



Data Enablement Plan (DEP) SME Training Day 1

April 2022
DTO & CSO

DEP | Welcome to the Data Enablement Plan

We are excited to have you here with us.

You are part of a program that will change the way TELUS views and manages data initiatives for the better.

Together, we will work together and learn, as we look to roll out the Data Enablement Plan across TELUS.

Thank you for being here!

- The DEP Project Team





Journey to Become a Data Enablement Plan Super Star!

Day 1 – Apr 7

Topic 1:
DEP & Process
Overview

Topic 2:
OneTrust
Navigation

Day 2 – Apr 11

Topic 3:
Process Deep
Dive

Day 3 – Apr 18

Topic 4:
Example
Walkthroughs

Outcome: Understanding your role in the Data Enablement Process

Journey to Become a Data Enablement Plan Super Star!

Day 1 – Apr 7

Topic 1:
DEP & Process
Overview

Day 2 – Apr 11

Topic 2:
OneTrust
Navigation

Day 3 – Apr 18

Topic 3:
Process Deep
Dive

Topic 4:
Example
Walkthroughs

Outcome: Understanding your role in the Data Enablement Process

DEP | What is the Data Enablement Plan?

Launched in Q4 2021, the Data Enablement Plan (DEP) empowers the business to be an active participant in the identification, mitigation and acceptance of risk when using data. The DEP generates a roadmap to enable the use of data for each initiative.

Key Features & Benefits



One front door streamlined questionnaire incorporates and replaces numerous existing processes, including the Privacy Impact Assessment and Secure by Design reviews.



Integrates the identification of risks associated with a DEP early in the process to ensure risks are addressed up-front in a project or initiative.



Agile, timely review is enabled through dedicated support from the DTO & CSO in a streamlined POD review process.



Designated **Business Data Stewards** are trained for improved upfront risk identification and documentation.



Technology-enabled, through the user-friendly OneTrust platform, which allows transparency, accountability and automation.

Together with the Business Data Stewards, our stretch goal is to roadmap 75% of DEPs in 2 weeks by year-end.

DEP | Key Players in the DEP Process



Business Data
Stewards



Business Deputies
(Optional Data Entry
Role)

DEP Questionnaire
Management



DEP SME (Privacy
Partners, CSO
Consultants & other
SMEs)

DEP Reviewers &
Risk Managers



POD Coordinator



POD members

POD Coordination &
Review



Risk Owners

Risk Acceptance &
Sign off

BDS certification path

Level 1 BDS accurately complete the Data Enablement Plan (DEP) and support their business with responsible data use.



Know your
data



Enable your
data



Working
together



Using
OneTrust



Complete 3
DEPs



CERTIFY
Level 1 BDS

SELF-SERVICE COURSE (45 minutes)

Know Your Data

Introductory course providing an overview of data governance, how the DEP facilitates best practices, roles and responsibilities, and the value provided to the business by the BDS. [Learn More.](#)

LAB - 45 Minutes

BDS Meet & Greet

SELF-SERVICE COURSE (45 minutes)

Enable Your Data

Protecting customer and team member privacy and security, understanding data sensitivity. [Learn More.](#)

LAB - 45 Minutes

Privacy & Security on the Case

SELF-SERVICE COURSE (45 minutes)

Working Together

Understanding successful collaboration with people, processes and technology to effectively govern data, and how to champion responsible data stewardship at TELUS. [Learn More.](#)

LAB - 45 Minutes

Data RISK

SELF-SERVICE COURSE (45 minutes)

Using OneTrust

Submitting DEPs for new initiatives and managing data risks using the OneTrust data governance platform. [Learn More.](#)

LAB - 45 Minutes

OneTrust

Summary



What you'll learn

Foundational privacy, security and data governance; DEP stakeholders; POD readiness and participation; Assessments and data risk management in OneTrust.



Courses

4



Labs

4








Completed DEPs

3

DEP Questionnaire Stages

- **In Progress:** BDS / Deputy is working on DEP and has not submitted yet
- **Under Review:** DEP has been submitted, BDS is working on the pre-POD tasks and also working with the DEP SME to review risks / gaps. Once all risks have been actioned, the BU Director will approve the DEP, moving it to the next stage
- **Implementation:** The Plan is approved by the BU Director. There may still be open tasks that need to be completed as part of the Plan, and are being monitored by the BDS
- **Completed:** Once all tasks and risk are closed, the BDS marks the DEP as complete

DEP Roadmap

-  **1 Info Requests** - Use when you need more information after reviewing a question in the DEP
-  **0 Notes** - Use to add any notes in the DEP. Notes have three visibility options: yourself, approvers, or everyone
-  **0 Comments** - The BDS uses comments to make statements that help add context to the DEP question
-  **4 Risk Flags** - Review potential risks/gaps that need to be assessed (auto-generated by the system)
-  **7 Tasks** - Activities that need to be completed by the BDS prior to POD (Pre-POD tasks) or prior to completion of the DEP (DEP tasks)

DEP | What is POD and When is it Required

The DEP POD is an advisory body of DEP SMEs from the Data & Trust Office and Chief Security Office.

The POD advisory body is used to discuss risks and uncertainties that cannot be resolved between the Business Data Steward (BDS) and their DEP SME. PODs are comprised of a cross-functional team that works collaboratively to achieve an outcome.

If it is determined that a POD is required, the BDS, with support from the DEP SME will complete *Section 15: POD Review* in the DEP questionnaire.

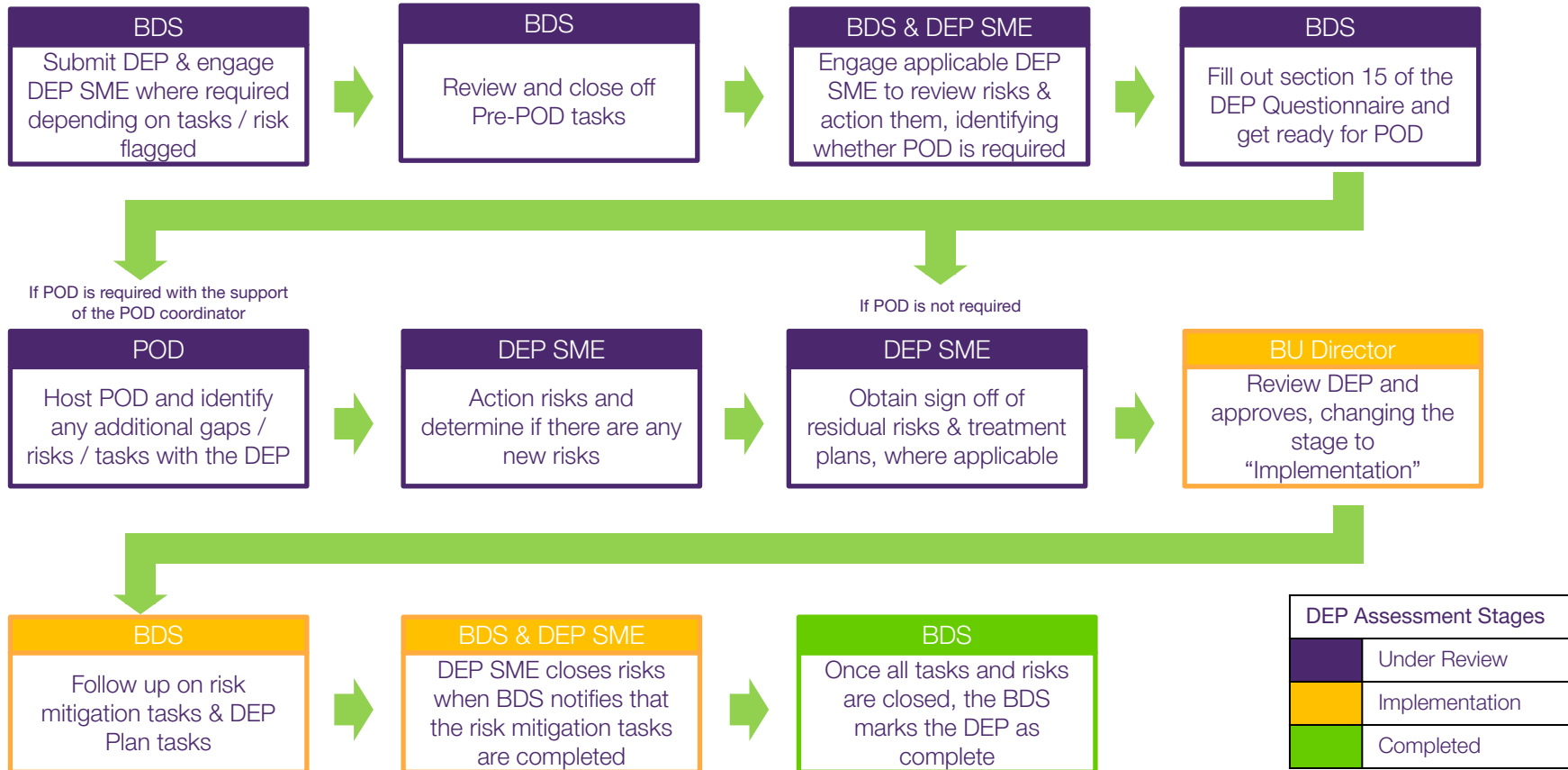
The BDS will reach out to the POD Coordinator, who will review and schedule the DEP. The BDS will then present the issues to the POD advisory body for resolution.

If the matter cannot be resolved in POD, the DTO may leverage Squad, comprised of the VP and Directors and/or their delegates within the Data & Trust Office. Squad may determine that the issue should be discussed at the Enterprise Data Council (EDC) and/or Executive Data Stewardship Steering Committee (EDS), leveraging TELUS' Data Governance organization.

Requirements before POD:

- 1) Completion of pre-POD tasks;
- 2) Closure of information requests; and
- 3) Review of flagged risks.

DEP | High Level Process



Journey to Become a Data Enablement Plan Super Star!

