement Risk Assessment....32

Appendices

Appendix 1: General Review of IT Survey....74
Appendix 2: IT risk identification....86
Appendix 3: IT Organisation and Management Control (OM) – Suggested Matrix/Audit Work Programme 87
Appendix 4: IT Physical & Environmental Controls (PE) – Suggested Matrix/Audit Work Programme 90
Appendix 5: Segregation of Duties (SD) – Suggested Matrix/Audit Work Programme....92
Appendix 6: IT Security Management (SM) – Suggested Matrix/Audit Work Programme....94
Appendix 7: IT Access Controls (AC) – Suggested Matrix/Audit Work Programme 96
Appendix 8: System Development and Change Control (CC)– Suggested Matrix/Audit Work Programme 99
Appendix 9: Business Continuity Planning Control (BC) – Suggested Matrix/Audit Work Programme 101
Appendix 10: Network Control (NC) – Suggested Matrix/Audit Work Programme 103
Appendix 11: Database Control (DC)– Suggested Matrix/Audit Work Programme 105

Appendix 12: Review of Application Controls – Suggested Matrix/Audit Work Programme 108
Appendix 13: Checklist for iBAS++ Documentation and Guidelines relating to Security and Operating Procedures 112

Abbreviations and Acronyms

AC	Access Controls (IT Security)
BAC	Backup & Recovery Controls
BC	Business Continuity (Planning and Disaster Recovery)
BCG	Budgetary Central Government
BNDA	Bangladesh National Digital Architecture
CA	Certification Authority
CAATs	Computer Assisted Audit Techniques
CC	(System Development and Programme) Change Controls
CDC	Change & Development Controls
CIA	Confidentiality - Integrity – Availability
CIRT	Critical Incidence Response Team
COBIT	Control Objectives for Information and Related Technology
COTS	Commercial Off the Shelf Software
CS	Cyber Security (Controls)
CSC	Critical Security Controls
DBMS	Database Management System
DC	Database Controls
DDoS	Distributed Denial-of-Service
DLP	Data Loss Prevention
DMZ	Demilitarised zone
DNS	Domain Name Server (DNS).
DOS	Denial of Service
EFT	Electronic funds transfer
ERP	Enterprise resource planning
GoBISM	Government of Bangladesh Information Security Manual
GRIT	General Review of IT
HTTP	Hypertext Transfer Protocol
IAC	Input Authorisation & Controls
iBAS++	Integrated Budget and Accounting System
ICT	Information and Communication Technologies
IFPP	INTOSAI Framework of Professional Practices
INTOSAI	International Organisation of Supreme Audit Institutions
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardization
ISSAI	International Standards for Supreme Audit Institutions
IT	Information technology
ITAF	IT Audit Framework (ISACA)
ITGC	Information Technology General Controls
ITGI	IT Governance Institute
LGC	Logging & Monitoring Controls
MDA	Ministries, Divisions and Agencies (Auditable Units)
NC	Network Controls
OAC	Output Accuracy Controls
OCAG	Office of the Comptroller & Auditor General of Bangladesh
OM	Organisation and Management Controls

PAC	Processing Accuracy Controls
PE	Physical and Environmental Controls
RDP	Remote Desktop Protocol
RP	Responsible Party
SAI	Supreme Audit Institution
SD	Segregation of Duties
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SM	Security Management (IT Security)
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
UAC	User Access & Authentication

FOREWORD

With the increasing use of information technology (IT) in government and public sector operations in Bangladesh, the government audit is widening its remit to embrace this new domain. In this context, it has become imperative for my office to build the capability to conduct audits in IT environment and evaluate the IT systems in place effectively.

Bearing in mind the importance of capacity building, an IT Audit Guidelines has been prepared to support the OCAG auditors. The Guidelines provides comprehensive guidance on IT audit principles and methodologies. It also includes exhaustive information, enabling auditors to conduct field audits in an IT environment efficiently.

The guidelines draw on the OCAG IT Audit Manual 2015, originally prepared by the SPEMP-B Project supported by the World Bank. The IT Audit Guidelines is compliant with the auditing standards as prescribed in the Government Auditing Standards of Bangladesh (GASB), OCAG Audit Guidelines (Compliance Audit, Performance Audit and Financial Audit), the International Standards for Supreme Audit Institutions (ISSAIs), ISO 27000-1 and the Bangladesh National Digital Architecture (BNDA) Directives 2019**.** The guidelines are fully aligned with the INTOSAI GUID 5100 (Guidance on Audit of Information Systems) and other relevant professional standards such as the Information Technology Audit Framework (ITAF 2020) of the Information Systems Audit & Control Association (ISACA). It may also be applied within a co-sourcing arrangement.

I extend my sincere thanks to the technical assistance team of the EU-funded 'Technical Assistance to Support the Implementation of the PFM Reform Strategic Plan in Bangladesh' in preparing this guidelines. My sincere appreciation goes to my officers, who made substantial contributions to enrich the contents of this guidelines.

I am confident that the guidelines will contribute significantly to enhancing the quality and effectiveness of IT audits.

Md. Nurul Islam
Comptroller and Auditor General of Bangladesh

Dhaka XX November 2025

PREFACE

As an integral part of the overall audit process, IT Auditing has been embedded within financial, compliance and performance audits. In this context, a separate set of IT Audit Guidelines has become essential. These guidelines outline the control objectives the audit team should consider while evaluating IT-related controls, providing examples of control techniques along with recommended audit procedures. In certain areas, the audit team may require specialised technical expertise from external professionals to effectively carry out their tasks.

The IT Audit Guidelines will serve as a key reference for the IT audit teams in conducting IT Audits. However, it is not intended to be an exhaustive or definitive document on IT Auditing. Instead, it provides a structured framework to ensure that IT Audits are conducted following internationally accepted standards and best practices.

The guideline has been structured in seven parts:

Chapter 1 establishes the conceptual framework for IT Auditing, including auditing in an IT environment, audit objectives and scope, IT audit standards and frameworks, IT controls framework and IT audit methodologies.

Chapter 2 presents the strategic IT and annual IT audit planning. It also describes the IT audit process and risk-assessment methodologies for selecting IT audits.

Chapter 3 introduces the IT Audit engagement process.

Chapter 4 focuses on IT general controls outlining control objectives and audit procedures,

Chapter 5 introduces cyber-security controls outlining control objectives and key audit procedures.

Chapter 6 covers application control objectives and audit procedures,

Chapter 7 discusses IT audit in support of the audit of Budgetary Central Government Finance Accounts

The guidelines should be considered as a living document, subject to periodic updates to address emerging audit needs and evolving requirements.

INTRODUCTION

The Comptroller and Auditor General is appointed by the President and is the Head of the Supreme Audit Institution of Bangladesh. Mandated by Article 128(1) of the Constitution of Bangladesh, the Office of the Comptroller and Auditor General of Bangladesh (OCAG) is responsible for auditing government receipts and public spending and providing opinion as to whether these are duly accounted for and comply with the financial rules and regulations of the Government. Section 5(1) of the CAG (Additional Functions) Act, 1974 further gives the authority to audit statutory public authorities, public enterprises, and local authorities. The Constitution empowers the CAG to audit the public accounts of the Republic and, for that purpose, to have unrestricted access to all records, vouchers, documents or other items required for the audit.

The use of information technology for financial management and for performing their operations has become increasingly significant within the Government. IT auditing can make a significant contribution to the ability of the OCAG to fulfil its mandate.

As IT systems become increasingly integral to government operations, the role of OCAG is to provide assurance that appropriate processes are in place to manage IT-related risks. This includes verifying that controls have been implemented to ensure confidentiality, integrity, and availability of computerised data and systems. Additionally, the OCAG is responsible for reporting meaningfully on the efficiency and effectiveness of government operations supported by these IT systems.

The IT Audit Guidelines is compliant with the auditing standards as prescribed in Government Auditing Standards of Bangladesh (GASB), the INTOSAI Framework of Professional Pronouncement (IFPP), the International Standards for Supreme Audit Institutions (ISSAIs), ISO 27000-1 and the Bangladesh National Digital Architecture (BNDA)[1] Directives 2019**.** The guideline is fully aligned with the INTOSAI Guidance on Audit of Information Systems (GUID 5100)[2] and other relevant professional standards such as the Information Technology Audit Framework (ITAF 2020) of the Information Systems Audit & Control Association (ISACA)[3].

Users of the IT Audit Guidelines

The guidelines are intended primarily for use by OCAG IT Audit Teams who have demonstrated the necessary knowledge, skills and competencies to carry out audit procedures in an IT-based environment. It discusses the key control objectives that audit teams should consider when reviewing IT-related controls, and it provides examples of control techniques along with suggested audit procedures. The guidelines is mainly designed to support the review of both general and application controls.

On the other hand, this guideline is also applicable for conducting and supervising regular Compliance Audits, Financial Audits and Performance Audits carried out in IT environments. Furthermore, this guideline may also be used by OCAG for supervising the work of co-sourced specialists/experts.

[1] https://bnda.gov.bd/standards

[2] INTOSAI Guidance on Audit of Information Systems, June 2019 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

[3] https://www.isaca.org/about-us/newsroom/press-releases/2020/isaca-updates-it-audit-framework-itaf

Content and Structure of the Guidelines

The guidelines is organised into 7 chapters as set out below:

Table 1: Outline of Chapters

Chapter	Outline
Chapter 1 - Principles of IT Auditing	This chapter lays down the basic principles of IT audit that should be followed by the IT audit teams.
Chapter 2 - IT Audit Strategic Plan and Annual Audit Plan	This chapter includes the planning process and risk assessment for IT audit. It guides in working out strategic and annual plans for IT Audits.
Chapter 3 - The IT Audit Engagement Process	This chapter covers the IT audit engagement process that includes audit commencement, documenting IT architecture, risk assessment and engagement strategy, review and test IT controls, audit reporting and quality assurance review.
Chapter 4 - Review of IT General Controls	This chapter provides an in-depth analysis of IT General Controls domains, including key control objectives, associated risks, audit procedures, and co-sourcing considerations.
Chapter 5 - Review of Cyber Security Controls	This chapter outlines the key cybersecurity control areas, risk factors and assessment methodologies.
Chapter 6 - Review of Application Controls	This chapter provides guidelines on key application control domains, including control objectives, risk factors, audit procedures, and co-sourcing considerations
Chapter 7 - IT Audit in Support of Audit of the Budgetary Central Government Accounts	The chapter provides guidance to the audit teams in carrying out review of the control activities (input controls, processing controls and output controls) as part of the financial statement audit process.

Technical guidance on the use of Computer Assisted Audit Techniques (CAATs) and VAPT (Vulnerability Assessment and Penetration Testing) are beyond the scope of these Guidelines.

Scope of the Guidelines

Common audit issues are covered in separate audit manuals. This guidelines may be used to conduct Performance and/or Compliance Audits on the specific subject matter of Information System, as well as where audit of Information System is part of a larger audit engagement which may be a Financial, Compliance and/or Performance Audit.

Revisions to the Guidelines

These guidelines should be reviewed regularly and amended by periodic revisions to reflect the rapid changes in information technology as well as audit procedures.

1. CHAPTER 1 - PRINCIPLES OF IT AUDITING

This chapter lays down the basic principles of IT audit that should be followed by IT audit teams.

1.1. Effect of IT on Audit Procedures

1.1.1 The use of Information Technology (IT) within the Government and public sector entities in Bangladesh has become increasingly dependent on information systems for operations, particularly in processing and reporting essential financial information. As responsible party entities increasingly rely on IT systems, both the reliability of computer-generated information and the integrity of the systems themselves have a significant impact on the overall control environment and the audit process.

1.1.2 While IT offers significant benefits, it also presents a range of risks such as accidental loss of information, system failures, compromised data integrity, unauthorised access, misuse of system resources and vulnerability to fraud. To mitigate these risks, management must establish a system of controls. The whole set of controls in the IT environment is a combination of automated processes and manual control procedures designed to safeguard the system and ensure data integrity.

1.1.3 The audit mandate of the C&AG encompasses performing procedures to assess risks arising from the use of IT and reviewing IT system controls and processes with a view to obtain the expected level of Confidentiality, Integrity and Availability (CIA) through inter alia, the following assurances:

- **Safeguarding of IT/Digital Assets:** The IT physical assets and logical assets (information and software) are protected from damage or destruction, loss, unauthorised disclosure and unauthorised manipulation.
- **Data integrity:** financial and operational data captured, transmitted, stored, in-use and processed by IT systems are authorised, accurate, complete, non-redundant, timely and tamperproof.
- **Achievement of organisational objectives**: The IT/ digital systems are used efficiently and effectively to support achievement of organisational objectives, and the cost of acquisition and operation of IT system is justified by the benefits accrued.

1.2. Key Definitions in IT Audit

1.2.1 Audit of Information Systems may be defined as the examination of controls related to IT-driven information systems, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement i.e. financial audit, compliance audit or performance audit [4]

1.2.2 The WGITA-IDA Handbook on IT Audit for Supreme Audit Institutions defines IT Audit as an examination of aspects of an organisation's use of IT, including IT infrastructure, policies and

[4] INTOSAI GUID 5100 Guidance on Audit of Information Systems, June 20-19, pp 6 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

procedures, applications and use of data.[5] In other words, the audit of information systems, controls and processes is also referred to as an IT Audit.[6]

1.2.3 The ASOSAI IT Audit Guideline defines IT Audit as 'The process of collecting and evaluating evidence to determine whether an information system has been designed to maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and use resources efficiently'.[7]

1.2.4 The Information Systems Audit and Control Association (ISACA) defines the term IS Audit[8] as "IS audit is the formal examination and/or testing of information systems to determine whether-

- Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines.
- Information systems and related processes comply with governance criteria and related and relevant policies and procedures.
- Confidentiality, integrity and availability of IS data meet appropriate levels based on measurable metrics.
- IS operations are being accomplished efficiently and effectiveness targets are being met".

1.3. Auditing in IT Environments

1.3.1 In the context of compliance and financial audits, the use of IT has significantly transformed the methods of processing, recording and controlling financial information. Many functions that were previously handled separately are now integrated. Although efficiency has improved, the risk of material misstatements and instances of non-compliance has greatly increased.

1.3.2 While the overall objectives and scope of financial or compliance audits do not change in an IT environment, the use of technology changes the processing, storage and communication of financial information. This impacts the accounting and internal controls, making IT related risks a key concern. The financial auditors need to assess the risk of material misstatements due to incorrect processing of financial information. The compliance auditors will need to assess the risk of non-compliance arising from incorrect use of IT or ineffective management of IT systems. Therefore, there is a need to review and evaluate IT system controls in both financial and compliance audit to ensure such risks are adequately managed.

1.3.3 In performance auditing, IT Auditors shall examine the IT systems against the criteria of economy, efficiency, and effectiveness. Examining for economy in respect to the implementation of IT systems would essentially involve that resources are available at the best price and should be of appropriate quantity and quality and available at the right time. i.e. from the system acquisition to system implementation and regular operation. Examining for efficiency in respect of implementation of IT Systems would involve maximising the utilisation of the resources ensuring that output is complete, reliable and timely. Examining the effectiveness in respect of implementation of IT Systems means meeting the objectives set and achieving the intended results at the right time.

---

[5] https://idi.no/work-streams/relevant-sais/lota/wgita-idi-handbook-on-it-audit

[6] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions, INTOSAI IDI, Version 2022, pp. 1 (https://idi.no/work-streams/relevant-sais/lota/wgita-idi-handbook-on-it-audit)

[7] IT Audit Guidelines, 6th ASOSAI Research Project, October 2003, pp. 1

[8] CISA® Official Review Manual, 28th Edition, ISACA, pp. 31

1.3.4 To be able to perform audits in IT environments, the financial, compliance and performance auditors also need to understand how the specific applications process data and information and have the skills to access electronic data and perform data analysis using specialised tools such as Computer Assisted Audit Techniques (CAATs) for the purpose of gathering and analysing audit evidence. **The term capacity for "Auditing in IT environments" refers to acquisition of skills and knowledge to perform the audits in an IT environment. This includes the skills to evaluate IT risks and controls, ability to access electronic data and use CAATs to analyse data.**

1.4 IT Audit Objectives

1.4.1 The objective of IT Audit is to ensure that the IT resources allow organisational goals to be achieved effectively and use resources efficiently. IT audits cover ERP Systems, IS Security, acquisition, System Development and Business Continuity – all of which are specific areas of IS implementation.

1.4.2 IT audits vary based on the types of audits within which they are performed. **The objectives of IT audit within the scope of a financial audit include:**

- to review key general controls and related application controls within information systems that impact the reliability of system generated data,
- to assess the adequacy and effectiveness of management controls over IT processes,
- to evaluate the processes involved in the operations of a given area – a payroll or financial accounting system,
- to assess the effectiveness of controls on IT processes which affects information processing

1.4.3 **Audit objectives in the context of a compliance audit include:**

- to assess key general controls and related application controls on information systems,
- to ensure whether the information systems operation comply with relevant criteria, e.g., applicable laws, rules & regulations and standards.
- to assess the extent to which Third Party or Vendor management practices comply with IT security and regulatory requirements.

1.4.4 **The objectives of IT audit within the scope of a performance audit includes:**

- to ensure whether IT resources allow organisational goals to be achieved economically, efficiently and effectively,
- to review the performance of an IT systems
- to determine whether the acquisition and operation of the IT system meet the requirements and deliver value for money

1.5 Scope of IT Audit

1.5.1 IT audits are frequently a subject area within the context of a broader audit (i.e. performance, financial or compliance). IT Audits are generally performed in conjunction with a financial statement audit, a compliance audit, and/or as performance audits of IT systems or IT applications. Irrespective of the type of audit, the IT audit would be required to assess the

policies and procedures that guide the overall IT environment of the Responsible Party, ensuring that the corresponding controls and enforcement mechanisms are in place.

1.5.2 As part of financial audits, the auditors may need to understand, assess, and respond to the risk that arises from the use of IT. Therefore, an IT Audit may be needed to assess IT controls of the entity's information system, which are relevant to preparing the financial statements to evaluate whether it appropriately supports preparing the entity's financial statements (Refer to ISSAI 2315 (Revised 2019), 21 and 22).[9]

1.5.3 A compliance audit of the specific subject matter of information systems or, as part of a larger engagement, may entail gaining assurance on compliance of the information systems processes with the laws, policies and standards that apply to the audited entity.

1.5.4 A performance audit of the specific subject matter of information systems or as part of a larger engagement may entail drawing assurance that IT resources allow organisational goals to be achieved efficiently and effectively. This may include assessing whether the relevant general and application controls effectively prevent, detect and correct instances of excess, extravagance and inefficiency in the use and management of information systems.

1.5.5 The scoping of the IT Audit would involve deciding the extent of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations of IT systems to be covered, and the time to be covered.

1.6 IT Auditing Standards and Audit Criteria

1.6.1 The specialised nature of IT auditing and the skills necessary to perform such audits is based on certain standards. In response to this need, various professional and government organisations have developed and maintained standards and guidelines for IT auditing. The professional standards provide a framework and define the mandatory requirements of the audit. These includes the International Standards for Supreme Audit Institutions (ISSAI) and the INTOSAI GUID 5100 Guidance on Audit of Information Systems[10]. It is also compliant with the ISACA IT Assurance Framework (ITAF) 2020[11] and the Bangladesh National Digital Architecture (BNDA) Directives 2019. In addition to IT auditing standards, IT auditors need to be alert to other laws and regulations that may impact upon the conduct of an IT audit.

1.6.2 IT Governance principles, security frameworks and control guidelines have been developed by Government and various professional IT bodies. These are primarily designed for use by the management and IT personnel of an organisation to operate Information Technology systems for achieving organisational objectives and for ensuring system security and efficiency of IT systems. These standards also serve as audit criteria, enabling IT Audit Teams to assess risks and evaluate IT controls in responsible party organisations.

1.6.3 This Guidelines contain suggested matrix/audit work programmes for review and testing of IT controls with reference to audit standards and IS regulatory frameworks as set out below table. However, these are not exhaustive, and other standards and authorities may also apply in the audit process.

