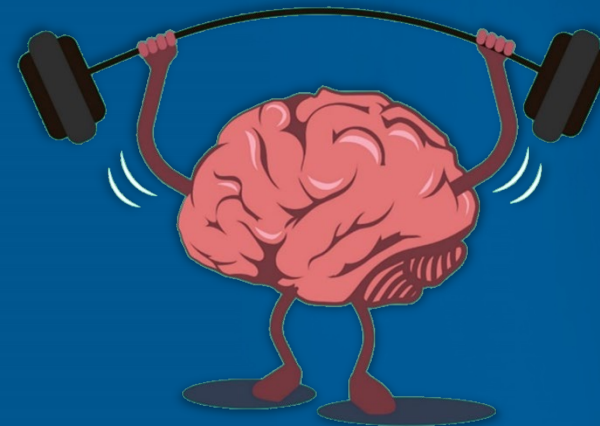


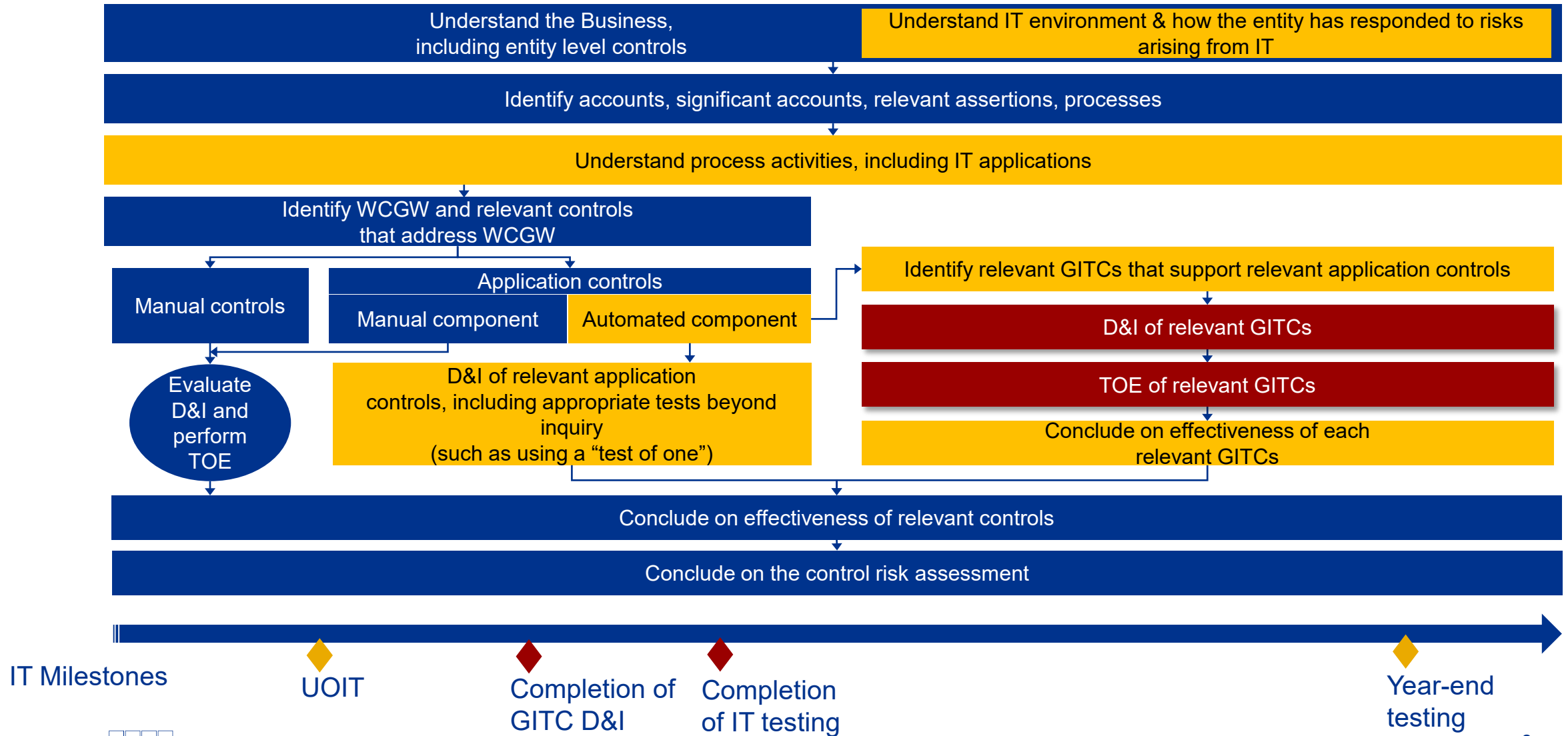


Train The Brain Program Changes

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

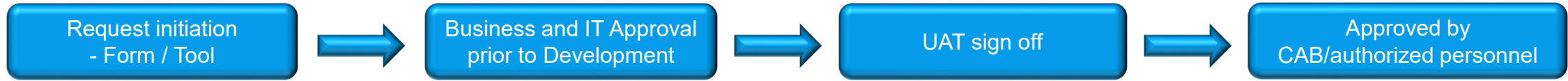


Mitigation –

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



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

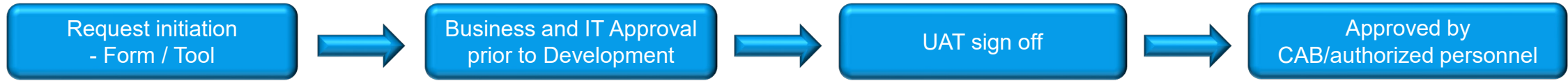


Mitigation procedures –

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



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
- Post UAT testing changes authorized in Change Advice