Day 1 – Apr 7

Topic 1:
DEP & Process
Overview

Topic 2:
OneTrust
Navigation

Day 2 – Apr 11

Topic 3:
Process Deep
Dive

Day 3 – Apr 18

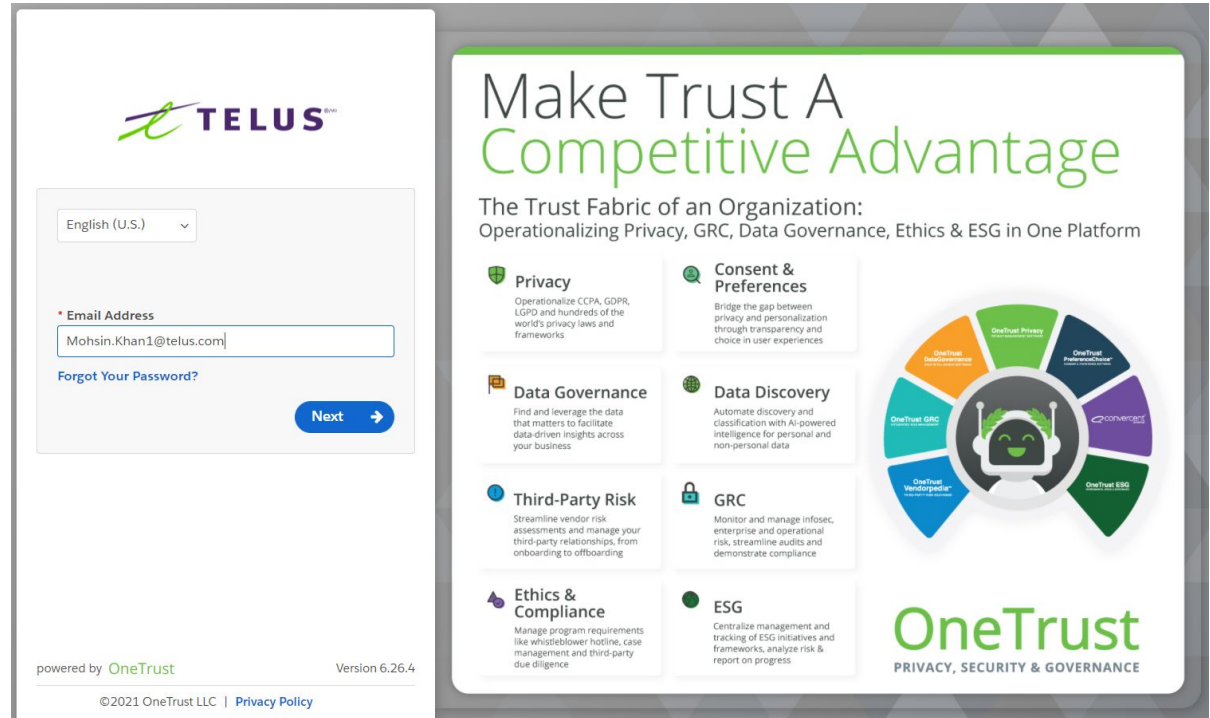
Topic 4:
Example
Walkthroughs

Outcome: Understanding your role in the Data Enablement Process

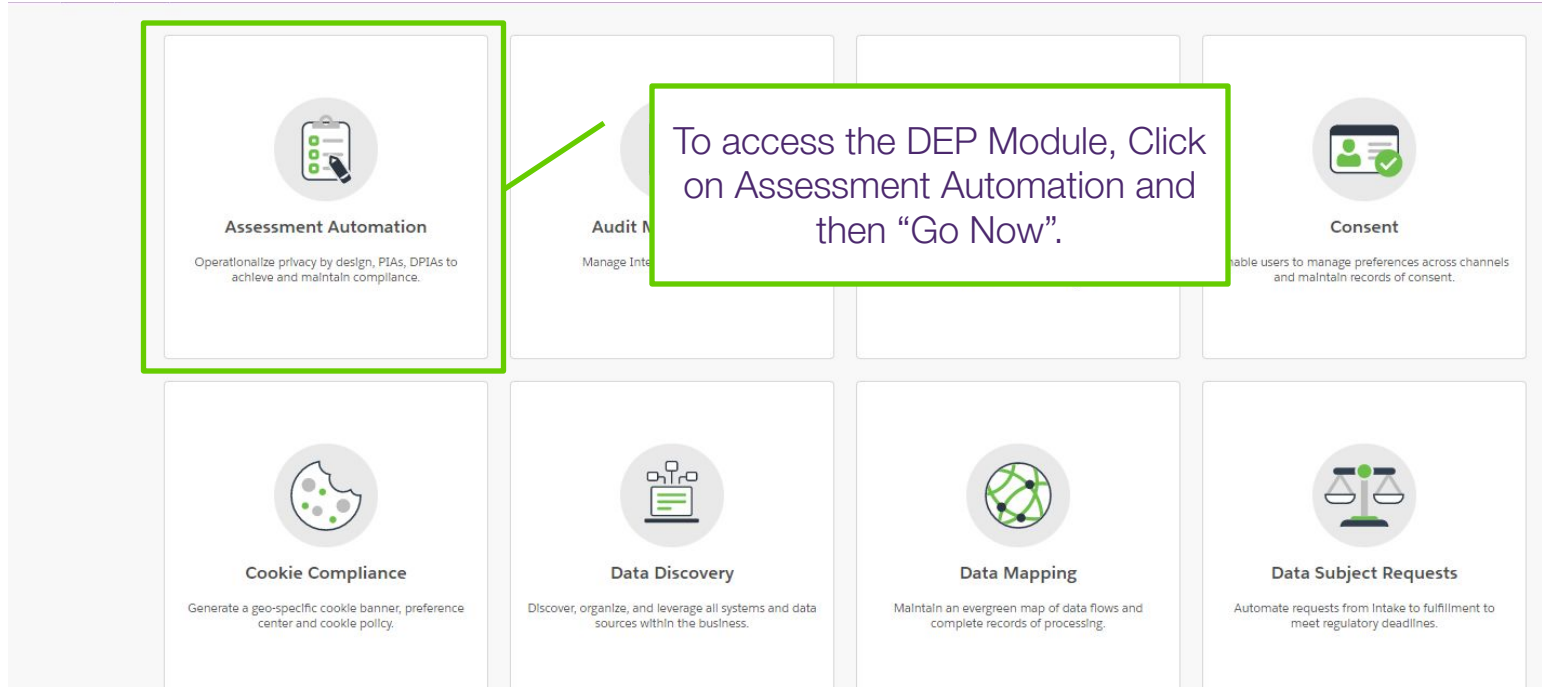
DEP | Logging into One Trust

Steps to access One Trust:

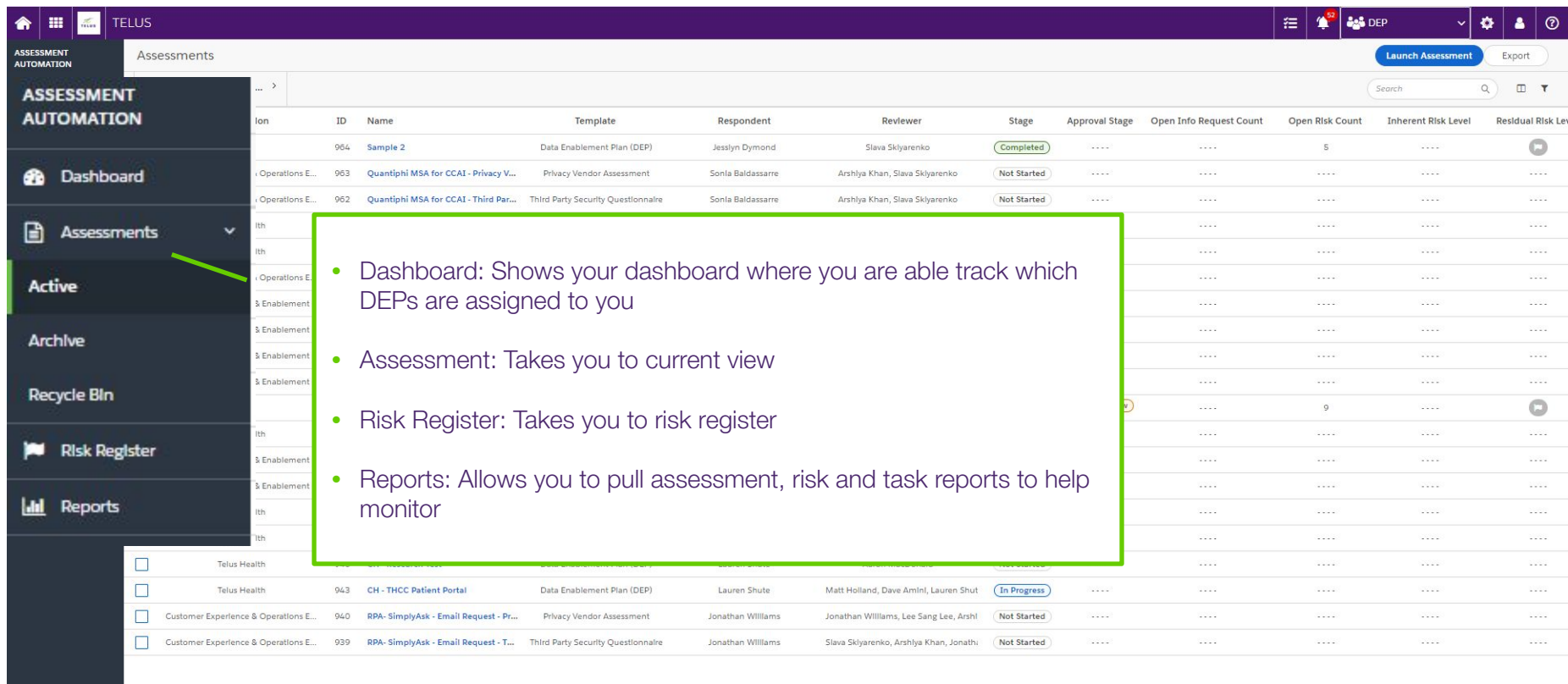
- Go to <https://telus.my.onetrust.com/> or [go/onetrust](#)
- Enter your TELUS email address.
- Click 'Next' (do NOT click 'Forgot Your Password' since we use SSO).



