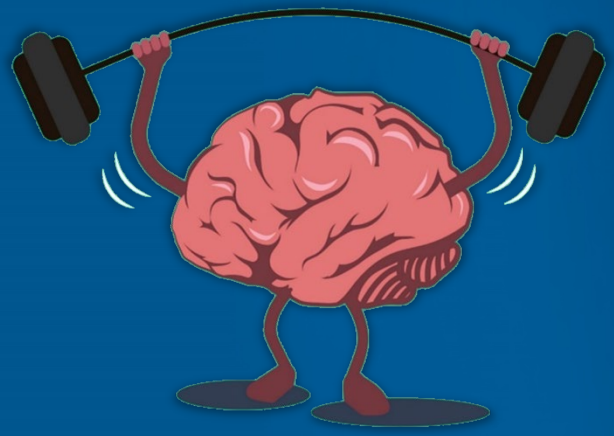
KPMG

#KPMG josh

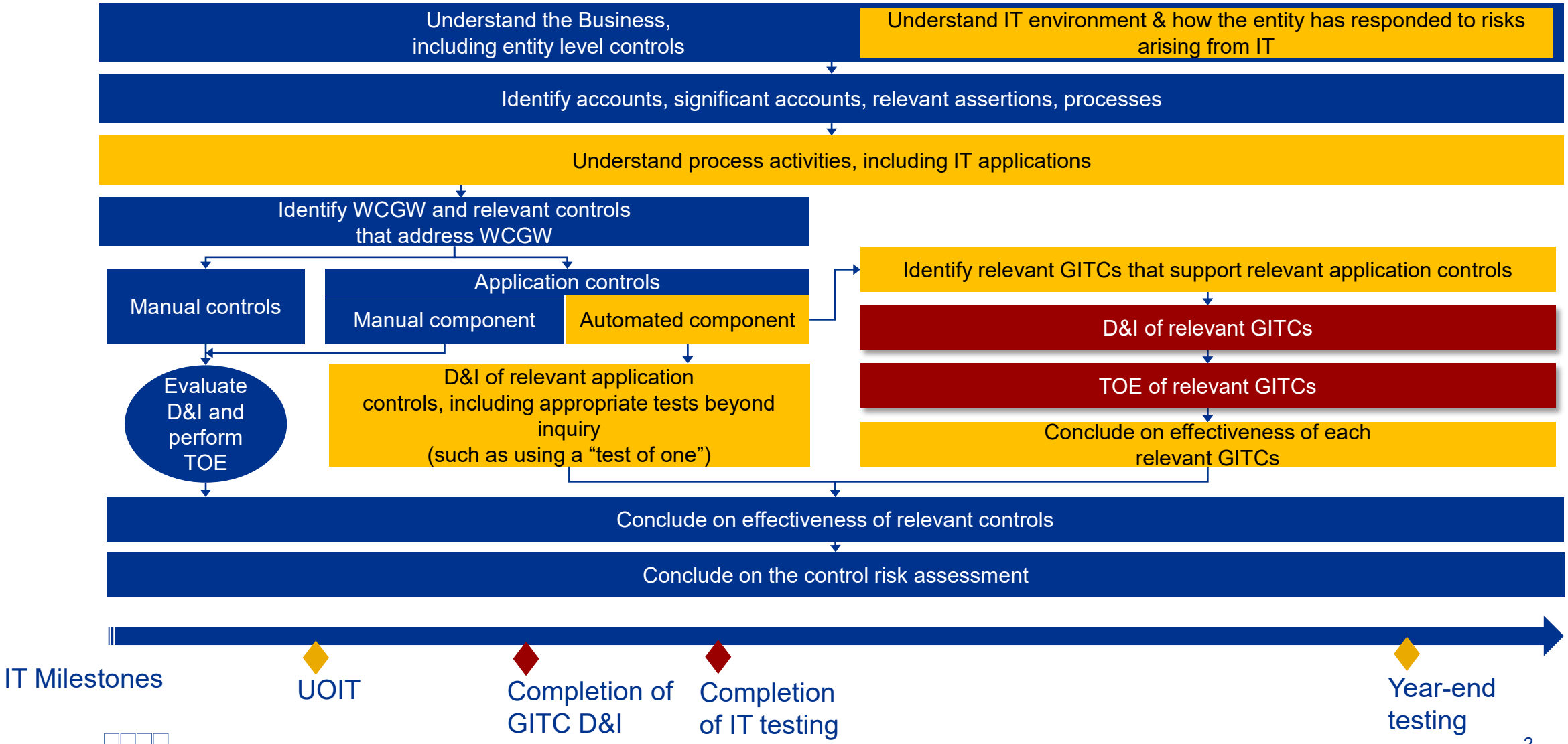
Train The Brain

Access to Programs & Data



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

Access to programs and data controls are controls established by management to reduce the risk of unauthorized/inappropriate access to the relevant information systems related to financial reporting and prevent individuals from perpetrating and concealing an error or irregularity.

- User access management policy
- User Creation/Modification
- User Revocation
- User Access Review
- Privileged user access
- Generic user IDs
- Access Administration

APD - What to look for?

Access management process

- Is there an access management policy?
- Who manages access to the system?
- Are processes followed common across systems?
- Where is the system hosted?
- Is any portion of access management outsourced?

How is the system accessed?

- Application specific user ID and password
- Authentication through domain credentials
- Single sign-on through domain credentials or otherwise
- Dual authentication (password + OTP)
- Access through a privileged ID management solution

What kind of users have access to the system?

- Unique user IDs vs generic user IDs
- Default accounts
- System accounts
- External or internal users
- Super users

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

APD- User Access Management Policy

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

Data Required – (PBC)

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

Control attributes

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

Common Observation -

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

Mitigation –

1. Effectiveness of processes implemented

APD 01, 02 - User Creation/ User Modification

The access to Application is granted based on the formal approval from the authorized personnel

Request initiation - Form / Tool → Manager Approval → HOD/SOD Approval → Team - User Creation/Modification

Data Required – (PBC)

1) System generated Report for user creation/modification [IPE]
2) Authorization matrix

Risk

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

Control attributes

- Existence of authorization matrix
- Authorization for user IDs created/ modified
- Access granted / modified based on request