[9] INTOSAI GUID 2900, Guidance to the Financial Auditing Standards, 2021 (www.issai.org/wp-content/uploads/2021/12/GUID-2900-Guidance-to-the-financial-auditing-standards.pdf)

[10] https://www.issai.org/pronouncements/guidance-on-audit-of-information-systems/

[11] https://www.isaca.org/about-us/newsroom/press-releases/2020/isaca-updates-it-audit-framework-itaf

Table 2: IT Standards and Regulatory Frameworks

Audit Standards and IS Regulatory Frameworks	Description and Application
The Cyber Security Ordinance, 2025	The Cyber Security Ordinance, 2025 establishes a legal framework to protect national cyber and digital space of Bangladesh. It outlines responsibilities for both public and private sectors to prevent cyber threats, attacks, and data breaches.
Bangladesh Telecommunication Act, 2001 (Amended 2010)	The Bangladesh Telecommunication Act, 2001 (Amended 2010) regulates the establishment and operation of telecommunication services in Bangladesh. The Act also outlines provisions for fair competition, consumer rights, and penalties for violations in the telecommunications sector.
Right to Information Act, 2009	The Right to Information Act, 2009 empowers citizens to access information held by public authorities, promoting transparency and accountability. The Act plays a crucial role in fostering an open government and enabling public participation in governance.
Bangladesh High-tech Park Authority Act, 2010	The Bangladesh High-Tech Park Authority Act, 2010 establishes the Bangladesh High-Tech Park Authority to promote, regulate, and develop high-tech parks across the country. It aims to attract investment, encourage innovation, and create a knowledge-based economy by providing necessary incentives and infrastructure.
The Bangladesh Computer Council (BCC) Act, 1990	The Bangladesh Computer Council (BCC) Act, 1990 established the BCC as a statutory body to promote and support computer and IT development across Bangladesh. Overall, the Act aims to drive ICT growth and capacity building to advance national progress.
Agency to Innovate (a2i) Act, 2023	The Agency to Innovate (A2i) Act, 2023 formally established the Agency to Innovate (A2i) as a semi-autonomous government body under the Ministry of Information and Communication Technology. Its mission is to foster innovation in the information technology sector and support the government's efforts in building a knowledge-based society.
Information Technology (Certifying Authorities) Rules, 2010	The Information Technology (Certifying Authorities) Rules, 2010 provide the regulatory framework for the issuance and management of digital certificates in Bangladesh. These rules establish the roles and responsibilities of certifying authorities to ensure secure electronic transactions and authentication.
Bangladesh High-tech Park Authority Rule, 2015	The rules are pursuant to the Bangladesh High-tech Park Authority Act, 2010
International Standards for Supreme Audit Institutions (ISSAI)	The ISSAIs are the authoritative international standards on public sector auditing. These include Fundamental Principles of Financial Auditing (ISSAI 200) and Standards (2000-2899), Performance Auditing Principles (ISSAI 300), Standards (ISSAI 3000-3899) and Compliance Auditing

Audit Standards and IS Regulatory Frameworks	Description and Application
	Principles (ISSAI 400), Standards (ISSAI 4000-4899).
GUID 5100 (Guidance on Audit of Information Systems) – June 2019	INTOSAI Guidance is issued by the International Organisation of Supreme Audit Institutions as part of the INTOSAI Framework of Professional Pronouncements. INTOSAI GUID 5100[12] provides the framework for conducting audit of Information Systems. It provides guidance on how to conduct Performance and/or Compliance audits related to the specific subject matter of Information Systems or where the audit of information systems may be part of a larger audit engagement which may be financial, compliance or performance audit.
WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions (Version 2022)[13]	The WGITA/IDI handbook follows the general auditing principles as laid down under the International Standards for Supreme Audit Institutions (ISSAI). [14] The handbook also draws from internationally recognised IT frameworks, including ISACA's COBIT framework, ISO Standards and IT guides and manuals of some SAIs.
COBIT (Control Objectives for Information and Related Technologies) Framework	IT Governance framework developed by the Information Systems Audit & Control Association (ISACA) for information technology (IT) management and to support IT governance. It provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices to ensure that IT is aligned with the business, IT maximises benefits, IT resources are used responsibly, and IT risks are managed appropriately. The COBIT framework divides the IT processes into four main domains: ● Plan and Organise (PO) ● Acquire and Implement (AI) ● Deliver and Support (DS) ● Monitor and Evaluate (ME) Together these domains encompass 34 standard IT processes for which the COBIT provides the best practices guidelines.
ISO/IEC 27001 series of IT security standards have been developed by the International Standards Organisation (ISO). Third Edition 2022[15]	ISO 27000 series of IT security standards have been developed by the International Standards Organisation (ISO). ISO 27001 provides a framework for IT security management and ISO 27002 prescribes the Code of Practice

[12] INTOSAI GUID 5100 - Guidance on Audit of Information Systems, June 2019 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

[13] https://idi.no/elibrary/relevant-sais/lota/wgita-idi-handbook-on-it-audit-for-sais/1632-wgita-idi-handbook-on-it-audit-for-sais-2022-en?format=html

[14] www,issai.org

[15] https://www.iso.org/standard/27001

Audit Standards and IS Regulatory Frameworks	Description and Application
	for IT security controls. ISO 27000 series standards for IT security. IS0 38500 (IT Governance) provides a framework for effective IT Governance. **Major Coverage** ● **Security Policy** - Information Security Policy document and Review of Information Security Policy ● **Organisation of Information Security** - Internal Organisation, External Parties, ● **Asset Management** - Responsibility for assets, Information Classification ● **Human resources security** - Prior to employment, During Employment, Termination or change of employment. ● **Physical and Environmental security** - Secure Areas, Equipment Security ● **Communication and Operations Management** - Operational procedures and responsibilities, Third party service delivery management
Bangladesh National Digital Architecture (BNDA) Directives 2019[16]	The BNDA is the national standard that governs the implementation and management of information systems. Collection of policies, standards, and guidelines to guide government agencies in the design, acquire, implement, and manage ICTs. BNDA Version 2.0 Standards comprises of the following: ● Application Architecture Standards ● Business Architecture Standards ● Data Architecture Standards ● e-GIF Standards ● Mobile Service Delivery Platform Standards ● Security Standards ● Technology Architecture Standards ● Hardware Specification Standards
Government Email Policy	Secure and effective use of the government email services.
Data Loss Prevention (DLP) Policy for National Data Center (NDC)	The requirements for data leakage prevention, as defined by numerous compliance standards, industry best practices and associated processes.
National ICT Policy	The Bangladesh government defined a single vision, 8 objectives, 55 strategic themes and 343 action items through this policy.
Government of Bangladesh Information Security Manual (GoBISM)[17]	Based on international standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013. The controls presented in GoBISM are applicable to all government

[16] https://bnda.gov.bd/standards

Audit Standards and IS Regulatory Frameworks	Description and Application
	unclassified systems and information.
The Computer Personnel Recruitment Act 1985 (Correction 1995)	Recruitment roles of IT personnel in government organization.

1.7 IT Controls Framework

1.7.1 Controls in an information technology environment (Figure-1)[18] reflect the policies, procedures, practices and organisational structures designed to provide reasonable assurance regarding effectiveness and efficiency of IT systems operations, reliability of information and compliance with the rules and regulations.

1.7.2 The presence of controls in a computerised system are crucial for audits because inadequately controlled systems may allow duplication of input or processing, concealment and unauthorised manipulation of data. IT audit provides assurance that adequate information system controls are in place.

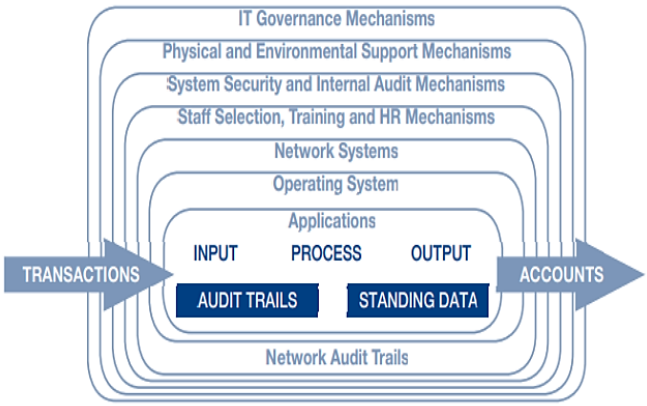
1.7.3 For some of the entities audited by OCAG, where IT systems are outsourced to external service providers, there is an increased risk from the service providers failing to implement adequate controls or adhere to appropriate IT Standards.

1.7.4 Internal controls may be more complex in computerised accounting systems due to the presence of automated programmed procedures. In a manual system, controls may have been developed and implemented over time. However, for an IT system the controls need to be built into the system at the development stage. Adding or modifying controls after implementation can be difficult and expensive.

1.7.5 In the IT environment, controls form part of the overall internal control structure of an entity and are divided into two broad categories:

- **General IT Controls**
- **Application Controls**

Figure 1: IT Controls Framework



17 https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/publications/2deab15c_0f40_467c_b904_f6b452cefb98/2020-10-20-00-06-3c4d70967af91d8cdfffe90030da839d.pdf

18 AFROSAI-E INFORMATION SYSTEM AUDIT GUIDELINE – 2023, pp. 17, URL- https://afrosai-e.org.za/wp-content/uploads/2024/07/AFROSAI-E-IS-Audit-Guidelines_Nov-2023.pdf

1.8 IT General Controls

1.8.1 . IT General Controls are manual or automated procedures which aim to ensure confidentiality, integrity and availability of information in the physical environment within which information systems are developed, maintained and operated.[19] These controls are not specific to individual applications or transaction streams.

1.8.2 This guidelines provides guidance on review and evaluation of major categories of IT general controls:

- Organisation and Management Controls (OM)
- Physical and Environmental Controls (PE)
- Segregation of duties (SD)
- IT Security - Security Management (SM)
- IT Security - Access controls (AC)
- System/Service Acquisition, System development and Programme Change Controls (CC)
- Business Continuity Planning and Disaster Recovery (BC)
- Network Controls (NC)
- Data Management Controls (DC)
- Cyber Security Controls (CS)

1.9 Application Controls

Application controls are controls specific to an application. They include controls that help to ensure the proper authorisation, completeness, accuracy and validity of transactions and other types of data input[19]. Application controls address three major operations of data input, data processing and data output. However, data transmission may also be considered as a part of application controls within the operational scope of the application.

1.10 An Overview of IT Audit Methodology (Three Level Approach)

1.10.1 Planning for IT Audits

1.10.1.1 GUID 5100[19] requires that SAIs adopt **a risk-based audit planning for IT audits**. Planning a risk-based audit is carried out at three levels:

- Strategic IT Audit Plan
- Annual IT Audit Plan
- IT Audit Engagement Plan (following a risk-based approach)

1.10.1.2 IT Audit Strategic Plan: For preparing the IT Audit Strategic Plan, the IT and Public Services Audit Directorate and concerned Audit Directorates should periodically undertake a survey of the IT systems in operation across the government and responsible party organisations. This will enable to identify the entire range of auditable IT systems and activities and define the IT Audit Universe.

1.10.1.3 The risk of each auditable IT system will be assessed using a risk scoring method and the auditable IT systems will be categorised in accordance with their respective risk rankings with a view to prioritizing the audits.

[19] INTOSAI GUID 5100 - Guidance on Audit of Information Systems, June 2019, pp 7 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

1.10.1.4 This process will enable the development of a rolling Strategic IT Audit Plan for conducting IT audit engagements over a period of 3-5 years and annual IT audit work plans.[20]

1.10.1.5 **Engagement Level Risk Assessment:** An IT audit engagement is divided into three distinct phases.

- Risk assessment and planning.
- Performance of the audit
- Reporting.

1.10.2 Audit Risk

1.10.2.1 At the IT audit engagement level, the **Audit Risk** is defined as the risk that the IT Audit Team may fail to report a material IT control weakness. According to the audit risk model, audit risk is essentially a combination of three components. These are: inherent risk, control risk and detection risk. Inherent and control risk pertain to the audited entities. Detection risk falls within the domain of the audit team.

1.10.2.2 If any audit engagement is performed without assessing the audit risks, the engagement will not be considered as conforming to Government Auditing Standards of Bangladesh, regardless of the number of analytical procedures and substantive tests.

1.10.2.3 Inherent Risk is a risk that something might go wrong because of reasons of the nature of the organisation or the activities of the organisation and not due to any specific control failure.[21] For example, all online information assets are exposed to the risk of hacking. No matter what technology-driven mitigating controls are used to reduce the possibility of the threat materialising, this threat will always be there. In case of an IT audit engagement, the audit team assesses the Inherent risk arising from the use of IT. This is achieved by obtaining an understanding of the entity's operations, IT architecture and IT systems.

1.10.2.4 Control Risk is the risk that something might go wrong because of lack of internal control or an incident of control failure. For example, an information system of an audited entity is required to ensure that access to confidential data is restricted to authorised personnel may adopt the control of requiring the presentation of a username and password by personnel attempting to gain access. The control risk in this situation is that the username and password are not adequately secure and can be guessed by unauthorised personnel through repeated attempts, resulting in loss of confidentiality and potential adverse impact on the entity. To assess control risk, the audit team must first obtain an understanding of the responsible party's control structure sufficient to identify the types of potential material IT risks. For this purpose, the IT Audit Team performs a preliminary review of IT controls and prepares an audit engagement plan for detailed testing of the controls.

1.10.2.5 **Relationship between Inherent Risk and Control Risk:** It is desirable that higher the inherent risk, control risk should be lower. In other words, if the inherent risk is perceived high, there should be more control measures in the organisation so that the overall risk comes down. This will lead to low control risks. However, inherent risks and control risks being entity risks and beyond the control of the audit team, the latter should use detection risk to minimise audit risk.

---

[20] Detailed procedures on IT audit strategic planning process are at Chapter 2 of this Guidelines

[21] Compliance Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 22 October 2021, pp. 143 (https://cag.org.bd/storage/app/uploads/public/64a/65f/bd9/64a65fbd947c7705459153.pdf)

1.10.2.6 **Relationship with Audit Risk:** There is a direct relationship between audit risk, inherent risk and control risk. If inherent risk is high, the audit risk will be high. Similarly, if the control risk is high, audit risk will be high. If the inherent risk is high or the control risk is high, then the chances of not being able to detect a misstatement or deviation goes up. This increases the audit risk. One way to bring down the audit risk (i.e. to minimise chances of not detecting a misstatement or deviation) is to increase the scope and volume of audit tests. This minimizes the detection risk.

1.10.2.7 Detection Risk is a controllable variable in the audit risk equation and depends on the assessment of inherent and control risk. It follows that if the audit testing is increased in scope and volume, chances of failing to detect a misstatement or deviation would go down. The level of detection risk is inversely related to the extent of substantive testing required.

1.10.2.8 On the basis of the level of audit risk, the audit team determines substantive audit procedures. The assessment of control risk, combined with the assessment of inherent risk form the basis for determining the detection risk and designing substantive audit programmes. Any material weaknesses identified during the assessment of control risk must be communicated to the management.

1.10.3 Materiality

1.10.3.1 Materiality refers to the extent to which any misstatement or omission or deviation impacts the judgment of the users and stakeholders of the report. The concept of materiality is crucial in assurance audit because it is a key factor for determining the nature, timing and extent of audit procedures. The perspective of materiality may vary depending on the nature of the IT audit engagement.[22] In case of a financial statement audit, materiality is determined considering the extent or value of the misstatements. In the context of an IT audit, it depends on the potential consequences of IT control failure.

1.10.3.2 A material IT control weakness significantly impacts IT operations and the achievement of organisational objectives. The IT Audit Team shall consider potential weaknesses or absences of controls during audit planning, and whether such weaknesses or absences of controls could result in a significant deficiency, material weaknesses or financial losses. Materiality will be determined using judgement and consider the overall materiality for the organisation such as quantitative and qualitative aspects, as in financial statement audits.

1.10.4 IT Audit Engagement Process [23]

1.10.4.1 In the IT audit engagement, a risk-based audit methodology is followed. The IT audit engagement has the following stages:

Table 3: IT Audit Engagement Stages

Stage	Outline
Risk assessment and Planning	Obtain information on the responsible party and its IT environment. This will enable the IT Audit team to assess the inherent risks arising from the use of IT. This will also enable the general financial / compliance audit team to determine whether to seek the assistance of the specialist IT Audit Team/external experts in the evaluation of the controls and in conducting

[22] ISSAI 100 paragraph 41 states that ”materiality is often considered in terms of value, but it also has other quantitative as well as qualitative aspects”.

[23] Chapter 3 of this Guideline provide detailed guidance on conducting an IT audit engagement and Chapter 4-6 provide the detailed audit work programmes for review and testing of IT controls.

Stage	Outline
	substantive testing.
Tests of controls	The IT audit team will review and test the IT General Controls first and then Application Controls to gain an assurance that the controls are effective and that they have operated as intended throughout the applicable scope. This will enable the audit team to suitably reduce the control risk and reduce the extent of the substantive procedures.
Compliance Testing	These are audit tests designed to confirm that controls have been operated as intended. Usually, it includes only testing key controls i.e. those which are relied on to meet control objectives.
Substantive Testing	Based on the assessment of IT controls, the audit team may identify priority areas for substantive testing, which involves detailed testing of the IT controls using various techniques for enquiry, data extraction and analysis of data. To ensure that the audit findings are well supported, the IT audit team must collect and document sufficient, reliable and accurate electronic evidence. For this purpose, the audit team may need to seek assistance from specialist IT Audit Teams to access computerised data and perform tests of transaction and operational data using computer assisted audit techniques (CAATs).
Reporting	The IT Control weaknesses identified during the audit should be discussed with the Responsible Party at the 'Exit Meeting'. The material control weaknesses and unresolved issues with IT systems should be brought to the attention of the stakeholders through a management letter and the IT Audit Report.
Review and Quality Control	IT Audit needs to be subject to the same degree of quality control as other audit work.

CHAPTER 2 IT AUDIT STRATEGIC PLAN AND ANNUAL AUDIT PLAN

Chapter 2 describes the IT audit planning process and methodology of risk-assessment for selecting IT audits. This chapter will guide the OCAG and relevant audit directorate in working out strategic and annual plans for IT Audits.

2.1 Overview of IT Audit Planning

2.1.1 Audit planning is a key part of any audit, including IT Audit. Planning for audits is carried out at three levels – strategic planning, annual planning, and entity level planning. The audit directorates are the focal points for preparation of audit plans.

2.1.2 The IT and Public Services Audit Directorate and concerned audit directorates will plan for conducting IT Audits using a risk-based approach in line with the process described in ISACA Information Technology Audit Framework (ITAF), ISSAI 100, ISSAI 200 (Financial Audit), ISSAI 300 (Performance Audit) and ISSAI 400 (Compliance Audit), depending upon the objectives of the audit engagement. The IT audits will be prioritised and select what audits will be conducted based on risk assessment. Figure 2 shows that IT audit plans will be developed at three levels – strategic, annual and engagement.

2.1.3 Audit plans are required to be prepared in accordance with time schedule circulated by the Accounts and Reports (A&R) wing of OCAG to ensure timely submission. The audit plans shall be implemented only after approval by the C&AG or an officer delegated with powers in his office. It is expected that the plans are discussed in detail before approval.

Figure 2: Levels of IT Audit Planning



2.2 General IT Survey and the Audit Universe

2.2.1 An audit universe represents the potential range of all IT audit activities and Responsible Parties (RPs). As far as IT audit is concerned, the auditable activities will include the IT systems and applications that contribute to the achievement of the organisation's objectives. As the first step in implementing a successful risk-based audit process, the OCAG will define the audit universe by collecting information about the IT systems in use in the various entities. For this purpose, **Appendix *1*: General Review of IT Survey** may be used.

2.2.2 The OCAG will prioritize IT systems with high risk. The classification will be based on the understanding of the system and its environment and professional judgement. The IT and Public Services Audit Directorate and concerned Audit Directorate will undertake a risk assessment and prepare IT audit strategic plan and the IT audit annual plan as per guidance contained in the next section.

2.3 IT Audit Strategic Plan and Annual Audit Plans

2.3.1 IT audit standards and best practices provide three levels of IT audit planning.

- Strategic Planning
- Annual Audit Plan
- Audit Engagement Plan

Table 4: Three Level Approach to IT Audit Planning

Planning Level	Purpose
Strategic Audit Plan	The Strategic IT Audit Plan sets a framework for identifying the tasks of the OCAG over a longer timeframe, usually covering a period of 3 years and identifies the audit engagements to be taken up in each of the years. It also outlines the objectives and scope and allocation of resources for the planned audit assignments. A list of new and emerging IT areas to audit may be included in the strategic plan.
Annual Audit Plan	The objectives of the Annual Audit Plan are to identify and schedule the audit engagements for the year. The annual audit plan for the current year should be derived from the IT audit strategic plan.
Audit Engagement Plan	The audit engagement level plan covers a particular IT audit engagement including details such as the risk assessment of the IT system or application to be audited, the audit strategy and work programme, details of the members of the audit team and allocation of work and logistical details.

2.3.2 The IT audit strategic plan and annual IT audit plans are essential requirements for meeting the goals and objectives of the IT audit function. The risk-based audit planning exercise will enable to decide what areas will be audited annually. Given the rapid expansion of modern IT systems across the government and the limited resources available to OCAG, adopting a risk-based approach to prioritize and select topics that would be appropriate. The IT audit work plans should be developed as a **strategic three-year rolling plan** by considering the potential risks to the organisation in accordance with the methodology described in the section below.

2.3.3 This methodology provides a technique for risk assessment and prioritization of the audit areas by assigning scores to various risk factors for each auditable activity. The IT audit strategic plan should be reviewed annually by re-evaluating and refining the risk factors and risk scores periodically or as needed.

2.3.4 In accordance with the Government Auditing Standards of Bangladesh, OCAG may seek and utilize the assistance of outside experts to support IT Audit planning, particularly in the areas of risk assessment and prioritisation of audit areas. As the capabilities of government automated systems continue to expand and become more complex, a thorough understanding of these systems requires specialised technical experts.

2.4 Risk-Based Audit Planning Process

2.4.1 The process for identification of the audit universe, risk assessment and preparation of the audit strategic plan and annual audit work plan is a structured four step process comprising the following:

- Obtain information and knowledge of IT systems and applications in the government.

- Identify the audit universe that will comprise the listing of all Information Systems and Processes of Responsible Parties under the jurisdiction of OCAG.
- Assess the risks associated with the auditable IT activities using a predetermined set of risk factors and ranking the auditable IT activities in accordance with assessed risk.
- Prepare IT Audit Strategic and Annual Audit Plans

2.5 Obtain Knowledge of Responsible Party IT Systems

2.5.1 With the increased computerization of financial and operational systems amongst the responsible party organisations, it is necessary for the IT and Public Services Audit Directorate and the concerned Audit Directorates to gather and document information on the IT systems. This information will enable to assess the risks arising from the use of IT by these organisations.

2.5.2 The General Review of IT Survey is designed to enable Audit Directorates to gain an understanding of hardware and software, IT personnel, IT budget, policies and procedures, nature of operations and extent of any known problem areas.

2.6 The Audit Universe

The next step leading to the development of the risk-based IT audit strategic plan and the annual audit plan is to establish the audit universe representing the total population of potential IT audit engagements. The output from the previous process will be used as input for developing the IT audit universe.

2.7 Consideration of Risk Factors

2.7.1 The IT audit strategic plan will prioritize the IT audit systems with the greatest risk exposure. For this purpose, the risk assessment methodology explained in the following sections may be followed.

2.7.2 Risks can be assessed both quantitatively and qualitatively. As a means of narrowing subjectivity and increasing consistency of evaluation, a numerical scale is adopted in which the IT audit team provides scores to each of these factors in a scale of 1-5. A methodology may be selected which is appropriate for the purpose. Such methodologies will be on the classifications of the risk profile of the IT environment and numeric calculations which quantify the risk rating based on objective data gathered from the audited organisation. The classification will be based on the understanding of the entity and the IT system and professional judgement. Professional judgement would mean that collectively the audit engagement team will assess the risks and allot quantitative values to each of these risks. Each of these risk factors is given a weight in accordance with their perceived influence to determine the overall risk exposure to an auditable activity.

2.7.3 The qualitative assessment would be three levels namely High, Medium and Low. The acceptable level of audit risk should be ‘LOW’. To keep the audit risk at ‘LOW’, at least two levels of risks should be low and the third one at medium. Audit risk cannot be low if detection risk is high. The best scenario would be to have inherent risk and detection risk at low level and control risk at not more than medium level.

2.7.4 The risk exposure of auditable IT systems is given risk scores based on consideration of “impact factors” and “probability factors”. The impact factors and the probability factors listed below are used to determine the overall impact of the risk exposures.