The image shows two side-by-side screenshots. The left screenshot is the OneTrust login page for TELUS. It features the TELUS logo at the top, a language dropdown set to 'English (U.S.)', an email address field containing 'Mohsin.Khan1@telus.com', a 'Forgot Your Password?' link, and a blue 'Next' button with a right arrow. At the bottom, it says 'powered by OneTrust' and 'Version 6.26.4', with a copyright notice '©2021 OneTrust LLC | Privacy Policy'. The right screenshot is a dashboard titled 'Make Trust A Competitive Advantage'. It describes OneTrust as 'The Trust Fabric of an Organization' for operationalizing Privacy, GRC, Data Governance, Ethics & ESG. The dashboard includes a grid of icons for Privacy, Consent & Preferences, Data Governance, Data Discovery, Third-Party Risk, Ethics & Compliance, GRC, and ESG, each with a brief description. A central circular graphic shows a stylized face with a headset, surrounded by various OneTrust product logos like OneTrust Privacy, OneTrust GRC, OneTrust Vendorpedia, OneTrust ESG, OneTrust Consent, and OneTrust Data Governance. The bottom of the dashboard features the 'OneTrust' logo and the tagline 'PRIVACY, SECURITY & GOVERNANCE'.



DEP | DEP Assessment View – Menu



ASSESSMENT AUTOMATION

Assessments

Launch Assessment Export

Search

ID	Name	Template	Respondent	Reviewer	Stage	Approval Stage	Open Info Request Count	Open Risk Count	Inherent Risk Level	Residual Risk Level
954	Sample 2	Data Enablement Plan (DEP)	Jesslyn Dymond	Slava Skiyarenko	Completed	5
953	Quantiphi MSA for CCAI - Privacy V...	Privacy Vendor Assessment	Sonia Baldassarre	Arshya Khan, Slava Skiyarenko	Not Started
952	Quantiphi MSA for CCAI - Third Par...	Third Party Security Questionnaire	Sonia Baldassarre	Arshya Khan, Slava Skiyarenko	Not Started
943	CH - THCC Patient Portal	Data Enablement Plan (DEP)	Lauren Shute	Matt Holland, Dave Amiri, Lauren Shut	In Progress
940	RPA - SimplyAsk - Email Request - Pr...	Privacy Vendor Assessment	Jonathan Williams	Jonathan Williams, Lee Sang Lee, Arshi	Not Started
939	RPA - SimplyAsk - Email Request - T...	Third Party Security Questionnaire	Jonathan Williams	Slava Skiyarenko, Arshya Khan, Jonath	Not Started

- Dashboard: Shows your dashboard where you are able track which DEPs are assigned to you
- Assessment: Takes you to current view
- Risk Register: Takes you to risk register
- Reports: Allows you to pull assessment, risk and task reports to help monitor

DEP| DEP Assessment View – Main View

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Assessment Workflow

Assessment Results

Integrations

Email Templates

Automation Rules

Settings

Assessments

One Trust Assessment VI... >

Launch Assessment

Export

Search

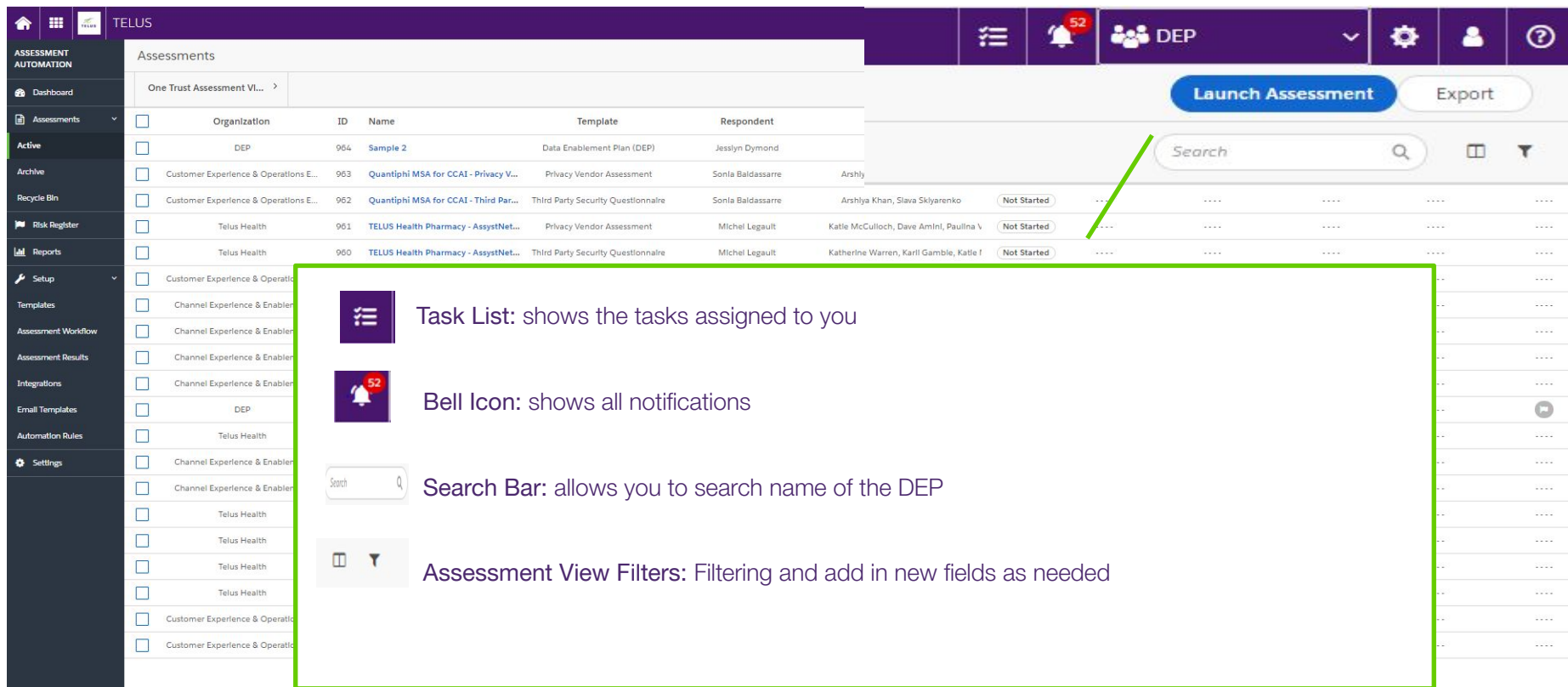
	Organization	ID	Name	Template	Respondent	Reviewer	Stage	Approval Stage	Open Info Request Count	Open Risk Count	Inherent Risk Level	Residual Risk Level
<input type="checkbox"/>	DEP	954	Sample 2	Data Enablement Plan (DEP)	Jesslyn Dymond	Slava Sklyarenko	Completed	----	----	5	----	
<input type="checkbox"/>	Customer Experience & Operations E...	953	Quantiphi MSA for CCAI - Privacy V...	Privacy Vendor Assessment	Sonia Baldassarre	Arshlya Khan, Slava Sklyarenko	Not Started	----	----	----	----	
<input type="checkbox"/>	Customer Experience & Operations E...	952	Quantiphi MSA for CCAI - Third Par...	Third Party Security Questionnaire	Sonia Baldassarre	Arshlya Khan, Slava Sklyarenko	Not Started	----	----	----	----	
<input type="checkbox"/>	Telus Health	951	TELUS Health Pharmacy - AssystNet...	Privacy Vendor Assessment	Michel Legault	Katie McCulloch, Dave Amini, Paulina V...	Not Started	----	----	----	----	
<input type="checkbox"/>	Telus Health	950	TELUS Health Pharmacy - AssystNet...	Third Party Security Questionnaire	Michel Legault							
<input type="checkbox"/>	Customer Experience & Operations E...	959	ACX - YNAW - Third Party Google Dr...	Data Enablement Plan (DEP)	Stephanie Niles, Jonathan...							
<input type="checkbox"/>	Channel Experience & Enablement	957	Fox/Atlas M&H Acceleration	Data Enablement Plan (DEP)	Julie McGranahan							
<input type="checkbox"/>	Channel Experience & Enablement	956	Evolving Retail Experience	Data Enablement Plan (DEP)	Julie McGranahan							
<input type="checkbox"/>	Channel Experience & Enablement	955	Best Buy on HSD	Data Enablement Plan (DEP)	Julie McGranahan							
<input type="checkbox"/>	Channel Experience & Enablement	954	Wordly	Data Enablement Plan (DEP)	Julie McGranahan							
<input type="checkbox"/>	DEP	953	Sample	Data Enablement Plan (DEP)	Jesslyn Dymond							
<input type="checkbox"/>	Telus Health	952	CH - ITECHART	Privacy Vendor Assessment	David.DeSantis@itech...							
<input type="checkbox"/>	Channel Experience & Enablement	951	mHub - Privacy Vendor Assessment	Privacy Vendor Assessment	Julie McGranahan							
<input type="checkbox"/>	Channel Experience & Enablement	950	mHub - Third Party Security Quest...	Third Party Security Questionnaire	Julie McGranahan							
<input type="checkbox"/>	Telus Health	949	CH - Ebb Patient App - Privacy Vend...	Privacy Vendor Assessment	Kassandra Fournier							
<input type="checkbox"/>	Telus Health	948	CH - Ebb Patient App - Third Party S...	Third Party Security Questionnaire	Kassandra Fournier							
<input type="checkbox"/>	Telus Health	946	CH - Research Test	Data Enablement Plan (DEP)	Lauren Shute							
<input type="checkbox"/>	Telus Health	943	CH - THCC Patient Portal	Data Enablement Plan (DEP)	Lauren Shute							
<input type="checkbox"/>	Customer Experience & Operations E...	940	RPA - SimplyAsk - Email Request - Pr...	Privacy Vendor Assessment	Jonathan Williams							
<input type="checkbox"/>	Customer Experience & Operations E...	939	RPA - SimplyAsk - Email Request - T...	Third Party Security Questionnaire	Jonathan Williams							