Common Observations -

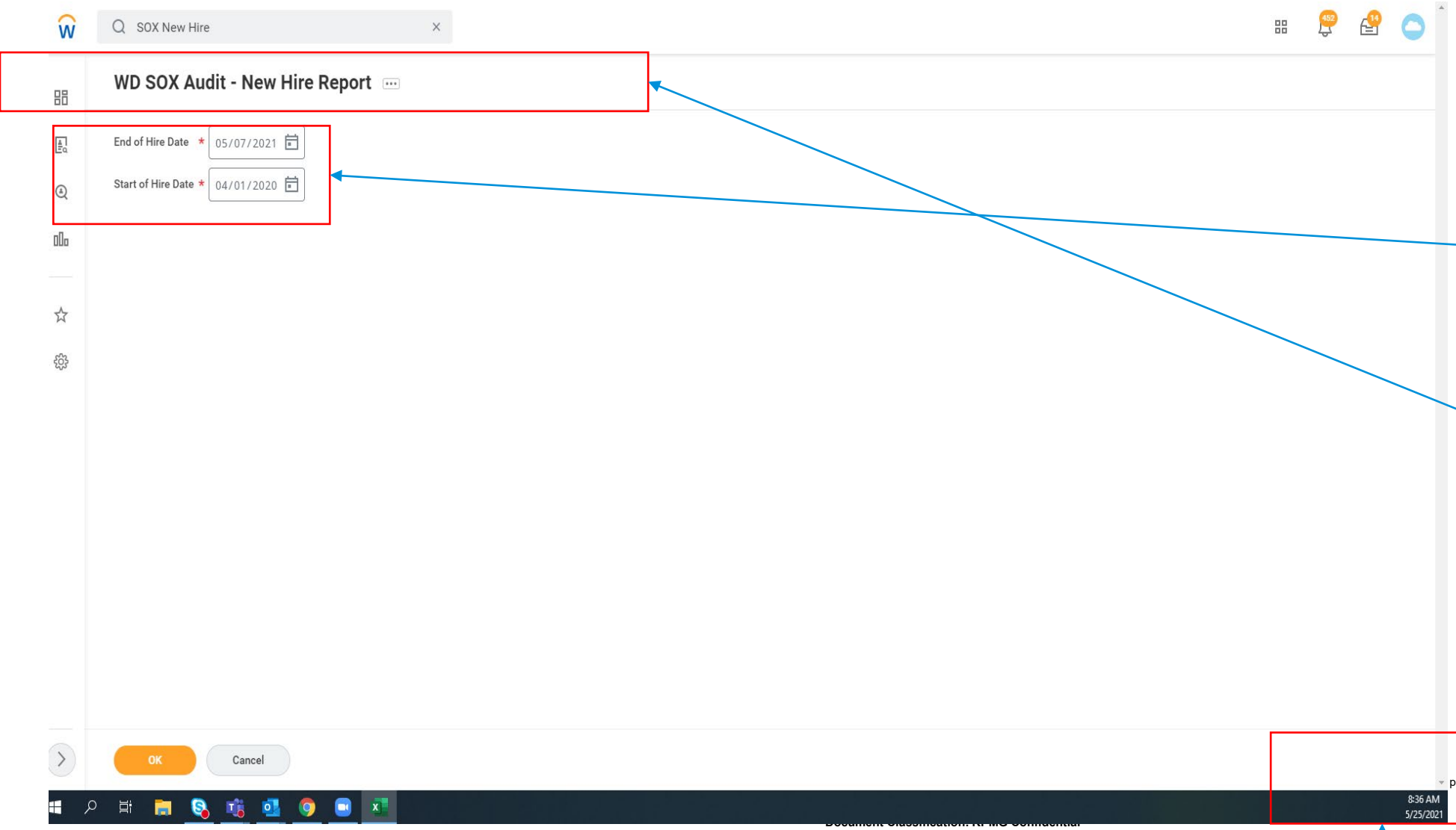
1. Insufficient documentation to demonstrate that user creation accounts/access rights are appropriate and provided by authorized person
2. Absence of authorization evidence
3. Absence of system generated population for user creation/modification

Mitigation procedures –

1. Evaluate each identified exception to determine if the access was reviewed in access review process (UAR)
2. Assessment of roles to validate if those are critical to relevant ITACs
3. Evaluate accuracy of roles granted if approval was not granted