2.7.5 **Impact Risk Factors** - The risk scores allocated for the impact risk factor are determined by risk conditions where 1 = low and 5 = high. The impact risk factors with their respective weights are listed below:

Table 5: Impact Risk Factors

Impact Risk Factors	Allocated Weighting (%)
Strategic importance (Importance of the IT system or application for achieving the strategic objectives of the organisation)	20%
Operational criticality (Non-availability of IT system or application is of critical importance for the operations)	30%
Materiality (Size of the budget allocation compared to total budget)	25%
Stakeholder/Management interest (The degree of management interest in having an independent assessment of the IT system)	25%
TOTAL	**100%**

2.7.6 The **Probability Risk Factor** conditions increase the probability of the risk exposure for the auditable activity where 1 = low and 5 = high. The probability risk factors with their respective weights are listed below:

Table 6: Probability Risk Factors

Probability Risk Factors	Allocated Weighting (%)
Nature of operation and external environment (SWOT analysis)	25%
Major changes in Policy/Process/Personnel	15%
Past audit issues (degree of seriousness of the unresolved audit issues)	25%
Complexity of IT systems	15%
Fraud vulnerability (fraud control policies and procedures)	20%
TOTAL	**100%**

2.8 Risk Assessment of Auditable IT Systems

Based on the available information on the IT systems, the IT Audit Team uses judgement to evaluate the risk scores for each impact and probability risk factor. This may form the basis for determining the high-risk areas that may be audited.

2.9 Preparing the Strategic IT Audit Plan

After conducting a risk assessment, the audit team may develop an overall audit strategy that determines the priorities for the effective allocation of audit resources. The objective of the audit strategy is to document the scope, timing and direction of the audit being performed. Where the engagement is part of a larger audit (financial, compliance or performance) engagement, there is no need for a separate strategy.

2.10 Developing the Annual Audit Plan

The annual audit plan will be prepared from the strategic plan after considering the available personnel and other resources. Annual audit planning involves the development of a detailed audit plan of the selected audit organisation, beginning with outlining the audit objectives. The audit plan will assist the audit team in preparing an IT audit programme. This can be done at annual intervals and could be a recurring plan.

CHAPTER 3 THE IT AUDIT ENGAGEMENT PROCESS

This chapter covers the IT audit engagement process that includes audit commencement, documenting IT architecture, risk assessment and engagement strategy, review and test IT controls, quality assurance review and IT audit reporting.

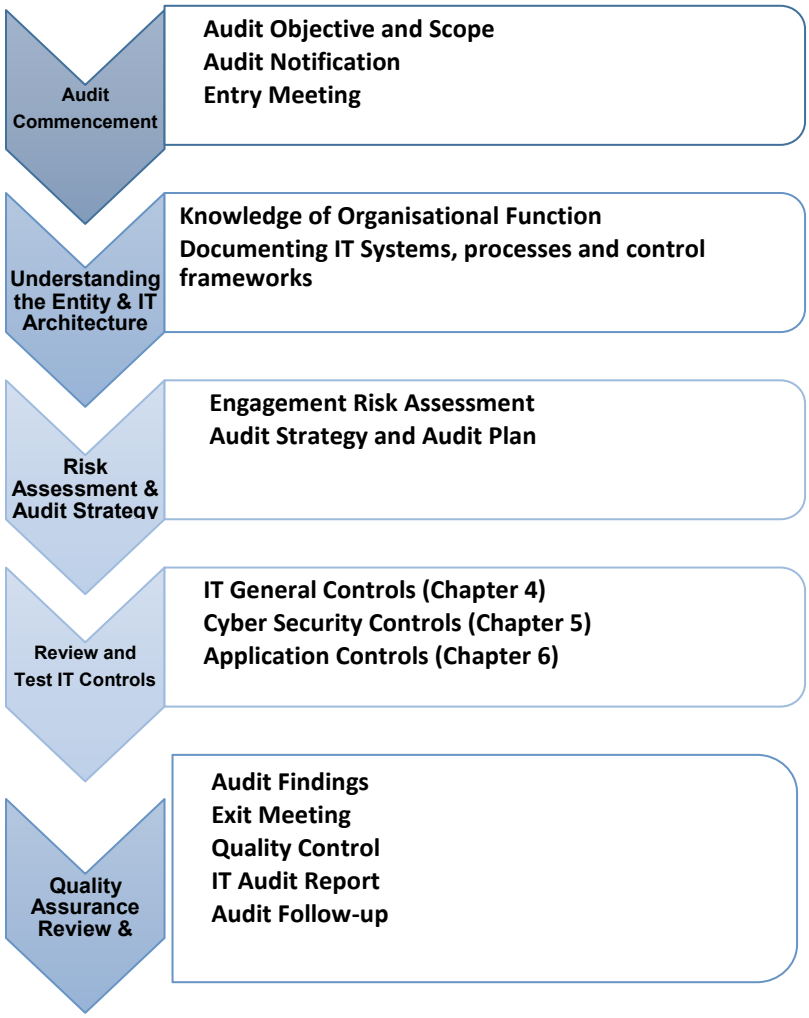
3.1 Types of IT Audit Engagement

3.1.1 An IT audit engagement may be one of two types which this section provides guidance to perform:

- standalone assurance audit of an IT system or an IT application or one of a specific domain such as IT governance and management, IT security, IT acquisition or a system under development
- review of IT systems controls conducted as part of a financial, performance or compliance audit.

3.1.2 Figure 2 below represents the various phases and steps in the IT audit engagement process.

Figure 3: IT Audit Engagement Process



3.2 Audit Commencement

For scheduled IT audits, the commencement information will come from the Annual IT Audit Plan. The Annual IT audit Plan may include IT audits conducted as part of financial or compliance or performance audits. The estimated time budget for the engagement is obtained from the annual audit plan.

3.2.1 Audit Objective

3.2.1.1 For planned IT audit engagements, the audit objectives will derive from the risks identified during the preparation of the annual IT audit plan. For non-plan engagements, the objectives are established prior to the start of the engagement and are designed to address the specific issue that prompted the engagement.

3.2.1.2 The initial audit objectives and scope may be further refined, and other significant areas of concern may be identified, based on an understanding of the IT systems and the specific risks associated with these IT systems.

3.2.2 Audit Scope

The 'scope' for the IT audit engagement involves the extent of audit coverage and includes consideration of all relevant IT systems, IT infrastructure and facilities, IT processes, electronic records, personnel and outsourced IT activities to be covered. The scope defines the subject matter that the audit team will assess and report on, such as a particular system or application, the necessary documents or records, the period reviewed and the locations that will be included. The audit scope statement should also identify any areas, processes or activities which are *kept outside* the audit and the reasons for not including them.

3.2.3 Audit Notification

The purpose of the audit notification letter provides a formal statement regarding the terms and objectives of the engagement and of the nature and scope of the IT audit to be conducted. It also introduces the IT audit team to the responsible party management and informs about the timelines of the key deliverables and milestones. Aspects which should be covered in the IT audit engagement letter include:

- The objective of the audit
- Management responsibilities about the IT systems controls
- Scope of the audit
- Unrestricted access to documentation and other information including data held inside the responsible party computer system requested.

3.2.4 Entry Meeting

3.2.4.1 The goal of the entrance meeting is to reach a clear understanding with the responsible party management and IT personnel regarding the objective and scope of the IT audit engagement, the audit methodology and cooperation needed from the responsible party.

3.2.4.2 The entry meeting is held to create awareness of the responsible party about the following:

- The purpose and objective of IT audits
- OCAG's mandate to perform audits of government IT systems.
- Concepts of IT risks and controls
- The audit criteria and standards to be used.
- The IT audit methodology and the IT audit process
- Access to system documentation, policies, plans and records needed for the audit.

- Access to system data for using digital audit tools like CAAT.

3.3 Understanding the Entity and IT Environment

The audit team should first develop and document a high-level understanding of the entity and how the entity is supported by automated systems. This should include obtaining an overview of the application.

3.3.1 Knowledge of Organisational Function

3.3.1.1 The primary objective of the IT systems is to support the organisational functions, work processes and achievement of its objectives. The IT audit team should obtain a high-level understanding of the responsible party organisational objectives, the nature of its operations and services that are significant to the audit process.

3.3.1.2 For this purpose, the IT Audit Team should review the entity's organisational strategy and objectives, long term and short-term plans, the organisational structure and the environment in which it operates. This knowledge helps the IT audit team to identify the *IT systems and applications that support critical organisational processes and the risks arising from the use of IT*. **Appendix *1*: General Review of IT Survey** includes a Background Information Questionnaire to facilitate this initial step.

3.3.2 Documenting IT Systems and Control Frameworks

3.3.2.1 For planning engagement, the IT audit team will develop a thorough understanding of the responsible party's IT infrastructure and applications architecture. A detailed understanding of the criticality of the IT systems will enable the audit team to assess IT risks and the expected key controls.

3.3.2.2 For this purpose, the IT audit team will use techniques like examination of documents, interviews with key personnel and observation of procedures. Study of IT policies and procedures, application-specific user manuals, documentation on IT outsourcing contracts, functional design documents, vendor-supplied technical reference manuals and list of reports.

3.3.2.3 The IT audit team will gather information and supporting documents and record understanding of the IT system covering the following:

Table 7: Knowledge of IT Systems

Objectives	Scope and Tasks
Understand key functional processes supported by IT	Identify and record functional processes and critical operations
	Identify all IT applications
Evaluate policies and procedures	IT Security and Related Other Policies and Procedures
	Identify Change and Problem Management practices
	Identify System Acquisition and Development processes
	Identify Disaster Recovery and Contingency Planning
	Review and Record Physical Security.
Evaluate IT organization	Obtain IT organisational charts
	Review job descriptions of IT personnel responsible for the IT infrastructure, operating systems, and the applications
Evaluate IT environment and technology infrastructure	Record the IT environment and technology infrastructure including list of applications, systems software, and database software
	Record the operating systems software and other systems software
Assess Data centre and facilities	Draft or obtain data centre diagram
	Identify all servers

Objectives	Scope and Tasks
	Record all server configurations and virtualisation
	The servers such as network servers (e.g. Windows 2022/2025, Linux), the application and database servers, email servers are fully segregated using different physical servers or in a virtualised environment
	Identify server virtualization specifications and architecture documentation.
	Record environmental protection equipment
Assess network and communication equipment	Record or obtain Network diagram
	Identify all Routers
	Identify all Switches
	Identify all Firewalls
	Identify all DMZ (Demilitarized Zone)
	Identify all Gateways
	Identify all Wi fi equipment
	Identify all Internet connections
Review IT applications	For supporting the audit of application controls, the IT audit team will need to obtain an in-depth understanding of the information flow and develop documentation and flowcharts of the application covering: • Draft or obtain system description and flowcharts • Identify data input processing and outputs • Identify all application owners, custodians, and users • Identify standing data including master files and data files

3.4 Risk Assessment Engagement Strategy and Audit Plan

3.4.1 Risk Assessment

3.4.1.1 The engagement risk assessment will enable the audit team to rank the IT General Domains based on their respective risks[24]

3.4.1.2 Based on the risk assessment the audit team will provide the Likelihood and Impact scores for each IT General control domain and enter the scores in the following matrix: (refer to **Figure *3*: Engagement Risk Assessment**)

Figure 4: Engagement Risk Assessment

SL no	Control Domain	Likelihood	Impact	RISK	
1	Organisation and management controls (OM)	5	5	25	Critical
2	Physical and environmental controls (PE)	3	5	15	Very High
3	Segregation of duties (SD)	1	1	1	Negligible
4	IT security - Security Management (SM)	5	5	25	Critical
5	IT security - Access controls (AC)	5	5	25	Critical
6	System development and program change (CC)	2	3	6	Medium
7	Business continuity planning and disaster recovery (BC)	2	4	8	Medium
8	Network controls (NC)	2	2	4	Low
9	Database control (DC)	3	3	9	Medium
10	Cyber security controls (CS)	5	5	25	Critical

[24] Refer to **Appendix 2: IT risk identification** for guidance of the risk assessment process

3.4.2 Engagement Strategy and Audit Plan

3.4.2.1 The audit team should ordinarily make a preliminary evaluation of the controls and develop the audit plan based on this evaluation. The audit plan summarizes the results of the following audit procedures performed at the planning phase:

- Obtaining knowledge of entity's business
- Understanding of IT environment and applications
- IT risk assessment

3.4.2.2 The audit plan records the IT audit team's approach and strategy to determine if the significant IT risks have been reduced to acceptable levels. For this purpose, the IT audit team will verify if the identified key IT controls are working as expected (*detailed test of controls*) and gather evidence to substantiate the extent of residual risks (*substantive tests*).

3.4.2.3 The plan and work programmes enable the–audit team to effectively use the audit resources and achieve the audit objectives during the audit execution phase. The plan specifies the nature, timing and extent of the tests to be performed and the sources of audit evidence in response to the assessed risks. The audit programmes and testing plans will specify:

- The detailed test of IT controls to be performed.
- The nature of the tests and the objectives of the tests
- The sources of audit evidence
- The way audit evidence will be gathered.
- Transactions and events to be tested.
- A sampling plan indicating the manner of selection of the transaction.
- How the results of the tests will be evaluated, and audit conclusion will be reached

3.4.2.4 The Audit Plan is divided in ten sections which will provide direction to the audit team and is summarised below:

Table 8: Audit Planning Memorandum

Ref	Section	Guidance Notes
1.	Preliminary Information	Name of the Responsible Party, Period of Audit
2	Objective and scope of the audit	Based on the risk assessment conducted at the planning stage, the audit objective and scope will be further refined.
3	Previous audits	Summary of the findings from a previous IT audit of the entity and the status of the issues and recommendations. The previous findings will be followed up and the progress made reported on.
4	Knowledge of the Responsible Party and the IT system	In this section a brief description of the entity, its objective and nature of operations will be provided. Additionally, the audit team should identify all key IT systems and processes that serve those business operations.
5.	Proposed commencement date of the audit	The proposed date should consider the availability of the Responsible Party and the readiness of auditable records, allowing sufficient lead time between notification and planning procedures, risk assessments, and audit team scheduling.

<table>
<tr><th>Ref</th><th>Section</th><th>Guidance Notes</th></tr>
<tr><td>6.</td><td>Proposed end date of the audit</td><td>The proposed end date should align with the timeline taking into account the audit scope and complexity.</td></tr>
<tr><td>7.</td><td>IT System Overview</td><td>In this section, a brief description of the IT architecture of the entity and its critical application will be included (Summarised from Appendix 1: General Review of IT Survey
The plan will also make a critical analysis to what extent the entity is dependent on the applications and IT systems and any special requirements the IT systems must comply with such as legal requirements, need for confidentiality etc.</td></tr>
<tr><td>8</td><td>Reference Authorities</td><td>Authoritative references will be used by the audit team throughout the audit. This will form the criteria to assess the audit entity. The Audit team needs to be as specific as possible and identify what will be referenced. Some of the common authorities and references are:
Legislation/Acts
Regulations
Policy
Directives
Professional Standards</td></tr>
<tr><td rowspan="2">9</td><td rowspan="2">Risks Identified and Scope of the IT Controls Review</td><td>This section will summarise the IT Audit Team’s assessment of risks (Preliminary Inherent Risk Assessment and Control Risk Assessment) within the entity’s IT environment. These include specific risks related to IT processes, the control environment and assessment of fraud risk.</td></tr>
<tr><td><table>
<tr><th>IT process and risks identified</th><th>Audit procedures that will address the risks identified</th></tr>
<tr><td></td><td>Reference can be made to the working paper with the procedures which will address the risks.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Ref</th><th>Section</th><th>Guidance Notes</th></tr>
<tr><td>10</td><td>IT Audit Strategy</td><td>The audit strategy will explain the approach of the IT Audit Team and describe the steps that will be taken to achieve the audit objectives.
The way these key controls will be tested and the Maximum Acceptable Risks
The approach and methodology of testing i.e. whether test of controls or substantive testing or any special audit procedures
The timing and extent of testing,
Sources of audit evidence
Audit evidence gathering techniques to be used i.e. examination of documents, physical Verification, confirmation from a third party.
Sampling plan
The possible use of CAATs Data Analysis Software and the scope and the way such IT based audit techniques will be used.
For this purpose, the IT Audit Team will make use of the standard IT audit programmes and IT control questionnaires</td></tr>
<tr><td>11</td><td>RP Contacts</td><td>The names and positions of the responsible party contacts.</td></tr>
<tr><td>12</td><td>Audit Engagement Team</td><td>The names of the IT audit team members including external IT experts should be provided. Additionally, the names of the audit management personnel (relevant officer(s) of the concerned Audit Directorate including the IT and Public Services Audit Directorate) should be included.</td></tr>
<tr><td>13</td><td>Audit Resources</td><td>This section of the audit engagement plan provides information on resources available for the IT audit and logistics</td></tr>
<tr><td>14</td><td>External experts</td><td>Areas to be covered by external experts/specialists</td></tr>
<tr><td>15</td><td>Level of effort and resources required</td><td>Task Allocation Schedule
<table>
<tr><th>Area</th><th>Number of Working Days</th><th>Expenses (If Applicable)</th><th>Target Completion Date</th></tr>
<tr><td>Planning</td><td></td><td></td><td></td></tr>
<tr><td>Fieldwork</td><td></td><td></td><td></td></tr>
<tr><td>Reporting</td><td></td><td></td><td></td></tr>
<tr><td>Review</td><td></td><td></td><td></td></tr>
<tr><td>Travel</td><td></td><td></td><td></td></tr>
<tr><td>Training</td><td></td><td></td><td></td></tr>
<tr><td>Others</td><td></td><td></td><td></td></tr>
<tr><td>Contingency</td><td></td><td></td><td></td></tr>
<tr><td>Total</td><td></td><td></td><td></td></tr>
</table>
Allocation of responsibilities of the Audit Team
Locations and Units to be visited for Field Work
The concerned Audit Directorate reviews and approves the Engagement Audit Plan prior to the commencement of the audit procedures</td></tr>
</table>

3.5 Review and Test IT Controls

The IT audit team shall gather appropriate and sufficient audit evidence and analyse to ensure that the audit objectives are adequately addressed. During this phase the IT audit team performs detailed tests of IT controls in the identified high-risk areas. For this purpose, the IT audit team will draw on the guidance and matrix/audit work programmes and IT control questionnaires provided in this Guidelines.

3.5.1 Review of IT General and Application Controls

The following paragraphs provide guidance for conducting review and evaluation of IT controls in the following domains. There are three levels of controls set out in **Table *10*: IT General Controls**), **Table *11*: Cyber Security Controls (CS)** and **Table *12*: Application Controls (AC)**.

Table 9: IT General Controls

Abbreviation	Explanation
OM	IT Organisation and Management
PE	Physical and Environmental Controls
SD	Segregation of Duties (SoD)
SM	IT Security Management
AC	Access Control
CC	System/Service Acquisition, Development and Change Controls
BC	Business Continuity Planning
NC	Network Controls
DC	Data Management Controls

Table 10: Cyber Security Controls (CS)

Category	Description
GRC	Governance, Risk & Compliance
IAM	Identity & Access Management
NWC	Network Security Controls
DSC	Data Security & Protection
APP	Application Security

Table 11: Application Controls (AC)

Category	Description
IAC	Input Authorization & Controls
PAC	Processing Accuracy Controls
OAC	Output Accuracy Controls
UAC	User Access & Authentication
CDC	Change & Development Controls
LGC	Logging & Monitoring Controls
BAC	Backup & Recovery Controls

3.5.2 Control Objective

3.5.2.1 To mitigate IT related risks, the Responsible Party designs and implements IT controls. An IT control objective is a statement about what a set of control procedures are designed to reduce a particular risk. If the control objectives are achieved, the residual risk is reduced to acceptable levels.

Example

Risk - Data is the most critical resource of an organisation. Unless effective data back-up, storage and restoration procedures exists, the organisation may completely fail to continue with its normal business. Control objective - Effective data back-up, data storage and restoration procedures are established and implemented.

3.5.2.2 If the risk of data loss was assessed as HIGH, the IT Audit Team will perform detailed procedures to test the controls such as existence of documented data backup procedures, allocation of the responsibility of data back up to qualified IT personnel and perform substantive testing such as verifying records of data backup, visiting off site storage facilities and examining evidence of tests of restoration of data from backup media.

3.5.3. Testing and Evaluation of Controls

The objective of an IT audit procedure is to ascertain:

Whether appropriate controls exist

- Whether the controls are being effectively implemented
- To what extent the control objective has been achieved
- In this Guidelines, for each control objective a detailed audit programme has been indicated.

3.5.4 Evidence Collection and Forensic Analysis

Purpose: To ensure that digital evidence is properly collected, preserved, and analysed in a manner that maintains its integrity and ensures its admissibility in formal investigations or legal proceedings.

Key Components

3.5.4.1 Evidence Collection

Objective: To collect digital evidence while maintaining its integrity and ensuring its admissibility in legal proceedings.

Key Activities:

- Identification: Determine and locate potential sources of digital evidence, such as computers, mobile devices, network logs, and cloud storage services.
- Preservation: Safeguard the integrity of digital evidence by preventing any modification, damage or tampering.
- Collection: Use appropriate tools and standardized techniques to collect digital evidence, ensuring that the process is well-documented.
- Documentation: Maintain detailed records of the entire evidence collection process, including chain of custody logs.

Best Practices:

- Order of Volatility: Collect evidence based on its volatility, starting with the most volatile data (e.g., RAM) and progressing to more stable data sources (e.g., hard drives).
- Live Data Collection: When necessary, collect live data from active systems to capture transient information such as active network connections and running processes.
- Forensic Imaging: Createexact bit-by-bit copies of digital storage devices to preserve the original evidence in an unaltered state.
- Chain of Custody: Document each stage of evidence handling to establish and maintain a clear chain of custody

Audit Considerations:

- Evidence Handling Procedures: Confirm that procedures for handling digital evidence are clearly documented and consistently implemented.
- Tool Validation: Verify that tools used for evidence collection have been properly validated and are reliable.
- Chain of Custody: Examine the chain of custody documentation to ensure that they are complete and accurate.
- Training and Competence: Assess whether personnel involved in evidence collection have received adequate training and possess the necessary competence.

Audit Objective: to ensure that digital evidence is systematically collected and preserved in a manner that maintains its integrity.

Audit Procedures:

- Review the documented policies and procedures for digital evidence collection.
- Confirm that validated tools and techniques are used during evidence collection.
- Examine the chain of custody records to ensure accuracy, completeness, and proper handling.
- Evaluate the qualifications, training and competence of personnel involved in evidence collection.

3.5.4.2 Forensic Analysis

Objective: To analyse digital evidence in order to uncover relevant information, detect security incidents, and support legal proceedings.