Note: Select "Name" to open up questionnaire

Assessment view includes:

- Respondent (who is entering in information which would be a BDS or a Deputy)
- Reviewer (could be the DEP SME, Director or the BDS)
- Approval Stage (Not Started, In Progress, Under Review, Implementation & Completed)
- Template (if it is a DEP or another assessment)
- # of Open Info Requests
- # of Open Risks
- Inherent and Residual Risk Levels
- Assessment Result
- Date Created & many others to help you understand the state of the DEP

DEP| DEP Assessment View – Drop Downs



The screenshot displays the TELUS DEP Assessment View interface. The top navigation bar includes a home icon, a grid icon, and the TELUS logo. The main header area contains a 'Launch Assessment' button and an 'Export' button. Below the header is a table of assessments with columns for Organization, ID, Name, Template, and Respondent. A green box highlights four key features:

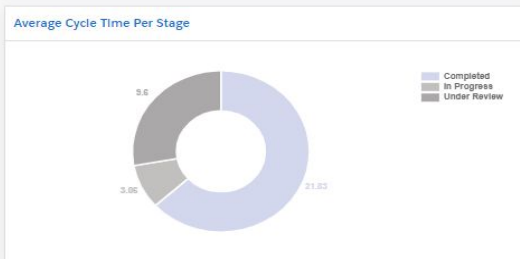
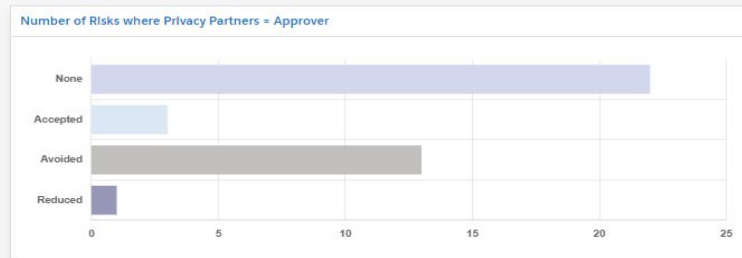
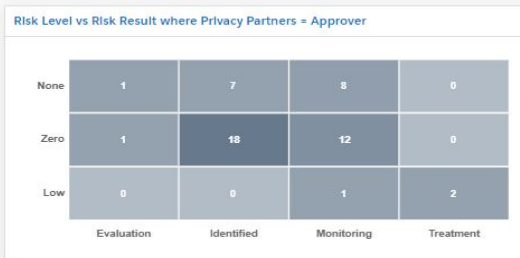
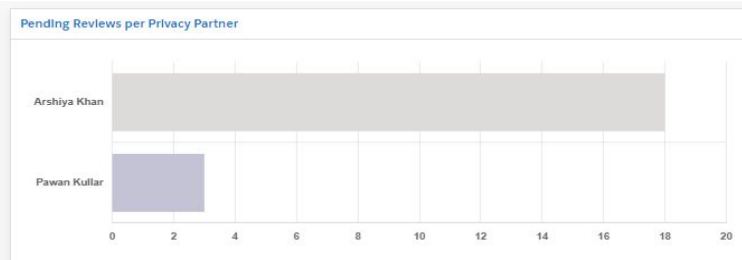
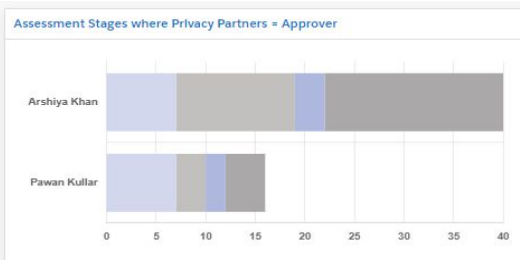
- Task List:** shows the tasks assigned to you (indicated by a list icon).
- Bell Icon:** shows all notifications (indicated by a bell icon with a red '52' badge).
- Search Bar:** allows you to search name of the DEP (indicated by a search input field).
- Assessment View Filters:** Filtering and add in new fields as needed (indicated by a filter icon).

Organization	ID	Name	Template	Respondent
DEP	954	Sample 2	Data Enablement Plan (DEP)	Jesslyn Dymond
Customer Experience & Operations E...	953	Quantiphi MSA for CCAI - Privacy V...	Privacy Vendor Assessment	Sonla Baldassarre
Customer Experience & Operations E...	952	Quantiphi MSA for CCAI - Third Par...	Third Party Security Questionnaire	Sonla Baldassarre
Telus Health	951	TELUS Health Pharmacy - AssystNet...	Privacy Vendor Assessment	Michel Legault
Telus Health	950	TELUS Health Pharmacy - AssystNet...	Third Party Security Questionnaire	Michel Legault

Dashboard View highlights the following:

- Pending DEPs which require your review
- Risk Metric including risk levels and risk results
- Cycle time of DEPs
- Volume metrics

With the dashboard, you will be manage your workload and identify problem areas.



DEP | DEP Questionnaire View – Questions Menu

Data Enablement Plan (DEP)

Review

00415...

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

4 - Data Quality

5 - Data Lifecycle

6 - Privacy by Design

7 - Health Privacy

8 - Data Ethics

9 - Responsible AI

10 - Secure by Design

11 - PCI DSS

12 - Data Solutions Review

13 - Partner

14 - TELUS Stakeholders

15 - POD Review

ome to the Data Enablement Plan (DEP).

goal is to help maximize the success of your initiative for TELUS through transparency and collaboration. The DEP empowers the business to be an active participant in the identification, mitigation and acceptance of risk when using data. Use this form to learn about the relevant and specific roadmap for your initiative.

a Data Enablement Plan is required for the design of, or changes to, products, services, initiatives and systems that involve access to, collection, storage, use or disclosure of data.

a Data Enablement Plan is a living document, you can leverage it for end-to-end lifecycle management, and it is designed to allow for easy reassessments as your project progresses.

DEP replaces the existing PIA / SoD / HPIA / SIA process that is managed in the RSA Archer and Sherpa tools.

Examples of when to use the DEP:

- When data will be transmitted
- Migrating data to the cloud
- Building a new survey for collection
- Integrating or sharing data
- Developing new patient or client experiences
- Marketing campaigns that require data
- Adoption of new tools that require data
- Collecting, using or disclosing data
- Introducing new access controls
- When integrating or augmenting data

Questions or more information?

0 Approvers

Send Back

<>

Finish Review

The DEP has 15 sections. Depending on selections made by the BDS, some or all sections may be required. Each section has a range of multiple choice questions, which the BDS will answer. In the event the BDS is unable to answer a question, a task will be created for the BDS to follow up with the DEP SME.

TELUS Proprietary

18

DEP | DEP Questionnaire View - Roadmap

TELUS insights Test

Under Review

0

0

4

16

15

...

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

4 - Data Quality

5 - Data Lifecycle

6 - Privacy by Design

7 - Health Privacy

8 - Data Ethics

9 - Responsible AI

10 - Secure by Design

11 - POC OSS

12 - Data Solutions Review

13 - Partner

14 - TELUS Stakeholders

15 - POD Review

Welcome to the Data Enablement Plan (DEP).

Our goal is to help maximize the success of your initiative for TELUS through transparency and collaboration. The DEP empowers the business to be an a specific roadmap for your initiative.

A Data Enablement Plan is required for the design of, or changes to, products, services, initiatives and systems that involve access to, collection, storage, use or disclosure of data.

As the Data Enablement Plan is a living document, you can

The DEP replaces the existing PIA / SdD / HPIA / SIA process

Some examples of when to use the Data Enablement Plan p

- When data will be transmitted through a new network
- Migrating data to the cloud;
- Building a new survey for customers;
- Integrating or sharing data with a 3rd Party;
- Developing new patient or customer portals;
- Developing new methods for patient or customer authentication
- Marketing campaigns that target customers using geo
- Adoption of new tools that collect, use or disclose customer data
- Collecting, using or disclosing new data elements related to
- Introducing new access controls to a system including
- When integrating or augmenting existing datasets for

For questions or more information, see go/dep.

View Approvers

Send Back

Roadmap Menu

0

Info Requests

- Use when you need more information after reviewing a question in the DEP. There may be multiple requests per question.

0

Notes

- Use to add any notes you want documented in the DEP.

4

Comments

- The BDS uses comments to make statements that help add context to the DEP question

16

Risk Flags

- Review for potential risks / gaps that need to be assessed (auto-generated by the system).

15

Tasks

- Activities that need to be completed by the BDS prior to POD (Pre-POD tasks) or prior to completion of the DEP (DEP tasks)

<

>

Finish Review



ASSESSMENT AUTOMATION

Dashboard
Assessments
Active
Archive
Recycle Bin
Risk Register
Reports
Setup
Templates
Assessment Workflow
Assessment Results
Integrations
Email Templates
Automation Rules
Settings

TELUS Insights Test

Under Review

6.7

Exception to consent

Go to Question

Details

Identification

Risk ID

1111

Risk Statement

There is a risk an exception in the legislation is not applied appropriately which may lead to customer complaints resulting in a regulatory investigation, damage to our brand, and/or loss of customer trust.

Source Reference

TELUS Insights Test

PCI

SOX

Date Created

04/04/2022

PIA Reference # (If Applicable)

GRA created

No

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Risk Manager

Mohsin Khan

Source of Risk Identification

DEP

Privacy

Yes

CRTC

Date Closed

--/--/----

CSO Residual Risk Assessment (RRA) # (If Applicable)

Organization

Data Strategy & Enablement

Assessment

Risks

All risks

6.7 Privacy Risk: Exception Consent

8.11 Pod review - Brand Impact

8.9 Pod Review - Media Impact

8.6 Pod review - Harms

8.5 Pod Review - Review grouping and segmentation

8.3 Pod Review - Surveillance

2.18 POD Review: Data Access

10.18 POD Review: Security Analysis

10.5 POD Review: Access review

6.22 POD Review: TELUS privacy documents may need to be updated.

6.20 POD Review: Privacy by Design

2.10

Identifies the question where the flag was raised based on BDS input.

