INTERVIEW PREPARATION DOCUMENT

(IT AUDIT, TECHNOLOGY RISK & THIRD-PARTY RISK)

PROFILE BASED INTERVIEW QUESTIONS

TELL ME ABOUT YOURSELF?

My name is Azeez Hassan and I am a professional with years of experience in Technology Risk and IT Audit Assurance, GRC & Governance. I currently work with Focal Point Associates & Company as a Manager, Technology Risk, IT Audit, and Data Governance, where I plan and execute audit testing to assess sufficient risk mitigation measures and control effectiveness. I am responsible for overseeing technology assurance audits, evaluating security audits, data governance implementation, audit reviews and compliance.

I also lead the execution of IT internal audit engagements to assess the adequacy of internal controls and deliver value-added reports on findings and inadequacies within the internal control.

Prior to joining FocalPoint Associates & Company, I worked with Lagos State Internal Revenue Service as an Internal IT Audit Associate, where I was heavily involved with performing Internal Audit and Risk Compliance reviews, Internal control testing, security assessments, and evaluation of security compliance requirements and helping the organization implement Corrective Action Plans on audit findings.

Over the years, I have worked with high-performing teams on several engagements across different domains of IT Risk & Assurance services such as IT Internal and External Audits, Security Audit and Compliance Assessment, SOX ITGC testing, SOC reporting, and ISO 27001 Audit review.

I am a goal-oriented individual and understand the importance of team collaboration, self-development, and delivering quality at all times. I am a good team player and I ensure to build good relationships with clients and most importantly my colleagues.

Outside of my daily work, I engage in self-developmental activities to improve myself and also to contribute to different communities. On the flip side, I enjoy playing soccer and meeting new people.

WHAT IS YOUR EXPERIENCE AT YOUR PRIOR PLACE OF WORK (I.E. AS AN EXTERNAL AUDITOR)

While in this role, I supported the Tech Risk team on the review and execution of IT Audit engagement for clients here in the finance, insurance and manufacturing sectors. I also supported different Technology Advisory projects such as the review of IT infrastructure controls in line with the CIS critical security controls (CSC). I led teams on smaller engagements and led an evaluation of an entity's environment to evaluate their Information Security controls in line with CIS Critical Security Control standard. Generally, I assisted clients with assessing IT Risks, testing ITGC and ITAC controls during an audit, evaluating controls against security compliance frameworks such as ISO27001, SOC, NIST, CIS, and implementing continuous monitoring processes s for critical controls and measures to mitigate the risks.

I've had the opportunity to work with different clients, studying other processes and reviewing different adopted procedures, leaving me with a broadened scope of interaction and adaptation to different situations.

WHY DO YOU WANT TO LEAVE YOUR CURRENT POSITION?

The major reason why I want to leave my current position is for Growth opportunities and also my desire to be part of a larger team. I believe that the bigger the portfolio the more the experience, and I am keen on working in a fast-paced environment where I would be able to learn as much as make an impact within the team and on the clients.

WHY DID YOU APPLY TO THIS ROLE?

The reason why I applied for this role is that the responsibilities highlighted for the role are relevant to my experience. I believe I have the required knowledge and am certain that this opportunity will enable me to learn, grow and make an impact within the team through effective collaboration.

As an Auditor, I am keen on identifying risks and roadblocks, recommending solutions, and supporting the implementation of the solutions to enhance critical business processes and new products.

WHY DID YOU APPLY TO OUR FIRM?

Answer: Asides from having the requisite skills needed for the role, there are a number of reasons why I have chosen this opportunity at the company.

- The main attraction for me is the diversity and inclusion at XXXX. The firm is an equal opportunity employer that believes in the strength of diversity and employs across different races and backgrounds. I equally enjoy working with people across different races and backgrounds as it helps to foster inclusion and to learn more about our cultural differences.

- Freedom to Be Creative: The firm supports creativity and believes in employees' ability to innovatively deliver quality with high levels of productivity. I believe I will greatly benefit from this gesture.

- Team Collaboration - I would be able to leverage other people's diverse experiences within the work environment. Given the company's diversity level, this will even be more interesting.

- Learning and development: I am a firm believer in self-development through lifelong learning. I believe the firm would avail me of the opportunity to acquire more skills through coaching, learning, and development.

- Growth Opportunities: Growth is part of the firm's agenda, and the growth opportunities are cascaded across all levels. I also believe I will greatly benefit from the career growth opportunities within the firm.

WHAT IS YOUR CAREER ASPIRATION?

Answer: At the moment, I want to work in a place that provides me with opportunities to make the best impact in a fast-paced environment. A place that will enable my growth, fosters inclusion, and creates opportunities for employees to collaborate and learn. In the foreseeable future, I see myself growing up the ladder; I aspire to get promoted to the senior management level within the firm.

WHAT DO YOU CONSIDER IN A COMPANY WHEN MAKING A CAREER MOVE?

Answer: There are a lot of factors I consider in a company when thinking of a career move but these are the three (3) most important to me:

• Learning and development opportunities

•Career growth opportunities

• The work culture and ethics of the company

WHAT ARE YOUR EXPECTATIONS IN THIS ROLE, IF CONSIDERED FOR THE JOB

Answer: As a Senior Associate within the IT Audit/ Security Audit/ GRC team, I am expected by the team leader to plan, coordinate and execute IT Audit review, Identify and manage risks, and evaluate IT Systems and relevant internal controls that are in place to mitigate risks and protect assets.

As such, In this role, I would hit the ground running by first understanding the landscape and the architecture, performing a current state assessment, reviewing previous IT and IS audit engagement files and reports, evaluating our audit programs and approach, and leveraging risk-based approach to performing Information system audit.

To successfully deliver on my early expectations, I will leverage my colleagues' expertise and also seek to collaborate with SMEs in relevant teams.

HOW DO OUR CORPORATE VALUES RELATE TO YOUR VALUES?

Answer: everyone within the company is expected to innovate, act with integrity, show empathy for each other, foster inclusion, and collaborate for maximum impact.

These are values invested in me as an individual and these are values that have gotten me this far in my career as an IT Auditor professional.

WHAT MOTIVATES YOU?

Answer: I'm motivated by the need to do more and to build excellence into whatever I'm involved in. I'm always driven by impact. Specifically, I derive joy in helping organizations make the best decisions on technological investment and planning ahead for its risks.

COMPETENCY BASED INTERVIEW QUESTIONS

GENERAL

GIVE A BRIEF DESCRIPTION OF ANY IT AUDIT / ASSURANCE ACTIVITIES THAT YOU HAVE PERFORMED.

Answer: In my previous role, I have supported and led several assurance activities particularly leading IT Audit and assurance engagements. Specifically, I was responsible for planning the engagement, agreeing on the scope of testing and also creating the budget and task allocation for the team.

I led the audit walkthrough execution through testing of entity level controls, IT General controls and IT application controls, thereby testing the design and operating effectiveness of internal controls that have been implemented to protect information assets.

I document findings accordingly in our final report and schedule client close out call to discuss relevant findings as expected

DO YOU HAVE EXPERIENCE OF WORKING IN AN IT ADVISORY RELATED TYPE OF ROLE (E.G. SECURITY ADVISORY, IT ASSESSMENT OR CYBER GRC).

Yes I have experience working on Information Assurance, IT Risk and Advisory related projects. I have been part of the GRC implementation project and also supported ISO 27001 implementation for an entity during the implementation of their ISMS.

In addition, I have experience with data assurance stemming from a migrations project where I was responsible for reviewing the migration process and providing assurance on the completeness and accuracy of the data that was migrated and the approach that was followed.

I have expertise in implementing controls in line with security frameworks such as ISO 27001, CIS CSC, NIST, and CSA CCM.

In addition, I have also performed due diligence reviews on mergers and acquisition processes to reduce the risk associated with mergers and ensure that absorption of a new entity does not interrupt our internal control processes.

DO YOU HAVE EXPERIENCE MANAGING ASPECTS OF AN ORGANIZATION'S EXTERNAL AUDIT RELATIONSHIP? PLEASE GIVE DETAILS

In my previous role, as a team lead on different engagements, I was responsible for managing relationships with clients. senior management, and control operators.

Specifically, I led conversations on scope discussions, agreed on work approaches, coordinated client care/ check-ins, ensured to create a collaborative environment with the client contact, and provided expert opinion and recommendations on how to improve their internal audit programs.

As an individual, I understand the importance of team collaboration and I ensure to build good relationships with my clients and colleagues.

TELL ME ABOUT A TIME YOU INFLUENCED A TEAM WITHOUT AUTHORITY. OR DESCRIBE A TIME WHEN YOU CHALLENGED AN IDEA OR APPROACH?

Answer: To influence my team or superior without authority, I ensure to support my suggestions and actions with clear RATIONALE.

I could remember during an audit engagement for a client, while reviewing the IT General Controls on this audit, I noticed that the team was not managing the backup and recovery control appropriately. Although the design of the backup control is effective and it's a daily control, however, I noted that for a particular day which was included in my randomly selected sample for test of operating effectiveness, the backup activity was not performed for critical systems that are in scope of the audit.

Further discussion with the IT Manager, we noted that the omission in performing the backup for this particular day was an oversight. My team lead suggested that the control should be classified as effective. I then made a comment to suggest that we need to perform a follow-up procedure on the control before we can conclude on its effectiveness.

Initially, my team lead disagreed with my suggestion on performing a follow-up review to determine the pervasiveness of the omission of taking daily backups because we have a short time to complete the audit reviews.

I was able to influence his decision by providing clear rationale to support my suggestion. I also mentioned that there is a need for us to uphold standards in what we do. More importantly, we need to be able to defend our conclusion to the client and also to the engagement manager.

Given my rationale, she agreed for us to select more samples to test for pervasiveness. I selected 15 additional samples at random, and from this we noted that backups were not taken for an additional 6 days out of the 15 samples.

My team lead appreciated my suggestion and we were able to conclude that the control is ineffective given that backups were not performed for different days from the samples we selected.