Key Activities:

- Data Recovery: Retrieve deleted, hidden or lost data from digital storage devices.
- Log Analysis: Examine system and network logs to detect suspicious activities and trace the source of security incidents.
- Malware Analysis: Examine malicious software to determine its behavior, origin, and potential impact.
- Timeline Analysis: Reconstruct a chronological sequence of events to understand the context of activities.

Best Practices:

- Forensic Tools: Utilise specialised digital forensic tools (e.g., EnCase, FTK, Autopsy) for acurate and reliable evidence anlysis.
- Documentation: Maintain thorough documentation of forensic methodologies, procedures and findings.
- Reporting: Develop comprehensive forensic reports that clearly present the findings and support conclusions.
- Legal Compliance: Ensure that all forensic activities adhere to relevant legal standards and requirements.

Audit Considerations:

- Tool Validation: Confirm that forensic tools have been properly validated and are used appropriately.
- Analysis Procedures: Review whether forensic analysis procedures are comprehensive, consistent, and well documented.
- Reporting: Review the accuracy and completeness of forensic reports.
- Compliance: Ensure that all forensic activities adhere to relevant legal and regulatory requirements.

Audit Objective: To ensure that forensic analysis is conducted comprehensively and supports both legal proceedings and investigative objectives.

Audit Procedures:

- Review the policies and procedures governing forensic analysis to ensure that they are comprehensive and up-to-date.
- Confirm that only validated forensic tools are used during analysis.
- Examine the documentation of forensic processes and findings for accuracy and completeness.
- Assess the quality and completeness of forensic reports, ensuring they effectively support investigative objectives.
- Ensure that all forensic activities comply with legal and regulatory requirements.

3.6 Audit Reporting and Quality Assurance

The reporting phase of the audit includes debriefing the responsible party, drafting the report, issuing initial and subsequent drafts, exit meeting and finalizing the IT audit report.

3.6.1 Audit Findings

Performance of the IT audit procedures may result in audit findings on control weaknesses (high residual risk) and/or instances of non-compliance or errors or deviations. An audit finding should be recorded when the audit team has detected a material control weakness or when the residual risk (determined using the control evaluation tool) is assessed as unacceptably high.

3.6.2 Exit Meeting

At the end of the audit an exit meeting is held during which all audit findings are reviewed and discussed with the responsible party management. The IT audit team lead should formally

discuss all significant audit findings and conclusions with concerned members of the management before the report is drafted.

3.6.3 Audit Quality Control and Quality Assurance

3.6.3.1 An effective quality assurance and continuous improvement helps the IT audit function achieve quality audits. Quality Control and quality assurance are related processes. Quality Control is a process through which the OCAG audit supervisors ensure that all phases of an audit process are carried out in compliance with the professional standards, rules, and procedures. Quality Assurance is an assessment process undertaken by persons independent of the audit under review with a view to ensuring that the quality control system is operating as intended.

3.6.3.2 The Quality Control System of the OCAG is described in the Quality Control System at the OCAG.[25] The Quality Assurance Review process examines the audit team's compliance with the OCAG policy and the IT Audit guidelines. It aims to assure the quality of the individual audit engagement and to identify opportunities for systematic improvements. Although the overall responsibility of Quality Control rests with the DG, each of the audit assignments has a team leader who does the initial review that is carried out by the audit team. The second level of QC should be carried out by the Director or Deputy Director. The review should be carried out during the audit planning, fieldwork, reporting and follow-up. As per section 8.01 to 8.05 of the Quality Control System in OCAG, the monitoring of the Quality Control system will be carried out by other senior officials who are not less than the rank of DG Senior officials must remain entirely independent and not be involved with the work of the Directorate at any time during the period under review.

3.6.3.3 After the completion of the IT audit engagement, an independent quality assurance review may be performed.

3.6.4 IT Audit Report

3.6.4.1 The IT audit reports shall reflect the findings from the IT audit process depending upon the materiality of such findings vis-a-vis the audit objectives.

3.6.4.2 IT audit findings may contain sensitive information that, if exposed, could be exploited to the detriment of the audited entity by malicious actors. To mitigate this risk, the IT audit report should be prepared in two separate versions:

- **Confidential Version**
  This is the full IT audit report, containing both sensitive and non-sensitive information. Access to this version must be strictly restricted and safeguarded through a predefined chain-of-custody protocol.

- **Public Version**
  This is a sanitized version of the IT audit report containing only non-sensitive information. If the inclusion of any sensitive data becomes necessary, it must first undergo an appropriate sanitisation process before being disclosed.

3.6.4.3 The purpose of the IT audit report is to communicate the results of the audit to the Parliament, responsible party and the key stakeholders. Despite the technical nature of IT audit, the messages must be clear and precise. The report should be fair and balanced, noting where management has taken corrective actions. The general layout of a standalone IT audit report will include the following:

[25] https://cag.org.bd/storage/app/media/reports/Quality%20Control%20System%202021.pdf

Executive Summary

PART-1

a) Introduction and Background
b) Description of the IT System – Modules, Workflow, etc.
c) The Responsible Party
d) Audit Objectives
e) Scope and Limitations
f) Audit Criteria
g) Audit Methodology
h) Audit Engagement Team
i) Period of audit
j) Number of Meetings with the Responsible Party

Part-2

k) Audit Findings
l) Conclusion
m) Overall Recommendations

Part-3 Audit Criteria and Appendices

Part-4 Enclosure and Evidence

3.6.4.4 Since IT Audit is a subject area within the context of a broader audit (i.e. performance, financial or compliance), the reporting format outlined in the respective guidelines should be followed. As for compliance audits, refer to the report format specified in the Compliance Audit Guidelines.[26] In case of financial audits, the indicative templates for providing opinion on Finance and Appropriation Accounts may be used according to the Financial Audit Guidelines.[27] For performance audits, the guidance notes on the structure of the performance audit report should be followed.[28]

3.6.5 Audit Follow Up

The OCAG and the Audit Directorates should follow-up the implementation of the recommendations made in the audit findings with the responsible party entity. Implementation of any management action plan for correcting the control weaknesses that might have been agreed with responsible party management also need to be monitored. The status of outstanding recommendations related to prior IT audit reports should be communicated to the stakeholders during follow-up audit or next audit engagement.

[26] Compliance Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 22 October 2021, pp. 195 (https://cag.org.bd/storage/app/uploads/public/64a/65f/bd9/64a65fbd947c7705459153.pdf)

[27] Financial Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 30 June 2021, pp. 52-53 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

[28] Performance Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 11 May 2023, Para 6.5, pp. 63-66 (https://cag.org.bd/storage/app/uploads/public/64b/f44/110/64bf441102cb4147637819.pdf)

CHAPTER 4 REVIEW OF IT GENERAL CONTROLS

This chapter provides an in-depth analysis of IT General Controls (ITGC) domains, including key control objectives, associated risks, audit procedures, and co-sourcing considerations. It integrates co-sourcing strategies into ITGC domains, elaborating key risks, control objectives, and best practices.

4.1 IT General Control Domains

4.1.1 The ITGCs to be assessed fall into the following categories:

Table 12: IT General Control Domains

Abbreviation	IT General Control	Key Control Objectives
OM	IT Organisation & Management	Strategic alignment of IT with OCAG objective, IT governance, IT risk management, resource management
PE	Physical & Environmental Controls	Protection of IT assets from unauthorised physical access, environmental hazards, and disasters
SD	Segregation of Duties	Separation of critical IT roles and responsibilities to prevent fraud and unauthorised changes
SM	IT Security Management	Establishment of security policies, risk assessments, and incident response mechanisms
AC	Access Control	Control of user access to data, applications, and systems to prevent unauthorised access
CC	Service/System Acquisition, Development & Change Control	Ensure proper controls related to business case and need assessment, SDLC processes, authorization, testing, and approval of system changes
BC	Business Continuity Planning	Maintain IT resilience through disaster recovery and business continuity planning
NC	Network Controls	Secure network infrastructure through firewalls, IDS/IPS, and monitoring
DC	Data Management Controls	Secure generate, acquire, storage, transmit, backup retrieval and destruction of sensitive data

Each domain includes key control objectives that guide audit teams in evaluating ITGC effectiveness.

4.1.2 Specialised technical expertise through management of co-sourced experts and professionals[29] can significantly enhance audit capabilities in assessing complex areas. Possible areas that may need to be co-sourced for review of IT General Controls are as follows:

- IT Security Management
- Risk Management
- System Development Methodologies
- Software Requirement Specification (SRS) and Software Design Document (SDD) Review
- Access Control Review
- User Log Analysis
- Network Security Management
- Cryptography Process
- Database Architecture and Schema Review
- Data Migration
- Application Software Evaluation
- Virtualisation and Hyper Convergence
- BCP or DRP Procedures
- BlockChain Network Assessments
- System Reviews and Substantive Testing.

In such cases, a co-sourcing approach will allow the audit function to effectively address highly technical and specialised issues where the OCAG may not have adequate in-house skills or expertise.

4.2 OM: IT Organisation & Management

4.2.1 From an audit perspective, **IT Organisation & Management** plays a critical role in ensuring that an organisation's technology infrastructure and practices are aligned with its overall objectives while also adhering to regulations, industry standards, and best practices. The primary goal of IT audit in this area is to assess the effectiveness, efficiency, and compliance of IT management to safeguard organisational assets and mitigate risks. Major control areas are as follows:

OM.1 IT Governance & Strategic Planning

IT governance ensures that IT aligns with the organisation's objectives. It includes strategic IT planning, risk management, and policy implementation. Key elements include:

- Establishment of IT policies and standards.
- Alignment of IT strategy with organisation’s goals.
- Oversight by an IT Steering Committee.
- Inclusion of co-sourced experts in governance reviews and audits.

[29] Co-sourcing takes place when an organisation combines in-house and external services to achieve its objectives. Co-sourced external experts and professionals may include certified IT professionals, information systems analysts, etc.

OM.2 Risk Management

Risk management involves identifying potential IT risks, measuring their impact, implementing risk mitigation strategies and monitoring Key Risk Indicator (KRI). Key controls include:

- Enterprise-wide risk management frameworks including policies and procedures.
- Adoption of standardized risk response methodologies.
- Development of IT risk register and action plans.
- Engagement of co-sourced specialists for advanced risk assessments.

OM.3 IT Organisational Structure

A well-structured IT department ensures effective service delivery and accountability. This includes:

- Clearly defined IT roles and responsibilities.
- Adequate resource allocation and succession plan.
- Supervision of outsourced and co-sourced IT services.

4.2.2 Key Control Objectives:

- IT policies and strategic plans are documented and aligned with organisational goals. (Responsible Parties policy and strategy)
- An IT governance framework exists, including an IT Steering Committee.
- A structured IT risk management process is in place.

4.2.3 Key Audit Considerations:

- Determine whether management has established IT policies.
- Assess the effectiveness of IT governance structures.
- Review IT risk assessments and action plans.
- Evaluate the involvement of co-sourced IT specialists in governance reviews.

[Suggested matrix/Audit work programme for IT Organisation & Management (OM) Control is shown in Appendix *3*]

4.3 PE: Physical & Environmental Controls

4.3.1 Physical & Environmental Controls are essential components of an organisation's overall risk management and security strategy. From an audit perspective, these controls are designed to protect physical assets, data, and systems from unauthorised access, damage, theft, and environmental hazards. The goal is to ensure that the physical security measures are robust enough to safeguard sensitive information and IT infrastructure against internal and external threats while maintaining the organisation's continuity.

PE.1 Physical Access Controls

Organisations must secure IT assets against unauthorised physical access and potential damage. Measures include:

- Identification of sensitive facilities of the Responsible Party.
- Perimeter security (e.g., surveillance, controlled entry) of the organisation.

- Visitor access management.
- Co-sourced security audits for compliance validation.

PE.2 Environmental Controls

Environmental factors such as fire, power surges, and temperature fluctuations must be managed to prevent data loss. Recommended controls include:

- Fire detection and suppression systems for IT facilities.
- Power surge protection and backup generators for IT facilities.
- HVAC systems to regulate temperature and humidity for IT facilities.
- Co-sourced review of disaster recovery measures.

4.3.2 Key Control Objectives:

- Physical security measures protect IT assets from unauthorised access.
- Environmental controls mitigate risks such as fire, power failure, and climate factors.

4.3.3 Key Audit Considerations:

- Assess the implementation of physical security mechanisms (e.g., access logs, CCTV, restricted areas).
- Verify compliance with environmental safety measures.
- Review co-sourced evaluations of data center security.

[Suggested matrix/Audit work programme for Physical and Environmental Controls (PE) is shown in Appendix *4*

4.4 SD: Segregation of Duties

4.4.1 Segregation of Duties (SoD) is a key internal control principle designed to reduce the risk of errors, fraud, and unauthorised activities within the Responsible Party by ensuring that no single individual is responsible for multiple conflicting tasks. It is based on the concept that certain functions, especially those related to financial transactions and sensitive systems, should be divided among different personnel to ensure that no one person can both initiate and approve a transaction, or execute and record the same process.

From an audit perspective, **Segregation of Duties** is crucial in maintaining an effective internal control environment, as it helps to detect and prevent fraudulent activities, errors, and potential misstatements in financial reporting, compliance, and operational activities.

4.4.2 Key Control Objectives:

- Critical IT functions are segregated to prevent unauthorised transactions and fraud.
- System access and administrative privileges are assigned based on role-based security principles.

4.4.3 Key Audit Considerations:

- Assess whether job functions are adequately separated.
- Evaluate enforcement of access control policies.
- Verify if co-sourced assessments detect potential conflicts of interest.

[Suggested Matrix/Audit work programme for Segregation of Duties (SD) Control is shown in Appendix *5*]

4.5 SM: IT Security Management

4.5.1 IT Security Management refers to the policies, procedures, and practices that an organisation implements to ensure the confidentiality, integrity, and availability of its information and IT systems. It involves the protection of digital assets, systems, networks, and data from unauthorised access, cyberattacks, loss, or corruption. Effective IT security management is vital for reducing risks and ensuring compliance with regulatory requirements while enabling continuity.

From an audit perspective, **IT Security Management** involves reviewing and assessing the security policies, practices, and controls within the Responsible Party to identify vulnerabilities, ensure compliance with standards, and confirm that systems and data are being protected appropriately.

SM.1 Security Policies & Procedures

Organisations must establish security frameworks based on best practices (e.g., ISO 27001, BNDA, COBIT).

Key components:

- Documented security policies and procedures.
- Regular security risk assessments.
- Annual policy reviews and updates.
- Co-sourced security assessments for enhanced oversight.

SM.2 Incident and Problem Management

A robust incident and problem management minimizes security breaches. Best practices include:

- Defining incident and Problem Management roles and responsibilities.
- Establishing a dedicated Computer Incident Response Team (CIRT).
- Conducting regular incident simulations and training.
- Utilizing co-sourced forensic expertise for incident investigations.

Incident Management:

Purpose: Incident management aims to restore normal service operation as quickly as possible and minimize the impact on business operations, ensuring that agreed service levels are maintained.

Audit Objective: Ensure that incident management processes are effective in restoring regular service operation promptly.

Key Components:

- Detection and Recording: Identifying and logging incidents as they occur.
- Classification and Initial Support: Categorizing incidents and providing initial support to resolve them.
- Investigation and Diagnosis: Analyzing incidents to determine their root cause.
- Resolution and Recovery: Implementing solutions to resolve incidents and restore services.
- Closure: Ensuring that incidents are fully resolved and formally closed.
- Post-Incident Review: Analyzing incidents after resolution to identify improvements and prevent recurrence.

Problem Management

Purpose: Problem management aims to identify and eliminate the root causes of incidents, preventing their recurrence and minimizing the impact of incidents that cannot be prevented.

Audit Objective: Ensure that problem management processes effectively identify and eliminate the root causes of incidents.

Key Components:

- Problem Identification: Detecting problems through incident trends, major incidents, or proactive identification.
- Problem Logging: Recording problems in a problem management system.
- Problem Diagnosis and Root Cause Analysis: Investigating problems to determine their root cause.
- Workarounds and Known Errors: Developing temporary solutions (workarounds) and documenting known errors.
- Problem Resolution: Implementing permanent solutions to eliminate problems.
- Problem Closure: Ensuring that problems are fully resolved and formally closed.
- Proactive Problem Management: Identifying and resolving problems before they result in incidents.

4.5.2 Key Control Objectives:

- A documented security policy exists and is reviewed annually.
- IT security risk assessments are conducted regularly.
- Incident and problem management plans are well-defined and tested.

4.5.3 Key Audit Considerations:

- Review IT security policies and their alignment with related regulatory frameworks.

- Assess the effectiveness of security awareness programmes.
- Verify the role of co-sourced experts in forensic investigations.
- Incident Logging: Verify that all incidents are logged and tracked.
- Response Times: Assess whether incidents are resolved within agreed service levels.
- Root Cause Analysis: Ensure that root causes are identified and documented.
- Incident Documentation: Review the completeness and accuracy of incident records.
- Post-Incident Reviews: Check if post-incident reviews are conducted and documented.
- Problem Logging: Verify that all problems are logged and tracked.
- Root Cause Analysis: Assess the thoroughness of root cause analyses.
- Workarounds and Known Errors: Ensure that workarounds and known errors are documented and communicated.
- Problem Resolution: Review the effectiveness of problem resolution processes.
- Proactive Problem Management: Check if proactive measures are in place to identify and resolve problems before they cause incidents.

4.5.4 Audit Procedure:

- Review related policies and procedures.
- Review incident management policies and procedures.
- Verify incident logging and tracking mechanisms.
- Assess response times and resolution effectiveness.
- Conduct interviews with IT staff to understand incident management practices.
- Review post-incident review reports.
- Review problem management policies and procedures.
- Verify problem logging and tracking mechanisms.
- Assess the thoroughness of root cause analyses.
- Review documentation of workarounds and known errors.
- Evaluate the effectiveness of problem resolution processes.
- Check for proactive problem management activities.

[Suggested matrix/Audit work programme for IT Security Management (SM) is shown in Appendix *6*]

4.6 AC: Access Control

4.6.1 Access Control refers to the mechanisms, policies, and practices used to manage and restrict access to systems, applications, networks, and data within the Responsible Party. The goal of access control is to ensure that only authorised individuals or entities can access specific resources and perform predefined actions, based on their roles or responsibilities. This helps protect sensitive information and systems from unauthorised access, alteration, or misuse while maintaining organisational security.

From an audit perspective, evaluating access control involves reviewing how access is granted, monitored, and managed, ensuring that access rights are consistent with the principle of least

privilege, and confirming that there are appropriate safeguards to prevent unauthorised activities.

AC.1 Logical Access Controls

Logical access controls restrict unauthorised data access and manipulation. Key controls include:

- Review Identify, Authentication, Authorization, Accountability (IAAA) principles
- Review the usages of multi-factor authentication (MFA).
- Role-based access control (RBAC).
- Regular audits of access logs.
- Co-sourced validation of access control policies.

AC.2 Password Management

To strengthen authentication, Responsible Parties should:

- Enforce strong password policies.
- Replace default vendor passwords.
- Implement measures to detect password-related security threats.
- Engage co-sourced experts for password security audits.

AC.3 User Account Administration

User accounts must be strictly controlled. Key principles:

- Formal approval for user creation.
- Regular reviews of user privileges.
- Immediate deactivation of inactive or terminated accounts.
- Co-sourced monitoring for enhanced user access compliance.

4.6.2 Key Control Objectives:

- Classification of information resources according to their criticality and sensitivity
- Access controls are enforced to ensure only authorised users access IT resources like servers, applications, databases and any IT facilities.
- Password policies and authentication mechanisms prevent unauthorised access.
- Privileged access is monitored and periodically reviewed.

4.6.3 Key Audit Considerations:

- Examine compliance with access control and password policies.
- Assess effectiveness of multi-factor authentication (MFA) and user provisioning.
- Evaluate co-sourced audits of access control configurations.

[Suggested matrix/Audit work programme for IT Access Controls is shown in Appendix 7]

4.7 CC: Service/System Acquisition, Development & Change Control

4.7.1 Service/System Acquisition, Development and Implementation

Purpose: To ensure that the acquisition, development, and implementation of information systems or services are conducted in a controlled and efficient manner, aligning with organizational objectives and minimizing risks.

Key Components

4.7.1.1 Information System or Service Acquisition

Objective: To ensure that the process of acquiring information systems or services is sercured, systematic, transparent, and aligned with the organization's strategic goals.

Key Activities:

- Needs Assessment: Conduct a thorough assessment to identify the specific needs and objectives of the organization.
- Vendor Evaluation and Selection: Evaluate potential vendors based on criteria such as functionality, cost, support, and compliance with standards.
- Contract Management: Ensure that contracts with vendors include clear terms regarding deliverables, timelines, costs, copyrights, non-disclosure and mutual responsibilities.
- Risk Assessment: Identify and assess risks associated with the acquisition process, including vendor reliability and system compatibility.

Audit Considerations:

- Documentation Review: Verify that needs assessments, vendor evaluations, and contracts are well-documented.
- Compliance Check: Ensure that the acquisition process complies with organizational policies and regulatory requirements.
- Risk Management: Assess the effectiveness of risk management practices related to IS acquisition.

Audit Objective: Ensure that the acquisition process is secured, systematic, transparent, and aligned with organizational goals.

Audit Procedures:

- Review needs assessments and vendor evaluations.
- Verify contract terms and compliance with policies.
- Assess risk management practices related to acquisition.
- Information System Development:

4.7.1.2 Information System Development

Objective: To ensure that the development of information systems follows a structured methodology, incorporating best practices in software development and project management.

Key Activities:

- System Development Life Cycle (SDLC): Follow a structured SDLC, including phases such as planning, analysis, design, development, testing, and deployment.

- Requirements Definition: Clearly define and document system requirements in collaboration with stakeholders.
- Secure Development Practices: Implement secure coding practices to prevent vulnerabilities and ensure data protection.
- Testing and Quality Assurance: Conduct thorough testing at various stages of development to ensure the system meets requirements and is free of defects.

Audit Considerations:

- SDLC Adherence: Verify that the development process adheres to the defined SDLC.
- Requirements Management: Review documentation of system requirements and ensure they are comprehensive and approved by stakeholders.
- Testing Documentation: Assess the adequacy of testing procedures and review test results for completeness and accuracy.
- Security Practices: Ensure that secure development practices are followed and documented.

Audit Objective: Ensure that the development process follows a structured methodology and incorporates best practices.

Audit Procedures:

- Verify adherence to the SDLC.
- Review documentation of requirements and stakeholder approvals.
- Assess testing procedures and security practices.

4.7.1.3 Information System Implementation

Objective: To ensure that the implementation of information systems is planned and executed effectively, minimizing disruption to business operations.