TELUS Proprietary

20



ASSESSMENT AUTOMATION

Dashboard
Assessments
Active
Archive
Recycle Bin
Risk Register
Reports
Setup
Templates
Assessment Workflow
Assessment Results
Integrations
Email Templates
Automation Rules
Settings

TELUS Insights Test
Under Review

Welcome to the DEP
Exception to consent
Go to Question

6.7

1 - Intake
2 - Overview
3 - Metadata Management
4 - Data Quality
5 - Data Lifecycle
6 - Privacy by Design
8 - Data Ethics
9 - Responsible AI
10 - Secure by Design
12 - Data Solutions Review
13 - Partner
14 - TELUS Stakeholders
15 - POO Review

The DEP replaces t
Some examples of
When data v
Migrating da
Building a ne
Integrating o
Developing i
Developing i
Marketing ci
Adoption of
Collecting, u
Introducing
When Infigh

IDENTIFICATION
ASSESSMENT
RESPONSE
MONITOR
CLOSED

Identification

Risk ID
1111

Risk Statement
There is a risk an exception in the legislation is n customer complaints resulting in a regulatory In customer trust.

Source Reference
TELUS Insights Test

PCI

SOX

* Date Created
04/04/2022

PIA Reference # (If Applicable)

* GRA created
No

Assessment

Risks
All risks

Each Risk / Gap has 5 stages that correspond to a section in the form below. Please note, you have to manually change the stage (system limitation).

- **Identification:** Risk Name, Risk Statement and any other identifying information
- **Assessment:** Risk Assessment, Treatment Plan Summary and mitigation tasks
- **Response:** Risk Result (accepted, mitigated, avoided, shared, not applicable or monitored by GRA)
- **Monitor:** When there are opens tasks corresponding to the risk
- **Closed:** All tasks are closed



ASSESSMENT AUTOMATION

TELUS Insights Test

Under Review

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Assessment Workflow

Assessment Results

Integrations

Email Templates

Automation Rules

Settings

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

4 - Data Quality

5 - Data Lifecycle

6 - Privacy by Design

8 - Data Ethics

9 - Responsible AI

10 - Secure by Design

12 - Data Solutions Review

13 - Partner

14 - TELUS Stakeholders

15 - POO Review

Welcome to the D

Our goal is to help specific roadmap f

A Data Enablement

As the Data Enable

The DEP replaces t

Some examples of

For questions or m

6.7

Exception to consent

Go to Question

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Details

Tasks

Controls

Comments

Attachments

More

Risk ID

1111

Risk Statement

There is a risk an exception in the legislation is customer complaints resulting in a regulatory in customer trust.

Source Reference

TELUS Insights Test

PCI

SOX

* Date Created

04/04/2022

PIA Reference # (If Applicable)

* GRA created

No

Assessment

Risks

All risks

6.7 Privacy Risk: Exception Consent

9.8 Pod review - explainability

10.9 No control transfer system

Details: Main view of the risk/gap section

Tasks: Space to create tasks related to the mitigation of a risk/gap. This section is important as it allows us & the BDS to track progress on a solution. Example: follow up with project manager to determine if firewall solution is in place.

Controls: Not used in phase 2.

Comments: used when there are multiple risks signed off by one email. Can be used to indicate which risk has an attachment to help simplify the process.

Attachments: allow for you to attach email approvals from VPs / Directors based on the DRM framework

ASSESSMENT AUTOMATION

TELUS Insights Test

Under Review

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Assessment Workflow

Assessment Results

Integrations

Email Templates

Automation Rules

Settings

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

4 - Data Quality

5 - Data Lifecycle

6 - Privacy by Design

8 - Data Ethics

9 - Responsible AI

10 - Secure by Design

12 - Data Solutions Review

13 - Partner

14 - TELUS Stakeholders

15 - POO Review

Welcome to the D

Exception to consent

Go to Question

6.7

IDENTIFICATION

ASSESSMENT

Details

Tasks

Identification

Risk ID

1111

Risk Statement

There is a risk an exception in the legislation is not applied appropriately which may customer complaints resulting in a regulatory investigation, damage to our brand, and customer trust.

Source Reference

TELUS Insights Test

PCI

SOX

* Date Created

04/04/2022

PIA Reference # (If Applicable)

* GRA created

No

Assessment

6.7

Exception to consent

Go to Question

IDENTIFICATION

ASSESSMENT

Details

Tasks

Identification

Risk ID

1111

Risk Statement

There is a risk an exception in the legislation is not applied appropriately which may customer complaints resulting in a regulatory investigation, damage to our brand, and customer trust.

Source Reference

TELUS Insights Test

PCI

SOX

* Date Created

04/04/2022

PIA Reference # (If Applicable)

* GRA created

No

Assessment

6.7

Exception to consent

Go to Question

IDENTIFICATION

ASSESSMENT

Details

Tasks

Identification

Risk ID

1111

Risk Statement

There is a risk an exception in the legislation is not applied appropriately which may customer complaints resulting in a regulatory investigation, damage to our brand, and customer trust.

Source Reference

TELUS Insights Test

PCI

SOX

* Date Created

04/04/2022

PIA Reference # (If Applicable)

* GRA created

No

Assessment

There are 3 sections in the risk form that are important to the DEP SME:

Identification: Risk Name and Risk Statement

Assessment: Inherent Risk Assessment, Treatment Plan Summary and Residual Risks Assessment.

Response (Risk Acceptance):

Risk Result:

- Accepted:** When a VP / Director accepts a residual risk.
- Mitigated:** Mitigating actions have been put in-place (current, not ongoing) to reduce risk down to a point where risk rating is below TELUS' risk threshold.
- Avoided:** The activity that introduces/would introduce the risk has been foregone or abandoned.
- Shared:** The risk and activity that introduces the risk is taken on and owned by multiple business units.
- Not Applicable:** When the risk is deemed to be no longer relevant or applicable after review.
- Monitored by GRA:** This is a special case for CSO (more details in day 2)

Note: Please ignore all the remaining sections which are only for the GRA team.

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Assessment V

Assessment R

Integrations

Email Template

Automation S

Settings

TELUS insights Test

Under Review

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

Welcome to the Data Enablement Plan (DEP).

Our goal is to help maximize the success of your Initiative for TELUS through transparency and collaboration. The DEP empowers the business to create a specific roadmap for your Initiative.

A Data Enablement Plan is required for the design of, or changes to, products, services, Initiatives and systems that involve access to, collection, use, storage, and/or processing of personal information.

As the Data Enablement Plan is a living document, you can leverage it for end to end lifecycle management, and it is designed to allow for ongoing updates and changes.

Tasks are broken into two categories.

- Pre-POD Tasks: Tasks that are required before POD. These can range from clarifying aspects with the DEP SME to completing additional work required to provide substance to the DEP. These tasks are a guiding point to start the discussion.
- DEP Task: Those required to enable the data as part of the plan and are required to mark the DEP as complete.

BDS have the ability to close these tasks.

0

0

4

16

14

Closed

Reopen Task

DEP Task - Business Definitions

Assignee: Elena Novas

Priority: Medium

Collaborators: - - - -

Deadline: 03/25/2022

Description: Please refer to Q3.1 Business Definitions. This task is part of the plan to enable data. This task is not required for pod. Use the template

Attachments: 0

Drop attachment or click to browse. Files larger than 2 GB are not supported. Upload File