TELL ME ABOUT A TIME YOU CARRIED OUT RESEARCH TO COMPLETE A TASK?

Answer: Learning is a continuous process on risk advisory and cybersecurity-related projects. We do research to get deep knowledge about a particular subject matter. For instance, during a security review and cyber maturity assessment for a Bank, I researched several security tools (e.g., SIEM tool) and also control maturity assessment techniques that would be suitable to the client's needs based on the current state assessment performed and the desired state communicated by the management. I realized that the best practice is often what is fit for the client's risk profile and what addresses the client's problem statement.

TELL ME ABOUT A TIME YOU MANAGED A TEAM MEMBER THAT WAS UNDERPERFORMING.

Answer: I once had a team member who could not deliver his task as expected of him due to personal issues. Although his performance on previous engagements was commendable, however, he was struggling to deliver on this engagement and his turnaround time was really poor. I quickly noticed how his reactions and attitude to work were affecting the team's performance and our ability to meet deadlines.

I then engaged him to have a brief discussion. During this meeting. I started by appreciating him for the work he was able to complete and then pointed out to him that his performance on previous engagements was of high impact to the team. However, his attitude towards work has been reduced and his turnaround time is below expectations. I then went on to ask him to please be free to share his ordeals and challenges with me.

He responded positively stating that he appreciates my genuine concerns. He informed me that he is preparing for his AWS cloud practitioner exams and could only find time at midnight to study and practice. As a result of the little time to sleep his energy level during the day is often low thus affecting his ability to complete tasks promptly. Mind you, he has attempted and failed this the first time.

My response to this was to allow flexibility in his work. Since we are working remotely, I suggested that he could start resuming work by 12 pm so he could get enough sleep and then close by 6 pm as opposed to resuming at 8 am and closing by 5 pm. He accepted my proposal and I communicated this to the senior manager and partner and they both gave their approval.

In addition, I kept him motivated all through the engagement by ensuring that for each specific task assigned to him we both agreed on realistic, measurable, and time-bound goals. Also, I ensured he gets the necessary coaching he needs to deliver his task.

He was able to give his best always and at all times. He worked tirelessly and together with other team members we successfully delivered the engagement without missing the deadline. But what was more important to me was that Dominion passed his exam and we had a team bonding event where he expressed his gratitude for our concerns and flexibility.

I learnt that when a team lead shows genuine care for the well-being of his/her team members they return the favour by giving their best and trusting in their leader.

HOW DO YOU LEAD A TEAM/WHAT IS YOUR LEADERSHIP STYLE?

Answer: Over time, I have adopted a participatory and an engaging form of leadership. As a team lead,

- I ensure to communicate effectively & efficiently with team members, project leadership & stakeholders

- I ensure to build a professionally genuine relationship with all stakeholders and team members

- I am a good listener, welcoming to ideas and contributions and I have good conflict resolution abilities

- I am able to delegate efficiently, even though tasks may be shared, I show great responsibility & accountability for all project tasks as the team lead

I encourage flexibility and I ensure to provision for it during project planning

- Empathy gets the job done faster than strictness, and I ensure to always show empathy to everyone whether working with me or not

TELL ME ABOUT A TIME YOU COACHED JUNIOR COLLEAGUE TO PERFORM A TASK ON YOUR ENGAGEMENT?

Answer: Coaching has two impacts, it helps me to increase my knowledge on the subject matter, while I also impact knowledge on others which I really love to do.

Whenever there are new hires or junior colleagues working with me on any of my assurance or IT Audit engagement, I make a conscious effort to train them and also to monitor their development. I ensure to coach the juniors for us to sustain the expertise and knowledge of IT Risk and control testing within the team.

TELL ME ABOUT A TIME YOU MANAGED A DIFFICULT CLIENT.

Answer: The Head of Information Technology Unit at a particular Merchant Bank is a very difficult person who will contest all audit findings. I recall that while reviewing the Bank's IT Controls, I noted several deficiencies in the design and implementation of certain controls, and there are no compensating controls to mitigate the risks. For instance, we noted that certain employees are not fully aware of the information security policies, default passwords were not changed for Oracle System Admin users. Also, we noted generic users on the client's core banking application. This is not in line with best practice and the bank's information security policy.

I arranged a meeting with the head of IT, and other key stakeholders to discuss the audit findings. At the start of the meeting, the Head of IT was already creating an impression that he would not accept any findings from the auditors as his IT environment is clean of any deficiency. I stayed calm during the meeting and kept a smiling face. Once I got the opportunity to speak, I started by making the Head of IT realize that our review is to assist the client in ensuring a compliant and secured environment. After which I explained to them defaults passwords on Live Databases could be used to gain unauthorized access to the client's environment. In addition, I also stated that employees that are not aware of the Bank's policy could fall victim to social engineering which could be leveraged to gain unauthorized access to the client environment.

At the end of the meeting, the Client accepted the audit findings and promised to improve on our noted areas of deficiencies ahead of the next audit review.

The lesson learnt for me was that effective communication skills are very useful when dealing with a difficult client.

TELL ME ABOUT A TIME YOU MANAGED CONFLICTING PRIORITIES FROM TWO MANAGERS?

Answer: Sometimes in January, I was overseeing five (5) IT Audit and Revenue Assurance Engagement concurrently. In addition, I was the team lead on the Quality Assurance review for an ERP implementation where I have 7 team members reporting to me on different workstreams. These projects were being managed by separate managers and had almost the same deadline except for the Quality Assurance engagement.

To achieve the desired result, I did the following:

- I allocated responsibilities to each team member with a timeline and checked if the resource we have is adequate.

- I kept my team motivated all through the engagement by making sure that all my team members understood the objective and the need to meet daily deliverables. I also provided on the Job coaching and support to junior colleagues and ensured we had daily team discussion at the end of each working day. Whenever we slipped on a deadline, I worked extra hours to bring the team back on track.

I gave daily updates to the engagement managers on the progress of these engagements and ensured they are well briefed on the status of work.

I successfully delivered all engagements without missing the deadline and I was rated as Highly Effective Performer during the evaluation.

DESCRIBE WHEN OR WHERE YOU LEARNED THE MOST ABOUT YOUR STRENGTHS AND WEAKNESSES

As a GRC professional, one needs to be familiar with relevant IT and information security frameworks. I have been on a project where we had to evaluate controls with ISO 27001, CIS CSC, NIST 800-53, COBIT and AICPA SOC 2.

While working on a security assessment project, I realized my knowledge gap with the CSC and CCM framework, so I had sped up my knowledge of both frameworks. Being in this role made me realize that learning is lifelong as a security auditor and GRC professional, whether technically or theoretically. This experience has helped me in my career as a consultant especially working with clients and adapting to changing requests and requirements.

Also, I discovered another strength in my career which is being able to manage upwards. Specifically, this is more like helping my line manager to focus more on my development and improve their ability to manage other people. As a Technology Risk professional, I would often request feedback from my superior, but I also engage the senior members of the team for me to provide feedback to them as well. This is what I refer to as the 360-feedback mechanism

About areas of improvement, I tend to forget things when I get overwhelmed, so I take a lot of notes, and over time I've learned to use personal development tools like Trello and Note taking apps to manage productivity. I also found that within a team, there is a need for us to decentralize knowledge to mitigate key man risk, so I ensure to delegate tasks to colleagues where required.

GIVE ME AN EXAMPLE OF HOW YOU GAINED OTHERS' CONFIDENCE WHEN YOU WORKED WITH THEM FOR THE FIRST TIME.

This was about a time when I single-handedly presented audit findings to the board audit committee as the engagement Manager and the Director could not make it to the client site on time.

It was my first time working with the manager, and I was a year 2 analyst at the time. During the audit reporting, we were to present to the audit committee. I had resumed to the client site, while my manager and the partner were meant to join me. However, they could not make it in time due to heavy traffic caused by a road accident.

When it was time to present the audit findings by our team, I was the only representative of the company at the meeting. Although I was nervous at first given the calibre and the level of people in the committee, in addition to the fact that this is my first time presenting to a committee of high-profile individuals. Eventually, I was able to present our findings with less hassles.

Since I was the one who tested the ITGCs, I was very familiar with the findings, and I also ensured that I have evidence to support all the findings if requested. The client contested a few of the findings, but I was able to provide sufficient evidence and also stated the risks that are present with deficiencies that we noted.

My manager and the Director were very impressed and proud of me for this act of bravery and this event helped me improve my confidence when dealing with clients.

GIVE ME AN EXAMPLE OF A TIME YOU INCREASED A TEAM'S EFFECTIVENESS OR PRODUCTIVITY.

This was a time when we had resource constraints at my previous place of work, and we have had instances where team members suddenly get pulled out of a project for them to work on a new project due to this resource constraint. Sometimes, a team member might become unavailable due to fatigue and it was really affecting some of the engagement we were working on at the time.

Particularly during the implementation of an ISMS using ISO 27001 project for a client. It was 3 of us and we had already shared the tasks amongst ourselves. I was responsible for performing the gap assessment, risk management workstream, and to document some procedures that are yet to be established.

Given that we have a very small team and knowing that a team member can get pulled off or become unavailable, I suggested that we decentralize the tasks and we should build redundancy into our work approach. That way, if one person is unavailable, the other team members will be able to pick up his/her workstream and run with it.

I suggested that we should leverage an approach I refer to as "Active-Passive Delegation Strategy". The way the strategy works is that. If one person is actively working on a workstream (ie, their active task), the person will be passively reviewing another team member's workstream (i.e. their passive task). Similarly, the first team member will have someone passively reviewing their own workstream too.

That way, we will be able to continue to work efficiently if one person leaves the team or suddenly becomes unavailable. This approach ensured that we positioned ourselves well to be fault tolerant in nature. When one of us was sick, the impact on the project team was very minimal as the person that was passively reviewing her workstream was able to step in for them.

This approach became widely accepted within my unit and I believe it is being currently used till today. I was credited for this as well

WHAT'S YOUR PROCESS FOR APPROACHING AN AUDIT BEFORE IT'S OFFICIALLY INITIATED?

