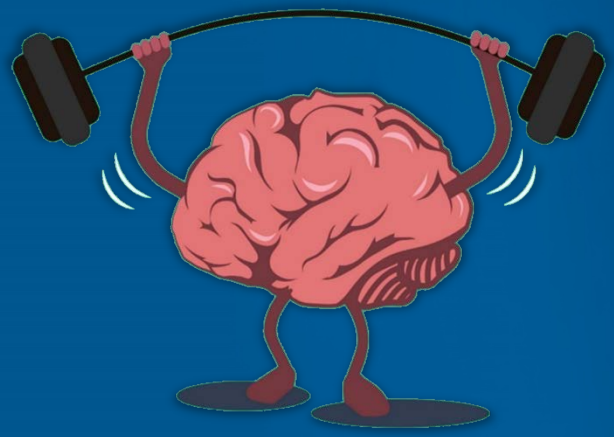
KPMG

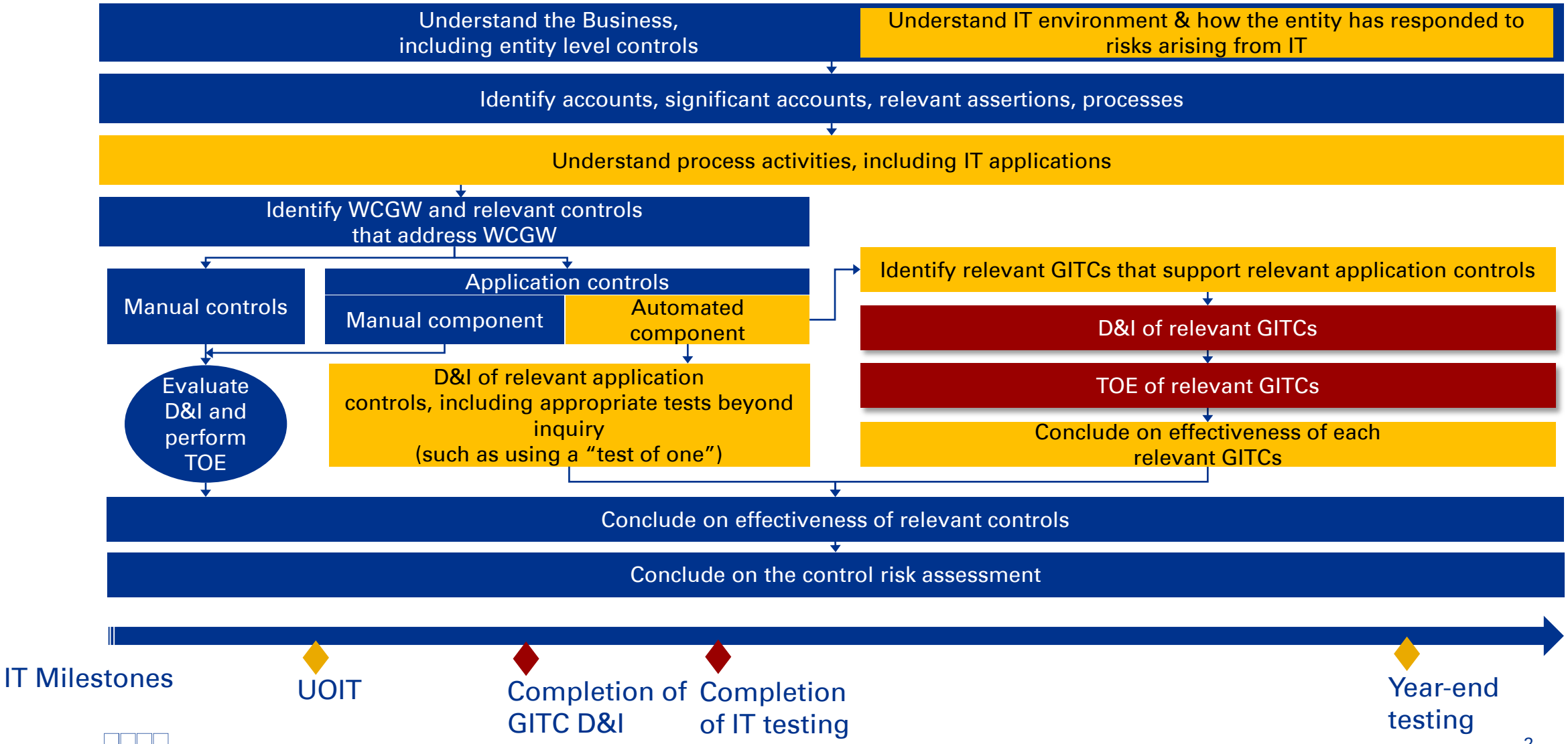
#KPMG josh

Train The Brain
Computer Operations



October 2021

Where are we in the audit cycle?