Comments: No Comments

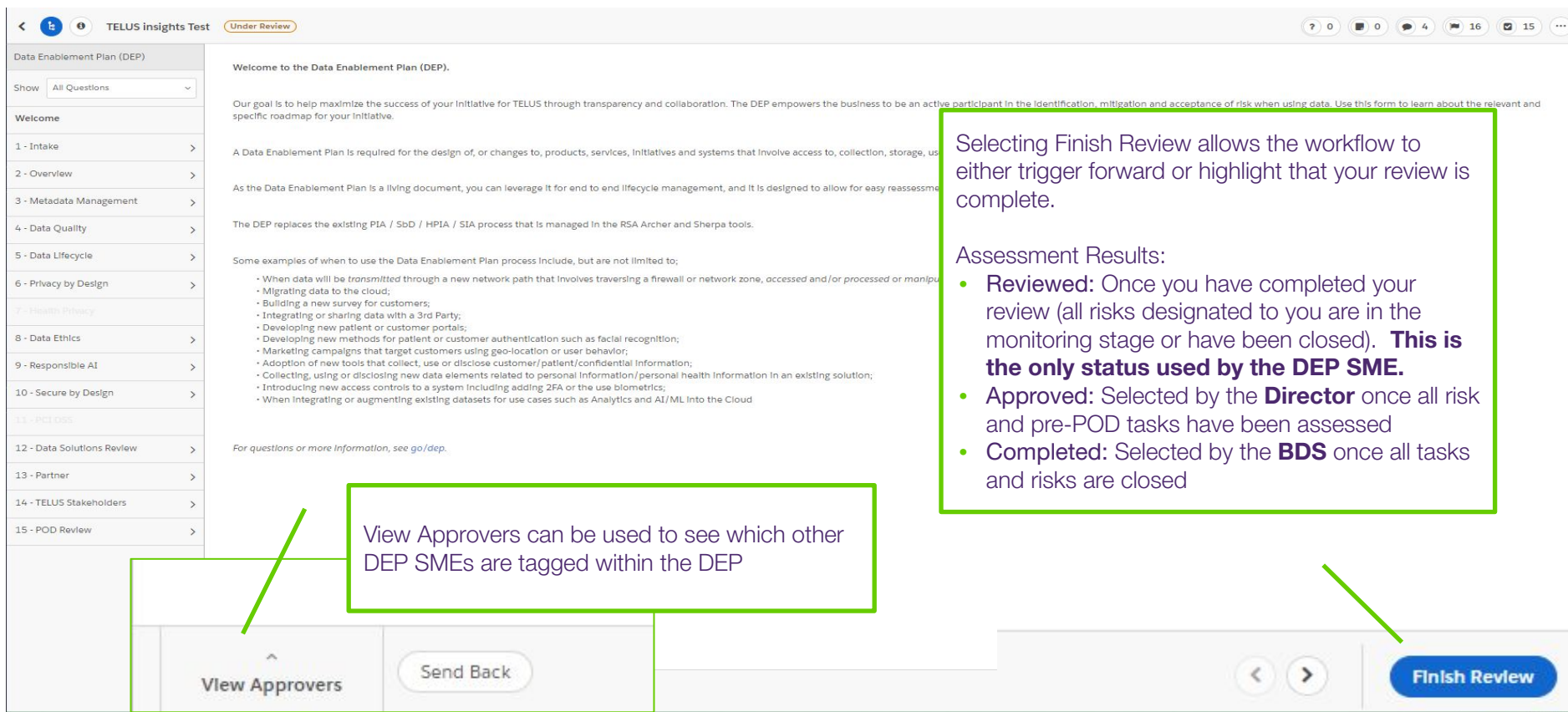
Tasks

All

Add

- DEP Task - Business Definitions. Please refer to Q3.1 Business Definitions. This task is part of the plan to enable data.
- DEP Task - Network design doc. Please refer to Q10.17 Network design doc. This task is part of the plan to enable data.
- DEP Task - Privacy training. Please refer to Q6.21 Privacy training. This task is part of the plan to enable data.
- Pre-pod Task - Roles. Please refer to Q2.19 Roles. Required to complete the Data Enablement
- Pre-pod Task - Data type. Please refer to Q2.4 Data type. Required to complete the Data Enablement
- DEP Task - Outside Canada DNTL. Please refer to Q 2.28 DNTL & 2.22 Jurisdiction
- DEP Task - Scope - Data Solution Review. Please refer to Q2.10 Scope. This task is part of the plan to enable data. This
- Pre-pod Task - Central logging. Please refer to Q10.9 Central logging. Required to complete the Data Enablement
- DEP Task - DSR Review. Please refer to Q2.10 Scope. This task is part of the plan to enable data.
- DEP Task - New data. Please refer to Q2.5 New data. This task is part of the plan to enable data.

DEP | DEP Questionnaire View – Finish Reviews



TELUS insights Test Under Review

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

4 - Data Quality

5 - Data Lifecycle

6 - Privacy by Design

7 - Health Privacy

8 - Data Ethics

9 - Responsible AI

10 - Secure by Design

11 - POC DSS

12 - Data Solutions Review

13 - Partner

14 - TELUS Stakeholders

15 - POD Review

Welcome to the Data Enablement Plan (DEP).

Our goal is to help maximize the success of your initiative for TELUS through transparency and collaboration. The DEP empowers the business to be an active participant in the identification, mitigation and acceptance of risk when using data. Use this form to learn about the relevant and specific roadmap for your initiative.

A Data Enablement Plan is required for the design of, or changes to, products, services, initiatives and systems that involve access to, collection, storage, use, or disposal of data.

As the Data Enablement Plan is a living document, you can leverage it for end-to-end lifecycle management, and it is designed to allow for easy reassessment.

The DEP replaces the existing PIA / SoD / HPIA / SIA process that is managed in the RSA Archer and Sherpa tools.

Some examples of when to use the Data Enablement Plan process include, but are not limited to:

- When data will be transmitted through a new network path that involves traversing a firewall or network zone, accessed and/or processed or manipulated.
- Migrating data to the cloud;
- Building a new survey for customers;
- Integrating or sharing data with a 3rd Party;
- Developing new patient or customer portals;
- Developing new methods for patient or customer authentication such as facial recognition;
- Marketing campaigns that target customers using geo-location or user behavior;
- Adoption of new tools that collect, use or disclose customer/patient/confidential information;
- Collecting, using or disclosing new data elements related to personal information/personal health information in an existing solution;
- Introducing new access controls to a system including adding 2FA or the use of biometrics;
- When integrating or augmenting existing datasets for use cases such as Analytics and AI/ML into the Cloud.

For questions or more information, see [go/dep](#).

View Approvers

Send Back

Finish Review

Selecting Finish Review allows the workflow to either trigger forward or highlight that your review is complete.

Assessment Results:

- Reviewed:** Once you have completed your review (all risks designated to you are in the monitoring stage or have been closed). **This is the only status used by the DEP SME.**
- Approved:** Selected by the **Director** once all risk and pre-POD tasks have been assessed
- Completed:** Selected by the **BDS** once all tasks and risks are closed

Risk Register											
DEP Data Risk Managem... >											
Search...											
	<input type="checkbox"/>	Risk ID	Risk Owners	Risk Manager	Source Reference	Risk Title	Inherent Risk Level	Residual Risk Level	Stage	Risk Result (DEP only)	Result
Active	<input type="checkbox"/>	1110	----	----	Sample 2	Pod review - Brand impact	----	----	Evaluation	----	----
Archive	<input type="checkbox"/>	1109	----	----	Sample 2	Pod Review - New information to review	----	----	Identified	----	----
Recycle Bin	<input type="checkbox"/>	1108	----	----	Sample 2	POD Review: Access review	Zero	Zero	Identified	----	----
Risk Register	<input type="checkbox"/>	1107	----	----	Sample 2	POD Review: Reasonableness	Zero	Zero	Identified	----	----
Reports	<input type="checkbox"/>	1106	----	----	Sample 2	POD Review: Data provided by a third party.	Zero	Zero	Identified	----	----
Setup	<input type="checkbox"/>	1105	----	----	Sample	Pod review - Brand impact	----	----	Identified	----	----
Templates	<input type="checkbox"/>	1104	----	----						----	----
Assessment Workflow	<input type="checkbox"/>	1103	----	----						----	----
Assessment Results	<input type="checkbox"/>	1102	----	----						----	----
Integrations	<input type="checkbox"/>	1101	----	----						----	----
Email Templates	<input type="checkbox"/>	1100	----	----						----	----
Automation Rules	<input type="checkbox"/>	1099	----	----						----	----
Settings	<input type="checkbox"/>	1098	----	----						----	----
	<input type="checkbox"/>	1097	----	----						----	----
	<input type="checkbox"/>	1096	----	----						----	----
	<input type="checkbox"/>	1095	----	----						----	----
	<input type="checkbox"/>	1094	----	----						----	----
	<input type="checkbox"/>	1093	----	----						----	----
	<input type="checkbox"/>	1092	----	----						----	----

Note: select the risk ID to open a risk or the source reference to open up the DEP.

Risk Register has the following key fields:

- Risk ID
- Risk Owner (Director, VP or ELT) & Risk Manager (you)
- Risk Title: Name of the risk and what type (Security, Privacy etc.)
- Inherent & Residual Risk
- Risk Result (DEP only): these include accepted, mitigated, avoided, shared, not applicable or monitored by GRA.

DEP | Asks for the DEP SME

Our Ask: Support the roll out of DEP within TELUS by advocating for the DEP and supporting BDS as they embark on their journey

Our ask

Access the [test environment](#) and create a test DEP, and action the risks and tasks associated to that DEP. Provide your [feedback here](#).

What's next?

1

Attend the next DEP training (Apr 11) which will walk through the process in more detail.

2

Support BDS as they learn the new tool and process- there will be a learning curve.

3

Share your ideas and feedback with the project team early and often to help us (Jesslyn, Elena and Mohsin) quickly action any suggestions as roll-out continues in Q2 and Q3.

Visit [go/dep](#) for more information. Check out the [DEP Primer](#) slides for the basics.

let's make the future friendly™



Data Enablement Plan (DEP) SME Training Day 2

April 2022
DTO & CSO

Journey to Become a Data Enablement Plan Super Star!