Key Activities:

- Implementation Planning: Develop a detailed implementation plan, including timelines, resource allocation, and risk mitigation strategies.
- Data Migration: Ensure that data migration processes are secure, accurate, and complete.
- User Training and Support: Provide comprehensive training and support to users to facilitate smooth adoption of the new system.
- Post-Implementation Review: Conduct a review after implementation to assess the system's performance and identify areas for improvement.

Audit Considerations:

- Implementation Plan Review: Verify that the implementation plan is detailed and includes all necessary components.

- Data Migration Validation: Assess the accuracy and completeness of data migration processes.
- User Training Documentation: Review training materials and attendance records to ensure users are adequately prepared.
- Post-Implementation Assessment: Evaluate the effectiveness of the post-implementation review and any corrective actions taken.

Audit Objective: Ensure that the implementation process is planned and executed effectively.

Audit Procedures:
- Review the implementation plan and data migration processes.
- Verify user training and support documentation.
- Assess the effectiveness of post-implementation reviews.

4.7.2 IT system changes must be managed systematically to prevent disruptions. Best practices include:

- A formalized change control process.
- Testing and validation of all modifications.
- Change approval from relevant stakeholders.
- Co-sourced code review from compliance and security

4.7.3 Key Control Objectives:

- System changes follow a structured change management process.
- Testing and validation occur before system changes are deployed.
- All changes are authorised and documented.

4.7.4 Key Audit Considerations:

- Conduct structured walk-through procedure for change control processes
- Review the change management process and documentation.
- Assess testing and validation procedures for system changes.
- Verify co-sourced code reviews for security and compliance.

[Suggested matrix/Audit work programme for System Development and Change Control (CC) is shown in Appendix *8*]

4.8 BC: Business Continuity Planning

4.8.1 A Business Continuity Plan (BCP) ensures operational resilience in case of disruptions. Essential components include:
- Risk assessment and Business Impact Analysis (BIA).
- Development of business continuity and Disaster Recovery Plans (DRP).
- Regular BCP and DRP testing and employee training.
- Inclusion of co-sourced resources in disaster recovery planning.

4.8.2 Key Control Objectives:

- Business Continuity (BCP) and Disaster Recovery (DRP) plans are documented and updated as necessary.
- BCP and DRP is established and tested regularly.
- IT systems are resilient to disruptions.
- Backup and recovery procedures ensure data availability.

4.8.3 Key Audit Considerations:

- Assess the adequacy of business continuity planning and DR testing.
- Verify if backup and recovery processes are effective.
- Evaluate co-sourced contributions to BCP assessments.

[Suggested matrix/Audit work programme for Business Continuity Planning (BC) Control is shown in Appendix *9*]

4.9 NC: Network Controls

4.9.1 Network security ensures data confidentiality, integrity and availability. Effective controls involve:

- Firewall implementation at the perimeter and network segmentation.
- Intrusion detection and prevention systems (IDS/IPS).
- Periodic network security audits.
- Co-sourced penetration testing for network security assessment.

4.9.2 Key Control Objectives:

- Network infrastructure is secured against cyber threats.
- Firewalls, intrusion detection/prevention systems (IDS/IPS), and encryption are implemented.
- Continuous monitoring detects and responds to security threats.

4.9.3 Key Audit Considerations:

- Review firewall configurations and network segmentation practices.
- Assess the effectiveness of IDS/IPS in detecting threats.
- Verify if co-sourced penetration testing strengthens network security.

[Suggested matrix/Audit work programme for Network Controls (NC) is shown in Appendix *10*]

4.10 DC: Data Management Controls

4.10.1 Data Management controls protect stored data from unauthorised access and corruption.

Key areas:

- Data Life Cycle (Generation, Acquire, Store, Retrieval, Transmit and Destruction) Management.
- Standing Data File and Meta Data Management
- Data Model and Schema Management
- Database Configuration (Instance) Management
- Automaticity, Consistency, Integrity and Durability (ACID) enforcement review (transactional level or RDBMS)
- CRUD (Create, Read, Update and Delete) Principles.
- Role-based database access.
- Segregation of Duties (SoD)
- Data encryption for sensitive information.
- Routine data backup and recovery procedures.
- Data retention and media management
- Secure destruction of Personally Identifiable Information (PII) and Confidential Data
- Co-sourced assessments for data security compliance.

4.10.2 Key Control Objectives:

- Implement Data Management Best Practices
- Authorization of Data Model and Schema
- SoD
- Use of latest version of the Database System
- Data are protected against unauthorised access and modifications.
- Data encryption and backup procedures safeguard sensitive information.

4.10.3 Key Audit Considerations:

- **Identify data management practices and determine the level of effectiveness**
- **SoD review**
- Identify database systems and versions in use and the status concerning database software patches.
- Review access controls and cryptographic mechanisms.
- Assess data backup and recovery testing.
- Evaluate co-sourced reviews of database security compliance.

[Suggested matrix/Audit work programme for Database Controls (DC) is shown in Appendix *11*]

CHAPTER 5: REVIEW OF CYBER SECURITY CONTROLS

As digitalisation continues to transform public sector operations, cybersecurity has emerged as a critical area of focus within IT Auditing. This chapter outlines the key cybersecurity control domains, associated risk factors and assessment methodologies. The control areas covered under this chapter includes Governance, Risk and Compliance, Identity and Access Management, Network Security Controls, Data Security and Protection and Application Security. It also highlights the importance of co-sourcing strategies to enhance audit capabilities and address the growing complexity of cybersecurity challenges.

5.1 Types of Cyber Attack

A list of cyber attacks is presented below:

Table 13: Type of Cyber Attack

Type of Cyber Attack	Description
Denial of service	A denial of service (DOS) attack attempts to make a resource, such as a web server, unavailable to legitimate users. The attack overwhelms the target system with excessive traffic (such as messages) from a single source and disrupts normal operations. It can prevent the system from communicating with other systems or accessing the Internet.
Distributed denial of service (DDOS)	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. Through automation, the computers are coordinated to flood a target, often without the knowledge of the computers' owners.
Brute force attacks	A brute force is a trial-and-error attempt to guess a system's password. Automated software is often used to guess hundreds or thousands of password combinations. There are many ways to defend against brute force attacks. One of the simplest is to lock accounts after several login attempts. Blocking IP addresses after multiple login failures is another.
Browser attacks	Browser-based attacks target end users who are browsing the internet. The attacks may encourage them to unwittingly download malware disguised as a fake software update or application. Malicious and compromised websites can also force malware onto systems. They often do this by exploiting a weakness in a visitor's browser or related software, typically caused by the software being out of date. One of the best ways to avoid browser-based network attacks is to regularly update web browsers and browser-related services.
SSL Secure Sockets Layer attacks	SSL attacks aim to intercept data that is sent over an encrypted connection. A successful attack enables access to the unencrypted information.
Botnet attacks	A botnet is a network of compromised computers remotely controlled by malicious actors. Hackers often attempt to infect systems with malware. Attackers use botnets for malicious activity or rent the botnet to others for malicious purposes. Common uses of botnets include launching DDOS attacks,

Type of Cyber Attack	Description
	sending out spam email, and conducting click-fraud.
Backdoor attacks	A backdoor is a type of attack that bypasses normal authentication to allow remote access. Backdoors can be present in software by design.
Sniffer	A programme that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Malware Virus	A programme that "infects" computer files, usually executable programmes, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files.
Malware Worms	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate
Malware Trojan horse.	A computer programme that conceals harmful code. A Trojan horse usually masquerades as a useful programme that a user would wish to execute
Malware Logic bombs	A form of sabotage in which a set of codes is inserted into a programme that causes the programme to perform a destructive action when some triggering event occurs, such as termination of the programmer.

5.2 Cyber Security Control Areas

5.2.1 Cybersecurity controls are classified into the following key areas:

Table 14: Cybersecurity controls

Abbreviation	Cyber Security Control Area	Key Control Objectives
GRC	Governance, Risk & Compliance	Ensure security policies, risk assessments, and regulatory adherence.
IAM	Identity & Access Management	Enforce strong authentication and access restrictions.
NWC	Network Security Controls	Protect network infrastructure from cyber threats.
DSC	Data Security & Protection	Secure sensitive data and implement cryptographic mechanisms.
APP	Application Security	Ensure secure coding practices and vulnerability management.

5.2.2 Each area includes critical control objectives that guide the audit teams in assessing cybersecurity effectiveness. **Co-sourcing will facilitate expert-driven analysis, ensuring comprehensive evaluations of advanced security threats and regulatory requirements. Given the technical complexity and rapidly evolving nature of cybersecurity, this is a**

domain where OCAG may strategically co-source specialised experts to provide deeper insights and ensure a comprehensive assessment. Understanding of cybersecurity best practices, threat intelligence and vulnerability management is an essential skill for an IT auditor. Due to the technical complexity involved in these matters, OCAG may collaborate with external experts to ensure a thorough assessment of cyber-security controls.

5.3 GRC: Governance, Risk & Compliance

5.3.1 Governance, Risk, and Compliance (GRC) is an integrated approach that organisations use to manage their governance structures, assess and mitigate risks, and ensure compliance with relevant laws, regulations, and standards. It is a holistic framework that aligns organisation objectives with risk management and legal requirements to enhance organisational performance, reduce risks, and maintain transparency.

From an audit perspective, GRC involves reviewing the effectiveness of governance structures, risk management practices, and compliance controls within an organisation to ensure that they are in place, well-documented, and functioning effectively. This helps auditors assess whether the organisation is adequately protecting its assets, complying with regulations, and following best practices in terms of corporate governance.

5.3.2 Key Control Objectives:

- Establish and maintain cybersecurity policies and frameworks.
- Conduct periodic risk assessments and gap analyses.
- Ensure adherence to industry regulations and compliance standards (ISO 27001, NIST, BNDA and COBIT).

5.3.3 Key Audit Considerations:

- Evaluate cybersecurity governance structures and accountability frameworks of a Responsible Party.
- Assess the effectiveness of security awareness and training programmes.
- Review co-sourced regulatory compliance audits.

5.4 IAM: Identity & Access Management

5.4.1 Identity and Access Management (IAM) refers to the policies, processes, and technologies that organisations use to manage and control user identities and their access to critical systems, applications, and data. The goal of IAM is to ensure that only authorised individuals (or systems) have access to the resources they need to perform their jobs while safeguarding sensitive data and minimizing the risk of unauthorised access, data breaches, and security incidents.

IAM is an essential component of an organisation's cybersecurity strategy, as it enables secure access to systems and data, supports compliance with regulations, and strengthens overall governance and risk management frameworks.

5.4.2 Key Control Objectives:

- Implement robust authentication mechanisms (e.g., multi-factor authentication).
- Enforce least privilege and role-based access controls (RBAC).
- Conduct regular access reviews and privilege audits.

5.4.3 Key Audit Considerations:

- Review user provisioning and de-provisioning procedures.
- Assess the effectiveness of access logging and monitoring mechanisms.
- Validate co-sourced assessments of IAM configurations.

5.5 NWC: Network Security Controls

5.5.1 Network Security Controls are measures implemented to protect the integrity, confidentiality, and availability of data and resources as they are transmitted across or accessed over a network. These controls are critical for defending against unauthorised access, cyberattacks, data breaches, and other security threats that can compromise the network infrastructure, applications, and sensitive information. From an audit perspective, a review of **Network Security Controls** involves assessing the design, implementation, and operational effectiveness of the network defences to ensure alignment with industry standards, regulatory requirements, and organisational policies.

5.5.2 Key Control Objectives:

- Deploy and manage firewalls, IDS/IPS, and network segmentation.
- Perform regular vulnerability scans and penetration testing.
- Continuously monitor network traffic for anomalies.

5.5.3 Key Audit Considerations:

- Assess firewall rule management and intrusion detection capabilities.
- Evaluate network segmentation to reduce attack surfaces.
- Validate co-sourced penetration testing results.

5.6 DSC: Data Security & Protection

5.6.1 Data Security & Protection refers to the strategies, practices, and technologies used to safeguard data from unauthorised access, corruption, loss, or theft, ensuring its confidentiality, integrity, and availability. It is a critical component of any organisation's information security strategy, as data is one of the most valuable assets for an organisation. Whether the data is stored on-premises, in the cloud, or during transit, protecting it against both internal and external threats is vital for regulatory compliance, business continuity, and customer trust.

From an audit perspective, **Data Security & Protection** involves reviewing the controls and mechanisms in place to protect data, verifying their effectiveness, ensuring compliance with data protection laws, and assessing whether the organisation’s data protection practices align with industry standards and best practices.

5.6.2 Key Control Objectives:

- Implement data encryption at rest, in-use and in-transit.
- Establish data loss prevention (DLP) mechanisms.
- Enforce proper data classification and retention policies.

5.6.3 Key Audit Considerations:

- Review encryption key management policies.
- Assess DLP solutions for data leakage monitoring.
- Evaluate co-sourced forensic audits on data security incidents.

5.7 APP: Application Security

5.7.1 Application Security refers to the measures and practices employed to protect software applications from security threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of the application and its data. Application security aims to safeguard applications from both external and internal threats, including hackers, malicious software, and user errors, by identifying and mitigating vulnerabilities throughout the software development lifecycle (SDLC).

From an audit perspective, **Application Security** involves assessing the security posture of the applications an organisation uses or develops, ensuring that they are resilient against potential threats and align with security best practices, regulatory requirements, and industry standards.

5.7.2 Key Control Objectives:

- Implement secure software development lifecycle (SDLC) practices.
- Conduct automated and manual vulnerability testing.
- Ensure timely patching of application security flaws.

5.7.3 Key Audit Considerations:

- Assess application security policies and coding standards.
- Review vulnerability scanning and remediation processes.
- Validate co-sourced secure code reviews and penetration tests.

CHAPTER 6 REVIEW OF APPLICATION CONTROLS

This chapter provides guidelines on key application control domains, including control objectives, risk factors, audit procedures, and co-sourcing considerations. It also provides guidance on testing and evaluation of application controls.

6.1 Major GoB IS/IT Systems

Major government agencies have implemented IT based information systems. Key IT systems within GoB include the multi-module flagship reform iBAS++ (Integrated Budget and Accounting System), e-Government Procurement (e-GP), Banking applications, and systems of computation and collection within revenues and taxation including ASYCUDA[30]. Apart from iBAS++, e-GP system and ASYCUDA, an OCAG Committee Report identified 46 significant IT application systems used in the public sector of Bangladesh. Priority IT systems on various platforms pertaining to different applications/systems of the government include, inter alia, the following:

- Automated Challan System
- Government to Person (G2P) Payment System
- Government Pension Management System
- Customs e-auction
- e-VAT
- BRTA Service Portal (BSP)
- Online fish feed licensing
- e-filing system
- Container Terminal Management System (CTMS)
- DESCO e-bill
- Online payment (Dhaka WASA)
- Railway e-ticketing service
- Biman e-Ticketing system
- e-service centre (National E-Services (NESS)
- E- Mutation System
- Online MRP Application
- e-TIN
- NID Online Services
- Online Birth and Death Registration System, etc.
- Bangladesh Automated Clearing House (BACH)
- National Payment Switch Bangladesh (NPSB)
- Bangladesh Electronic Funds Transfer Network (BEFTN)
- Real Time Gross Settlement (RTGS)

The growing use of Information systems in the government requires that these systems are adequately controlled and secured, records are accurately maintained, and risks are acceptably reduced.

[30] https://asycuda.org/en/ (The Automated System for Customs Data is a computerized system designed by the United Nations Conference on Trade and Development to administer a country's customs)

6.2 Application Control Domains

6.2.1 Application controls are those controls that pertain to an application and have a direct impact on the processing of individual data or transactions.

6.2.2 The review of complex application systems is generally performed by specialists, while a more limited approach is designed for the generalist members of the audit teams. A comprehensive system review involves a thorough assessment and testing of IT controls within a computer system for the full range of its application functions. In contrast, a limited review targets specific data elements and generally requires a less in-depth understanding of the broader application controls. **Given the technical complexity and rapid pace of technological advancement, the OCAG may strategically co-source specialized experts to provide deeper insights. This approach will ensure a comprehensive evaluation of application related controls, address emerging risks and evolving technologies. Possible areas that may need to be co-sourced in the review of IT Application Controls are as follows:**

- **Vulnerability Assessment and Penetration Testing (VAPT)**
- **Application software design**
- **Source Code Review**
- **Application Programming Interface (API) and Integration Review**
- **Application Software Review, etc.**
- **Software Requirement Specification (SRS) and Software Design Document (SDD) Review**
- **Data Architecture and Schema Review**

6.2.3 Application controls ensure the accuracy, completeness, validity, and security of data processed by applications. The following key domains are critical for an effective application control framework:

Table 15: Application Control Domains

Abbreviation	Application Control Domains	Key Control Objectives
IAC	Input Authorization & Controls	Ensure data input is valid, complete, and authorised.
PAC	Processing Accuracy Controls	Validate correct and complete data processing.
OAC	Output Accuracy Controls	Ensure the accuracy and reliability of system outputs.
UAC	User Access & Authentication	Restrict unauthorised access to applications.
CDC	Change & Development Controls	Enforce change management processes in application development.
LGC	Logging & Monitoring Controls	Monitor and track application activities to detect anomalies.
BAC	Backup & Recovery Controls	Ensure application data integrity and availability through backup mechanisms.

Each domain comprises key control objectives that guide audit teams in assessing application control effectiveness.

[Suggested matrix/Audit work programme for Application Controls is shown in Appendix *12*]

6.3 IAC: Input Authorisation & Controls

6.3.1 Input Authorization & Controls refer to the mechanisms put in place to ensure that data entering a system is valid, accurate, and authorised. These controls are critical for preventing errors, fraud, and unauthorised access to sensitive systems and data. They ensure that only legitimate, authenticated input is processed, enabling the Responsible Party to maintain the integrity of information systems.

From an audit perspective, **Input Authorisation & Controls** involve reviewing the policies, procedures, and technical safeguards that govern how data is entered into systems, verifying that only authorised individuals or processes are allowed to input data, and ensuring that the data entered is appropriate, complete, and accurate.

6.3.2 Key Control Objectives:

- Implement validation rules to ensure data completeness and accuracy.
- Require user authentication and approval for data entry.
- Establish real-time error detection mechanisms.

6.3.3 Key Audit Considerations:

- Assess input validation controls to prevent erroneous or unauthorised data entry.
- Verify approval processes for critical transactions.
- Evaluate co-sourced assessments of data validation mechanisms.

6.4 PAC: Processing Accuracy Controls

6.4.1 Processing Accuracy Controls are essential for ensuring that data is processed correctly within a system, without errors or unauthorised alterations. These controls are designed to detect and prevent mistakes during the processing of data, ensuring that the results of any processing actions, such as calculations, updates, or transactions, are accurate, consistent, and reliable.

From an audit perspective, **Processing Accuracy Controls** focus on assessing the effectiveness of the controls in place to verify that the processing of data is performed accurately and that any discrepancies or errors are detected and addressed promptly.

6.4.2 Key Control Objectives:

- Validate data integrity and confidentiality during processing at the application layer.
- Ensure calculations and automated workflows are error-free in the respective application.
- Implement reconciliation and exception handling procedures in the financial application.

6.4.3 Key Audit Considerations:

- Assess processing accuracy through system testing and validation.
- Review automated workflow configurations.
- Verify co-sourced assessments of application processing integrity.

6.5 OAC: Output Accuracy Controls

6.5.1 Output Accuracy Controls are mechanisms put in place to ensure that data output from a system is accurate, complete, and protected from unauthorised alterations or errors. These controls focus on maintaining the trustworthiness of data after it has been processed by the system and before it is used or shared externally. This is crucial in environments where incorrect or compromised data could have serious legal, financial, or operational consequences.

From an audit perspective, **Output Accuracy Controls** are evaluated to ensure that the processes and systems in place adequately protect the integrity of the data as it moves through different stages—from generation to presentation, storage, or distribution.

6.5.2 Key Control Objectives:

- Ensure generated reports and system outputs are accurate and complete.
- Implement access controls for sensitive output data.
- Establish mechanisms for verifying data consistency.

6.5.3 Key Audit Considerations:

- Review system-generated reports for accuracy and completeness.
- Assess controls over unauthorised access to reports and output files.
- Validate co-sourced evaluations of output integrity measures.

6.6 UAC: User Access & Authentication

6.6.1 User Access & Authentication are foundational aspects of data security and IT governance. These concepts ensure that only authorised individuals can access specific systems, applications, and data. The combination of access controls and authentication mechanisms is crucial for maintaining the confidentiality, integrity, and availability of sensitive information, as well as preventing unauthorised access that could lead to security breaches or data loss.

6.6.2 Key Control Objectives:

- Implement strong authentication mechanisms (e.g., multi-factor authentication) in application access.
- Restrict access based on the principle of least privilege.
- Enforce periodic user access reviews.

6.6.3 Key Audit Considerations:

- Assess compliance with access management policies.
- Evaluate authentication methods and access logging mechanisms.

- Review co-sourced audits of access control configurations.

6.7 CDC: Change & Development Controls

6.7.1 Change and Development Controls refer to the processes and mechanisms used to manage and govern changes made to an IT system, application, infrastructure, and offer technical components. These controls are crucial for maintaining the integrity, security, and functionality of systems as they evolve over time. Effective change and development controls help ensure that changes do not introduce vulnerabilities, errors, or unintended consequences that could affect the operations or security of the Responsible Party.

From an audit perspective, **Change and Development Controls** focus on assessing how changes are requested, authorised, tested, implemented, and reviewed to ensure they align with organisational policies, regulatory requirements, and best practices.

6.7.2 Key Control Objectives:

- Ensure structured change management processes.
- Ensure application changes are tested and approved before deployment.
- Maintain version control and rollback capabilities.

6.7.3 Key Audit Considerations:

- Review change management policies and compliance.
- Assess testing procedures for system changes.
- Validate co-sourced reviews of application development controls.

6.8 LGC: Logging & Monitoring Controls

6.8.1 Change and Development Controls are critical mechanisms used to manage modifications within an organisation's IT environment. These controls help ensure that any changes made to systems, software, infrastructure, or data are conducted in a secure, organised, and controlled manner, reducing the risk of errors, vulnerabilities, and unintended consequences. Effective change management is essential for maintaining the stability, security, and compliance of IT systems.

The purpose of **Change and Development Controls** is to systematically evaluate, approve, implement, and monitor changes to IT systems. The goal is to ensure that changes do not disrupt operations, compromise security, or result in compliance issues. By adhering to best practices and frameworks for managing changes, organisations can minimize risk while ensuring that their systems remain reliable, efficient, and secure.