Illustration: APD 01, 02 - User Creation/ User Modification

Report Generated from System for user creation for a given time period



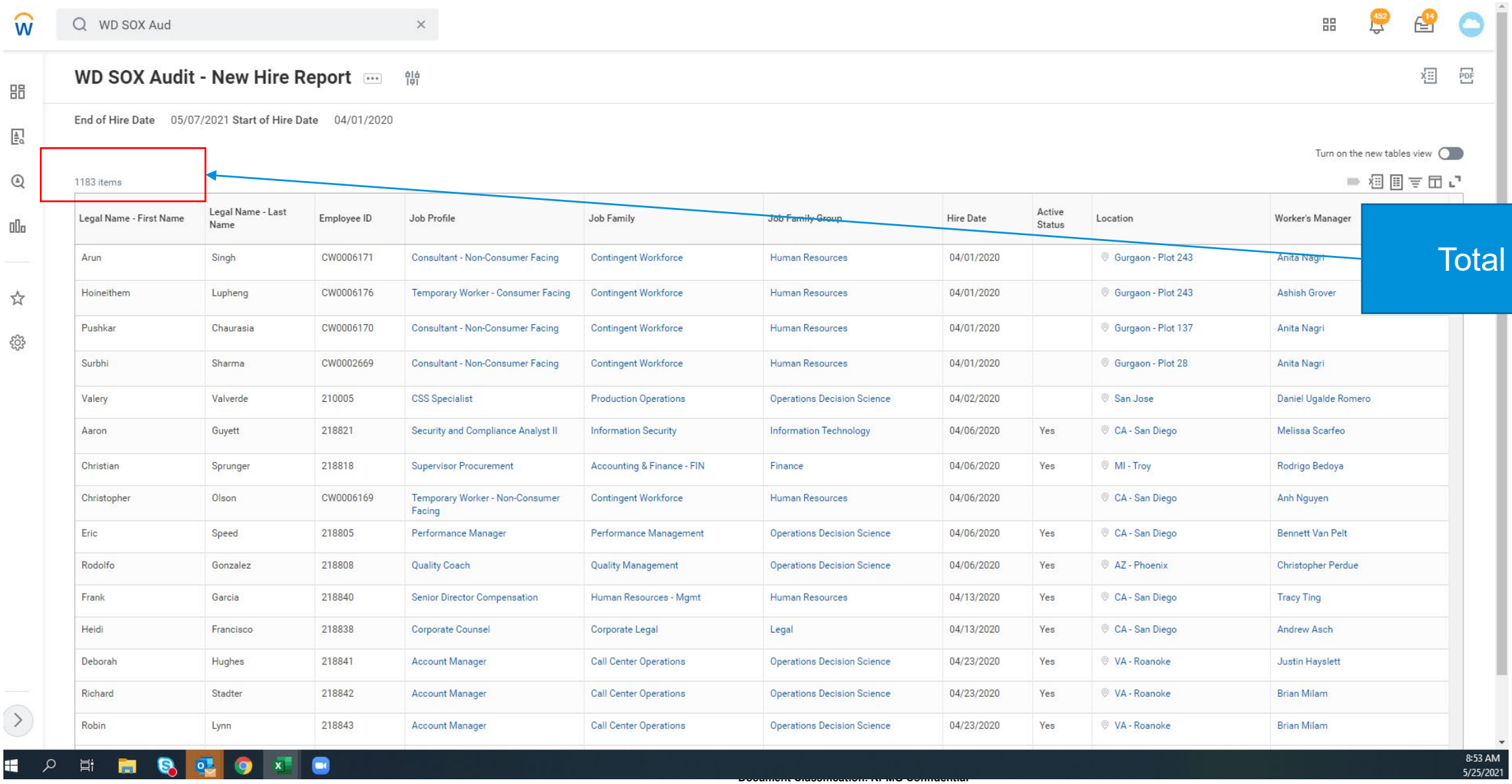
Time period defined

Report- User Creation

System details with Date and Timestamp

Illustration: APD 01, 02 - User Creation/ User Modification

Report Generated from System for user creation for a given time period



Legal Name - First Name	Legal Name - Last Name	Employee ID	Job Profile	Job Family	Job Family Group	Hire Date	Active Status	Location	Worker's Manager
Arun	Singh	CW0006171	Consultant - Non-Consumer Facing	Contingent Workforce	Human Resources	04/01/2020		Gurgaon - Plot 243	Anita Nagri
Hoineithem	Lupheng	CW0006176	Temporary Worker - Consumer Facing	Contingent Workforce	Human Resources	04/01/2020		Gurgaon - Plot 243	Ashish Grover
Pushkar	Chaurasia	CW0006170	Consultant - Non-Consumer Facing	Contingent Workforce	Human Resources	04/01/2020		Gurgaon - Plot 137	Anita Nagri
Surbhi	Sharma	CW0002669	Consultant - Non-Consumer Facing	Contingent Workforce	Human Resources	04/01/2020		Gurgaon - Plot 28	Anita Nagri
Valery	Valverde	210005	CSS Specialist	Production Operations	Operations Decision Science	04/02/2020		San Jose	Daniel Ugalde Romero
Aaron	Guyett	218821	Security and Compliance Analyst II	Information Security	Information Technology	04/06/2020	Yes	CA - San Diego	Melissa Scarfeo
Christian	Sprunger	218818	Supervisor Procurement	Accounting & Finance - FIN	Finance	04/06/2020	Yes	MI - Troy	Rodrigo Bedoya
