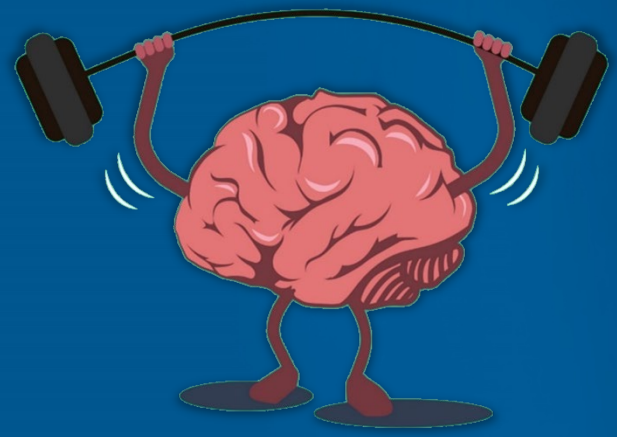
KPMG

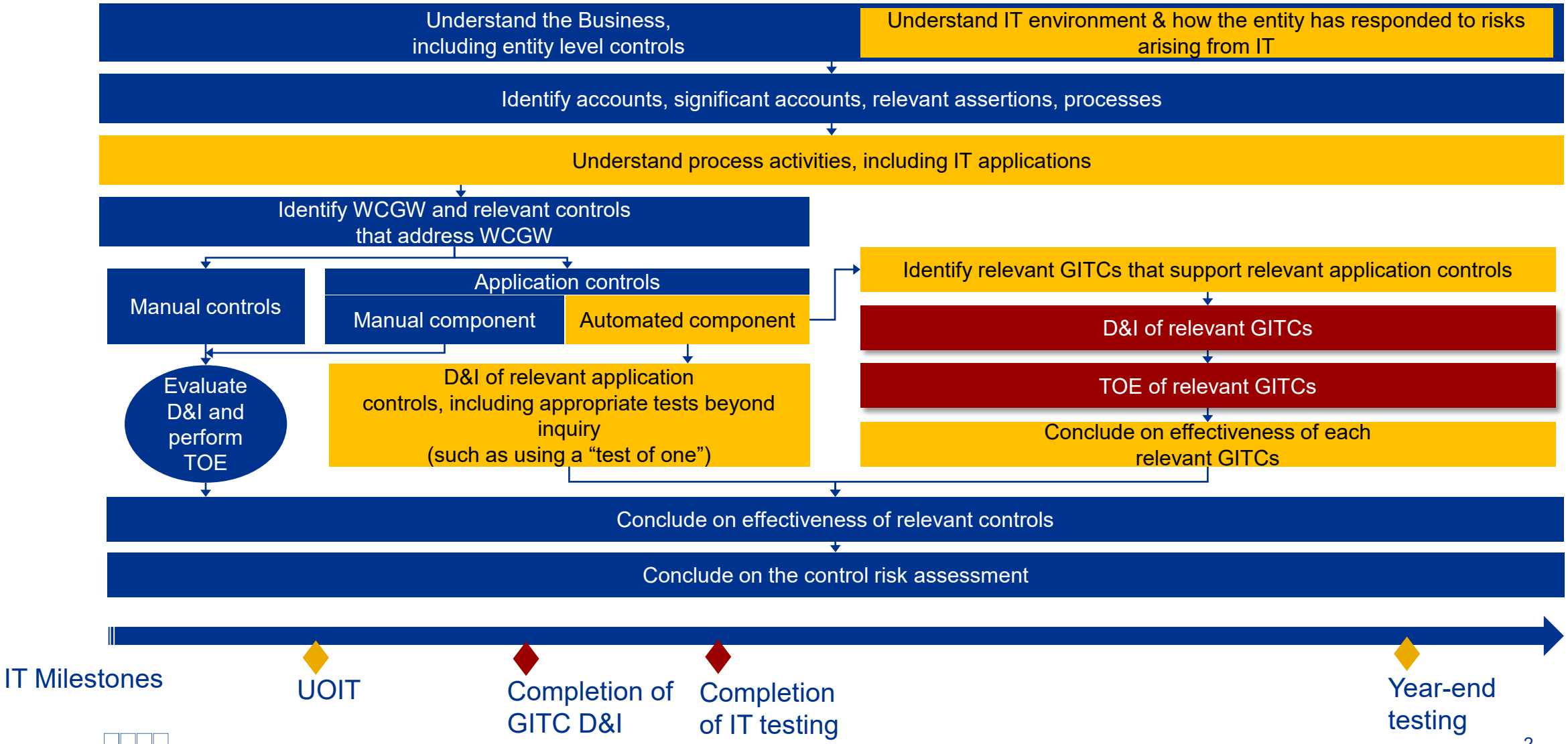
#KPMG josh

Train The Brain Program Changes



October 2021

Where are we in the audit cycle?



Risks Arising from IT

Access to Programs and Data

- Access to programs and data is unauthorized or inappropriate

Program Changes

- Changes to existing systems / IT applications are unauthorized, untested, unapproved or improperly implemented or documented

Program Acquisition and development

- New IT systems that are developed or acquired are unauthorized, untested, unapproved or improperly implemented or documented

Computer Operations

- IT systems processing is unauthorized or inappropriately scheduled, and deviations from scheduled processing are unidentified and unresolved

Program change controls are controls established by management to determine that **changes to existing systems/IT applications are authorized, tested, approved, properly, implemented, and documented.**.

- Change management policy
- Authorization, Development, Testing and Approval
- Configuration Changes
- Emergency Changes
- Migration to the Production environment

PC - What to look for?

Change management process

- Is there change management policy?
- Type of changes
- Who manages changes to the system?
- Are processes followed common across systems?
- Is any portion of change management outsourced?

Emergency and Configuration changes

- Process for emergency and configuration changes
- How is the process different from that for normal changes?
- Who manages the changes to the system?
- Are there post facto approvals in place for emergency changes?
- Who can make the configuration changes in the applications?

Segregation of Environments and Duties?

- Are development, UAT and production servers logically segregated?
- Who can deploy the changes into the production environment?
- Whether development is handled by the vendor and is the development server within client premises or vendor premises.
- Are the change deployment activities logged through PIM / PAM tools?

Key points to remember

- Perform effective one sample walkthrough to understand process and related control implementation
- Document TOD with detailed process explanation and evidence markups
- Samples for TOE to be based on frequency or number of occurrences of a control