6.8.2 Key Control Objectives:

- Maintain detailed and immutable audit logs of user activity.
- Detect and respond to unauthorised access attempts.
- Regularly review logs for anomalies and security threats.

6.8.3 Key Audit Considerations:

- Assess the effectiveness of log retention and analysis mechanisms.
- Review security monitoring processes and incident response capabilities.
- Validate co-sourced evaluations of logging and monitoring practices.

6.9 BAC: Backup & Recovery Controls

6.9.1 Backup & Recovery Controls are crucial to safeguarding the data and ensuring that, in the event of an emergency, critical systems and information can be restored without major disruption. These controls define the process for regularly creating backup copies of data and establishing procedures for data recovery in the event of failure, loss, or corruption. The primary objective is to minimize downtime, ensure data integrity, and meet organisation's operation continuity requirements.

From an audit perspective, the main objective is to ensure that backup and recovery strategies are effective, secure, compliant with regulatory requirements, and able to recover from interruptions quickly with minimal data loss. Backup and recovery controls are designed to reduce the likelihood of data breaches, maintain operational stability, and protect against potential system failures.

6.9.2 Key Control Objectives:

- Implement automated checkpoint and recovery mechanisms for critical application data.
- Ensure data recovery procedures are tested and documented.
- Maintain redundancy and failover mechanisms for high availability.

6.9.3 Key Audit Considerations:

- Verify the adequacy of backup policies and procedures.
- Assess the effectiveness of recovery testing.
- Evaluate co-sourced assessments of data restoration capabilities.

CHAPTER 7 IT AUDIT IN SUPPORT OF BUDGETARY CENTRAL GOVERNMENT ACCOUNTS

This chapter covers IT Audit aspects relevant to the Budgetary Central Government (BCG)[31] Accounts with reference to the guidance and principles under the OCAG Financial Audit Guidelines, ISSAI 2000-2999 as well as INTOSAI GUID 5100 (Guidance on Audit of Information Systems) and GUID 2900 (Guidance to the Financial Auditing Standards) [32]**.** The chapter provides guidance to the audit teams in carrying out review of the control activities (input controls, processing controls and output controls) as part of the financial statement audit process.

7.1 IT Audit and Government Financial Statements

7.1.1 As information technology continues to advance, government entities increasingly rely on computerized information systems to perform operation, and to process, maintain and report essential information. As a result, the reliability of these systems and the data generated is a key concern for the audit team. The audit team is also required to assess the accuracy and reliability of computer-generated data. Additionally, the adequacy of controls within these systems needs to be evaluated to reduce the risk of errors, fraud and other incidents that may compromise system availability.

7.1.2 In the context of a financial audit, an IT audit involves an examination of controls designed to ensure the proper operation of the information systems supporting an entity's financial processes, as reflected in the financial statements.[33]

7.2 Budgetary Central Government Finance Accounts

7.2.1 The Finance Accounts are prepared in accordance with the forms and manners prescribed by the Comptroller and Auditor General of Bangladesh with the approval of the President as per Article 131 of the Constitution of the People's Republic of Bangladesh. These accounts represent the Receipts, Payments and Balances resulting from all transactions that have taken place under the Budgetary Central Government.

7.2.2 Budgetary Central Government (BCG) includes all Ministries/Divisions, Departments and Directorates excluding the SOEs and SPAs. **The purpose of a financial audit of BCG Finance Accounts is to express an opinion as to whether the financial statements are free from material misstatements in accordance with the applicable financial reporting framework.**

7.2.3 The prescribed Finance Accounts of the Government contain the following five statements:

(i) Statement 1: Cash Receipts and Payments – Cash inflows, cash outflows and cash balances are reported in this statement.

[31] BCG includes all Ministries/Divisions, Departments and Directorates

[32] INTOSAI GUID 2900, Guidance to the Financial Auditing Standards, June 2021 (https://www.issai.org/wp-content/uploads/2019/08/Guid-2900_Guidance-to-the-financial-auditing-standards-Endorsement-Version.pdf)

[33] https://idi.no/work-streams/relevant-sais/lota/wgita-idi-handbook-on-it-audit

(ii) Statement 2 – Comparison of Budget and Actual Amount – The original budget, final budget, actual amounts and variance between budget and actual amounts are presented in this statement.

(iii) Statement 3 – Comprehensive Receipts and Disbursements under Public Accounts – Receipts and disbursements under the Consolidated Fund and Public Account of the Republic are shown separately.

(iv) Statement 4 – Summary of Financing Activities – discloses the recurrent and capital expenditure incurred from the revenue and other receipts.

(v) Statement 5 – Summary of Balances – shows all financial assets and liabilities of the Government to display their balances with full details.

7.2.4 The Financial Statement of BCG covers the Consolidated Fund and the Public Accounts of the Republic. It discloses annual receipts and disbursements of the Government. Financial results by Revenue and Capital Accounts and balances of Public Debt, Liability and Assets are also included. This is also supplemented by audited Appropriation Accounts.

7.3 IT Auditing Approach and Process

7.3.1 The primary focus of IT Auditing of the BCG Accounts is on the transactions and balances associated with these accounts. This includes testing the receipts and payments relating to transaction level data. Given the large volume of transactions, there is a necessity to apply IT audit techniques into the audit approach.

7.3.2 The approach involves the following interrelated processes:

- Understanding financial statements (value of transactions, volume of transactions, nature of transactions, etc.) (refer to OCAG Financial Audit Guidelines)[34]
- Audit Steps for Budgetary Central Government Accounts (Finance Accounts[35] and Appropriation Accounts[36]) (refer to Financial Audit Guidelines)
- Obtain an understanding of the iBAS++ (Integrated Budget and Accounting System)[37] including the application controls.
- Identifying the components of the application and mapping the flow of transactions
- Audit procedures for testing the controls.
- Testing of controls supplemented by analytical procedures and other substantive testing procedures.
- Identify the extent of IT systems auditing required to achieve the audit objective.

7.3.3 As an integral part of the overall audit process, the IT component **of a financial audit is to assess the reliability of IT controls that support the processing of financial information.**

---

[34] Financial Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 30 June 2021, pp. 7-9 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

[35] Financial Audit Guidelines, OCAG, Chapter 13, pp. 102-106 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

[36] Financial Audit Guidelines, OCAG, Chapter 14, pp. 150-155 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

[37] iBAS++ is an Integrated Financial Management Information System of the Government. It has been a core component of financial reforms to promote real time transactions, transparency, and comprehensiveness in financial reporting.

7.3.4 OCAG may ensure that the audit team is composed of members that collectively have the competence to conduct IT audit engagements to achieve the intended objectives. This requires a collaborative audit approach between the information system auditors and financial auditors. While the financial auditor is ultimately responsible for assessing the inherent and control risk, understanding the impact of a computerised financial management system requires the assistance of an IT auditor. The OCAG may also engage external IT specialists and experts for data analytics and review of application controls.

7.4 Understanding the IT environment, Information System and System Controls

7.4.1 Prior to initiating the assessment of controls in an information system, the audit team should develop an understanding of the system architecture, the underlying data and its sources. Each application is unique in its design, architecture, functionalities, transaction flow and users. As a result, the IT Audit of the BCG Accounts requires learning about the iBAS++ system, the processing routine of input transactions (batch entry/real time), the transaction flow and outputs, the major transactions involved, the volume of transactions and production of the Accounts. **A checklist of iBAS++ documentation and guidelines relating to security and operating procedures is at Appendix 13.**

7.4.2 INTOSAI GUID 2900 (Guidance to the Financial Auditing Standards) requires the audit team to follow the following principles:[38]

- Obtaining an understanding of the entity and its environment in accordance with ISSAI 2315 (Revised 2019).19 (particularly the budget process and execution of the budget, consistent classification of codes for reporting budgetary and actual amounts).
- Obtaining an understanding of the entity's system of internal controls relevant to the audit as required by ISSAI 2315 (Revised 2019).21
- Identify and assess the risks of material misstatement in accordance with ISSAI 2315 (Revised 2019.28 and 29)

7.4.3 The understanding of the information system includes the IT environment relevant to the flows of transactions and processing of information within the system. This includes how the transactions are initiated and information captured.

7.4.4 Based on the ISSAI requirements, the audit team is required to obtain an understanding of the system and information processing relevant to the preparation of the financial statements. For this purpose, a brief description of the application is required to be prepared:

- Indicating the significant classes of transactions, account balances and disclosures
- Describing the transaction flow and main outputs
- Indicating the major data files maintained
- Providing approximate figures for transaction volumes.

7.4.5 In developing the documentation of iBAS++ IT environment and methodology including use of automated tools when conducting financial audits, it is necessary to comply with the guidance and principles provided under the ISSAI. Use of automated tools and techniques enables direct access to, or a digital download from, the databases in the entity's information system that store transaction records. By applying these automated tools or techniques, the

[38] INTOSAI GUID 2900, Guidance to the Financial Auditing Standards, June 2021 (https://www.issai.org/wp-content/uploads/2019/08/Guid-2900_Guidance-to-the-financial-auditing-standards-Endorsement-Version.pdf)

audit team may confirm the understanding of how transactions flow through the information system. Analysis of complete or large sets of transactions may result in the identification of risks of material misstatement.

7.4.6 The financial auditing standards (ISSAIs 2000-2999) require that assessment of IT risks and controls are integrated in the financial audit methodology.

7.5 Assessment of Risks and the Control Environment

7.5.1 After gaining an understanding of the information system, the inherent and control risks will be assessed. Based on the risks, the nature, timing and extent of substantive audit procedures necessary will be determined to achieve the resultant detection risk.

7.5.2 Computerised operations can introduce additional inherent risk factors not present in a manual system. Each of the following factors may be considered to assess the overall impact of computer processing on inherent risk.

- Uniform processing of transactions – any misstatements arising from erroneous computer programming will occur consistently in similar transactions.
- Automatic processing – system may automatically initiate transactions or perform processing functions.
- Increased potential for undetected misstatements – increases the potential for individuals to gain unauthorised access to sensitive information and to alter data.

7.6 Assessment of IT Controls

7.6.1 The objectives are to obtain reasonable assurance whether the financial statements are free from material misstatements and assess the effectiveness of the controls through control tests. **While IT control testing is generally performed by an IT Auditor, financial auditors with appropriate expertise may undertake specific tasks in this area. Close coordination between both teams is essential.**

7.6.2 Prior to testing, relevant IT controls should be identified to ensure the proper authorisation, completeness, validity and accuracy of the transactions. Moreover, controls required for prevention, detection and correction of overpayments, unauthorised payments and fraudulent transactions to be identified.

7.6.3 IT control testing should be performed by an IT Audit specialist with support from the financial audit team where appropriate. To assess the operating effectiveness of the control, it may be necessary to test a sample of transactions to verify that the control has functioned effectively throughout the audit period. **IT controls are classified into General Controls and Application Controls**. A review of IT General Controls is provided in **CHAPTER 4**, while Application Controls are discussed in **CHAPTER 6**.

7.6.4 General Controls – General controls are manual or automated procedures which aim to ensure confidentiality, integrity and availability of information in the physical environment within which information systems are developed. During a financial statement audit, the audit team will collect evidence to support their opinion on the Financial Statement. When reviewing the implementation of controls, it may be necessary to perform data analysis to substantiate that controls have been functioning as intended. After obtaining sufficient and appropriate audit evidence regarding the effectiveness of general controls, the audit team may be able to conclude on the operating effectiveness of application control procedures.

7.6.5 Application Controls – Application controls are specific controls particular to an application and have a direct impact on the processing of individual transactions. Application Controls are IT dependent manual or automated procedures within an information system that

affect the processing of transactions and may relate to validation of input data, accurate processing of data, delivery of output data and controls related to integrity of master data.[39]

7.6.6 In the context of IT auditing of BCG Accounts, it is important to understand the risks associated with application control and to design appropriate audit procedures to test the adequacy and reliability of these controls.

7.6.7 Based on the identified risks and prior to initiating detailed audit procedures, the audit team will require transaction-level access to the iBAS++ system. This access should allow the team to log in and select specific Ministries, Divisions or Grants and extract transactions related to the relevant fiscal year FY and corresponding Economic Codes. Transactions taking place during the month of June are of special significance from the point of view of Finance and Appropriation Accounts. The process will involve examining any unusual patterns in expenditure by economic code and by month and identify high risk transactions.

7.6.8 Application controls address three major operations – data input, data processing and data output. Respective control objectives, risks and audit procedures are as follows **(refer to Appendix *12* – Review of Application Controls for a more detailed work programme):**

Table 16: Input Controls, Processing Controls and Output Controls

Controls	Control Objective & Risk areas	Audit procedures
Input controls	**Control Objectives** ● The data received for processing are genuine, complete, not previously processed, accurate and properly authorised. ● Data/transactions are entered accurately and without duplication. **Risk areas** ● Entry of unauthorised data/ transactions ● Data/Transaction entered into the application may be irrelevant. ● Incomplete data/ transaction entry ● Entry of duplicate/redundant data/transactions ● Risk of fraudulent, or irregular transactions	▪ **Authorisation of Input** - All inputs/transactions and changes are appropriately authorised before entry into the app. Verify login IDs against a predefined transaction approvals list. ▪ Check password access controls to data input devices and data entry permissions. ▪ Confirm that appropriate levels of authority are correctly set-up which involves access control matrices, user permission reports, and audit logs of permission changes. **Completeness of Inputs** – Ensure that all key transactions are entered without omissions or material misstatements or disclosures. Review controls ensuring that input is complete i.e. transactions have not gone missing. The total of individual transactions should agree with the manually calculated total. ▪ Check the use of pre-numbered data input forms and investigate any discrepancies. ▪ All transactions are presented to the system in batches and incomplete batches are detected. ▪ Conduct input validation checks[40] including out-of-range values, invalid characters, missing or incomplete data, upper and lower data volume limits and inconsistent data control. **Duplicate Checks and matching** – Identify duplicate processing of a source document. ▪ Match IT-based records against corresponding source

[39] INTOSAI GUID 5100 - Guidance on Audit of Information Systems, June 2019 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

[40] iBAS++ Software Development Life Cycle (SDLC) Guideline & Procedure, Finance Division, Ministry of Finance, 24/051202Para 4 (c) iv (iii),

Controls	Control Objective & Risk areas	Audit procedures
		documents to assess input errors. Match source records against corresponding IT-based records to determine that the data had been entered into the system. ▪ Use of CAATs to detect duplicate records in transaction file **Rejected Input** – Determine if documented procedures exist for correcting and resubmitting rejected transactions. ▪ System Rejections - Procedures should be in place to ensure controls that all transactions rejected are subsequently corrected, re-input and accepted by the system. ▪ Suspense Items – Transactions held in suspense are identified, corrected, successfully processed and cleared. Also, identify figures recorded in iBAS++ but omitted and not disclosed in the Finance Accounts
Processing Controls	**Control Objectives** The objectives are to ensure that. ● transaction processing is accurate. ● transaction processing is complete. ● transactions are unique (i.e. no duplication) ● all transactions are valid. **Risk Areas** ● Inaccurate processing of transactions leading to wrong outputs/results ● Transactions being processed may remain incomplete. ● Allowing for duplicate entries or processing which may lead to duplicate payment. ● Unauthorised changes to the existing data	● Ensure that documented procedures exist for proper data processing. ● Verify that system history logs record all application processing events. ● Confirm that processing controls exist to ensure that input and output counts are equal. Application processes perform further validation by checking data for duplication and consistency with other information held by other parts of the system. ● Perform transaction level testing to detect incomplete or inaccurate processing. ● Confirm that expenditure figures and balances reported in the Appropriation Accounts and Finance Accounts tie-up with the figures reported in iBAS++. ● Check for sequence error, duplication, transactions/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow and automated calculations.
Output Controls	Output controls ensure that all output is: ● Produced and distributed on time. ● Fully reconciled with pre input control parameters ● Physically always controlled, depending on the confidentiality of the document ● errors and exceptions are properly investigated and acted upon.	● Verify physical and logical access controls to protect computer output files against unauthorised amendments to the data/transactions. ● Check controls to ensure that outputs are accurately transferred between processing stages. Output from one IT system may form the input to another system, ● Reconcile input and output record counts and control totals to confirm that no data is lost or added during processing. ● Carry out a reconciliation between the expenditure figures reported in iBAS++ and that is disclosed in the BCG Accounts. Identify the inconsistency errors in the BCG Accounts with the figures reported in the iBAS++.

Controls	Control Objective & Risk areas	Audit procedures
	Risk Areas ● Unauthorised data modification ● Repeated errors in the output generated. ● Non-availability of data at the time when it is desired. ● Availability of data to an unauthorised user ● Overpayments, unauthorised payments and fraudulent transactions	

7.7 Substantive Tests

7.7.1 Based on the IT controls assessment, priority areas for substantive tests of financial information should be identified. Substantive tests provide reasonable assurance that financial statements and related assertions are free from material misstatement. These tests generally involve examining source documents supporting transactions.

7.7.2 Substantive testing also involves detailed examination of the IT controls to ensure transactions are complete, valid and accurate. This requires the ability to analyse large datasets to identify trends, anomalies and potential risks. The use of Computer Assisted Audit Techniques (CAATs) increases the audit coverage that can be used for data enquiry, extraction and analysis of large volumes of data (GUID 5100, 6.10).[41] However, CAATs require connectivity to PFM systems and transaction level read-only access. **Given the advanced skills and resources required to acquire and use CAATs software for data analytics, OCAG may consider co-sourcing CAATs services to professional external experts.**

7.7.3 The audit team may not always be able to examine all transactions or modules of IT systems. In such cases, audit sampling and testing may be conducted based on the principle of materiality in accordance with ISSAI 2530[42] and the Financial Audit Guidelines (refer to Para 13.6 iv)[43]

7.7.4 Materiality levels, as outlined in ISSAI 2320.10 and 11, may be set at a lower level for classes of transactions, account balances or disclosures (refer to Para 13.4-13.6 of the Financial Audit Guidelines)[44]. While materiality in financial audits considers the extent or value of misstatements, in IT audits it depends on the potential consequences of IT control failures.

[41] INTOSAI GUID 5100, Guidance on Audit of Information Systems, June 2019, pp. 15 (https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf)

[42] INTOSAI GUID 2900, Guidance to the Financial Auditing Standards, June 2021, pp. 68 (https://www.issai.org/wp-content/uploads/2019/08/Guid-2900_Guidance-to-the-financial-auditing-standards-Endorsement-Version.pdf

[43] Financial Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 30 June 2021, pp. 104 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

[44] Financial Audit Guidelines, OCAG, pp. 102-103 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

ISSAI 2330.8 describes the circumstances in which the audit team is required to perform controls testing to obtain sufficient appropriate audit evidence.[45]

7.7.5 If controls are not considered to be effective, substantive tests to be performed for each material class of transaction, account balances and disclosure, irrespective of the assessed risk level.

7.7.6 The results from substantive tests, control tests and other audit procedures determines whether the Responsible Party has effective compliance controls.

7.8 Reporting

7.8.1 During the reporting phase, the audit team draws conclusions and reports on the financial statements including all misstatements and all control deficiencies (refer to Chapter 7 of the Financial Audit Guidelines)[46]. Regarding controls, the auditor expresses an opinion whether the controls are sufficient to meet the following control objectives:

- Transactions are executed in accordance with the budget authority and with rules and regulations.
- Transactions are properly recorded, processed and summarized to permit the preparation of financial statements.

7.8.2 The combined assessment of the entity's control forms the basis of the audit opinion.

[45] INTOSAI GUID 2900, Guidance to the Financial Auditing Standards, June 2021, pp. 47 (https://www.issai.org/wp-content/uploads/2019/08/Guid-2900_Guidance-to-the-financial-auditing-standards-Endorsement-Version.pdf

[46] Financial Audit Guidelines, Office of the Comptroller and Auditor General of Bangladesh, 30 June 2021, pp. 50-53 (https://cag.org.bd/storage/app/uploads/public/64a/662/db0/64a662db0249b722028762.pdf)

Appendix 1: General Review of IT Survey

	Prepared by	Reviewed by	Index
Name			
Date			
Signature			

PURPOSE OF THE SURVEY

The review of the IT survey is designed to collect information about Information Systems and Software Applications in use at the Responsible Party entity audited by OCAG. It is structured into following sections:

1. General Information
2. System Architecture
3. Software Development
4. Vendor Management
5. IT Budget
6. Training and Awareness
7. Security and Access Controls
8. Business Continuity Plan (BCP)
9. Incident Management and Response
10. Information Security Policy
11. Physical Security
12. Audit Trails and Monitoring
13. Compliance
14. Applications

1. General Information

a) Name of Responsible Party:

_____

b) Address:

_____

c) Contact Information

	Name	Phone/Mobile/Email
Head of the Organisation		
Head of Finance & Accounts		
Members of the IT Steering Committee		
Chief Information Officer (CIO)		
Chief Information Security Officer (CISO)		

d) What are the purpose and objectives of the system?

_____

e) Describe the broad functional areas covered by the system.

_____

f) What modules are deployed (in use) and what modules are pending to deploy?

Deployed	Pending

g) What is the status of Integration of the System with other third-party software(s)?

_____

h) What is the bandwidth of Internet Service in the organisation?

_____

i) How many users are given access to the Internet Service?

_____

j) Is the Software/Web Applications hosted internally or outsourced?

_____

k) Are there any Standard Operating Procedures (SOP)?

Yes ☐ No ☐

If there are SOPs, are those SOPs documented, approved, implemented, and monitored?

SOP documented ☐ SOP approved ☐

SOP implemented ☐ SOP monitored☐

l) Are all assets, including critical information assets, identified and classified clearly?

Yes ☐ No ☐

2. System Architecture

a) Describe the System Architecture in production environment.

Client/Server Architecture ☐

Model View Controller (MVC) Architecture ☐

Layered Architecture (n-tire) ☐

Additional Description:

_____

b) Software Infrastructure - What software is used for the System?

	Manufacturer/ Brand	Number and Type of license	Technical specifications	Amount spent on annual maintenance contract
Network operating systems				
Virtualisation				
Antivirus/security				
Patch management				
Network management				
Database management system				
Any other				

C) Detail of all hardware items used in the System production environment:

Item	Description
Servers	
Switches	
Routers	
Firewalls	
UPS	

DATA CENTRES

D) Does the Responsible Party have more than one Data Center?

_____

E) What is (are) the location(s) of each Data Center?

_____

F) What is the size/capacity of each Data Center?