Christopher	Olson	CW0006169	Temporary Worker - Non-Consumer Facing	Contingent Workforce	Human Resources	04/06/2020		CA - San Diego	Anh Nguyen
Eric	Speed	218805	Performance Manager	Performance Management	Operations Decision Science	04/06/2020	Yes	CA - San Diego	Bennett Van Pelt
Rodolfo	Gonzalez	218808	Quality Coach	Quality Management	Operations Decision Science	04/06/2020	Yes	AZ - Phoenix	Christopher Perdue
Frank	Garcia	218840	Senior Director Compensation	Human Resources - Mgmt	Human Resources	04/13/2020	Yes	CA - San Diego	Tracy Ting
Heidi	Francisco	218838	Corporate Counsel	Corporate Legal	Legal	04/13/2020	Yes	CA - San Diego	Andrew Asch
Deborah	Hughes	218841	Account Manager	Call Center Operations	Operations Decision Science	04/23/2020	Yes	VA - Roanoke	Justin Hayslett
Richard	Stadter	218842	Account Manager	Call Center Operations	Operations Decision Science	04/23/2020	Yes	VA - Roanoke	Brian Milam
Robin	Lynn	218843	Account Manager	Call Center Operations	Operations Decision Science	04/23/2020	Yes	VA - Roanoke	Brian Milam

Illustration: APD 01, 02 - User Creation/ User Modification

Data Generated using SQL query for user creation for a given time period

```
1  select cms_user_name,cms_user_role,email_address,created_time, created_by from cms_admin where date(created_time) between '2020-04-01' and '2020
       -10-31';
```

Execute Query | New Query | Save Query | Load Query | Describe Table -> DROOLSACCESS

Run As Stored Procedure | Wrap Results | Render HTML | Unserialize | Save Results | Active Database -> hpcms_db_new