Day 1 – Apr 7

Topic 1:
DEP & Process
Overview

Topic 2:
OneTrust
Navigation

Day 2 – Apr 11

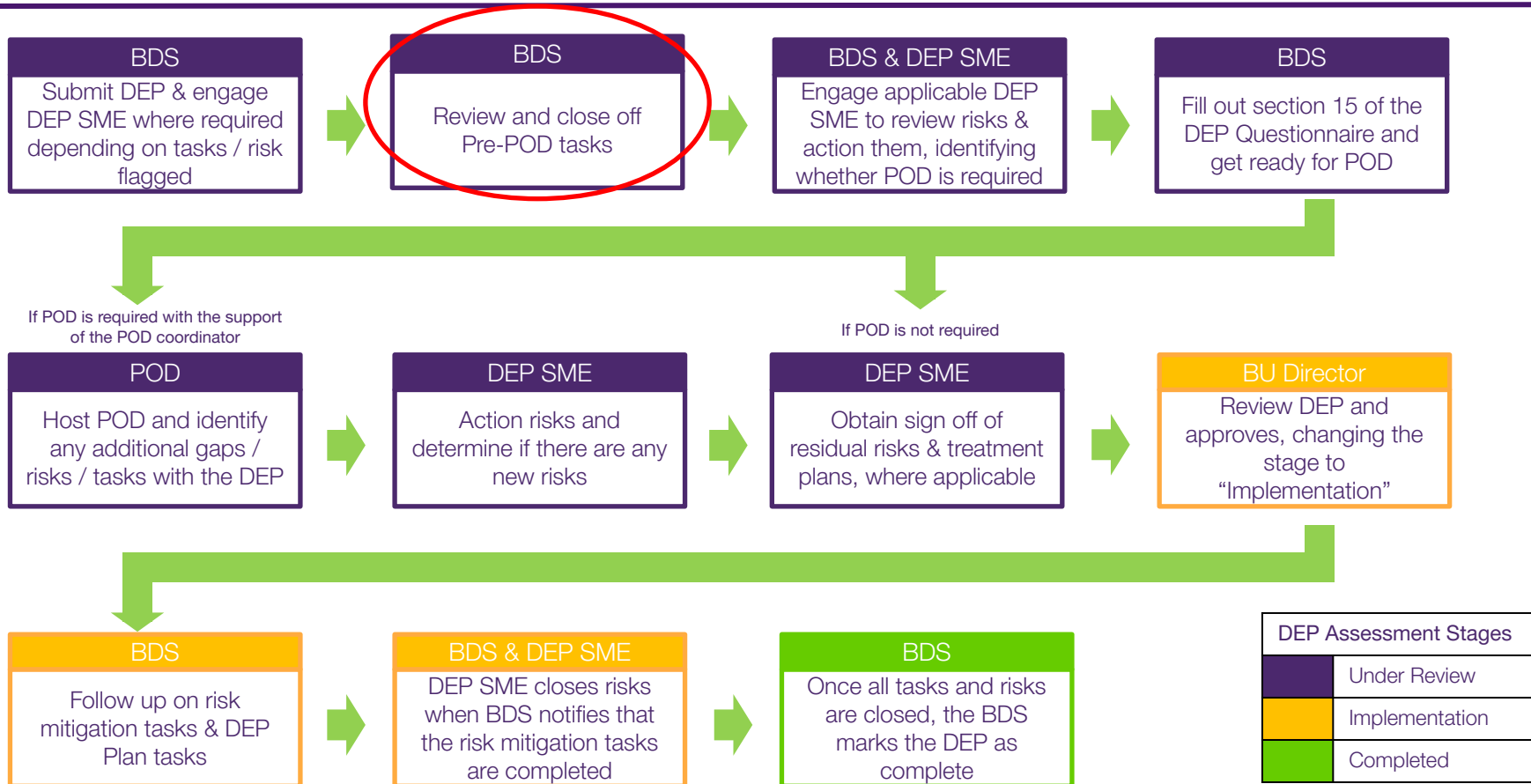
Topic 3:
Process Deep
Dive

Day 3 – Apr 18

Topic 4:
Example
Walkthroughs

Outcome: Understanding your role in the Data Enablement Process

DEP | High Level Process - Tasks



ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Assessment V

Assessment R

Integrations

Email Template

Automation S

Settings

TELUS insights Test

Under Review

Data Enablement Plan (DEP)

Show All Questions

Welcome

1 - Intake

2 - Overview

3 - Metadata Management

Welcome to the Data Enablement Plan (DEP).

Our goal is to help maximize the success of your Initiative for TELUS through transparency and collaboration. The DEP empowers the business specific roadmap for your Initiative.

A Data Enablement Plan is required for the design of, or changes to, products, services, Initiatives and systems that involve access to, collection and/or processing of personal information.

As the Data Enablement Plan is a living document, you can leverage it for end to end lifecycle management, and it is designed to allow for ongoing updates.

Tasks are broken into two categories.

- Pre-POD Tasks: Tasks that are required before POD. These can range from clarifying aspects with the DEP SME to completing additional work required to provide substance to the DEP. These tasks are a guiding point to start the discussion.
- DEP Task: Tasks that are required to enable the data as part of the plan and are required to mark the DEP as complete.

BDS have the ability to close these tasks.

0

0

4

16

14

Closed

Reopen Task

DEP Task - Business Definitions

Assignee: Elena Novas

Priority: Medium

Collaborators: - - - -

Deadline: 03/25/2022

Description: Please refer to Q3.1 Business Definitions. This task is part of the plan to enable data. This task is not required for pod. Use the template

Attachments: 0

Drop attachment or click to browse. Files larger than 2 GB are not supported. Upload File

Comments: No Comments

Tasks

All

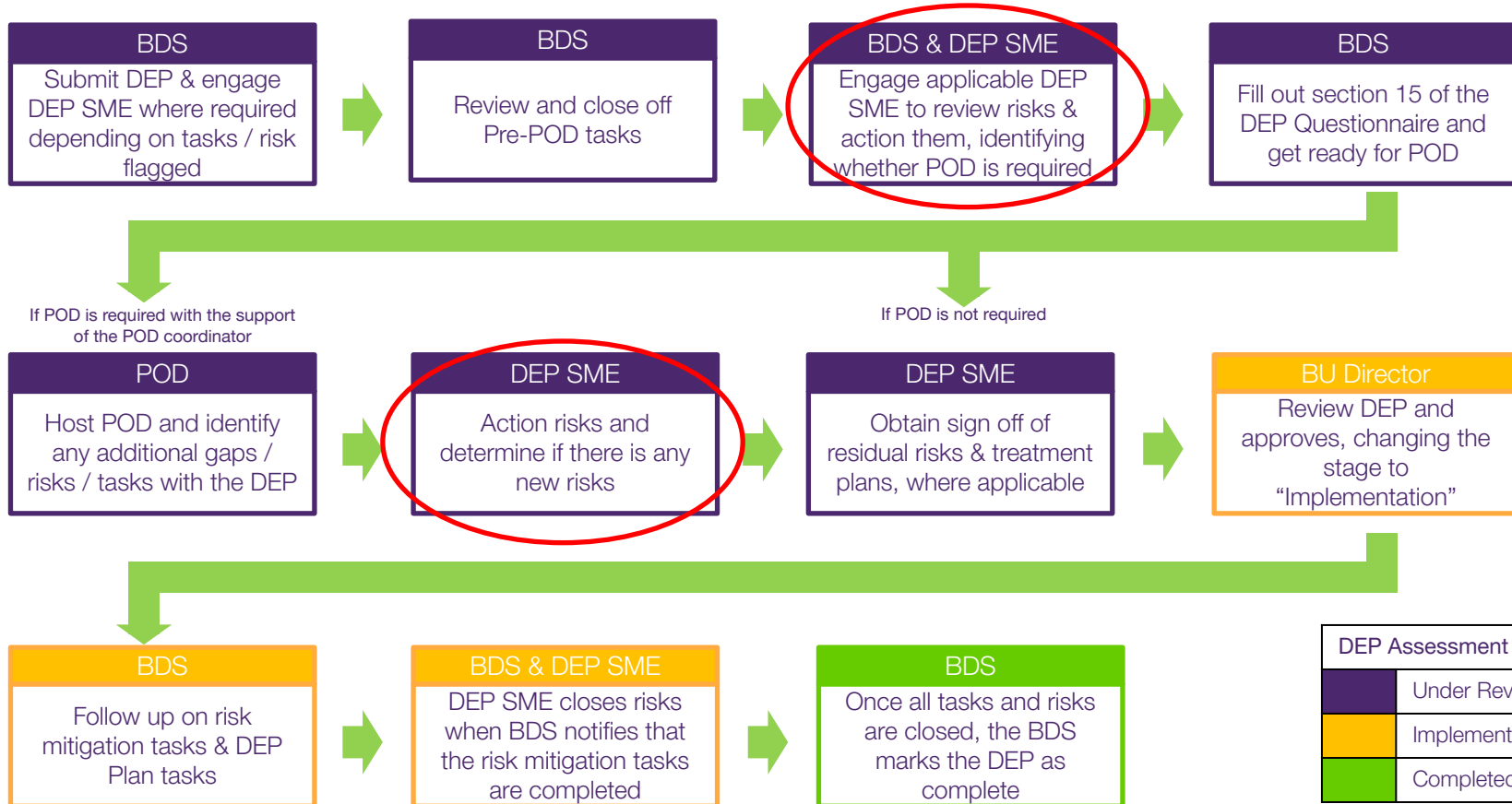
Add

- DEP Task - Business Definitions. Please refer to Q3.1 Business Definitions. This task is part of the plan to enable data.
- DEP Task - Network design doc. Please refer to Q10.17 Network design doc. This task is part of the plan to enable data.
- DEP Task - Privacy training. Please refer to Q6.21 Privacy training. This task is part of the plan to enable data.
- Pre-pod Task - Roles. Please refer to Q2.19 Roles. Required to complete the Data Enablement
- Pre-pod Task - Data type. Please refer to Q2.4 Data type. Required to complete the Data Enablement
- DEP Task - Outside Canada DNTL. Please refer to Q 2.28 DNTL & 2.22 Jurisdiction
- DEP Task - Scope - Data Solution Review. Please refer to Q2.10 Scope. This task is part of the plan to enable data. This
- Pre-pod Task - Central logging. Please refer to Q10.9 Central logging. Required to complete the Data Enablement
- DEP Task - DSR Review. Please refer to Q2.10 Scope. This task is part of the plan to enable data.
- DEP Task - New data. Please refer to Q2.5 New data. This task is part of the plan to enable data.

Guidance

- You will receive a message from the Business Data Steward (BDS) to start the review process where your support is required.
- Prior to the BDS contacting you, they would have reviewed the *Tasks* and *Risks* to help guide the discussion with the DEP SME. Pre-POD Tasks examples include:
 - The BDS is unsure if the data element is PI / PHI? (Privacy Partners)
 - The BDS is unsure if there is a record retention schedule? (Data Lifecycle Primes)
 - The BDS selected “Other” when selecting the encryption type at rest (SbD Primes)
- When you open the DEP, review the *Intake* section of the initiative and the associated *Risks* to understand the scope of the initiative. Once complete, review all other relevant sections in the DEP.
- If you have any questions for the BDS, you can use the *Information Request* icon or you can meet with the BDS to discuss the DEP.
- Full list of tasks will be provide in the job aid to help support.

DEP | High Level Process - Risk Management



DEP Assessment Stages	
	Under Review
	Implementation
	Completed

Guidance:

- Once engaged by the BDS, you will review all the applicable risks / gap flags associated to the DEP. Please note that in the risk name, it will highlight the type of risk (Privacy, Security, Responsible A.I etc.).
- Key items to consider while reviewing the risk / gap
 - Does this risk require any other DEP SME to review? (ex. security)
 - Is this risk / gap applicable to the project?
 - Who is the risk owner and who is the mitigation action item owner?
 - Would this risk / gap benefit from review with POD? (i.e. can the risk not be resolved or requires additional guidance from other stakeholders).

DEP | Reminder of what the Risk view looks like

2.2

Scope

Go to Question

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Details

Tasks

Controls

Comments

Attachments

More

Identification

Risk ID

1182

Risk Statement

"There is a risk that the data has not been appropriately de-identified which may lead to the re-identification of personal customer information resulting in customer complaints, a regulatory investigation, damage to our brand, and/or loss of customer trust."