I implement several steps before starting the initial audit to ensure it runs smoothly and experiences little to no errors. First, I make sure the audit team and the department receiving the audit know each other in order to build a collaborative and communicative relationship during the audit. Then, I help the company create an audit plan to properly establish the department getting audited. Next, I strategize an audit plan that defines its purpose and the resources required. Finally, I conduct a meeting with the management team and the auditors to communicate our plan.

IT AUDIT & INFORMATION ASSURANCE

DEFINITIONS (TO FAMILIARIZE YOURSELF WITH DEFINITIONS)

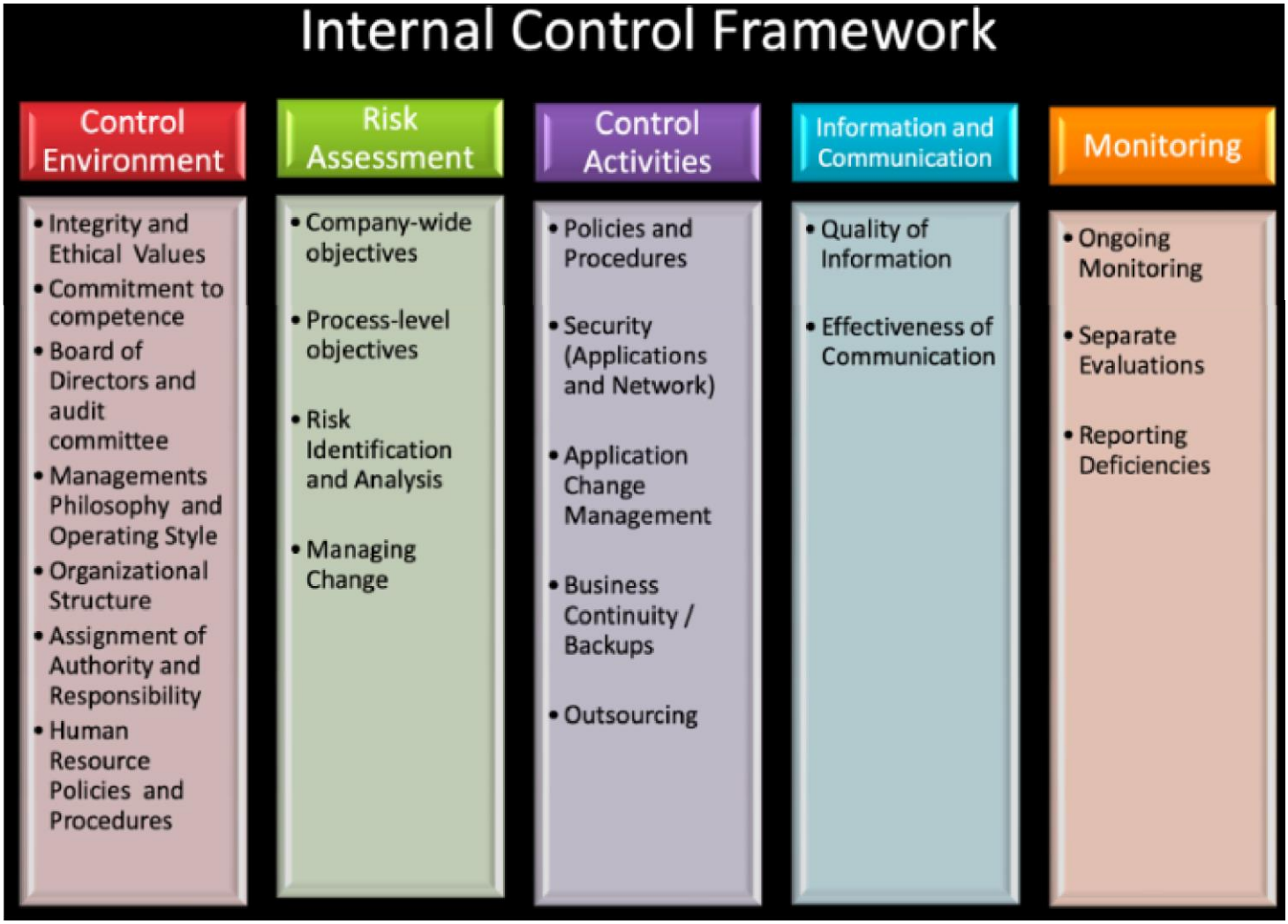
WHAT IS INTERNAL CONTROL?

Internal Control is a process that is laid down by an entity's board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Five Components of Internal Control System / Five component of COSO Framework:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring



Control environment. The control environment seeks to make sure that all business processes are based on the use of industry-standard practices. This can help ensure that the business is run in a responsible way. It may also reduce an organization's legal exposure if the organization is able to prove that its business processes are all based around industry standard practices. Additionally, the control environment can help with making sure that an organization is adhering to regulatory compliance requirements.

Risk assessment and management. Risk assessment and management -- which is sometimes referred to as enterprise risk management -- is based on the idea that risk is an inherent part of doing business. However, those same risks can sometimes cause a business to suffer adverse consequences. As such, organizations commonly adopt risk management plans that help them to identify risks and either reduce or eliminate risks deemed to pose a threat to the organization's well-being.

Control activities. Control activities are also tied to the concept of risk management. They are essentially internal controls that are put into place to make sure that business processes are performed in a way that helps an organization to meet its business objectives without introducing unnecessary risks into the process.

Information and communications. Communications rules are put in place to make sure that both internal and external communications adhere to legal requirements, ethical values and standard industry practices. For example, private sector organizations commonly adopt privacy policies establishing how customer data can be used.

• Monitoring. At a minimum, monitoring is performed by an internal auditor who makes sure that employees are adhering to established internal controls. However, in the case of public companies, it is relatively common for an outside auditor to evaluate the organization's regulatory compliance. In either case, the audit results are usually reported to the board of directors.

RISK

Risks are anticipated occurrences that expose one to damaging impact if not mitigated or if it materializes without a mitigation strategy in place. Specifically, risks are occurrences that negatively impact assets of value.

From a security perspective, a risk is the probability that a threat event will exploit a vulnerability in the system to impact the asset

Establishing a risk management plan and a mitigation strategy plays a major role in addressing security risks within an IT environment. The risk management plan would detail the process of risk Identification, risk assessment, and risk treatment processes such as implementing controls to reduce the risk impact if it materializes.

In addition, a risk management team should be established, and an appropriate structure should be developed with clearly defined roles and responsibilities.

What is the Risk Calculation Formula?

Risk = **Threat** x **Vulnerability** x **Assets**

WHAT IS INHERENT RISK?

Inherent risks are risks that exist within the IT controls environment before applying a countermeasure or before putting a control in place to mitigate the risk. This is largely considered as a risk that exists by nature of the IT environment processes and practices.

WHAT IS RESIDUAL RISK?

Residual risk is the risk that remains after your organization has implemented all the security controls, policies, and procedures you believe are appropriate to take. Residual risk refers to those risks that remain even after applying all the controls you intend to use.

Understanding residual risk is important for regulatory compliance. The ISO 27001 standard to manage information security, for example, requires companies to monitor residual risk. To be ISO 27001-compliant, businesses must have residual security checks in place along with inherent security checks.

WHAT IS CONTROL RISK

Control risk means the chance that auditors will not catch and correct a material mistake in the financial statements before they are issued. Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

WHAT IS AUDIT RISK?

Audit risk is the risk that an auditor will not detect errors or fraud while examining the financial statements of a client. Auditors can increase the number of audit procedures in order to reduce the level of audit risk. Reducing audit risk to a modest level is a key part of the audit function, since the users of financial statements are relying upon the assurances of auditors when they read the financial statements of an organization.

An audit aims to reduce the audit risk by adequate testing and appropriate evidence to a suitably low level.

WHAT IS IT AUDIT REVIEWS?

Auditing an information system involves the evaluation of administrative, technical and physical controls that are implemented to protect information assets within an IT/ Business Environment vis-à-vis review of Policies, Processes, People and Technology. IT Audit is used to evaluate the design and effectiveness of internal control over the IT environment.

IT Audit reviews seek to determine whether the existing IT controls can effectively protect the information assets, adhere to the regulatory standard, and are aligned with the overall business goal. The objectives are to:

• Evaluate the systems processes and controls in place that secure company information assets.

• Determine risks associated with the controls and identify attributes to test the effectiveness of the controls in place to mitigate the risks.

• Ensure information management processes are in compliance with IT-specific laws, policies and standards.

• Determine inefficiencies in IT systems and associated management processes.

WHAT IS THE PURPOSE OF IT AUDIT REVIEWS?

The purpose for IT Audit is to ensure that there are appropriate controls within the IT environment to:

- Protect information Assets
- Ensure integrity of transaction processing
- Ensure adherence to management standards
- Mitigate risk of fraud and misstatements (financial)
- Reduce impact of disaster that could affect the business
- Ensure appropriate governance of the IT environment.
- Security risks, exposures and threats are mitigated
- Support the business optimally with no vulnerabilities

WHAT ARE IT CONTROLS

Controls are measures implemented to protect information assets, and to minimize risks that could potentially impact these assets. These are specific activities performed by persons or designed systems to ensure that business objectives are met.

IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function. There are different categories of IT controls:

♦ **ITGC (IT General Controls)**

These are controls that apply to all systems, components, processes, and data for an organization's IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.

♦ **ITAC (IT Application Controls)**

IT application controls refer to transaction processing controls, sometimes called "input-processing-output" controls designed to ensure the complete and accurate processing of data, from input through to the output. The objective of ITAC is to ensure that Input data is accurate and correct, the Data is processed as intended in an acceptable manner, the Data stored is accurate, and the Outputs are accurate and complete.

Categories of IT application controls may include:

- Completeness checks - controls that ensure all records were processed from initiation to completion.
- Validity checks - controls that ensure only valid data is input or processed.
- Identification - controls that ensure all users are uniquely and irrefutably identified.
- Authentication - controls that provide an authentication mechanism in the application system.
- Authorization - controls that ensure only approved business users have access to the application system.
- Input controls - controls that ensure data integrity fed from upstream sources into the application system.