What is covered in Computer Operations?

Computer operation controls are controls established to ensure that the systems/IT applications continue to function consistently as planned. Computer operations controls mitigate the risk of unavailability of systems or programs for the users.

01 Batch Job Management

02 Backup and Recovery

03 Incident and Problem Management

Batch Job Scheduling and some common Batch Job Tools

To automate tasks which need to run on a defined time basis, but doesn't necessarily need human interaction with the system.

Consists of a schedule defined to run at specific point in a day or with a defined frequency multiple times in a day

May involve transfer of data from one system to another, for example, attendance swipe records data flowing to timesheet application.

Can run at various layers, for example, pushing data of sales made from POS every 5 minutes to accounting application – Application layer, Cron jobs in Oracle database.

Backup and Recovery and some common Backup Tools

To automatically backup data for systems used during financial reporting processes

Testing of Restoration of backed up data to get comfort on restoration process

Backup could be stored in a cloud managed by third party such as AWS, Ctrl+S in which case, it is recommended to obtain and evaluate the cloud provider's SOC report

Backup of data would encompass storing information/ data at application layer and database layer

Incident Management and Monitoring and some common Tools

To log any incident that could affect the functioning of the system/ applications which is subjected to Financial audit

Incident could be prioritized based on severity and some of them may need to be reported to regulator as part of protocol.

Resolved incidents form a knowledge base to help assist in troubleshooting similar future incidents faster, unresolved incidents may open a window for potentially similar future and larger attacks

Unresolved incidents may also snowball into something major which can affect the financial reporting process

servicenow

splunk>

bmc REMEDY

Jira Service Management

CO1 - Job Scheduling

Management has controls in place to determine accuracy, completeness, and timely processing of system jobs, including batch jobs and interfaces, for relevant information systems related to financial reporting.

Data Required – (PBC)

1) Batch job policy applicable for in-scope applications in the organization
2) System based list of jobs with schedule and comfort on completeness and accuracy of the same [IPE]
3) List of personnel authorized to modify batch job schedule and comfort on completeness and accuracy of the same [IPE]
4) Evidence for handling of batch job failures/ rerun of failed batch jobs including tickets raised

Risk

1. Absence of a process to monitor production job environment to identify job failures may lead to loss of business data if the job failure is not resolved in acceptable time frame. This may lead to inaccurate or incomplete financial records.

Control attributes

- Scheduled production jobs or batches are monitored daily for their successful execution.
- Failed batch jobs are identified, monitored and resolved through the entity's incident management process and are re-run post the incident resolution for their successful re-execution.

Common Observation -

1. Batch jobs are not performed according to a regular schedule as required by the business or policy procedures
2. There are no monitoring or resolution procedures over failed batch jobs

Mitigation –

1. Evaluate the impact of the incomplete/failed batch jobs to financial processing/reporting
2. Determine if manual procedures have been performed in the place of batch job activities

Illustrative - C01

Control Description:
Job processing procedures and operating procedures are documented and followed. In case of incomplete execution of the jobs there exists a formal process to escalate/ report and track to its resolution.

Test Procedures

- Batch Jobs Schedule
- Critical Batch Jobs
- Batch Jobs Scheduling
- Batch Jobs Monitoring
- Failed Jobs resolution testing

SAP Transaction Codes

- SAP Standard Table – TBTCO (Job Status Overview)
- SAP Standard Table – TBTCP
- SAP Standard Report – SM37

Evidences from SAP

Microsoft Excel Worksheet

Sample workpaper

Microsoft Excel Worksheet

CO 2 – Backup and Recovery Procedures

Management has controls in place to determine that data, transactions and programs that are necessary for financial reporting may be recovered.

Data Required – (PBC)

1) Backup and restoration policy applicable for in-scope applications in the organization
2) Backup jobs with schedule
3) List of personnel authorized to modify backup schedule and comfort on completeness and accuracy of the same [IPE]
4) Evidence for handling of backup failures/ rerun of failed backup jobs including tickets raised
5) Evidence of successful restoration for select restoration requests

Risk

1. Unavailability of backups leads to loss of business data if the primary data storage is corrupted / destroyed. It may result in a major impact on business operations and also in inability of business to perform usual business activity.
2. Incomplete or unsuccessful restoration of data may lead to inaccurate financial records

Control attributes

- Formalized backup and recovery procedures exist.
- Backups of the operating system, applications and company information are performed on a periodic basis to meet business requirements.
- Backup logs are monitored daily to ensure backups are successfully completed.
- Restoration requests are addressed post approvals and tested for completeness and accuracy

Common Observation -

1. Backup procedures are not performed on a regular basis or according to policy procedures
2. There are no monitoring or resolution procedures over failed backups
3. Lack of validation of restoration success

Mitigation –

1. Determine if the client has performed a successful backup and restore per their remediation procedures

Illustrative - CO 2

Control Description:
Periodic backup of SAP is taken as per backup policy defined and backup logs are maintained and reviewed on a periodic basis.