_____

G) Please describe the specification of Power Supply and/or back-up of each data center:

	Manufacturer/Brand	Quantity	Technical. Specification.
AC Power backup & UPS			
DC Power backup & UPS			
Surge Protection			
Generator			

H) Please describe the environmental control of the data center:

	Name/Brand	Quantity	Technical. Specification.
Cooling System			
Fire Detection			
Fire Suppression			
Anti-Static Mat			

NETWORKS

I) Does the Responsible Party have one or more networks?

_____

J) What is the network architecture?

_____

K) What VPN protocol is used?

OpenVPN □ IPSec / IKEv2 □L2TP/IPSec □

PPTP □ Wire-Guard □ SSTP □

L) Who is the owner of the *System's source code*? Who owns the *data* stored in the System?
_____

M) Which platform can this system operate (Desktop/Android/iOS)?

3. Software Development

a) Has the application system been developed in-house or outsourced?

In house□ Outsourced□ Co-sourced □

In the case of outsourcing/co-sourcing, specify the name of the agency/vendor and the contact person:

Agency: _____

Contact Person _____

Phone (Mobile) of Contact Person _____

When was the System made operational (MM/YYYY)? _____/_____

b) Are there any manuals available (as mentioned below)?

User documentation manual	Yes □	No □
Programming documentation manual	Yes □	No □

If the user manual is updated, which was the last release, please mention the version number with the date of release of the user manual.

Version number _____ Date _____

c) What is the arrangement for making modifications to the existing application that is being used regularly to support the function?
_____

d) Is there any Capacity Management Procedure followed for managing and monitoring the capacity of critical IT infrastructure and applications?

Yes □ No□

e) Is there any formal Change Management Procedure followed for implementing changes in the Application?

Yes □ No□

Please briefly describe the Change Management Procedure for implementing changes in the application.
_____

Are all emergency changes formally logged and approved after implementation?

Yes □ No□

f) Can the application, configuration, and all dependencies be redeployed using automated deployment scripts, built from a document in a reasonable time, or restored from backups in a timely fashion?

Yes □ No □

g) How much data is migrated from the legacy system (if any) to the system"?

_____

_____

h) What is the average and maximum volume of data generated monthly in terms of storage space?

Average data volume per month: _____
Maximum data volume per month _____

i) Other than the System, are there any Application(s) running on the same hardware? If yes, specify the name(s) of such IT Application(s).

_____

K) What kind of SDLC is followed here?

_____

4. Vendor Management

A) What is the status of the maintenance contract/service level agreement (SLA)? Pls. attach the maintenance contract/ Service Level Agreements.

Vendors	Maintenance Contract/SLA Details
Propriety software with vendors	
Customized software with vendors	
Data Centre (Cloud Service)	

B) Is there any clause in the contract that allows the audit of the service that is outsourced?

Yes □ No □

5. IT Budget (Indicate the IT budget in the past three years)

Recurrent Budget

- IT personnel
- Maintenance and repair
- Consumables
- Utilities Software Licensing
- IT recurrent expenditure as a percentage of the total recurrent budget

Development Budget

- Procurement of computers and peripherals

6. Training and Awareness

A) Is there a training programme for employees using the system? (Pls attach respective office order)

_____

B) Number of security awareness programmes conducted? (Pls. attach respective office order)
_____

C) Do the employees know their roles and responsibilities in maintaining information security? (Pls. attach respective Office Order)_____

7. Security and Access Controls

A) Are the Logging and Monitoring procedures documented, approved, and followed?
Documented ☐ Approved ☐ Followed ☐

B) Is the log information protected against unauthorised access, alterations, and operational problems?
Yes ☐ No ☐

C) Does the System use a common logging format and approach?
Yes☐ Not Exactly☐

Comment (if “Not Exactly” is selected)
_____

D) Is the Centralized network time protocol (NTP) server synchronized with an external authentic source to maintain the minimum time drift?
Yes ☐ No ☐

E) Does the system have a mandatory requirement for passwords using a combination of letters, numbers, and special characters?
Yes☐ Not Exactly ☐

Comment (if “Not Exactly” is selected) ----------

F) Does the system store encrypted passwords?
Yes☐ Not Exactly ☐

Comment (if “Not Exactly” is selected) ----------

G) Does the system allow the user to change their password?
Yes ☐ Not Exactly ☐

Comment (if “Not Exactly” is selected) ----------

H) Does the system allow a password strength meter to help users set a stronger password?
Yes☐ Not Exactly ☐

Comment (if “Not Exactly” is selected) ----------

I) Does the System allow periodic credential rotation or historical passwords?
No☐ Yes☐

Description of the status (if “Yes” is selected) ----------

J) What is the standard time (in hours) to renew time bound authenticators after sending the renewal instructions from the System?

_____

K) Does the System ensure that access to administration and management functions is limited to authorised administrators?

Yes ☐ No ☐

L) Does the system detect and alert on abnormal numbers of requests (such as by IP, by the user, total per hour/day, or whatever makes sense for the application)?

Yes ☐ No ☐

Kindly describe a similar incident that happened in the system.

_____

M) When will the User ID become inactive for unused User ID?

_____

N) Does the system force the normal user to change their password after a certain period?

Yes ☐ No ☐ Period _____ (days)

O) Has the Responsible Party identified the “Objective” of the Information Security and Management System (ISMS)?

Yes ☐ No ☐

If “Yes” is selected, what is the objective ISMS of the Responsible Party?

_____

P) Does the Responsible Party have a written “Information Security Plan”?

Yes ☐ No ☐

Q) Does the Responsible Party have a Risk Assessment Methodology, Risk Assessment Report, Risk Treatment Plan, and Risk Mitigation plan to establish and effectively run an Information System Management System?

Risk Assessment Methodology ☐

Risk Assessment Report ☐

Risk treatment Plan ☐

Risk mitigation plan☐

R) Is the system integrated with the NID server? And is there any option for two-step verification while logging in?

_____

S) Has any vulnerability assessment and penetration testing (VAPT) been done yet?

Yes ☐ No ☐

What is the outcome of VAPT if performed?

_____

T) Have any information security risk registers been maintained?

Yes ☐ No ☐

Is there any periodical review of information security risks and thus formulating/updating the risk mitigation plans accordingly to ensure the implementation of risk mitigation plans as per the agreed time frame?

Yes ☐ No ☐

8. Business Continuity Plan (BCP)

A) What was the average system outage per day of the System?

_____

What is the daily cost (revenue loss) of the system's unavailability?

_____

What is the system's Recovery Point Objective (RPO)?

_____

Is there any Business Continuity Plan (BCP) for all/critical modules? Kindly list the module name that has a Business Continuity Plan (BCP):

_____

If there is any BCP, when was the BCP last tested?

_____

B) Is there any log file-related testing and reporting of BCP?

Yes ☐ No ☐

C) Does the Organisation have any Disaster Recovery Plan (DRP)?

Yes ☐ No ☐

If the Responsible Party has a Disaster Recovery Plan (DRP), when it is last tested (dd-mm-yyyy? (Pls attach the report related to DRP testing.

_____

D) What are the arrangements to ensure that backups are stored securely to prevent data from being stolen or corrupted?

_____

E) Have regular backups of important data been taken, and has test restoration of data been performed?

Yes ☐ No ☐

Please mention the date when test restoration from a full backup was last checked.

_____

F) What types of backups have the assigned persons taken regularly?

Full Backup ☐ Incremental Backup ☐ Differential Backup ☐

G) How often do the assigned persons take Full Backup?

Daily ☐Weekly ☐Monthly ☐Never ☐

H) How often do the assigned persons take Differential/Incremental Backup?

Daily ☐ Weekly ☐ Monthly ☐ Never ☐

9. Incident Management and Response

A) Is there any Incident Management Procedure for Incident reporting, responding, escalation, and resolution?

Incident Reporting ☐ Incident Responding ☐

Incident Escalation ☐ Incident Resolution ☐

B) Does the information system team member record every incident, respond immediately, formally inform after resolution, and collect feedback about the service?

_____

Is there any log file for incident management?

Yes ☐ No ☐

C) Is the Security Incident (i.e., identifying the Security Incident, Resolving the Security Vulnerabilities, Reporting) properly documented?

Yes ☐ No ☐

D) Has the organisation assigned a team to identify, resolve, and report security incidents?

Yes ☐ No ☐

E) Is there any log file related to a security incident?

Yes ☐ No ☐

F) Is there any Security Operating Centre (SOC) installed?

Yes ☐ No ☐

If the answer is 'Yes'; Is there any assigned person(s) to monitor the Security Operating Centre?

Yes ☐ No ☐

What is the level/tire of the SOC?

Tier 1 — Triage Specialist ☐

Tier 2 — Incident Responder ☐

Tier 3 — Threat Hunter ☐

G) Have you used the SOC for the following events?

- Security operations
- Introductory incident response
- Malware analysis
- Threat hunting and threat emulation
- Monitor and investigate alerts.
- Configure and manage security tools.
- Develop and implement IDS signatures

10. Information Security Policy

A) Is there any written Information Security Policy?

Yes ☐ No ☐

If there is already an Information Security Policy when it was last modified the information Security Policy (dd-mm-yyyy)? Who has approved the IS policy?

_____

Have any Information Security Management System (ISMS) policies and guidelines been developed and deployed here?

B) Which of the following documents are available right now?

Operations Security Guidelines ☐	Communication Security ☐
Organisation of Information Security Guidelines ☐	Compliance Guidelines ☐
Physical & Environmental ☐	Cryptography Guidelines ☐
SDLC ☐	Human Resource Security Guidelines ☐
Supplier Relationship ☐	Incident Management Guidelines ☐
Access Control ☐	Information Security Aspect of Business Continuity Management ☐
Asset Management ☐	Information Security Guideline ☐

C) What Standards are being followed here?

_____

11. Physical Security

A) Is the system's physical access control measured by CCTV, Fingerprint scanner, biometric scanner etc.?

CCTV ☐ Fingerprint scanner ☐ Biometric scanner ☐

If the system is covered by CCTV, then is it monitored regularly?

Yes ☐ No ☐

B) What were the findings when the IS team last monitored the data center? What actions have been taken?

_____

C) Is the System Security protected by a Firewall?

Yes ☐ No ☐

D) Is the System covered by a Fire Suppression System?

Yes ☐ No ☐

E) Is there any log file to record the visitor in the server room/data center?

Yes ☐ No ☐

F) Is there any document on the Detail Network Diagram?

Yes ☐ No ☐

G) Is there any update/change on the Networking Diagram after it was first deployed?

Yes ☐ No ☐

H) Is there any update/change on the Networking Diagram after it was first deployed?

_____

12. Audit Trails and Monitoring

a) Does the Audit Trail record all login and logout from all devices?

Yes ☐ No ☐

b) Does the Audit Trail record all transactions, including insertion of attachments?

Yes ☐ No ☐

c) Does the audit trail contain the created user, last modified user, created time, last modified time, location, or IP address?

created user☐ modified user ☐

created time☐ modified time☐

location/IP address of creation ☐

location/IP address of modification ☐

D) Has the Responsible Party conducted an Internal Audit to implement and effectively use the Information System?

Yes ☐ No ☐

E) What are their key findings and recommendations if an Internal Audit has been conducted?

_____

F) Is there any Security Information and Event Management (SIEM) system deployed?

_____

13. Compliance

a) Bangladesh National Digital Architecture (www.bnda.gov.bd) has set policies, standards, and guidelines to guide government agencies in the design, acquire, implement, and manage IS. How does the System comply with the policies, standards, and guidelines? Explain in detail.

_____

B) ISO 27001 international standards specifies requirements for an information security management system (ISMS) and ensures confidentiality, integrity, and availability of information. How does the System comply with ISO 27001? Explain in detail.

_____

14. IT Applications

Please provide the details of Applications in use.

Type of the Application	Name of the Application	Operated in-house or outsourced	If In-house Package/Customised or developed as a Bespoke/COTS	If Package Name of the manufacturer and brand
	1	2	3	4
Financial Management				
Budgeting				
Payroll				
HR Management				

Accounting System				
Others (Please Specify)				

Major Functionalities and Modules

- Data Structures and Data Flow Diagrams
- Process Flow and Key Process Steps
  Master Data Files

IT Systems and Processes

Review and examine the following documents. However, these are not exhaustive, and other documents may also be reviewed.

- IT Strategic Plan and annual operational plans
- Organogram and job descriptions
- In-house, outsourced and co-sourced services
- Third party contracts, agreements and other documents
- IT security and other policies
- Procedural manuals
- IT solutions acquisition and development policies
- Disaster recovery and business continuity policy
- Management reports

Appendix 2: IT risk identification

Control element	Nature of operations and environmental factors	Significant Inherent risk	Likelihood 1-5	Impact 1-5	Risk assessment
1	2	3	4	5	6
IT Governance					
Organisation and management					
Policies standards and procedures					
Performance management					
IT Operations					
IT infrastructure					
Applications					
Physical and Environmental Controls					
Segregation of Duties					
IT Security Management					
IT Security Access Controls					
Service/System Acquisition, Development and Programme Change					
Business Continuity Planning and Disaster Recovery					
Network Controls					
Database Controls					
Cyber Security Controls					

Appendix 3: IT Organisation and Management Control (OM) – Suggested Matrix/Audit Work Programme

Control Objectives:

1. To assure that the management has established an appropriate IT governance framework to ensure efficient and effective use of IT resources towards achievement of organisational objectives.
2. To assure that the management establishes and communicates IT policies and standards and IT process guidelines to exercise proper control over the IT operations.
3. To ensure that IT services of the outsourced vendors/co-sourced experts are properly supervised.
4. To assure that the management establishes an organisation wide risk assessment framework, adopt a standard risk assessment methodology and develop a risk action plan to minimize risk exposures.

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
OM.1 IT governance				
Does the entity have an IT strategic planning process undertaken at regular intervals giving rise to long-term plans which are periodically translated into operational plans setting clear and concrete short-term goals?	*Review documentation relating to IT strategic plan, long term and short-term technology plans and software acquisition plans*	☐ Yes ☐ No		
Have the management established IT policies, standards and documented processes aligned with appropriate standards? Are these policies communicated to all levels of management?	*Interview senior manager responsible for IT.* *Review IT policies.* *Review steering committee* meeting *minutes.*	☐ Yes ☐ No		
Has the management established an IT steering committee comprising representatives from senior management, the IT Department and user management?	*Review Technology infrastructure plan*	☐ Yes ☐ No		
OM.2 Risk *Management*	*Interview members of the management and senior IT personnel.*			
Determine whether the Responsible Party has an entity and activity-level IT risk assessment framework that is used periodically to assess information risk to achieving organisational objectives?	*Review risk assessment documentation.*	☐ Yes ☐ No		
Does it consider the probability and likelihood of threats?	*Review the following documentation.* - *Policies and procedures relating to risk assessment.* - *Business risk assessment documents* - *Operating risk assessment documents* - *Information services function risk assessment*	☐ Yes ☐ No		
Does the IT department have a formal process in place to identify and respond to IT control deficiencies?		☐ Yes ☐ No		
Consider whether the Responsible Party is committed to active and continuous IT risk assessment processes as a tool in providing information on the design and implementation of internal controls and		☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
in the monitoring and evaluation mechanisms?	*documents*			
Is a formal risk assessment methodology in place? Have the responsibilities for risk assessment clearly defined? Has the Responsible Party prepared a complete inventory of IT assets for the purpose of risk assessment? Does the IT risk assessment framework measure the impact of risks according to qualitative and quantitative criteria, using inputs from different areas? Is a comprehensive security assessment performed for critical systems and locations based on their priority and importance to the Responsible Party? Where the Responsible Party uses third parties to process data, does it have appropriate procedures in place to address associated risks?	*Review the risk assessment methodology and the details of the basis upon which risk and exposure to risk are measured.* *Determine if the risk assessment framework designed to support cost-effective controls to mitigate exposure to risks on a continuing basis, including risk avoidance, mitigation or acceptance?* *Even if there is no formal risk assessment procedure, gauge the understanding of the consultants and IT personnel about requirement of risk assessment and methods*	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Has a risk action plan been designed and being implemented to mitigate risk exposures through putting in place cost-effective controls and counter measures?	*Review the risk action plan.* *Interview the concerned IT personnel.* *Determine whether a risk action plan has been designed and being implemented to mitigate risk exposures through putting in place cost-effective controls and counter measures*	☐ Yes ☐ No		
OM.3 IT organisation and management controls Is there an organisational chart for the IT department which shows the various positions and respective reporting lines and responsibilities? Are roles and responsibilities of the various positions within the IT department defined and documented? Has the organisation established an IT investment plan taking a medium-term budgeting perspective?	*Review the IT department's organisational chart* *Review IT job descriptions.* *Interview IT personnel* *Review IT budget*	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
Has the organisation established procedures for identifying and documenting IT related training needs?		☐ Yes ☐ No		
OM.4 Outsourced vendors/Third Party Service Providers and co-sourced IT experts/professionals Does the Responsible Party use third parties/co-source its IT function? Does it have appropriate policies and procedures in place? Is there any proper Service Level Agreements with IT service providers? Determine if adequate controls have been specified in the SLA Whether any criteria are used for selecting a vendor/co-sourced expert? Are there any provision for performance evaluation in the service level agreement? Are performance of vendors or co-sourced experts being carried out on a regular basis?	Interview HR management and IT staff. Review Service level agreements and contracts with outsourced vendor/co-sourced experts to determine if there are significant deviations. Interview consultants and vendors. Review management reports.	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Are there confidentiality or security agreements with contractors, which specify non-disclosure of sensitive information and unauthorised disclosure acts, contractual rights, and obligations? Is there any information confidentiality policy? Are there confidentiality or security agreements with vendors or co-sourced experts?	Review policies on confidentiality or security agreements	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

CONCLUSION: Are the Organisation and Management Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 4: IT Physical & Environmental Controls (PE) – Suggested Matrix/Audit Work Programme

Control objectives:

1. To prevent unauthorised access and interference to IT services and to protect IT facilities from environmental damage
2. To restrict access to IT resources to authorised personnel in accordance with their job requirements

Key control questions	***Audit procedure***	***Yes/No***	***Remarks***	***WP ref***
Physical Access Controls (PE1) Are there physical access controls for ensuring physical access to IT systems that are restricted only to authorised IT personnel (use of entry devices such as card readers or biometric devices such as fingerprint recognition etc.)	*Review a diagram of the physical layout of the computer room or the data centre.* *Review lists of individuals authorised access to sensitive areas and determine the appropriateness for access.*	☐ Yes ☐ No		
Does the management regularly review the list of authorised personnel? Who have access to sensitive facilities?	*Review visitor entry logs*	☐ Yes ☐ No		
Are the visits logged, and the logs reviewed periodically?		☐ Yes ☐ No		
Is the data centre located in a low-profile area? Is there guard protection of the data centre?	*Study the layout map of the building housing the data centre*	☐ Yes ☐ No		
Is there video surveillance of the data centre?	*Interview data centre manager and IT security manager*	☐ Yes ☐ No		
Is there a mechanism of storing and reviewing the video surveillance?	*Carry out physical observation*	☐ Yes ☐ No		
Environmental Controls (PE2) Are environmental controls for minimising the risk of the damage to IT equipment and threat to IT personnel from accidental or environmental factors such as heat, humidity. power surges and outages, fire, flooding etc., adequate?	*Review of fire, weather, electrical warning and alarm procedures and expected response scenarios for various levels of environmental emergencies is occurring.* *Review installation of air conditioning, surge protector, UPS, humidity control and fire-fighting equipment.*	☐ Yes ☐ No		
Have fire suppression and prevention devices been installed and are working, e.g. smoke detectors, fire extinguishers and sprinkler systems?	*Physical examination of firefighting equipment* *Review documentation/manuals and verify these are not obsolete or past expiration date.*	☐ Yes ☐ No		
Is the fire extinguisher system appropriate for the data centre?		☐ Yes ☐ No		
Have there been any recent incidents	*Verify if the fire drill is tested*	☐ Yes		

Key control questions	*Audit procedure*	*Yes/No*	*Remarks*	*WP ref*
of fire? If yes, have the causes been analysed? Have remedial measures been taken?	*periodically.*	☐ No		
Have data centre personnel received training in using fire extinguishers?		☐ Yes ☐ No		
Are there power surge protectors and a UPS/backup generator of adequate capacity?		☐ Yes ☐ No		
Are the maintenance contracts for properly maintaining the support equipment?		☐ Yes ☐ No		
Is maintenance being carried out regularly?		☐ Yes ☐ No		

CONCLUSION: Are the Physical and Environmental Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 5: Segregation of Duties (SD) – Suggested Matrix/Audit Work Programme

Control objectives:

1. The job descriptions should be documented, Responsibilities should be identified through an analysis of the IT operations and systems.
2. Management policy regarding segregation of duties should be documented and all concerned should be made aware of this policy.
3. The division of duties should be effectively implemented using physical and logical access.

Key control questions	***Audit procedure***	***Yes/No***	***Remarks***	***WP ref***
Have job description or terms of reference for various categories of personnel been developed?	Review the organization chart showing IS functions and assigned personnel. Review job descriptions for different positions.	☐ Yes ☐ No		
Have management identified the role of the users, system owners and custodians?		☐ Yes ☐ No		
Are the Security manager, IT personnel, and consultants aware how segregation of duties should be implemented in an IT environment?	Obtain and review pertinent policies and procedures. Interview IT personnel to determine the level of awareness regarding segregation of duties, especially in the data center operations.	☐ Yes ☐ No		
Is there a well defined segregation of duties between the in-house and co-sourced/outsourced services? Verify if co-sourced assessments detect potential conflicts of interest Have the necessary policies been developed? Does the policy identify the prohibited job responsibilities?		☐ Yes ☐ No		
Is there adequate segregation of duties within the Information Systems Division between following functions: ● Systems design and programming ● System Development & Operations ● IT operations and Data Control ● Data input and data control ● Database administration & System Development ● Application end users	Interview the system administrator and the IT security manager. Check the account lock out mechanism by inputting invalid passwords several times. Review the system logs and logs of failed attempts.	☐ Yes ☐ No		
Have logical access to the various resources given to data center personnel, in accordance with the segregation of duties? If there is no adequate segregation are their compensatory controls such as periodic supervision by higher staff?	Verify that passwords are set to require that once a user account is locked, it remains locked for certain period or until a system administrator resets the account. *Verify is segregation of duties is enforced using logical access control.* Download copy of the log files and analyze using-**CAATs**	☐ Yes ☐ No ☐ Yes ☐ No		

CONCLUSION: Are the Segregation of Duties Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 6: IT Security Management (SM) – Suggested Matrix/Audit Work Programme

Control objectives:

1. To prevent unauthorised access and interference to IT services and to protect IT facilities from environmental damage
2. To restrict access to IT resources to authorised personnel in accordance with their job requirements
3. To prevent and detect unauthorised disclosure, unauthorised amendment and breach of system integrity.