• Forensic controls - control that ensure data is scientifically correct and mathematically correct based on inputs and outputs

✦ **ELC (Entity Level Controls)**

These are controls that apply to all systems, components, processes, and data for an organization's IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operation.

♦ **EUC (End-user Computing Controls)**

These are controls that apply to all systems, components, processes, and data for an organization's IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operation.

♦ **Security Controls**

These are controls that apply to all systems, components, processes, and data for an organization's IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operation.

WHAT ARE IT INTERNAL CONTROLS? (NT THIS IS THE SAME AS IT CONTROLS)

IT internal controls include the activities within a company established by the management for addressing risks that can hold back the company from achieving its goals.

INTERVIEW QUESTIONS (COMPETENCY BASED)

WHAT IS YOUR UNDERSTANDING OF SOX, AND HAVE YOU TESTED SOX BEFORE? WALK ME THROUGH YOUR EXPERIENCE WITH SOX 404 TESTING?

Sarbanes Oxley is an Act established in 2002 in the US and this act that mandates review of internal controls over financial statements and financial processing within publicly listed entities. SOX rides on the COSO (i.e. Committee of Sponsoring Organization) framework which is a generally accepted model for evaluating internal controls to measure the effectiveness of these controls against risks.

SOX seeks to ensure that the components of the internal control system are available and effective within an enterprise organization. SOX 302 and 404 specifies the SOX compliance checklists and approach for evaluating internal controls that should be implemented to mitigate risks to financial processing within an organization.

As an IT Auditor, I have supported various **SOX ITGC controls** review vis-a-vis checking the controls that have been implemented to protect information assets, and also risks related to financial processing across the following objectives:

- Access Management
- Program Changes & Development
- Operations Management

I will also review the **Entity Level controls** by evaluating the

- IT Risk controls; and the

- IT Monitoring Control.

I will review the **IT Applications Controls (ITACs)** through evaluation of

- completeness and accuracy of transaction processing,

- review of system interfacing.

- evaluation of system access, and SOD matrix; and lastly,

- I will review of system approvals such as maker-checker, and system config settings

On all the SOX IT Controls testing engagement that I have been part of, I start by

- **Planning the scope of the IT Controls** that will be evaluated as part of my SOX compliance audit

- I also **assess IT Risks** as it affects the internal control, financial process and information assets

- I then **document the controls** to test, highlighting the control objectives and evaluating the design and operating effectiveness of these controls with protecting risks and information assets

- Once I test the TOD and TOE, I will **report the deficiencies** to the control operators and share the SOX compliance report with appropriate stakeholders. In this report, I will provide the risks related to control deficiencies and also recommendations on how to remediate deficiencies

- Lastly, I will **follow up** with control operators on the status of remediation for the findings noted in the SOX ITGC audit review.

TELL ME ABOUT A TIME WHEN YOU HAD A PROBLEM AND YOU DIDN'T KNOW WHAT TO DO

The first time I encountered SAP ERP system as an IT Auditor, and I had limited knowledge about the ERP system. Even now, I would not say I am a pro, but I understand the approach to follow when auditing complicated enterprise application systems.

During the audit, I didn't know what TCODES were (i.e transaction codes). These TCODES are required to be able to navigate around the system. I had to quickly develop myself to learn about TCODES and also how to view tables in SAP. Specifically, to view a table in SAP, one can use the TCODE SE16 or SE16N.

More so, I reached out to my colleagues who had more knowledge about SAP ERP system to explain my challenge and also leverage on his expertise

Also, I struggled a bit with the system interface, but as time goes, I was able to audit the application using the ITGC approach of checking:

1. How Access is being managed on the SAP system

2. How changes are being made and pushed to production system on SAP ERP, and lastly

3. What are the operational processes and controls in place to ensure that the system continues to be available to the business

In the end, I was able to effectively test the controls and review the system.

For me, whenever I have a problem and I don't know what to do, I ensure to leverage the expertise of my colleague. I also ensure to build good relationships and a collaborative work culture which enables me to seek help when I am in need.

More so, I ensure to learn and upskill myself to gain knowledge on areas where I have less expertise or whenever I am in doubt.

TELL ME ABOUT YOUR UNDERSTAND OF RISK-BASED APPROACH TO AUDITING INFORMATION SYSTEM

As a technology risk professional, when auditing an information system, or working on an advisory project that involves implementing controls, I ensure to follow a risk-based approach.

A critical aspect of GRC is to ensure that we manage resources when implementing control, and a risk-based approach helps organizations to manage resources when implementing controls. As an IT Auditor, it enables me to focus on high-risk areas when performing an audit review.

As best practices clearly state, when building an ISMS in line with ISO 27001 or when setting up internal controls in line with COSO framework, Organisations are required to evaluate risks and perform risk assessment to help identify, assess and treat risks accordingly.

To me, I believe that having a risk management function in itself is a control to protect against risks that are related to late detection of high risks.

By and large, whenever I am auditing information systems or implementing controls, I ensure to follow a risk-based approach to help me focus on areas with risks, and also manage resources.

TELL ME ABOUT A TIME YOU PERFORMED RISK ASSESSMENT, WHAT APPROACH DID YOU USE? WHAT RISKS WERE IDENTIFIED AND HOW DID YOU ASSESS THESE RISKS?

I have experience performing risk assessments especially on ISO 27001 implementation for key clients. I have knowledge of performing risk assessment using the qualitative approach and the quantitative approach.

Specifically, I have used more of the qualitative approach where we evaluate the risks that we are exposed to using the subjective approach and following the industry guidelines.

While working on the ISO implementation for an insurance client, I was responsible for the risk assessment workstream. My first approach to managing risks **involves identifying and listing all our information assets (i.e. tangible and intangible) across people, process, tools, buildings, software's and technologies.** Identifying all our assets will enable us to appropriately identify the risks they are exposed to, and plan to treat them accordingly.

Once the assets are identified, the next thing is to identify the risks that these assets are exposed to. For this, I leverage the qualitative approach to risk management by evaluating the threats that the assets are exposed to. I also check for the vulnerabilities within these assets (i.e. both technical and non-technical vulnerabilities) that could be exploited by these Threats. In evaluating the threats, we look at the assets and we also leverage on resources that are available online, in addition to my professional judgment.

Once the Risks are identified as well, the next thing for me is to assess the risk so I can appropriately rate them. To do this, I will assess the risk based on the impact and likelihood of occurrence using the risk rating heatmap. This will help me determine the risk rating whether it should be rated as high, medium or low depending on the rating scale that has been adopted within the organization.

After rating the risk, the next thing is to respond to the risk using the appropriate risk response methodology. I have a risk response model which I call the MATA model. This model has four risk response/treatment plan:

- M is for Mitigate i.e., to implement controls or countermeasures to reduce/ mitigate the risk impact if it materializes
- A for Avoid i.e.
- T for Transfer
- A for Accept

The appropriate risk treatment plan will be associated with the identified risks accordingly and documented in the risk register. Also, I will assign the risk owner to ensure that we have responsibilities covered for this risk.

Lastly, I will work with the risk owner to implement a continuous monitoring process for this risk, to enable us to re-assess and re-evaluate the risk treatment options for adequate safeguarding of the assets.

This is how I evaluate and assess risks and I have done this on several engagements.

TELL ME ABOUT YOUR UNDERSTANDING OR EXPERIENCE WITH THIRD PARTY RISK MANAGEMENT, AND HOW YOU WILL EVALUATE FOR THIRD PARTY RISKS. HOW WILL YOU ALSO MITIGATE SUCH RISKS?

With the current way of doing business, whereby organizations rely on integrations, and outsourcing to gain efficiencies, it is important to assess risks for relying on third parties for business-critical services.

Outsourcing a service does not eliminate a company of the responsibilities and duty of care over the service they outsource. It is the company's responsibility to ensure that the third-party service provider is committed to supporting the business by executing the service that has been outsourced to them.

Assessing third-party risks involves the following steps:

- Performing due diligence on the 3rd party organization by reviewing its director, services and dealing. This will also include reviewing public perception and opinion on similar organization that have used them
- Evaluate the criticality of the service that is being outsourced to the third-party organization
- Evaluate the impact that will be felt by the business if the outsourced service becomes unavailable
- Identify the threats that the 3rd party organization is exposed to
- Evaluate the vulnerabilities that the third-party service provided introduces into the business
- Assess the impact on the business

Given these factors and the likely risks from them, I will then ensure that appropriate risk response / treatment plan is associated with each risk that we identify.

To mitigate the risks, implement appropriate controls such a

- Ensuring that service organizations have the ability to secure our data by obtaining a SOC 1, 2 or SOC 3 report from them. I expect that the vendor has been reviewed by an external auditor and certified in accordance with AICPA Trust Service Criteria.
- Establish Service Level Agreement (SLA) and establish relevant KPIs and clauses in the SAL to ensure that the 3rd party organization
- Implement Performance Evaluation for all 3rd-party service level providers to review and evaluate how vendors are meeting with agreed KPIs
- For certain vendors, the outsourcing organization should enforce the right-to-audit in the service level agreement

- Determine the business continuity process / options and implement appropriate Business continuity plan in the event that a vendor for a critical service becomes unavailable

This is how I will manage third-party risks within an enterprise organisation

GIVE ME AN EXAMPLE OF RISKS YOU HAVE IDENTIFIED IN THE PAST; WHAT CONTROLS WERE IMPLEMENTED TO TREAT THIS RISKS

- Risk of unauthorized access to critical information system due to lack of appropriate access management process

- Inability to recover critical information asset in the event of data lost or disaster

- Theft/vandalisation of critical information assets due to inappropriate physical security mechanism

- Risks related to natural disaster leading to system unavailability and the inability to continue to operate due to lack of disaster recovery/business continuity plan

- Disruption to critical information system, leading to downtime as a result of Security incident (e.g. Denial of service) or as a result of unauthorized modification to system configuration settings

WHAT IS USUALLY CONTAINED IN A RISK REGISTER

A risk register is a document that contains the details of all identified risks within our environment. An IT Risk register usually contain the following information:

- Risk ID

- Risk Title

- Risk Description

- Risk Owner

- Associated Threats to the Risks

- The Assets that the risks impacts

- The vulnerabilities that exists within our environment given a pass for the risk

- Risk Type (e.g., System, environmental, political, etc)

- What aspect of CIA does the risk impact (i.e. Confidentiality, Integrity, Availability and Privacy

- Risk Treatment/Response (i.e. weather to mitigate, accept, transfer, or avoid)

WHAT WOULD WARRANT AN ORGANIZATION TO ACCEPT A RISK?