- Sampling to be performed as per KAM/ KAEG guidance
- Population to be tested as an IPE (Perform test of report logic + retain report download evidences)
- Identify IPEs used in performance of a control and test accordingly
- Identify and test additional controls for ERP systems where relevant

TOD – Test of Design

TOE – Test of Operating Effectiveness

IPE – Information provided by Entity

KAM – KPMG Audit Methodology

KAEG – KPMG Audit and Execution Guide

ERP – Enterprise Resource Planning

PC- Change Management Policy

There exists a user access management policy for in-scope applications

Data Required – (PBC)

1) Change Management policy applicable for in-scope applications in the organization

Control attributes

- Approval and review of Change management policies on periodic basis.
- Inclusion of relevant processes defined as per the controls

Common Observation -

1. Review of Change management policy does not happen on regular basis

Mitigation –

1. Effectiveness of processes implemented

PC 01, 02 - Authorization, Development, Testing and Approval

The changes to Application and supporting infrastructure is approved, developed, tested and approved by authorized personnel prior moving into production environment

Request initiation - Form / Tool → Business and IT Approval prior to Development → UAT sign off → Approved by CAB/authorized personnel

Data Required – (PBC)

1) System generated Report for changes [IPE]
2) Authorization matrix

Risk

Unauthorized changes to IT systems, applications and data may lead to inaccurate financial reporting

If changes to programs, systems, and configuration are not properly performed, it could impact the operating effectiveness of application controls, calculations, reports, and data that support accounting and financial reporting activities

Control attributes

- Existence of change approval matrix
- Authorization for changes prior to development
- User Acceptance Testing (UAT) performed by Business/IT
- Post UAT testing changes authorized in Change Advisory Board (CAB) / authorized individual

Common Observations -

1. Insufficient documentation to demonstrate that UAT confirmation received from Business and IT
2. Absence of authorization evidence
3. Absence of system generated population for changes
4. Changes are not maintained neither by client nor by vendor