Test Procedures

- Frequency of backup.
- Backup failures
- Backup monitoring
- Restoration testing

SAP Transaction Codes

- Transaction code : DB12 – Backup logs
- Transaction code : DB13 - Backup schedule

Evidences from SAP

Backup Logs.zip

Sample workpaper

Microsoft Excel Worksheet

CO 3 – Incident Management Procedures

Management has controls in place to determine that system problems that could potentially affect the financial reporting process are identified and resolved in a timely manner

Data Required – (PBC)

1) Incident and Problem Management policy applicable for the organization
2) List of incident tickets and comfort on completeness and accuracy of the same [IPE]
3) Evidence for resolution of tickets including RCA
4) Evidence for periodic review of open incidents/ problems

Risk

1. In absence of a process to log incidents and problems identified by users may lead to loss of business data if the incident or problem is not resolved on acceptable time frame. Such unavailability of data may result in a major impact on business operations and may also result in inability of business to perform usual business activity also may not be able to effectively service customers

Control attributes

- Formalized incident management process exist.
- Existence of service level agreements for incident resolution
- Root cause analysis and resolution of incidents within expected timelines

Evaluate if there were critical incidents during the year that may have led to an impact on Financial Reporting such as system unavailability for long period, data loss. Assess corrective actions taken by the entity and any additional procedures that may be necessary for us to perform

Common Observation -

1. No process exists for Incidents
2. Incidents not resolved in a timely manner

Mitigation –

1. For Incidents which were not resolved in timely manner, evaluate whether there was any financial/business impact

CO – Specific Exclusions

When there is no impact on the ITACs, some CO controls may be excluded from GITC testing. This will have to be documented in 2.6.10 on why there is no impact due to non-coverage. This call will have to be determined in consultation with EP and EM and then documented appropriately.

Example – There are only Config ITACs that need to be tested. In such cases, the rationale for not covering batch job controls may be explained clearly in 2.6.10

In case there is comfort that there are no incidents reported which affect the functioning of ITACs including cyber incidents, procedures performed to this effect may be included in 2.6.10 so that incident management controls could be excluded,

Illustrative - CO 3

Sample Incident Priority Matrix

Impact	Incident Record Priority				
	Critical	High	Medium	Service at Risk	Low
Financial	Projected or actual financial loss more than USD 500k.	Projected or actual financial loss USD 200k to USD 499k.	Projected or actual financial loss under USD 199k.	Potential or non-materialised financial loss to the line of business. Failure to apply a fix within 4 hours will trigger a critical, high or medium incident.	No projected or actual financial impact.
Operational	Large scale operational impact	Performance impact	Minor impact limited to small groups	Minor impact limited to individuals. Failure to apply a fix within 4 hours will cause operational impact to the entity.	Minor impact, limited to individuals
Regulatory	Critical breach of legal / regulatory requirements that would need to be reported to the regulator, with a projected penalty or censure.	Breach of legal / regulatory requirements that would need to be reported to the regulator.	Minor breach of regulatory reporting SLA's that would need to be reported to the regulator.	Breach of regulatory requirements. Failure to apply a fix within 4 hours will cause regulatory impact(s) to the entity.	No projected or actual regulatory impact.
Customer	Client SLA breaches over 24 hours for any client from the key client list, or more than 50 external corporate and institutional clients.	Client SLA breaches for any client from the key client list, or more than 50 external corporate and institutional clients.	Client SLA breaches for less than 50 external corporate and institutional clients.	Impact to external customers. Failure to apply a fix within 4 hours will cause customer impact(s) to the entity.	Direct impact to customers.
Reputational	Reputational damage such that it could cause a run on the entity or make “front page” of the major media.	Reputational damage such that it could cause 100 or more customer complaints (or fewer Very Important Person (VIP) / large revenue client complaints), which could lead to reports in the media.	Reputational damage such that it could cause less than 99 customer complaints (or fewer VIP / large revenue client complaints), which could lead to reports in the media.	Reputational damage to the bank. Failure to apply fix within 4 hours will cause reputational impact(s) to the entity.	No projected or actual reputational damage and no risk of any reports in

Sample workpaper

Microsoft Excel Worksheet

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.