Key control questions	***Audit procedure***	***Yes/No***	***Remarks***	***WP ref***
SM1. IT Security Policy and procedures				
Has the management formulated an IT Security Policy? Is the security policy based on standards?	*Review the security policy and plan and any related documentation indicating that it has been updated*	☐ Yes ☐ No		
Have effective measures been taken to create awareness regarding IT security amongst staff?	*Interview the security manager.* *Review documentation supporting or evaluating the awareness programme.*	☐ Yes ☐ No		
Has the Responsible Party developed an IT security action plan to effectively implement the IT security policy?	*Review IT security plan.* *Examine documentary evidence regarding implementation of the IT security plan and reports on IT security*	☐ Yes ☐ No		
Is there a procedure for periodically reviewing and updating the IT security policy and plans?		☐ Yes ☐ No		
Have the responsibility for carrying out IT security related tasks been properly allocated amongst capable staff?	*Review organisational chart and IT job descriptions*	☐ Yes ☐ No		
Is the IT security manager regularly reporting on the status of the security and security related issues to top management?		☐ Yes ☐ No		
Has the management carried risk assessment for identifying the threats to the systems, the vulnerability of system components and likely impact of an incident occurring and have countermeasures been identified to reduce the level exposure to an acceptable level?	*Review risk assessment policies.* *Review the most recent high-level risk assessment.*	☐ Yes ☐ No		
SM2. File control and privileged users.				
Are the password tables and system log files adequately secured?	*Interview security managers and review documentation provided to them.*	☐ Yes ☐ No		
Are the activities of privileged users		☐ Yes		

Key control questions	*Audit procedure*	*Yes/No*	*Remarks*	*WP ref*
such as the Systems Administration and Network Administration functions properly restricted and monitored by management about the following criteria: ● Availability, reliability and performance? ● Level of support provided to users. ● Continuity planning and security? ● Minimum acceptable level of satisfactorily delivered system: functionality. ● Change procedures?	*Review network security policy and network configuration.* *Interview network manager and system administrator.* *Assess effectiveness of network management tools*	☐ No		
SM3. Patch management and malware protection. Has the management established a framework for adequate preventive, detective, and corrective control measures to protect the IT systems from malicious software, such as computer viruses? Are there patch management policies and procedures? Are patches to critical software being regularly installed?	*Review virus control policy and procedures. Ascertain whether virus control software is installed and regularly updated*	☐ Yes ☐ No ☐ Yes ☐ No		

CONCLUSION: Are the IT Security Management Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 7: IT Access Controls (AC) – Suggested Matrix/Audit Work Programme

Control Objectives:

1. Information resources should be classified in accordance with their sensitivity and importance.
2. Implement appropriate logical access controls and a secure log in process.
3. Audit and monitor access logs.
4. Security settings, password files and log files are protected.

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
AC.1 IT Access Controls Is a system of information classification being followed? Have policies and criteria been developed? Are the classification policy and criteria appropriate?	Determine if a system for classification of information resources is being followed. If yes, review classification criteria and policies Interview system owners to gauge their understanding of information classification	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Is there an access control policy? Have the access security parameters set up in accordance with the Access Control Policy? Is there documentation of security parameters covering the following and have these been authorised. ● Password management ● Authorisation ● Automatic log out ● Failed log in attempts. Has a secure login process been implemented in accordance with the policy which requires identification and authentication? Are the passwords masked when being entered? Does the system automatically log out after a minimum period of inactivity? Does the system lock up after certain successive failed logs in attempts? Has the auditing feature (logging) been activated? Is the authorisation being provided on the basis of need-to-know/need-to-do principle either using Access Control List (ACL) or a Role Based Access (RBAC) matrix?	*Examine the login process for both network and application.* *Review security parameters documentation.* *Attempt to log in to determine if the login process is working properly.* *Verify automatic log out after a minimum period of inactivity.* *Compare the system security parameters with the documented access control policy.* *Examine the system configuration standards to verify that common security parameter settings are included.*	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
Does the IT security policy or current practices require maintenance of access logs? Are access logs for network and all applications being maintained? Are the access logs regularly reviewed by those responsible for IT security to discover unusual patterns in the access by users such as access during holidays and after office hours? Do the access logs capture failed log in attempts and the location of the workstations or remote sites from which the failed log in attempts were made? Is the failed log in attempts being investigated and adequate response measures taken?	Interview the system administrator and the IT security manager. Inspect system configuration settings to verify if the auditing feature (access logs) of the network software has been activated. Review the access log files. Take a copy of the access log files and analyze using **CAATs**	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Are the access paths to the files containing security profiles, usernames and passwords restricted? Are the password files encrypted? Is an audit trail of changes to the security parameters and password files maintained? Who can change and modify the security parameters? Does the IT security in-charge regularly review the security parameters?	*Interview the system administrator and the IT security manager.* *Review relevant documentation.* *Ensure that the password files are encrypted.* *Determine if the operating system and network operating system maintain logs of access by users.* *Verify if log files are protected from unauthorised modification*	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
AC2. Logical Access Controls Are the logical access controls aimed at protecting computer resources (data, programmes, and terminals) against unauthorised access attempts, adequate?	*Review access control policies. and procedures written policies and procedures.* *Interview system administrator and review supporting documentation*	☐ Yes ☐ No		
Is there an effective system of password administration consisting of security of password tables, password encryption, periodic changing of passwords by users and strict policy for password non-disclosure?	*Interview users* *Review password policy and procedures Review security software password parameters.* *Review documentation*	☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
Is there a mechanism for account lockout after several failed log-on attempts. Is there a method of logging a monitoring failed log on attempts by user account and by location? Are the password files encrypted and access to password file restricted? Is access to password files logged and monitored? Have the users been properly trained about the necessity of maintaining security and the use of strong passwords? Have they been warned about bad password maintenance and change practices such as writing down or sharing passwords? Is there a mechanism for transmitting the passwords securely? Are audit log flies of system and resource usage maintained and are these log files secured?	*supporting incident handling activities.* *Check the account lock out mechanism by deliberately inputting invalid passwords several times.* *Review the system logs and logs of failed attempts.* *Ascertain that the password files are encrypted.* *Review user training records. Password maintenance guideline. Interview users to assess level of awareness.* *Assess procedures for authorization for user account creation and generating and communicating passwords to users.* *Review log files*	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Are security events like unsuccessful attempts to gain access to system resources logged and investigated regularly?	*Review documentation supporting incident handling activities*	☐ Yes ☐ No		
Has the management established a framework of adequate preventive, detective, and corrective control measures to protect the IT systems from malicious software, such as computer viruses or Trojan horses?	*Review virus control policy and procedures. Ascertain whether virus control software is installed and regularly updated*	☐ Yes ☐ No		

CONCLUSION: Are the IT Access Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 8: System Development and Change Control (CC)– Suggested Matrix/Audit Work Programme

Control Objective:

1. To assure that appropriate system development methodology is followed in the a of new software or solutions.
2. To ensure that all changes to IT systems are property authorised, tested and that an audit trail of the changes made is maintained.

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Audit procedure***	***Yes/No***	***Remarks***	***WP ref***
CC1. System development controls				
Does the Responsible Party have an IT system development and acquisition policy? Is it aligned with international standards and best practices?	*Review system development policy*	☐ Yes ☐ No		
If major new IT system is being acquired, has the IT management ensured that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan?	*Review IT system acquisition plans and project plans.* *Interview project managers*	☐ Yes ☐ No		
Are new software projects implemented after conducting feasibility studies, development of user requirement specifications and the product is appropriately tested?		☐ Yes ☐ No		
CC2. Change controls				
Are the system development and testing environments physically and logically separated from the production environment	*Interview IT manager.* *Physically verify separation.* *Verify that personnel working in the development and test environments are separate from those working in the production environment*	☐ Yes ☐ No		
For proposed changes to applications, do the procedures provide for the analysis, implementation and follow-up of all changes requested and do take into consideration the following. ● identification of changes? categorization, prioritization and emergency procedures ● Impact assessment? ● change authorization? ● through testing before acceptance? ● management of release from development to production? ● adequate audit trait of the changes?	*Interview IT manager and IT personnel in charge of programming and maintaining software.* *Review programme change controls policies and documentation.* *Review documentation and records such a change authorization, record of testing to verify if change control is being implemented.* *Review procedures for*	☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/No*	*Remarks*	*WP ref*
Are there procedures to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails? Are the above procedures or similar controls, applied to amendments to operating system software?	*transfer of programmes from development to production.* *Review system software set up documentation*	☐ Yes ☐ No ☐ Yes ☐ No		

CONCLUSION: Are the System development and Change Control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 9: Business Continuity Planning Control (BC) – Suggested Matrix/Audit Work Programme

Control Objective:

1. to make IT services available as required and to ensure minimum business impact business in the event of a major disruption.
2. to ensure data can be reconstituted following file loss or corruption

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
BC1. Business Continuity and Disaster Recovery Planning				
Is there a written IT Continuity Plan or written procedure which provide for the following: ● Emergency procedures to ensure the safety of all affected staff members. ● Response procedures to continue critical IT applications? ● Recovery procedures meant to bring the operations to the state it was before the incident or disaster?	*Assess whether Critical data and operations are identified and prioritized.* *Review related policies and documentation.* *Review business continuity plan. Ascertain when it was last revised.* *Interview IT manager and security manager*	☐ Yes ☐ No		
Is the system continuity and disaster recovery plan adequately documented and tested at least annually?	*Review business continuity plan test documentation*	☐ Yes ☐ No		
BC2. Data Back Up				
Are adequate data file back-up procedures followed to ensure data can be reconstituted in the event of file loss or damage?	*Review data back up procedures and documentation.*	☐ Yes ☐ No		
Are copies of programmes and back up data files held in a remote facility?	*Interview responsible personnel.* *Observe procedures and related evidence*	☐ Yes ☐ No		
BC3. Standby Facilities Are that formalised and properly documented to enable critical processing to continue in the event of prolonged system failure? ● Do these arrangements cover data preparation where appropriate? ● Do these arrangements provide adequate operational control at the back-up site? ● Are the standby arrangements tested at least annually?	*Visit and review the remote facility (back up site)* *Assess its operational effectiveness by reviewing documentation and interviewing responsible personnel*	☐ Yes ☐ No		

CONCLUSION: Are the Section E control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 10: Network Control (NC) – Suggested Matrix/Audit Work Programme

Control Objective:

1. The network should be properly documented including a network diagram and details of hardware and software configuration.
2. A network manager function should be established.
3. Full inventory of network hardware and software should be maintained.
4. Policies and procedures regarding network operations and security should be developed and documented

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
Network Administration (NC.1) Have all components of the network been documented? Does the network diagram show details of the network connections and access paths?	Obtain a complete network diagram, including a copy of a hardware configuration diagram including all connections to the network topology. Ensure that the network diagram indicates how external parties access the network.	☐ Yes ☐ No ☐ Yes ☐ No		
Has the network manager responsibilities been assigned to a competent person? Is the job description, reporting lines and supervision arrangements documented? Is the job of network manager well segregated from that of database administrator and application system administration?	Review job description of network administrator. Determine it covers basic functions such as ● Network operations and maintenance. ● Back ups ● Starting and shutdown ● Monitoring and problem management ● Security	☐ Yes ☐ No ☐ Yes ☐ No		
Is there any inventory of data network equipment, including lines, terminals, modems, controllers, etc.? Has a network diagram, which illustrates physical and logical connections between network equipment, been prepared? Does network documentation include a description of: - Data network equipment used to support each network applications. - Protocols used. - Gateways to other networks Has networking equipment been labeled to facilitate cross-reference to documentation	Verify network inventory reports to ascertain that all hardware and software components have been labeled and recorded	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Are the network operations and maintenance policies and procedures documented?	List of vendors and customers with access to	☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
Are these policies being implemented? Are terminals physically or logically defined to the network based on written authorization? Is there a system access policy to be followed by external parties? Has the responsibility and liability of network vendors been defined (e.g., contracts)?	the network Determine policies cover essential areas such as security, performance management, business continuity planning and back ups	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Network Security Management and Monitoring (NC.2) Is the TCP/IP protocol properly configured? Has the network been segmented? Has a Demilitarised Zone been implemented? Are there procedures to monitor the network regularly?	Review TCP/IP configuration. Examine network segmentation and security zones	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

High	
Medium	
Low	

☐ YES ☐ NO

CONCLUSION: Are the Network Control objectives achieved?

If NO identify impact and assess the consequent risks

Appendix 11: Database Control (DC)– Suggested Matrix/Audit Work Programme

Control Objective:

1. To ensure that the role of a database administrator is defined.
2. The latest release/version of the Database System should be in use.
3. Configuration files used by the Database System should be maintained and appropriately protected.
4. To ensure that access to the physical files is restricted and end user access should be controlled.
5. System Level (DBA) accounts should be controlled and supervised.
6. All interfaces should be known and adequately controlled.
7. To ensure that software licensing controls are in place and full database backups should be taken on a regular basis.

For this section supply brief details of the controls identified in relation to the following questions

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
Database Controls (DC) Has the Database administration responsibilities been assigned to an IT professional? Have job descriptions been developed? How many DBAs are there? How are their roles differentiated?	Document the position(s) of the DBA(s). Determine the roles and responsibilities of the DBA(s). Inquire about what IT staff have access to the Database server(s).	☐ Yes ☐ No ☐ Yes ☐ No		
What are the possibilities of future upgrades? Procedures for retrieval of bugs, vulnerabilities and latest updates for Database System and environment	– Identify Database systems and versions in use and status concerning database software patches. – Interview Database Administrator(s) to identify the Database Systems and any specific Database applications installed. – Determine the releases/versions of the Database Systems supported by the vendor.	☐ Yes ☐ No ☐ Yes ☐ No		
Are the configuration files secure? Who can modify database configuration? Is there a process of authorization for changes in configuration?	– Identify configuration changes made when the database was installed and configured, such as: ● the database name ● information about table space(s) ● names and locations of all the data files ● information about	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
	files used for roll-forward capabilities. ● current state of archiving ● database ID number, name and timestamp of when the database was created. ● log history ● backup configuration - Use the database configuration guides to determine the configuration files native to the RDBMS.			
Have the default usernames been changed? Is the database and system administrator using usernames that give no indication of their respective roles? Is the use of super user passwords restricted and monitored?	– Consult vendor documentation for a full list of default database accounts. – Logon to the system with these accounts using the default passwords.	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		
Who can access the database physical files? Is this access monitored?	– Refer to vendor documentation for the Database System to determine a list of the physical files and where these are stored. – Determine the file ownership and permission settings for all physical files/ directories used by the Database System.	☐ Yes ☐ No ☐ Yes ☐ No		
Do users log onto the database via the command line or through an application interface? Are Login scripts used and their nature. Does the Administrator only have the permissions and access to this file / directory? Is the security manager reviewing the audit logs of DBA access on a regular basis?	– Confirm through discussions with the DBA(s) the logon process that they use to access the database. – Determine whether the DBA logs in using a normal Operating System user account before accessing the database. Or is there a	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
	generic account for DBAs to logon? – Determine how the administrators log onto the database and compare this method with predefined procedures.			
Are the end users restricted from directly accessing the databases?	Review the database account configuration and ensure that appropriate steps have been taken to restrict users to a specific application and menu	☐ Yes ☐ No		
Are all interfaces known and adequately controlled?	– Identify which interfaces are used and how these are defined, documented and controlled. – Identify all applications and what interfaces they use.	☐ Yes ☐ No		
Software licensing controls Does the organisation have an inventory of software? Is there a policy against using un-licensed software?	– Identify all software licenses. – Identify all contracts and levels of support	☐ Yes ☐ No ☐ Yes ☐ No		
Database backup procedures Are backup procedures documented? Have responsibilities for back-up clearly assigned? Are back-up processes being adequately supervised?	– Identify database systems and versions in use and status concerning database software patches. – Interview DBA regarding back-up procedures. – Determine whether full back-ups are being taken of the database files at regular and appropriate intervals?	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No		

CONCLUSION: Are the Database control objectives achieved?

☐ YES ☐ NO

If NO identify impact and assess the consequent risks

High	
Medium	
Low	

Appendix 12: Review of Application Controls – Suggested Matrix/Audit Work Programme

Control Objective:

1. Assure that all input data are authorised and complete, and data are consistently recorded, accumulated, processed, and reported in a controlled environment to produce timely and accurate information by the concerned applications.
2. Assure that the output produced is complete, accurate and useful for intended purposes. The goal is to minimise potential risks, exposures and losses due to processing error, omissions & irregularities.
3. Assure that there are appropriate controls data ownership and user account creation.

Identify the major financial applications. For each application supply brief details of the controls identified in relation to the following questions

Key control questions	***Audit procedure***	***Yes/ No***	***Remarks***	***WP ref***
E. Data capture and preparation **Control objective:** Adequate controls and procedures over data origination and preparation activities exist to ensure completeness, accuracy and validity of captured transactions				
Is there a procedure for capturing input data on pre-designed forms? Are input documents being authorised at appropriate levels?	*Review procedural manuals. Review data capture and data input forms* *Check a sample of input documents*	☐ Yes ☐ No ☐ Yes ☐ No		
E2. Data Input **Control objective:** Adequate controls and procedures over data input activities exist to ensure completeness, accuracy and validity of inputs				
Batch controls Have the batch controls over input documents been established? If yes, are procedures relating to establishing batch control totals and hash totals and preparation of batch headers are being followed? Are there a programmed procedures to automatically calculate the batch totals from the batch input documents and compare it with the manually established batch totals?	*Review procedural manuals.* *Interview users. Observe batching procedure* *Review user manuals.* *Observe batch data entry process*	☐ Yes ☐ No ☐ Yes ☐ No		
Is there is a procedure for correcting and resubmitting rejected batches? If yes, is it being followed? Are there validation programmes such as range checks, formats checks, limit checks, check digits etc. for detecting and correcting errors in batch data input?	*Interview user personnel.* *Review related documentation* *Review edits (validation checks) documentation*	☐ Yes ☐ No ☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
Online systems				
For on-line terminals, are input data are validated and errors are corrected as data are entered into the computer system?	*Test the validation checks*	☐ Yes ☐ No		
For on-line systems, are the methods to prevent data entry errors such as self-help features, pre-selected formats or menu selection, and operator prompting, effective?	*Review data entry forms and screens.* *Observe data entry procedures. Review manuals*	☐ Yes ☐ No		
For transactions entered through on-line terminals, are all input transactions automatically logged with date and time of transmission,	*Review application audit trail logs.* *Review application security documentation*	☐ Yes ☐ No		
Are information relating to user department, terminal, and user identification are captured as part of the input transaction record?		☐ Yes ☐ No		
Are transaction logs for on-line input terminals being reviewed by users to detect any unauthorised access and entry of data?	*Review procedures* *Interview supervisory personnel*	☐ Yes ☐ No		
Do the programmes include automated internal programme processing controls in the form of data input edit and validation routines (such as check digits, reasonableness tests, batch totals, and record counts). IF yes are these effective?	*Review validation checks documentation.* *Test the automated controls*	☐ Yes ☐ No		
Are input error correction and resubmission procedures adequate and effective?	*Review procedures*	☐ Yes ☐ No		
When a correction is re-entered into the system, is it subject to the same programme edit and validation controls as the original transaction?		☐ Yes ☐ No		
E3. Controls over master files and tables				
Are there strong controls over data entry into master files such as one for one check, validation programmes, edits and error correction and resubmission? Are these adequate?	*Review procedural manuals.* *Observe data entry into master files.*	☐ Yes ☐ No		
Are master files and internal tables reviewed periodically to ensure the	*Interview supervisory personnel*	☐ Yes ☐ No		

Key control questions	*Audit procedure*	*Yes/ No*	*Remarks*	*WP ref*
accuracy of their values?				
Have access to master files data and internal tables restricted to authorised personnel only?	*Review application security set up*	☐ Yes ☐ No		
Have adequate audit trails been incorporated in the application system?	*Review audit trail set up.* *Review audit trails*	☐ Yes ☐ No		
E4. Data Output				
Do users reconcile input control totals to output control and report totals.	*Review operational manuals. Observe procedures*	☐ Yes ☐ No		
Do data control personnel scan output reports to detect errors such as missing data fields, unreasonable values, and incorrect report format before distributing to users.		☐ Yes ☐ No		
Is the system of identification of e.g. report name and number, date, accounting month-end or other effective date, name of entity, page number, programme number, subtotals and report total adequate?		☐ Yes ☐ No		
Is a report distribution lists being used to prevent reports being received by unauthorised users?		☐ Yes ☐ No		
Are outdated output reports destroyed by shredding instead of placing them in a waste container?		☐ Yes ☐ No		
E5. Application ownership and administration				
Have an application system owner and system administrator been identified?	*Interview the manager in charge of the business process being supported by the application*	☐ Yes ☐ No		
Is there proper user account administration to ensure that only user authorised by the system owner are given access to the application	*Review user account management procedures.* *Select a sample of users and verify that there is evidence of authorisation of user creation*	☐ Yes ☐ No		
Is there role-based access mechanism to ensure segregation of duties?	*Review the access policy and review the access control lists for a sample of users*	☐ Yes ☐ No		

CONCLUSION: Are the application systems control objectives achieved?

☐ YES ☐ NO

High	
Medium	
Low	

If NO identify impact and assess the consequent risks.

Appendix 13: Checklist for iBAS++ Documentation and Guidelines relating to Security and Operating Procedures

IT infrastructure

1. Data centre
2. Network
3. Location
4. Users
5. Connectivity

Guidelines relating to Security and Operating Procedures (Date of release 24.05.2021)

- Review and examine the following Guidelines.
    1. iBAS++ Operations Security Guidelines
    2. Organisation of Information Security Guidelines
    3. Physical and Environmental Security Guidelines
    4. Software Development Life Cycle (SDLC) Guidelines
    5. Supplier Relationship Guidelines
    6. Access Control Guidelines
    7. Asset Management Guidelines
    8. Communications and Security Guidelines
    9. Compliance Guidelines
    10. Internet Usage Guidelines
    11. Cryptography Guidelines
    12. Human Resource Security Guidelines
    13. Incident Management Guidelines
    14. Information Security Aspects of Business Continuity Management Guidelines
    15. Information Security Guidelines

Documentation

1. iBAS++ modules
2. Integrated system flowchart
3. Network diagram
4. Data flow diagram
5. iBAS++ technical manual
6. User manuals
7. User training manuals

	Date	Initials
Prepared by		
Reviewed by member of IT specialist group		
Reviewed by Audit principal		