Mitigation procedures –

1. Evaluate each identified exception to determine if the change was approved prior to moving into production environment

PC 01, 02 - Authorization, Development, Testing and Approval

The changes to Application and supporting infrastructure is approved, developed, tested and approved by authorized personnel prior moving into production environment

Request initiation - Form / Tool → Business and IT Approval prior to Development → UAT sign off → Approved by CAB/authorized personnel

Data Required – (PBC)

1) System generated Report for changes [IPE]
2) Authorization matrix

Risk

Unauthorized changes to IT systems, applications and data may lead to inaccurate financial reporting

If changes to programs, systems, and configuration are not properly performed, it could impact the operating effectiveness of application controls, calculations, reports, and data that support accounting and financial reporting activities

Control attributes

- Existence of change approval matrix
- Authorization for changes prior to development
- User Acceptance Testing (UAT) performed by Busine
- Post UAT testing changes authorized in Change Advis

Common Observations -

1. Insufficient documentation to demonstrate that UAT c
2. Absence of authorization evidence
3. Absence of system generated population for changes
4. Changes are not maintained neither by client nor by v

Mitigation procedures –

1. Evaluate each identified exception to determ

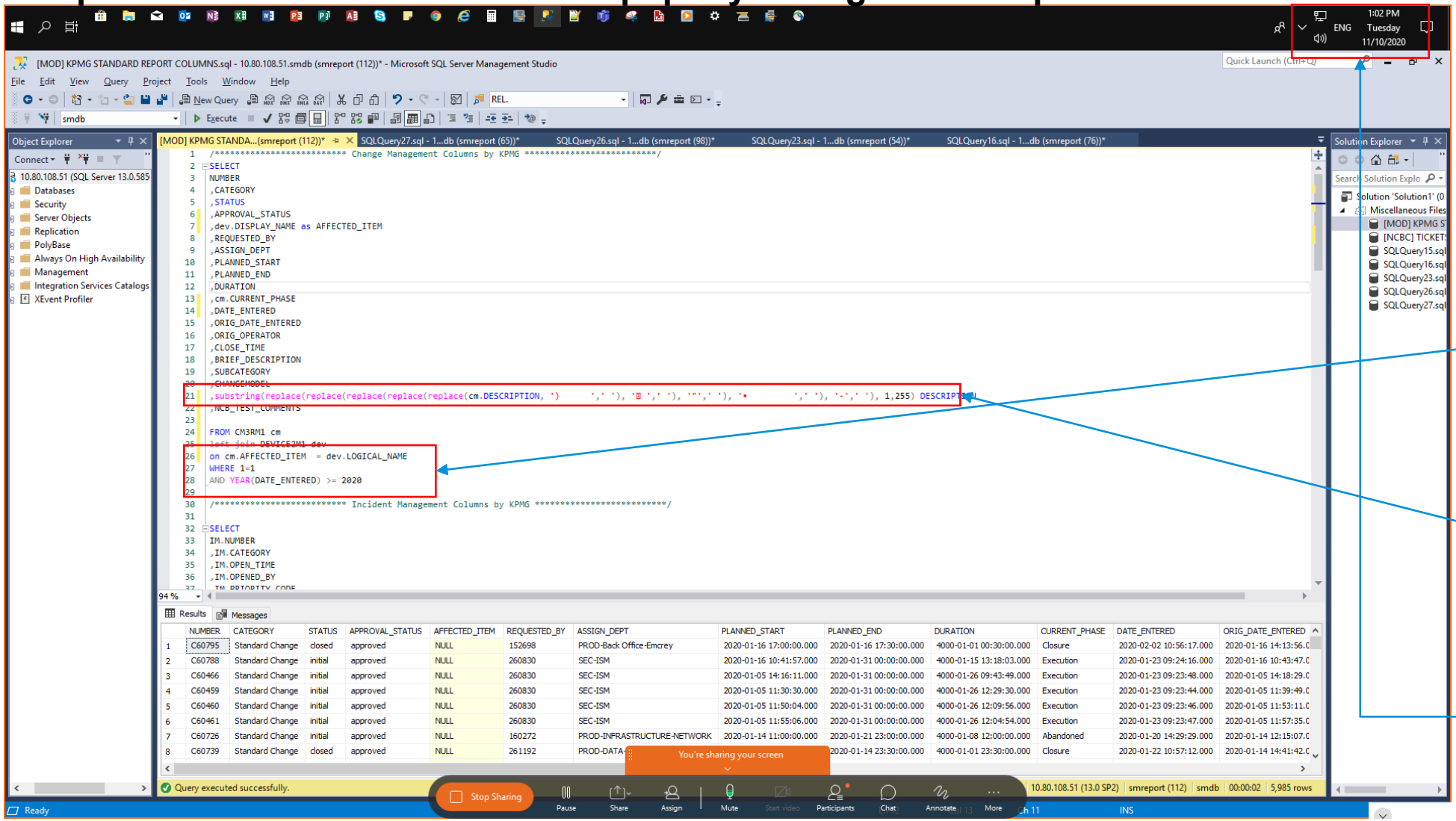
What if system generated listing of changes is not available from the system for GITC is being tested?