Although Risk Acceptance is a Risk Response methodology in itself, but when we treat a risk by putting in place a control or countermeasure, we are also doing this to reduce the risk impact to an acceptable level for the organization.

Risk acceptance is a risk treatment plan where an organization is willing to accept the consequences of a risk impact on their assets. Oftentimes, if the risk impact is within an Acceptable threshold for an organization, or within the Risk Tolerance Limit, then the organization may decide to accept the risk.

Alternatively, an organization may choose to accept a risk to an asset if the cost of implementing a control / safeguards to protect the asset is more than the value of the asset being protected.

WALK ME THROUGH YOUR APPROACH FOR PERFORMING AN END-TO-END IT AUDIT REVIEWS AS AN EXTERNAL AUDITOR

Auditing an information system requires relevant know-how, especially when it comes to minimizing detection risk which is associated with the audit itself.

As an IT Auditor, I have supported several audit reviews and led engagements either for FAIT, SOX, or Security Audits and assessments, where we evaluate controls that have been implemented to:

- address key objectives,
- protect information assets,
- Adhere to management and regulatory standards; and
- Mitigate risks of fraud, error in transaction processing or risk of financial misstatements

My end-to-end approach to auditing IT environment starts with:

1. Planning the engagement: During the planning phase, I seek to understand the client and their nature of business, and I will also seek more understanding on the scope of work, and to understand the extent of IT audit reviews.

Moreso, I will put my team together, create the team budget and create the audit workplan and task allocation document.

I will also get the engagement file open for us to organize our document. Also in this phase, I will reach out to the client contact (e.g. Head of IT) to introduce myself, understand the scope of review and plan the audit walkthrough meetings. I will also send the information request to the client contact ahead of us moving to client site for audit walkthrough

I will ensure to communicate to the client that the audit is an improvement exercise and this particular one should be seen as such. This helps the client to understand that we are helping them to improve on their controls and not trying to spot out their inefficiencies

2. Secondly, I will initiate the execution phase for us to begin with our walkthrough reviews. In this phase of the audit, I will start by **understanding the IT Environment**. This will enable us to have an understanding of their processes, tools and technologies, and their people. To understand the environment, I will review the:

i. the organogram to understand the IT organization and its people, and roles and responsibilities within the IT team;

ii. the IT Strategy against the business strategy to evaluate if the IT strategic intent are position to support the Business.

iii. the IT policies and benchmark it for adequacy against the COBIT 5 framework for governance and management of IT

iv. I will check how IT is being governed and directed by asking if there is an existence of IT Steering Committee; and lastly,

V. The key IT applications and systems that support business processes

The next activity is to test the controls that have been implemented to protect the information asset. I will test the design and implementation of these controls, and also test the operating effectiveness for the controls as well. Specifically, I will test the following controls:

1. The ENTITY LEVEL CONTROLS (ECL) vis-a-vis the review of Monitoring controls such as presence of internal IT Audit processes, and the Risk management control by evaluating the presence of a management approved process for evaluating IT Risks.

2. Subsequently, I will test the IT GENERAL CONTROLS (ITGC) by review the process and measures that have been implemented to achieve certain control objectives particularly for:

a. Access Management to critical Information Assets within the IT environment

b. Program Changes and Program Development (i.e. Change management process)

c. Operations Management to critical IT infrastructure and assets

3. I will test the relevant IT Applications Controls (ITACs) provided the ITACs are in scope. An example could be

to test:

a. the interface between two critical systems

b. Input Validation controls on an application

c. Maker-checker for critical process that requires 4-eye control or approvals

d. Configuration for calculated measures such as Interest

When testing the ITACs, I will also ensure to test if the ITACs are configurable i.e., if the configuration for the application control can be changed or altered from the frontend or the menu options without going through appropriate change management process

While performing the audit walkthrough review, I will collate the evidence, and document my findings and test results accordingly in the audit workpaper or audit documentation tool. I will ensure that these workpapers are review by my superior and address whatever comments they may have

3. Lastly, I will note and highlight the deficiencies noted during my walkthrough exercise in the audit report. Prior to sending the final report, I will send my report to my superior for review and also schedule a call with the Head of IT to discuss and agree on my findings. In this meeting. I will ensure that I have clear rationale and sufficient evidence for all the audit findings.

Once we agree on the audit findings, I will prepare my final audit report using Microsoft Word or PowerPoint and send the draft to the audit client contact for the senior management to provide their response to all the audit findings. This is the process I always follow for auditing client information system end-to-end

WALK ME THROUGH YOUR APPROACH FOR PERFORMING AN END-TO-END IT AUDIT REVIEWS AS AN INTERNAL AUDITOR

Auditing an information system requires relevant know-how, especially when it comes to minimizing detection risk which is associated with the audit itself.

As an IT Auditor, I have supported and coordinated several audit programmes and reviews as an internal auditor. Specifically, I have supported SOX reviews, Internal Security Audits and assessments, and collaborated with external auditors on joint audit testing where we evaluated controls that have been implemented to:

- address management objectives and protect information assets,

- Reduce risks related to weakness in internal control,

- Adhere to management and regulatory standards; and

- Mitigate risks of fraud, error in transaction processing or risk of financial misstatements

My end-to-end approach to auditing IT environment starts with:

1. Planning the engagement: During the planning phase, I will highlight the scope of the internal audit review and liaise with key stakeholders and relevant control operators across business units and functions to agree on a timeline for walkthrough meetings.

Moreso, I will create the audit workplan and task allocation document which will be used to delegate tasks to my colleagues.

Afterwards, I will:

- get the engagement file open for us to organize our documents for the audit program,

- reach out to the Head of IT,

- send out communication about the audit reviews to all the stakeholder, and

- send the information request to the appropriate personnel within the business.

2. Secondly, I will initiate the execution phase for us to begin with our walkthrough reviews. In this phase of the audit, I

will start by understanding the IT environment processes, tools and technologies, and their people. To support my understanding. I will review the:

i. the IT Strategy against the business strategy to evaluate if the IT strategic intent are position to support the business

ii. the IT policies and benchmark it for adequacy against the COBIT 5 framework for governance and management of IT

iii. I will check how IT is being governed and directed by asking if there is an existence of IT Steering Committee; and lastly,

iv. The key IT applications and systems that support business processes

The next activity is to test the controls that have been implemented to protect the information asset. I will test the design and implementation of these controls, and also test the operating effectiveness for the controls as well. Specifically, I will test the following controls:

D. The ENTITY LEVEL CONTROLS (ECL) vis-a-vis the review of Monitoring controls such as presence of internal IT Audit processes, and the Risk management control by evaluating the presence of a management approved process for evaluating IT Risks.

E. Subsequently, I will test the IT GENERAL CONTROLS (ITGC) by review the process and measures that have been implemented to achieve certain control objectives particularly for:

a. Access Management to critical Information Assets within the IT environment

b. Program Changes and Program Development (i.e. Change management process)

c. Operations Management to critical IT infrastructure and assets

F. I will test the relevant IT Applications Controls (ITACs). An example could be to test:

a. the interface between two critical systems

b. Input Validation controls on an application

c. Maker-checker for critical process that requires 4-eye control or approvals

d. Configuration for calculated measures such as Interest

When testing the ITACs, I will also ensure to test if the ITACs are configurable i.e., if the configuration for the application control can be changed or altered from the frontend or the menu options without going through appropriate change management process

While performing the audit walkthrough review, I will collate the evidence, and document my findings and test results accordingly in the audit workpaper or audit documentation tool. I will ensure that these workpapers are review by my superior and address whatever comments they may have

3. Lastly, I will note and highlight the deficiencies noted during my walkthrough exercise in the audit report. I will share my report to my superior for review and also schedule a call with the Head of IT to discuss and agree on my findings. In this meeting, I will ensure that I have clear rationale and sufficient evidence for all the audit findings.

Once we agree on the audit findings, I will prepare my final audit report using Microsoft Word or PowerPoint and send the draft to the audit committee and Risk Management function.

I will obtain the responses of the control owners on the finding and will initiate a follow-up process for control remediation.

This is the process I always follow for auditing an information system as an Internal IT Auditor

WHAT DO YOU CONSIDER WHEN SCOPING AND PLANNING FOR AN IT AUDIT ENGAGEMENT OR REVIEW?

Planning an engagement involves understanding the client and the scope of work. I have led IT Audit reviews and programs both as an internal audit and external auditor. When I am planning an engagement, I start by

1. Understanding the nature of the business and the client

2. Identify and liaise with the Stakeholders to align initiatives and agenda for the audit

3. Understand and agree on the scope of work with the stakeholders

4. Put together a team of IT Audit specialists with specific skillsets that is required for the audit

5. Create the workplan and task schedule which will be used to evaluate the time required for the work to be performed and also to assign responsibilities to the team

6. Create the team's budget and agree on fees and timeline as well

7. Lastly, communicate the information request to the stakeholders ahead of the audit walkthrough testing / the execution phase.

I will also set up a channel for providing progress and status of work to the senior management and stakeholders as the audit progresses, and a channel for escalating difficulties that stalls the progress of the audit reviews.

