AUDITING IT GENERAL CONTROLS

A DEEP DIVE

WHAT ARE IT GENERAL CONTROLS

IT General Controls are controls which relate to the environment that supports IT Applications.

They constitute policies and procedures that:

- Support application controls
- Relates to multiple applications
- Can Operate centrally or in multiple locations
- Support automated controls

Generally auditors cannot rely on the automated controls if your IT General Controls are not adequately designed and operating effectively.

CONTROLS UNDER IT GENERAL CONTROLS

General controls include, but are not limited to the following:

- IT governance,
- Risk management,
- Resource management,
- IT operations,
- Application development and maintenance,
- User management, logical security,
- Physical security,
- Change management,
- Backup and recovery, and business continuity,
- Segregation of duties or governance arrangements

General controls are reviewed by internal audit because they form the basis of the IT control environment.

KEY FOCUS AREAS DURING IT GENERAL CONTROLS AUDITS

- IT Governance
- User Access Management
- Programme Change Control
- Security Management
- IT Service Continuity
- Physical and Environmental Controls*

In complex environments we may also include

- IT Projects
- IT Contracts

* Not covered in this presentation

IT GOVERNANCE

GOVERNANCE OF ICT

WHAT IS IT GOVERNANCE

- An integral part of Organisational Governance
- Consists of the leadership, organisational structures, and strategies
- Directs IT resources and ensures that that:
  - IT is aligned to organisational goals
  - IT is used to enable organizational goals
  - IT Risks are appropriately managed
- Also consists of a set of policies and procedures designed to extract maximum value from IT Assets.

- Primary goals of IT Governance are:
- Delivery of value – driven by strategic alignment of ICT Strategy to organisational strategic goals.
- Mitigation of IT Risks – driven by embedding accountability into the organisation

RISKS WITHIN IT GOVERNANCE

1. The lack of an IT Governance Framework may result in lead to failure to understand and manage IT Risks
2. Lack of alignment between business and IT strategic objectives might lead to unnecessary IT expenditure on systems that do not meet user needs
3. Lack of oversight over IT spending which could result in benefits not being realized.
4. Insufficient IT capabilities may result in the IT unit not being able to support the organization's objectives

KEY FOCUS AREAS UNDER IT GOVERNANCE

No	Process
1	IT Governance Framework
2	IT Strategic Planning
3	IT Budget
4	IT Risk Management
5	Governance and Oversight Structures

IT GOVERNANCE STAKEHOLDERS

Stakeholder	Responsible	Accountable	Consulted	Informed
IT Manager	√			
EXCO Member	√			
MM/CEO		√		
IT Steering Committee			√	
Audit Committee				√
Council/Board		√		

USER ACCESS MANAGEMENT

USER ACCOUNT MANAGEMENT

WHAT IS USER ACCESS MANAGEMENT

- A framework of policies and procedures ensuring that authorised users have appropriate access to systems.
- It is important to Financial Auditors because it helps identify the risks relating to:
  - Accuracy of financial statements
  - Posting of unauthorized financial transactions
  - Unauthorised vendor payments.

RISKS WITHIN USER ACCESS MANAGEMENT

1. Users with unauthorised access may affect unauthorized and fraudulent transactions leading to a negative impact on the integrity of data.
2. Idle user accounts may be used to effect unauthorized transactions compromising the integrity of information systems.
3. Failure to log and formally communicate password changes may result in unauthorized and fraudulent transactions being processed.
4. Lack of regular user access reviews may result in users having inappropriate access processing unauthorized or fraudulent transactions compromising the integrity of information systems.

KEY FOCUS AREAS UNDER USER ACCESS MANAGEMENT

No	Process
1	User Account Management Policy
2	Creation of New User Accounts
3	Modification of Existing User Accounts
4	Password Changes
5	Termination / Suspension / Disablement of User Accounts
6	Review of User Activities
7	Review of Administrator Activities
8	Use of Unique User Account Credentials

USER ACCESS MANAGEMENT STAKEHOLDERS

Stakeholder	Responsible	Accountable	Consulted	Informed
IT Manager		√		
Administrator	√			
Process Owner		√		
User	√			
IT Steering Committee				√
Human Resources			√	
MM/CEO		√		

PROGRAMME CHANGE CONTROL

CHANGE MANAGEMENT

WHAT IS PROGRAMME CHANGE CONTROL

- Formal process used to ensure that changes to software, hardware and related documentation are introduced in a controlled manner.
- Intended to minimize the negative impact resulting from changes to IT systems through standardized process of governance.
- Change controls must be implemented to ensure that changes to systems configuration are authorised, tested, documented and controlled ensuring that systems operate as intended.
- Change controls are important to Financial Auditors because unauthorised changes may result in fraud and unstable systems.