cms_user_name	cms_user_role	email_address	created_time	created_by
MMT4463	admin	jbW196sUyaNOigFQbgN%2B1rHeBZuYokjeNHGdSvT6el8%3D	2020-04-01 13:22:41	mmt3302
MMT8454	admin	EW9h8dnkMlRRI0h8D2c39h9seKNE2bDGWBiPXgO1GCA%3D	2020-04-02 12:52:07	mmt3302
MMT7255	admin	2Yw4BuArdJMaspSK8PUZw5lYmg%2F9igTEAYZQBLryv%2B0%3D	2020-04-03 13:21:44	mmt7494
MMT8482	admin	htYpIpg7SSZ0u4XQgXZpSHyy4O91WSDqJyk9XOGFNZY%3D	2020-04-03 13:22:25	mmt7494
MMT4426	admin	73dduQfQvOkQIOWCg8nHoP3juQFptasPqA7SVsxtrfM%3D	2020-04-03 13:23:05	mmt7494
MMT8377	admin	UGzBl9cuvB3S7tkE5tmM%2BF9uJ%2B7Dea64nuvM5koUNlA%3D	2020-04-13 11:31:24	mmt7494
MMT8387	admin	3%2BS9XA8N52jCw4GROBRQUrqq%2Bx%2B4WSDDPsJ%2FFLiIdfA%3D	2020-04-13 11:37:45	mmt7494
MMT8378	admin	2IkUJjV778ZdyL0%2FPJF1jvsuEc4BlNNiN2cMhWsVGKY%3D	2020-04-13 11:38:41	mmt7494
MMT8414	admin	SLTWaEpIdH8AuMnNcZq2Tf3juQFptasPqA7SVsxtrfM%3D	2020-04-13 11:39:32	mmt7494
MMT8374	admin	aQwLuCrNZz4gGUA%2BhKlt8LHeBZuYokjeNHGdSvT6el8%3D	2020-04-13 11:40:14	mmt7494
MMT8510	admin	crFxvU%2B2Ewla7DWZux%2FdaT8yQwUCtzgo%2By4RzgGU02I3ZwyFaxUYpg%3D%3D	2020-04-13 11:41:09	mmt7494
MMT8528	admin	HiuiACelMYcaspSK8PUZw5lYmg%2F9igTEAYZQBLryv%2B0%3D	2020-04-13 11:42:19	mmt7494
MMT5514	admin	k80vHDUiyaW7ufveKQXVrzbuk2sIbeYw%2By4RzgGU02I3ZwyFaxUYpg%3D%3D	2020-04-13 11:43:30	mmt7494
MMT5161	admin	PkUND7kI3RGoDcOokW3PZrqq%2Bx%2B4WSDDPsJ%2FFLiIdfA%3D	2020-04-13 11:45:56	mmt7494
MMT8179	admin	yuLU11OgSNO%2Bjb4QpngZ9P3juQFptasPqA7SVsxtrfM%3D	2020-04-13 11:46:23	mmt7494
ManjuB	admin	EToEhn6nmRv0PSErvPIzUZlYmg%2F9igTEAYZQBLryv%2B0%3D	2020-04-13 11:47:23	mmt7494
Dummyproject	conteditor	c6SXTN03g8sOiTwIDsv54rqq%2Bx%2B4WSDDPsJ%2FFLiIdfA%3D	2020-05-06 12:54:33	mmt7494
MMT8518	admin	b8F11t2KT8WBA%2FNjC8C6IBMgjjekFJ%2Fs	2020-06-02 11:45:06	mmt7494
ravindra.goyal	admin	%2BCWBmJt012Rv%2FmPbmsP5mh9seKNE2bDGWBiPXgO1GCA%3D	2020-07-07 16:19:18	mmt3302
MMT8657	admin	Exp%2BqMF3aLTm0A5YdEbwJkIIcKjUxtSx	2020-07-14 10:37:54	mmt7494
YogeshJ	conteditor	nxpZZ5UCddbyB%2BP45Vo6N7qq%2Bx%2B4WSDDPsJ%2FFLiIdfA%3D	2020-07-16 11:01:05	mmt3302
AmanC	conteditor	LhY9WloFy4bBPCSKqRYrQrqq%2Bx%2B4WSDDPsJ%2FFLiIdfA%3D	2020-08-07 16:57:19	mmt7494
MMT8652	admin	R2rdEQNO7%2FWS9G24sMO3f8koHlw43Jo5N2cMhWsVGKY%3D	2020-09-02 09:50:03	mmt3302
MMT7343	admin	sqK%2BghOQF1cUf5Oi5ZUzGakoHlw43Jo5N2cMhWsVGKY%3D	2020-09-14 15:55:38	mmt7494

24 rows in set

ENG 22:06 21-10-2020

SQL Query Used

Total Count

Date time stamp

APD 03 - User Revocation

Leaver employee user accounts are appropriately disabled on a timely basis

HR Intimation → Manager/HOD Approval → IT Team – User ID Revocation

Data Required – (PBC)

1) Deleted user list from system or System generated report of active user list with deletion/ deactivation dates [IPE]
2) List of terminated/ transferred users [IPE]