This is how I plan IT Audit reviews and engagement

WHAT IS YOUR EXPERIENCE TESTING ITGC, TELL ME ABOUT A TIME YOU TESTED ITGC AND WHAT WERE THE AREAS YOU FOCUSED ON?

I have experience with tests IT GENERAL CONTROLS (ITGCs) by reviewing the process and measures that have been implemented to achieve certain control objectives particularly for:

• Access to programs and data i.e., Access Management to critical Information Assets within the IT environment

• Program Changes and Program Development (i.e., Change management process)

• Operations Management to critical IT infrastructure and assets

For access to programs and data, the control objective is to ensure that the entity has appropriately implemented controls to restrict access to only the authorized individuals, thereby protecting information assets from unauthorized access. To ascertain this control objectives is met, I will test the following controls:

• Existence of management approved information security policies and procedures, and benchmark the policies against relevant domains of ISO 27001 for adequacy. I will also check that the users and employees are aware of the policy and that there is an established process for communicating the policies to the users.

• Ascertain the Access administration process particularly User access provisioning and de-provisioning. This is to test how the organization manages access for JOINER, and MOVERS and how they terminate access to LEAVERS from the organization. I will review one sample to test the design and implementation of this control, and also select samples from the total population of joiners, movers and leavers using the approved sample size guidance to test the Operating effectiveness of the control respectively.

• Review the User Identification and Authentication process to evaluate that the entity has implemented a process to ensure every user on the system is identifiable, and that their generic accounts are used, the secret authentication of such accounts is restricted to only the IT administrators. Also, I will check the authentication mechanism that has been deployed and ascertain that users log into IT systems using a combination of their UNIQUE IDENTITY and their associated AUTHENTICATION MECHANISM (e.g. passwords or using multifactor authentication). Similarly, I will select one sample to test the design and implementation of this control, and also select multiple samples from the **list of users** within the organization based on my sample size guidance to test my operating effectiveness.

• Review the Super Users/Administrative Users for appropriateness by checking that there is a management approved policy for managing super users, and that access to privileged administrative rights/ permission is restricted to appropriate personnel within the organization. I will also check that the activities of users with admin privileges are logged, and the logs are not modifiable by anyone.

• Evaluate the Physical access controls that have been implemented to protect facilities and data centres that houses critical applications, systems and information assets. I will review the management approved policies and procedures, and ascertain the presence of physical security devices that have been deployed to protect information assets. I will test the design and also test the operating effectiveness of the physical access controls.

• Ascertain the existence of management approved processes for performing period user access reviews to determine users with unauthorized access on critical systems. I will access the practice for User Access Reviews (UAR) to determine if it aligns with the management approved procedure, and I will also select a sample for the UAR that was performed during the period under review to test the

design of the control. Depending on the population, and my sample size guidance, I will select more samples to test the operating effectiveness of this controls

• I will evaluate that appropriate monitoring controls have been implemented at the network layer to monitor and control access to the system.

For **Program Changes i.e. change management**, the control objective is to ensure that all changes to critical information assets are requested, authorized, tested, and approved prior to production deployment. To ascertain if these control objectives are met, I will test that there is an existing change management policy/procedure that has been approved by the senior management. I will ascertain that the policy document covers steps for follow for:

- Requesting for a change through a change request form or change request ticket

Approvals to obtain prior to change being considered for development e.g. Change Advisory Board (CAB) approval Ensuring that the change is adequately tested by the business process owner who requested for it. Evidence of testing should be documented

- Approvals are obtained for the changed to be released to production systems

- Change releases to production environments.

Subsequently, I will pick one sample of change that was released to the product environment during the period under review and review the management-approved change policy. I will check that the change was requested, tested and approved for production release accordingly.

Depending on the population, and my sample size guidance, I will select more samples to test the operating effectiveness of this controls

For Program Development, I will ascertain that appropriate

For Operations Management the control objective is to ascertain that appropriate measures have been implemented to ensure IT Systems continues to be available to the business in the event of adversities. To ascertain that controls have been implemented to meet this objective, I will review the following:

• Incident management process

• Backup and Recovery Process

• Job Processing

• Antivirus/ Anti-malware

• Service Level Management

• Disaster Recovery and Business Continuity

For each of these controls, I will ascertain the existence of management-approved policies and procedures, and also check if the controls are operated in accordance and alignment with the approved policies and procedures. For each control, I will select a sample to test the design and implementation of the control. Depending on the population for each of the controls, and my sample size guidance, I will select more samples to test the operating effectiveness of these controls.

HOW DO YOU AUDIT ACTIVE DIRECTORY

Active Directory (AD) is used to manage access and authentication to critical information assets within an enterprise. It uses LDAP (lightweight directory access protocol) and the AD is used for managing

users and computers on a corporate network for accessing information that is kept within the internal network of the organization.

Being a system that provides critical function within an enterprise architecture, it is important to evaluate that appropriately controls have been implemented around the AD itself.

In my previous roles, I have evaluated Microsoft AD multiple times as part of IT Audit reviews. Specifically, when I am reviewing the IT controls around the active directory system, I focus on Access management and the general system security settings for the AD server.

Specifically, I start by reviewing the:

1. User access administration to ascertain how users are being added, modified or deleted on the AD. I will review the user list on the Active Directory and compare it with the HR list to ascertain that all the users on the AD are legitimate employees and their access on the AD is appropriate.

Also, I will check the list of Terminated employees from the HR list to ascertain that there are no terminated users with active access on the AD list.

2. I will review the list of Domain Admins (i.e. administrators) on the AD to ascertain the adequacies and appropriateness of the users with domain administrative privilege.

3. I will ascertain that default AD accounts i.e. the Guest Account and the default Administrator accounts are disabled. Also ensure that password to the default administrator account is restricted to the IT team only admins.

4. I will ascertain that users on the Active Directory are identified with their unique user IDs and are required to authenticate to the AD using their password or a combination of authentication mechanism (multi factor authentication)

5. I will ascertain the password complexity settings on the active directory system conforms with best practices, and the management approved password security settings.

6. I will also check if logging has been turned on for failed and successful loggings in line with the logging and monitoring procedure.

7. Lastly, I will ascertain that the process for patching the AD server OS follows the appropriate change management policy or the patch management policy depending on what is obtainable.

In all of this review, I will ascertain the design by comparing what is in practice with the management approved policies and procedures. I will select samples from the population to test my operating effectiveness.

GIVEN AN ACCESS MANAGEMENT CONTROL OBJECTIVES, WHAT CONTROLS WOULD YOU TEST TO ASCERTAIN THAT ACCESS MANAGEMENT IS APPROPRIATE WITHIN AN ORGANIZATION?

For access to programs and data, the control objective is to ensure that the entity has appropriately implemented controls to restrict access to only the authorized individuals, thereby protecting information assets from unauthorized access. To ascertain this control objectives is met, I will test the following controls:

- Existence of management approved information security policies and procedures, and benchmark the policies against relevant domains of ISO 27001 for adequacy. I will also check that the users and employees are aware of the policy and that there is an established process for communicating the policies to the users.

- Ascertain the Access administration process particularly User access provisioning and de-provisioning. This is to test how the organization manages access for JOINER, and MOVERS and how they terminate access to LEAVERS from the organization. I will review one sample to test the design and implementation of this control, and also select samples from the total population of joiners, movers and leavers using the approved sample size guidance to test the Operating effectiveness of the control respectively.

- Review the User Identification and Authentication process to evaluate that the entity has implemented a process to ensure every user on the system is identifiable, and that their generic accounts are used, the secret authentication of such accounts is restricted to only the IT administrators. Also I will check the authentication mechanism that has been deployed and ascertain that users log into IT systems using a combination of their UNIQUE IDENTITY and their deployed and ascertain that users log into IT systems using a combination of their UNIQUE IDENTITY and their associated AUTHENTICATION MECHANISM (e.g. passwords or using multifactor authentication). Similarly, I will select one sample to test the design and implementation of this control, and also select multiple samples from the list of users within the organization based on my sample size guidance to test my operating effectiveness.

- Review the Super Users/Administrative Users for appropriateness by checking that there is a management approved policy for managing super users, and that access to privileged administrative rights/ permission is restricted to appropriate personnel within the organization. I will also check that the activities of users with admin privileges are logged, and the logs are not modifiable by anyone.

- Evaluate the Physical access controls that have been implemented to protect facilities and data centers that houses critical applications, systems and information assets. I will review the management approved policies and procedures. and ascertain the presence of physical security devices that have been deployed to protect information assets. I will test the design and also test the operating effectiveness of the physical access controls.

- Ascertain the existence of management approved processes for performing period user access reviews to determine users with unauthorized access on critical systems. I will access the practice for User Access Reviews (UAR) to determine if it aligns with the management approved procedure, and I will also select a sample for the UAR that was performed during the period under review to test the design of the control. Depending on the population, and my sample size guidance, I will select more samples to test the operating effectiveness of this controls

- I will evaluate that appropriate monitoring controls have been implemented at the network layer to monitor and control access to the system.

TO ASCERTAIN THE ADEQUACY OF A CHANGE MANAGEMENT PROCESS WITHIN AN ORGANIZATION, WHAT CONTROLS WOULD YOU TEST, AND HOW WOULD YOU TEST THESE CONTROLS.?

For Program Changes i.e. change management, the control objective is to ensure that all changes to critical information assets are requested, authorized, tested, and approved prior to production deployment. To ascertain if these control objectives are met, I will test that there is an existing change management policy/procedure that has been approved by the senior management. I will ascertain that the policy document covers steps for follow for:

- Requesting for a change through a change request form or change request ticket

- Approvals to obtain prior to change being considered for development e.g., Change Advisory Board (CAB) approval

- Ensuring that the change is adequately tested by the business process owner who requested for it. Evidence of testing should be documented

- Approvals are obtained for the changed to be released to production systems

- Change releases to production environments.

Subsequently. I will pick one sample of change that was released to the product environment during the period under review and review the management-approved change policy. I will check that the change was requested, tested and approved for production release accordingly.