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

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



Illustration: PC 01 - list of changes

Report Generated from backend sql query for a given time period

The screenshot shows the Microsoft SQL Server Management Studio interface. The top status bar indicates the time is 1:02 PM on Tuesday, 11/10/2020. The main window displays a SQL query in the Query Editor, which is highlighted with a red box. The query is a SELECT statement that filters for changes based on the year of the DATE_ENTERED field, specifically for the year 2020. The results of the query are shown in the Results pane at the bottom, displaying a table with columns for change details and timestamps. The table contains 8 rows of data, each representing a different change item.

SQL Query:

```
1 /***** Change Management Columns by KPMG *****/
2 SELECT
3     ,NUMBER
4     ,CATEGORY
5     ,STATUS
6     ,APPROVAL_STATUS
7     ,dev_DISPLAY_NAME as AFFECTED_ITEM
8     ,REQUESTED_BY
9     ,ASSIGN_DEPT
10    ,PLANNED_START
11    ,PLANNED_END
12    ,DURATION
13    ,cm_CURRENT_PHASE
14    ,DATE_ENTERED
15    ,ORIG_DATE_ENTERED
16    ,ORIG_OPERATOR
17    ,CLOSE_TIME
18    ,BRIEF_DESCRIPTION
19    ,SUBCATEGORY
20    ,CHANGEMODEL
21    ,substring(replace(replace(replace(replace(replace(cm.DESCRPTION, '
22    ,', ' '), 'B ', ' '), ' ', ' '), ' ', ' '), ' ', ' '), 1,255) DESCRPTION
23
24 FROM CM3RM1 cm
25 left join DEVICE3M1 dev
26 on cm.AFFECTED_ITEM = dev.LOGICAL_NAME
27 WHERE 1=1
28 AND YEAR(DATE_ENTERED) >= 2020
29
30 /***** Incident Management Columns by KPMG *****/
31 SELECT
32     ,IM.NUMBER
33     ,IM.CATEGORY
34     ,IM.OPEN_TIME
35     ,IM.OPENED_BY
36     ,IM.REPORTING_CODE
```

Results Table:

	NUMBER	CATEGORY	STATUS	APPROVAL_STATUS	AFFECTED_ITEM	REQUESTED_BY	ASSIGN_DEPT	PLANNED_START	PLANNED_END	DURATION	CURRENT_PHASE	DATE_ENTERED	ORIG_DATE_ENTERED
1	C60795	Standard Change	closed	approved	NULL	152698	PROD-Back Office-Emcrey	2020-01-16 17:00:00.000	2020-01-16 17:30:00.000	4000-01-01 00:30:00.000	Closure	2020-02-02 10:56:17.000	2020-01-16 14:13:56.000
2	C60788	Standard Change	initial	approved	NULL	260830	SEC-ISM	2020-01-16 10:41:57.000	2020-01-31 00:00:00.000	4000-01-15 13:18:03.000	Execution	2020-01-23 09:24:16.000	2020-01-16 10:43:47.000
3	C60466	Standard Change	initial	approved	NULL	260830	SEC-ISM	2020-01-05 14:16:11.000	2020-01-31 00:00:00.000	4000-01-26 09:43:49.000	Execution	2020-01-23 09:23:48.000	2020-01-05 14:18:29.000
4	C60459	Standard Change	initial	approved	NULL	260830	SEC-ISM	2020-01-05 11:30:30.000	2020-01-31 00:00:00.000	4000-01-26 12:29:30.000	Execution	2020-01-23 09:23:44.000	2020-01-05 11:39:49.000
5	C60460	Standard Change	initial	approved	NULL	260830	SEC-ISM	2020-01-05 11:50:04.000	2020-01-31 00:00:00.000	4000-01-26 12:09:56.000	Execution	2020-01-23 09:23:46.000	2020-01-05 11:53:11.000
6	C60461	Standard Change	initial	approved	NULL	260830	SEC-ISM	2020-01-05 11:55:06.000	2020-01-31 00:00:00.000	4000-01-26 12:04:54.000	Execution	2020-01-23 09:23:47.000	2020-01-05 11:57:35.000
7	C60726	Standard Change	initial	approved	NULL	160272	PROD-INFRASTRUCTURE-NETWORK	2020-01-14 11:00:00.000	2020-01-21 23:00:00.000	4000-01-08 12:00:00.000	Abandoned	2020-01-20 14:29:29.000	2020-01-14 12:15:07.000
8	C60739	Standard Change	closed	approved	NULL	261192	PROD-DATA	2020-01-14 11:00:00.000	2020-01-14 23:30:00.000	4000-01-01 23:30:00.000	Closure	2020-01-22 10:57:12.000	2020-01-14 14:41:42.000

Time period defined

Report- program changes

System details with Date and Timestamp

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 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



Common Observations -

1. Appropriate segregation of duties



Mitigation procedures–

1. Inspect the changes are approved prior moving

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



Q & A



home.kpmg/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

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.

© 2020 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only/Printed in India