- Evaluate what is the organization's mechanism for maintaining a current list of change requests that are moved to production -: Ticketing tool utilized to record changes and related approvals; manual list of changes with periodic management review controls to ensure completeness and accuracy
- Evaluate whether appropriate segregation of duties is maintained between change developers and migrators to ascertain unauthorized changes will be prevented

Document rationale for relying on the alternate listing provided by management and the tests conducted for engagement team to be comfortable with the alternate listing

Illustration: PC 01 - list of changes

Report Generated from backend sql query for a given time period



PC 03 - Segregation of environments

Management has a production environment that is segregated from non-production environments.

Change Management Policy → Segregation of environments

Data Required – (PBC)

1) Obtain list of servers with IP Addresses / URLs for Production, UAT and Development instances
2) Inspect whether the Development, UAT and Production environments are logically segregated

Risk

No segregation among development, UAT and production servers may lead to changes being developed / deployed directly into the production environments; which may in turn affect the operating effectiveness of the application controls.

Control Attributes–

- Development, UAT and Production environments are logically segregated

Common Observations -

1. There is no clear segregation between development and production servers.

Mitigation procedures–

1. Inspect the development and deployment logs for the changes to ascertain that the changes are developed and tested in non-production environments

PC 04 - Access to migration to the Production environment

Access to migrate changes into the production environment for systems and applications is restricted to authorized personnel

Change Management Policy → List of Developers & list of migrators

Data Required – (PBC)

1) Obtain system generated list of developers on development environment and users with the access to migrate the changes to production environment [IPE]
2) Evidence of changes in such access through the audit period and related authorization

Risk

Developers having access to both environments may misused to perform unauthorized changes.

Control Attributes–

- Appropriate segregation of duties is maintained between developers and migrators

Common Observations -

1. Appropriate segregation of duties

Mitigation procedures–

1. Inspect the changes are approved prior moving into production environment

PC 04 - Access to migration to the Production environment

Access to migrate changes into the production environment for systems and applications is restricted to authorized personnel

Change Management Policy → List of Developers & list of migrators

Data Required – (PBC)

1) Obtain system generated list of developers on development environment and users with the access to migrate the changes to production environment [IPE]
2) Evidence of changes in such access throu[illegible]h the audit period and related authorization

Risk

Developers having access to both environments may misused to perform unauthorized changes.

Control Attributes–

- Appropriate segregation of duties is maintained betw[illegible]

Common Observations -

1. Appropriate segregation of duties

Mitigation procedures–

1. Inspect the changes are approved prior movir[illegible]

What if devops environment is used and developers have been provided access to migration of code as well?

Many organizations utilize devops environment for development and implementation of changes. In such cases, developers may be provided access to production.

- Evaluate if the organization has implemented additional controls such as monitoring developer access to production, enabling time-based access for migration post approvals and/or enabling access through a privileged access management solution

KPMG

Q&A

home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

KPMG (Registered) (a partnership firm with Registration No. BA- 62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability partnership firm) with LLP Registration No. AAT-0367 with effect from July 23, 2020.