Depending on the population, and my sample size guidance, I will select more samples to test the operating effectiveness of this controls

For **Program Development**, I will ascertain that appropriate

TO ASCERTAIN THE EFFECTIVENESS OF IT OPERATIONAL PROCESSES / IT OPERATIONS MANAGEMENT PROCESS WITHIN AN ORGANIZATION, WHAT CONTROLS WOULD YOU TEST, AND HOW WOULD YOU TEST THESE CONTROLS.?

For Operations Management the control objective is to ascertain that appropriate measures have been implemented to ensure IT Systems continues to be available to the business in the event of adversities. To ascertain that controls have been implemented to meet this objective, I will review the following:

- Incident management process
- Backup and Recovery
- Process Job Processing
- Antivirus / Anti-malware
- Service Level Management
- Disaster Recovery and Business Continuity

For each of these controls, I will ascertain the existence of management-approved policies and procedures, and also check if the controls are operated in accordance and alignment with the approved policies and procedures. For each control, I will select a sample to test the design and implementation of the control. Depending on the population for each of the controls, and my sample size guidance, I will select more samples to test the operating effectiveness of these controls.

WHAT APPROACH WOULD YOU FOLLOW TO TEST A CONTROL TO DETERMINE WHETHER IT'S EFFECTIVE OR NOT? GIVE ME AN EXAMPLE OF CONTROLS YOU'VE TESTED IN THE PAST AND HOW YOU WERE ABLE TO TEST THE CONTROLS

To make correct judgment and conclude on control effectiveness, one needs to ensure an appropriate testing approach is applied when reviewing the control.

When I am required to test controls, I start by understanding the control objectives (e.g. Access management controls, which have the objective of restricting access to only authorized personnel).

Once I know the control objective, and the individual controls to test, I focus on developing my testing approach to evaluate the design and implementation of these controls. To evaluate the Design and Implementation of the control, my first approach will be to ascertain the existence of management-approved policies and procedures.

Secondly, I will inquire from the relevant control operator of the processes that are being followed in practice for executing the control. I will ascertain that the process in practice aligns with the management-approved policies and procedures. In addition, I will select ONE sample to test that the practice in place for executing the control is in line with the policies as approved by the senior management.

Lastly, depending on the total population for this control, and my sample size guidance, I will select more samples to test the operating effectiveness of the control.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE DESIGN AND OPERATING EFFECTIVENESS OF A PASSWORD SECURITY CONTROL DURING AN AUDIT?

Every time that I have tested effectiveness of a password security controls on critical IT systems, applications and the Active Directory, I usually follow this approach:

- firstly, I verify the existence of a management-approved password policy and check the standard password security settings that are documented in the information security policy:
- Then I obtain a screenshot of the password security settings from all the systems in scope including Active Directory and all key business applications.
- I then Benchmark the password security settings in the Information security policy, against best practice settings.
- Lastly, I also Benchmark the password security settings on the key IT applications and Active Directory against the Standard in the policy and also against the best practices

Once I am done testing. I will document my findings on the test of design and effective on the password security control in the audit workpaper

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE DESIGN AND OPERATING EFFECTIVENESS OF A USER IDENTIFICATION AND AUTHENTICATION CONTROL DURING AN AUDIT?

Every time that I have tested the design and operating effectiveness of User Identification and Authentication controls within an IT control environment, I usually follow this approach:

→ Firstly I check for the existence of a management-approved policy on user identification and authentication. I will also check the Information security policy to ascertain that it contains requirements for ensuring user identification on the Active Directory and also on the business

applications. This means that every user on the system must have unique identifiable accounts on the system.

→ I then check that the Information Security Policy (i.e. through password policy) talks about the system authentication and also specifies the standard password security settings that should be applied to all systems within the organization

→ I also discuss with the client contact during the walkthrough meeting to obtain details of the process being followed through an inquiry.

→ To test the design, I select a user at random and I Observe the user log into the system using their unique user ID and password to log in. I ensure to record this observation as my evidence of testing the design. Subsequently, I will obtain the user list of the systems in scope of the audit. These systems may include;

◆ The Active Directory

◆ All the Business Applications in scope of the audit

◆ Operating system that supports that application

◆ The database that supports the application

→ When obtaining the user list, I ensure that the list being provided is complete and accurate. To verify completeness and accuracy, I usually request for evidence of how the spool was generated for you to ensure that the spool or information being provided to me has not been tampered with, and that it is complete and accurate

→ Once I verify the completeness and accuracy of the system user list, I then check the list of users on the system to see if there are generic/ system accounts, or duplicate accounts. Generic accounts are accounts that are not easily attributed to employees/ individuals within the organization.

Once I have obtained all this information, I will review and document my findings on the test of design and test of operating effectiveness on the control in the audit workpaper.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE DESIGN AND EFFECTIVENESS OF AN APPROPRIATE SEGREGATION OF DUTIES WITHIN A CONTROL ENVIRONMENT.

When I am to test the design and operating effectiveness of a Segregation of Duties Matrix within an IT control environment, I usually follow this approach:

- ✓ Firstly, I ascertain the existence of management approved Segregation of Duties (SOD) Matrix, and a guidance or policy document that specifies how privileges should be assigned to users within the organizations.
- ✓ If the Matrix is not in existence, I obtain the system generate list of permissions and privileges on the system including the description of all the privileges and the permissions
- ✓ I then request for the list of users on all the key IT applications in scope including a field/ column that shows their associated privileges, and review if the assignment is appropriate
- ✓ Lastly, I will obtain a list of all employees from the HR team to cross check the user list with the system generated list of users with their access rights. This is to verify that a user on the system has been given the appropriate privilege in line with their job function as noted on the HR list.

Once I have obtained all this information, I will review and document my findings on the test of design and test of operating effectiveness on the control in the audit workpaper.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A USER ACCESS ADMINISTRATION OR JOINERS, MOVERS AND LEAVERS CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Joiners, Movers and Leavers process or User provisioning, modification and de-provisioning process within an IT control environment, I usually follow this approach:

Firstly, I verify the existence of a management-approved policies and procedure document that details the process for creating, modifying and deleting users on critical IT systems. In addition, I discuss with relevant personnel to obtain details **on the practice** in place for provisioning, modifying and de-provisioning user access on the system.

For User Profile Creation (i.e. Joiners)

I obtain an understanding of the process involved in creating a user on all the key IT applications. i.e. from the moment an employee joins the firms:

- Who provisions IT systems and resource for the new user,

- Who communicates to the IT team to create the new user,

- Who authorizes and approve the creation of the new user, and

- Who approves what privileges should be given to the new user.

For User Profile Modification

I obtain an understanding of the process involved in modifying a user on all the key IT applications. i.e. from the moment a user moves from one department to the other:

- How is the IT team notified about a user that moved from one department to another,

- Who modifies the permission that the user currently has on the system

- What process is followed to modify a system user (i.e. do you remove all old access first before granting new access)

- Who authorizes and approve the modification of system access for the user

-Who approves what privileges should be given to the modifying user.

For User Profile Deletion

I discuss with relevant personnel (i.e. including HR and IT team) to understand the process involved in deleting a user on all the key IT applications. i.e. from the moment a user indicates the intention to leave the organization:

- How is the IT team notified about a user that leaving the firm,

- How are IT assets recovered from the user that is leaving the firm

- What is the process for deleting or disabling users on the system

- Who deletes or disables the user on all the system

- How quickly is the user account deleted or disabled from the system

- Who authorizes and approves the deletion of the user.

Once I obtain the policy and detailed understanding. I will take one sample each from the joiners list, movers list and the leavers list for my test of design. Depending on the total population for this control, and my sample size guidance, I will select more samples to test the operating effectiveness of the control.

I will then document my work papers and present it for review. This is how I always test the design and operating effectiveness of JML.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A USER ACCESS REVIEWS CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the User Access Review control/ process within an IT control environment, I usually follow this approach:

Firstly, I verify the existence of a management-approved policies and procedure document that details the process for periodically reviewing user access rights on critical IT systems. In addition, I discuss with relevant personnel to obtain details on the practice in place for performing user access rights reviews on the IT system. I also ascertain the frequency that is documented in the procedure or policy document, to verify that the practice in place for user access review is in line with the documented frequency in the policy

Subsequently, I usually obtain evidence to show that the users' access rights on critical applications were reviewed during the period under review and in line with the approved procedure. To verify that the User Access review was performed, I normally would request for the following documents:

• List of users from the key applications that was generated at the time of the UAR review

• Emails that were sent to the verifiers (i.e. the people that will verify whether the access rights of a user was appropriate or not, usually their line managers)

• Responses of the line managers to the email that was sent to them to confirm the access rights of their direct report users.

• if any user access rights were requested to be modified by the Line Manage (i.e. maybe the user no longer requires that access rights), evidence to show that the IT team effectively actioned the request during the UAR review. I will check the system for the affected user's access rights to ensure that the change to access rights have been done.

I will also ascertain the coordination of the UAR reviews and review other relevant evidence to it. Once I obtain the evidence, I will take one UAR sample for my test of design. Depending on the total population for this control, and my sample size guidance, I will select more samples to test the operating effectiveness of the control.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A PRIVILEGED/ ADMINISTRATIVE ACCESS REVIEW CONTROL OR SUPER USER CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Privilege Access / Super User process within an IT control environment, I usually follow this approach:

Firstly, I verify the existence of a management-approved policies and procedure document that details the process for managing, assigning and reviewing the activity of super users/ admin users on all IT

systems. In addition I discuss with relevant personnel to obtain details on the practice in place for managing and assigning privilege access rights on the system

I will obtain the list of super users/ administrators on all key IT applications that are in scope. When receiving the list, ensure that you verify the completeness and accuracy of the information that is being provided by requesting the evidence of how the information provided to you was generated.

I also ensure that the super user privileges or the administrative privileges have been restricted to appropriate personnel only (ie., leads within the IT team)

I will inquire from the head of IT if the activities of the Administrators/ super users are logged on the system. In addition, I will obtain evidence to ascertain that the activities of the super users are logged on the system and that the audit trail is turned on for critical IT systems, and no one has the ability to modify / change the configuration settings of the audit log.