RISKS WITHIN PROGRAMME CHANGE CONTROL

1. Unauthorised changes may degrade the reliability of the system resulting in poor data integrity.
2. Unauthorised changes may result in fraudulent changes being made which may be used to process fraudulent transactions.
3. Lack of adequate change controls may result in systems erroneous processing and reporting.
4. Failure to follow strict change management may result in difficulties when conducting maintenance of the updated systems.

KEY FOCUS AREAS UNDER PROGRAMME CHANGE CONTROL

No	Process
1	Program Change Management Policy
2	Change Log / Register
3	Change Lice cycle

PROGRAMME CHANGE MANAGEMENT STAKEHOLDERS

Stakeholder	Responsible	Accountable	Consulted	Informed
IT Manager		√		
Change Manager	√			
Process Owner		√		
Change Requestor	√			
Change Management Committee		√		
Users	√			
IT Steering Committee			√	
Audit Committee				√
MM/CEO		√		

SECURITY MANAGEMENT

IT SECURITY MANAGEMENT

WHAT IS SECURITY MANAGEMENT

- It is the processes put in place to secure information technology assets by reducing the risk of loss of information to an acceptable level. The three major objectives of Information Security Management are:
  - Confidentiality
  - Integrity
  - Availability

- Three categories of information security:
  - Preventative security controls
  - Detective security controls
  - Corrective security controls

RISKS WITHIN SECURITY MANAGEMENT

- Without a formal IT Security Policy there may not be a foundation on how to protect the organization's information technology assets which may affect confidentiality, integrity and availability of financial systems.
- Attackers may exploit vulnerabilities and gain access to organisational networks / systems leading to access to sensitive information, malicious damage or complete control of the information systems.
- Failure to detect security breaches on a timely manner compromising confidentiality, integrity and availability of financial systems.
- Inadequate user security awareness and security incident skills may result in delayed response to security incidents / breaches compromising the organisation's brand reputation.
- Inadequate firewall redundancy / backups may impact the business continuity as a result of denial of service attacks and subsequently expose the internal network to attacks.

KEY FOCUS AREAS UNDER SECURITY MANAGEMENT

No	Process
1	IT Security Policy
2	Anti-Virus Controls
3	Patch Management
4	Password Configuration
5	Security Breaches
6	Sensitive Information
7	Firewall Controls
8	Security Awareness Training

SECURITY MANAGEMENT STAKEHOLDERS

Stakeholder	Responsible	Accountable	Consulted	Informed
IT Manager		√		
Administrator	√			
Process Owner			√	
Users	√			
IT Steering Committee			√	
Audit Committee				√
MM / CEO		√		

IT SERVICE CONTINUITY

CONTINUITY OF ICT SERVICES

WHAT IS IT SERVICE CONTINUITY

- The collection of policies, standards and procedures used by organisations to improve their ability to respond when major system failures occur while also improving resilience to major incidents and ensuring that critical systems and services do not fail or failure limited to acceptable Recovery Time Objective (RTO) limits.

- Some of the hazards that can lead to a disaster affecting application systems:
  - Power loss (loadshedding / blackouts)
  - Fire
  - Flooding
  - Cyber attacks – e.g. malware attacks

RISKS WITHIN IT SERVICE CONTINUITY

- Lack of a formal IT Disaster Recovery Plan may result in the organization not being able to recover services within acceptable time lines.
- Lack of disaster recovery testing may lead to the organisation not being able to continue normal operations during a disaster.
- Failure to perform backups may lead to the organisation not being able to recover critical systems.
- Failure to document and implement a formal backup policy may result in the organisation not performing backups increasing the risk of losing critical data.

KEY FOCUS AREAS UNDER SECURITY MANAGEMENT

No	Process
1	IT Disaster Recovery Plan (IT DRP)
2	Testing of the IT DRP
3	Backup Policy
4	Backup Scheduling
5	Testing of Backups
6	Off-site Storage of Backups
7	Encryption of Data Backups on the Cloud

IT SERVICE CONTINUITY STAKEHOLDERS

Stakeholder	Responsible	Accountable	Consulted	Informed
IT Manager		√		
Administrator	√			
Process Owner	√			
Users	√			
IT DR Team	√			
IT Steering Committee			√	
Audit Committee				√
MM / CEO		√		

CONTACT US

Nkosazana Sibiya

Contact Number: **061 413 4805**

Email Address: Nkosazana@iygroup.co.za

Thato Letlojane

Contact Number: **083 308 5652**

Email Address: thato@iygroup.co.za

www.iygroup.co.za

THANK YOU

NKOSAZANA@IYGROUP.CO.ZA

THATO@IYGROUP.CO.ZA