Risk

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

Control Attributes–

- Access revocation is performed within defined timelines

Common Observations -

1. Delay in de-activation of accounts from either HR or from IT
2. Users has logged in after the last working day

Mitigation procedures–

1. Inspect the access rights given to the leaver account and determine if it poses a risk to financial reporting
2. Check if any login/transactions are executed by user after the last working day; assess impact on associated ITACs

APD 04 - Password Configuration

Passwords and security configurations restrict access to authorized users

Password Policy → Password Parameters Configured

Data Required – (PBC)

1) Password policy applicable for in-scope applications in the organization
2) System generated password configuration evidence
3) Negative tests for password parameters

Risk

Absence of appropriate password configuration may lead to unauthorized access to systems

Control Attributes–

- Documented password policy exists and provides details of password parameters to be implemented
- Password parameters have been configured in line with the policy

Common Observations -

1. Password Policy is not in place or it isn't reviewed and revised timely
2. Password parameters configured for the application are not in line with the password policy

Mitigation procedures–

1. Determine if users have to pass any other authentication mechanisms prior to accessing the system (e.g. AD, citrix, 2 factor authentication)
2. Determine if other access administration controls are effective

APD 05 - Privileged / Super User Access

Privileged user access is restricted to authorized personnel and logs of activities are maintained and reviewed/monitored as per defined frequency

Request initiation - Form / Tool → Manager and/or HOD Approval → Granting of Privilege Access → Periodic review of activity logs

Data Required – (PBC)

1) System generated list of users having access to the privileged/super user roles [IPE]
2) Evidence of periodic review of activity logs for privilege users along with evidence of validation of completeness and accuracy of access logs reviewed [IPE used in control].

Control Attributes–

- Validate users with privileged access are appropriate as per job responsibilities
- Privileged user IDs on operating system and database mapped to a privileged access management tool (where relevant)
- Segregation of duties between business and IT users
- Privileged access logs are reviewed based on defined frequency; access logs are verified for completeness and accuracy prior to review

Note – Access creation, modification and revocation of privileged users is required to be covered in APD 1, APD 2 and APD 3

Common Observations -

1. Non admin users have access to privilege profiles
2. Activity logs of users having privilege access are not reviewed periodically

Mitigation procedures–

1. Review of access logs

APD 06 - User Access Review

User Access Review should be performed for defined frequency

Data Required – (PBC)

1) Evidence of periodic review of access including evidence of validation of completeness and accuracy of user access listing reviewed [IPE used in control].

Risk

Unauthorized access to IT systems, applications and data lead to errors in financial reporting or significant fraud.

Control Attributes–

- User access review including user roles was performed based on defined frequency
- User access list included all user IDs including privileged users, generic user IDs, and system user IDs was verified for completeness and accuracy prior to review
- Corrective actions highlighted as part of review were closed

Common Observations -

1. User Access Review Activity has not been performed for a specific period
2. User access listing was not verified for completeness and accuracy prior to review
3. Actions suggested by reviewers were not acted upon

Mitigation procedures –

1. Determine effectiveness of user access administration and privileged access controls
2. Review the last login/access activity of users who were suggested to be removed as part of the exercise.

APD 07 - Generic User ID (User Administration)

Generic user IDs are utilized only after approvals

Data Required – (PBC)

1) Evidence of periodic review of Access Review logs along with system generated report for general and privileged users

Risk

Unauthorized access to IT systems, applications and data lead to errors in financial reporting or significant fraud.

Control Attributes–

- Generic user IDs including system user IDs have been assigned designated owners and are approved
- Generic IDs with privileged access have been included in privileged access log review (APD 05)

Note – Access creation, modification and revocation of generic user ids is required to be covered in APD 1, APD 2 and APD 3

Common Observations -

1. Generic user IDs are utilized without documented approvals
2. Owners have not been assigned to generic IDs to establish accountability
3. Privileged generic IDs are not included in access log monitoring

Mitigation procedures –

1. Determine effectiveness of user access administration and privileged access controls
2. Review access logs for generic user IDs

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.