If anyone has the capability to turn on or off the audit trail, I will ascertain if the log turns on or off are also logged separately.

More so, I will Ascertain that the logs are not modifiable by anyone on the system, and that no one have the ability to delete this log on the system. also verify the repository where the log is being stored and how long are the logs retained for before disposal

Lastly, I will ascertain that there is a process in place whereby the logs of the activities of the super users/ administrative user are reviewed periodically. e.g. maybe the internal control team reviews the log monthly or quarterly for appropriateness. I will check the frequency of review and also ascertain that the log was reviewed ones for test of design during the period under review

Once I obtain the evidence, I will take one sample for my test of design. Depending on the total population for this control, and my sample size guidance, I will select more samples to test the operating effectiveness of the control.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A CHANGE MANAGEMENT CONTROL OR PROGRAM CHANGES CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the change management process within an IT control environment, I usually follow this approach:

Firstly, I verify the existence of a management-approved policies and procedure document that details the process for managing changes to production systems within the organization. In addition, I discuss with relevant personnel to obtain details on the practice in place for managing change requests, testing and approving changes prior to production deployment. This discussion will cover all types of changes whether Standard, Normal or Emergency changes. I will also inquire if the change management process is being supported by any helpdesk tool such as ServiceNow, Jira, Remedy or even Excel.

More so, I usually check to see that the server environment has been appropriately segregated into DEVELOPMENT, QA and PRODUCTION environments

I then request for the list of all the changes that were made to the in-scope applications during the period under review. I will ensure that the list of changes provided to me is complete and accurate by inspecting the process for generating the list, or asking for evidence to prove that the list is complete and accurate.

To test the design and implementation of this process, I will select one sample from the changes that we migrated to production during the audit period. I will check that the change followed the management approved procedure document to ensure that the change was:

- requested by an appropriate individual

- approved by the appropriate person/team/ CAB

- Change was Tested by the business user in QA and approved

- Change was released to production environment

Depending on the total population for this control, and my sample size guidance, I will select more samples to test the operating effectiveness of the control.

Lastly, I will ascertain that no code changes or modification is allowed on the production/ Live environment by reviewing the list of users with access to the Product server to ensure that no System Developer/ programmer is given access on the product system.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW THE PROCESS FOLLOWED FOR AN IMPLEMENTATION OF A NEW SYSTEM OR A NEW ACQUISITION DURING AN AUDIT PERIOD (NT THIS IS PROGRAM DEVELOPMENT CONTROL)

When I am required to test the design and operating effectiveness of the program development controls within an IT control environment, I usually follow this approach:

Firstly, I review the SDLC policy and ensure that it has been approved by the management. I also ensure it covers processes for:

• Initiating and authorizing system projects

• Assigning priorities to projects (i.e. project plan)

• Developing requirements and specifications

• Testing applications

• Business user testing and formal sign-off

• Migration from the test environment to the production environment

• Reconciliation of data migrated and sign-offs

In addition, I will also discuss with the appropriate personnel or the Head of IT to understand the practice for managing system implementation or new acquisition within the IT control environment.

Subsequently, I will inspect the PMO related documents for the system that was implemented or acquired during the audit period to ensure that:

- there was an approach, and that the stakeholders were engaged,

- the project was planned and the deliverables for planning were reviewed and signed.

- the requirements were gathered appropriately and documented,

- the system was tested efficiently and test defects were logged,

- that the solution was deployed and there was post implementation support to address issues after go-live

If the System Implementation/ new acquisition involved a Data migration

I will ascertain the existence of the data migration strategy and that it has been approved by management, and a guidance or policy document that specifies how privileges should be assigned to users within the organizations.

I will also review relevant documentation (e.g., migration plan, minutes of meeting, or emails) to show that during the migration process, the data migration team discussed key details prior to the migration

I will ascertain the process used for migrating the data. Ensure that the ETL (Extraction, Transformation and Load) process was documented, reviewed and agreed by the team

I will Check for the existence of a staging area and ensure that Trial uploads were performed. Furthermore, I will ascertain that during the trial uploads, the team performed reconciliations to ensure completeness, accuracy and validity of the data being migrated

I will check that prior to the actual migration, there was a cutover activity that was performed and confirmed also that there was a roll back plan in the event that the migration fails

Lastly, I will perform substantive testing by doing a reconciliation of the migrated data to ensure that the data migrated completely, and that the migrated data is accurate and valid

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A BACKUP AND RECOVERY CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Backup and Recovery within an IT control environment, I usually follow this approach:

Firstly, I ascertain the existence of a management-approved policy document and obtain the policy for backup and recovery. I will also Discuss with the head of IT to determine the process involved in performing backups, the approach, the tools, and the timing.

During your discussion with the head of IT, ensure to cover the following:

- Identification of critical systems/applications data to be backed up

- Frequency and nature of backup activities

- Recycling procedures for backup media

- Frequency and nature of restore activities.

- Personnel responsible for backup and test recovery

- Personnel responsible for reviewing backup and recovery register

- Identification of on-site and off-site storage locations.

I will also ascertain that if a Backup fails to run, there is a process to monitor and alert the IT System Administrator Control Operator. Check the backup management tool to ascertain that the backups for the application in the scope of your audit were performed during the audit period.

To test the TOE, I will ascertain the frequency of backups from the management-approved policy document, and obtain a spool of backup tickets from the backup scheduling tool, showing the system title, backup description, reporter, date, Status and time taken to complete. Randomly select samples based on the total population of backups and test similarly to the testing you perform with TOD

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF AN INCIDENCE MANAGEMENT CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Incident management control within an IT environment, I usually follow this approach:

Firstly, I verify the existence of a management-approved policies and procedure document for incident management. In addition, I discuss with relevant personnel to obtain details on the practice, tools and techniques in place for managing incidents.

To test the design, I will select ONE sample of IT incidents that were reported during the audit period to ascertain if the incident was handled and resolved in line with the management-approved procedure

To test the Operating Effective, I will obtain a spool of incident tickets from the IT ServiceDesk/ Helpdesk tool, showing the incident title, description, reporter, date reported, status, rating and priority. Randomly select samples from the list of incidents provided and test similarly to the testing you perform with TOD

I will then check to see if IT incidents are collated and reviewed by the Senior IT management, and inquire from the Head of IT if incidents are communicated to the senior management, and are included in the enterprise incident management process.

I will obtain evidence to show that the IT incident report was communicated at least once to the senior management during the period under review

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A JOB PROCESSING CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Job Processing control within an IT environment, I usually follow this approach:

Firstly, I ascertain the existence of a policy document and obtain the policy for scheduling jobs / automating repetitive tasks within the systems that are critical and in-scope for the audit. I then Discuss with the head of IT to determine the process involved in performing/scheduling jobs. Inquire about the tool and techniques being used.

I will also ensure that **access to modify the configuration of automated jobs** is restricted to authorized personnel only.

Through inquiry, observation, or evidence, I will ascertain that there is a **process for monitoring automated jobs statuses** i.e., especially in the event of failure, thereby asking who is responsible for receiving alerts when a system job fails to run?

To test the design, I will verify that at least **one job was performed** in line with the management **approved policy**. I will also verify that the job ran successfully at least once during the period under review

More so, I will **ascertain the adequacy of personnel with access** to modify the configuration settings of the job

If available, I will obtain at least **one sample alert** that was sent to the control operator on a day when the job failed to run

For the TOE testing, I will obtain the total population showing date, timing, frequency and status (i.e., failed or successful) and select samples from the list of scheduled jobs that are critical to the audit. Where jobs failed to run, I will obtain details showing that an alert was sent to appropriate personnel.

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF A DISASTER RECOVERY AND BUSINESS CONTINUITY CONTROL DURING AN AUDIT

When I am required to test the design and operating effectiveness of the Disaster Recovery and Business Continuity control within an IT environment, I usually follow this approach:

Firstly, I ascertain the existence of a policy and procedure document or a plan document for Disaster recovery planning and Business Continuity. I will also Discuss with the head of IT to determine the process involved in disaster recovery management, the approach, the tools, plan, and the DR facility type.

I will review the Disaster Recovery plan to ascertain that in covers:

(a) Identification of critical IT assets.

(b) Business impact analysis / Risk assessment.

(c) Recovery of critical assets.

(d) Key contacts in the event of a disaster.

More so, I will verify that a key contact in the plan is aware of his/her role in the event of a disaster.

I will ascertain if the DR processes were tested in line with the management-approved procedure, and obtain at ONE DR testing report and ascertain that the appropriate process was followed.

For testing the operating effectiveness based on the management-approved standard, ascertain the frequency of disaster recovery testing that is specified in the management-approved standard. Obtain the total population based on this frequency (i.e. If the policy says to test every quarter, then the total population will be 4) and select your samples to review for TOE

WALK ME THROUGH THE PROCESS YOU WOULD FOLLOW TO REVIEW / TEST THE EFFECTIVENESS OF AN ANTIVIRUS CONTROL DURING AN AUDIT.

When I am required to test the design and operating effectiveness of the Antivirus control within an IT environment, I usually follow this approach:

Firstly, I will ascertain the existence of a policy / procedure document and obtain the policy/procedure for Antivirus Management and security monitoring. Discuss with the head of IT to determine the process involved in managing security incidents (such as Virus, malware, worms, and ransomware), the approach, the tools, and techniques used within the organization.

Ascertain that the critical applications in scope including the Operating System and databases are covered as part of the security monitoring process within the organization.

I will also obtain evidence to show that all the critical IT systems (including the Active Directory, servers and operating systems) are covered in the security monitoring process. To do this, I will verify that the Anti-virus tool is implemented on at least ONE critical system within the scope of your audit.

For testing the operating effectiveness Verify the number of workstations within the organization by asking for a spool of computers that are added to the Active Directory. Depending on the number of systems and workstations within the organization, randomly select samples of critical systems and ascertain that there is an antivirus tool configured on these systems.