Source Reference

Elena Test

PCI

SOX

* Date Created

04/09/2022

PIA Reference # (If Applicable)

* GRA created

No

Risk Title

Privacy & Security Risk: De-identification

Risk Manager

Elena Novas

Source of Risk Identification

DEP

Privacy

Yes

CRTC

Date Closed

--/--/----

CSO Residual Risk Assessment (RRA) # (If Applicable)

* Organization

Data & Trust Office

Risks

All risks

2.2

Privacy & Security Risk: De-identification

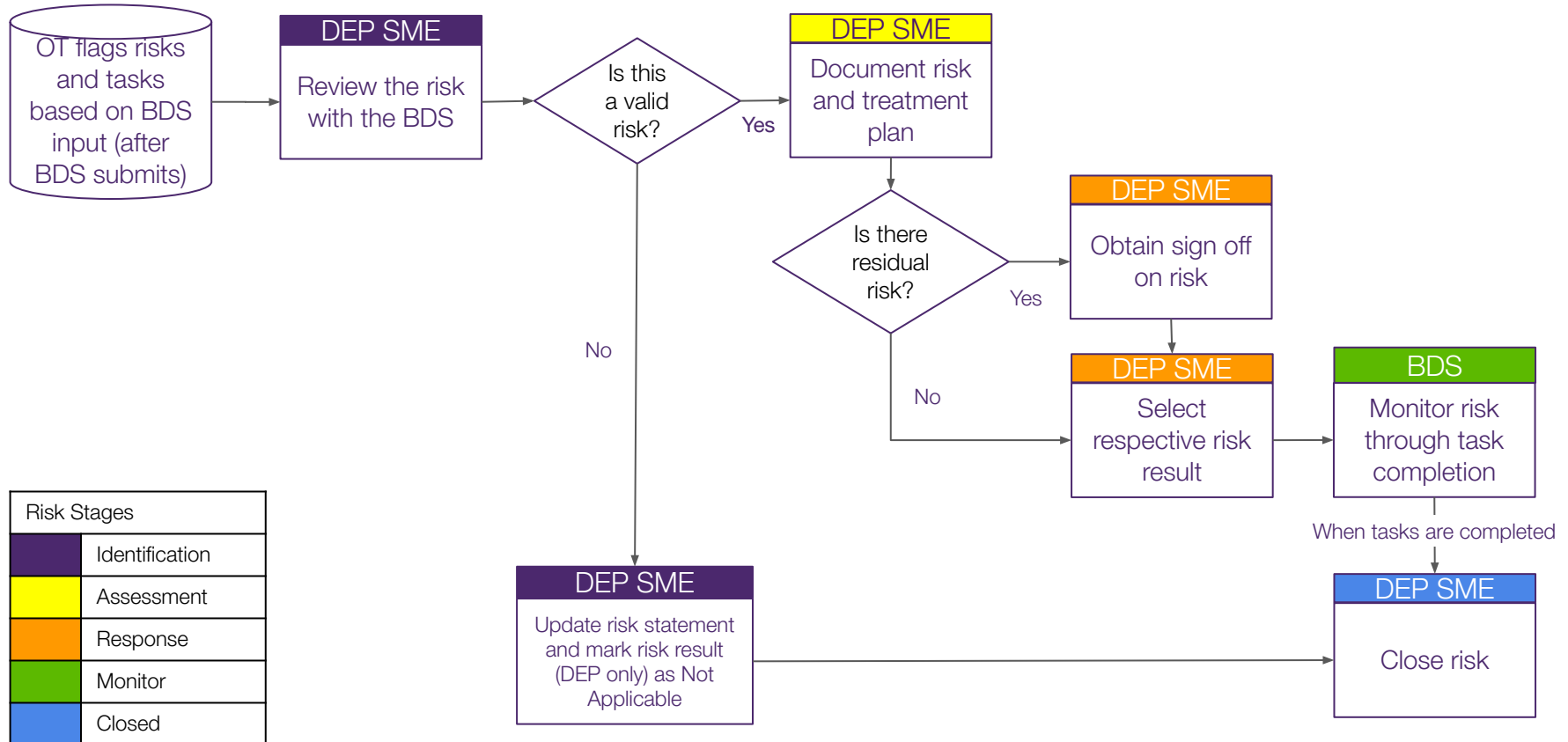
6.5

Privacy Risk: Minors Personal Information

TIP:

- Please make sure you hit Save everytime you switch screens

DEP | Simplified Risk View Workflow



DEP | Identification

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Identification

<p>Risk ID</p> <p>1182</p>	<p>Risk Title</p> <p>Privacy & Security Risk: De-identification</p>
<p>Risk Statement</p> <p>"There is a risk that the data has not been appropriately de-identified which may lead to the re-identification of personal customer information resulting in customer complaints, a regulatory investigation, damage to our brand, and/or loss of customer trust."</p>	<p>Risk Manager</p> <p>Elena Novas</p>
<p>Source Reference</p> <p>Elena Test</p>	<p>Source of Risk Identification</p> <p>DEP</p>
<p>PCI</p> <p>----</p>	<p>Privacy</p> <p>Yes</p>
<p>SOX</p> <p>----</p>	<p>CRTC</p> <p>----</p>
<p>* Date Created</p> <p>04/09/2022</p>	<p>Date Closed</p> <p>--/--/----</p>
<p>PIA Reference # (If Applicable)</p> <p>----</p>	<p>CSO Residual Risk Assessment (RRA) # (If Applicable)</p> <p>----</p>
<p>* GRA created</p> <p>No</p>	<p>* Organization</p> <p>Data & Trust Office</p>

Important Fields	Guidance
Risk ID	Auto-populated (ID in Risk Register).
Risk Statement	Pre-filled, but can be edited as appropriate. If the risk is not an actual risk, enter details in the Risk Statement (i.e. data is de-identified and minor's data is not in scope).
Risk Manager	DEP SME name based on the type of risk / gap.
Source Reference	Auto-populated (name of DEP).
Source of Risk Identification	Auto-populated to DEP, but can be changed to another source (i.e. audit)
PCI, Privacy, SOX, CRTC	Privacy is auto-populated, but can be edited.
Date Created	Auto-populated (date when the risk was created).
Date Closed	Auto-populated (date the risk is closed).
PIA Reference #	If you need to reference a previously submitted PIA, the number can be entered here.
RRA Reference #	If you are aware of a completed RRA, you can enter the number here.
GRA created	Auto-populated and only used by the CSO.
Organization	Pre-populated based on Organization selected when the DEP is launched.

DEP | Identification - how to

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Identification

Risk ID
1182

Risk Title
Privacy & Security Risk: De-identification

Risk Statement
"There is a risk that the data has not been appropriately de-identified which may lead to the re-identification of personal customer information resulting in customer complaints, a regulatory investigation, damage to our brand, and/or loss of customer trust."

Risk Manager
Elena Novas

Source Reference
Elena Test

Source of Risk Identification
DEP

Update the risk statement to reflect the situation.

Add yourself as the Risk manager.

* GRA created
No

* Organization
Data & T

Remember to save, and move to the next tab Assessment.

Important Fields

Guidance

If Risk is not Applicable: update (or rewrite) the Risk Statement to describe why and then add yourself as the Risk Manager

Then go to the section on Response ([slide 46](#))

Source Reference

Auto-populated (name of DEP).

Source of Risk Identification

Auto-populated to DEP, but can be changed to another source (i.e. audit)

PCI, Privacy, SOX, CRTG

Privacy is auto-populated, but can be edited.

Date Created

Auto-populated (date when the risk was created).

Date Closed

Auto-populated (date the risk is closed).

PIA Reference

If you need to reference a previously submitted PIA, the number can be entered here.

If you have completed a completed RRA, you can enter

and only used by the CSO.

based on Organization selected when ed.

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Assessment

Inherent Risk Likelihood

3_Moderate

Inherent Risk Level

25

Impact: High (Significant)
Likelihood: Moderate (Possible)

Treatment Plan

1. Update the Agreement.
2. Present to the Enterprise Data Council.
3. De-identification (Increase radius).

See tasks for details.

Residual Risk Likelihood

3_Moderate

Residual Risk Level

14

Impact: Moderate
Likelihood: Moderate (Possible)

Risk Owners

Mohsin Khan

Inherent Risk Impact

4_High

Inherent Risk Assessment Summary

High Impact and moderate likelihood render this a high risk overall. This is due due to the potential for media scrutiny which would include an erosion of trust with our customers, and the potential for a regulatory investigation. In addition, the X Agreement may not include the appropriate language for the use of the data.

Comments

Our Office consulted with Legal Counsel and they advised that the use of this data could be viewed by customers and the media as a breach of trust where an apology would be more appropriate than a reactive media statement.

Residual Risk Impact

3_Moderate

Residual Risk Assessment Summary

If the mitigating actions are implemented, the Impact of the risk would be lowered thereby reducing the overall risk to moderate.

Important Fields	Guidance
Inherent Risk Likelihood and Impact	Inherent assessment represents the amount of risk in the absence of controls. Reference the Data Risk Management (DRM) Matrix to determine the likelihood and impact.
Inherent Risk Level	Enter the likelihood and impact from the matrix.
Inherent Risk Assessment Summary	Include a summary of your assessment to help the business understand how you have arrived at your rating.
Treatment Plan	Work with the business to determine the treatment plan and add its summary here. Make sure you create tasks in the tasks tab to allow for tracking of the tasks.
Comments	Add any comments you which to have documented (i.e. consulted with Legal).

Calibrate the risk within the DTO to ensure agreement with the risk(s) and treatment plan.

DEP | Assessment, con't...

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Assessment

Inherent Risk Likelihood

3_Moderate

Inherent Risk Level

25

Impact: High (Significant)
Likelihood: Moderate (Possible)

Treatment Plan

1. Update the Agreement.
2. Present to the Enterprise Data Council.
3. De-identification (Increase radius).

See tasks for details.

Residual Risk Likelihood

3_Moderate

Residual Risk Level

14

Impact: Moderate
Likelihood: Moderate (Possible)

Risk Owners

Mohsin Khan

Inherent Risk Impact

4_High

Inherent Risk Assessment Summary

High Impact and moderate likelihood render this a high risk overall. This is due due to the potential for media scrutiny which would include an erosion of trust with our customers, and the potential for a regulatory investigation. In addition, the X Agreement may not include the appropriate language for the use of the data.

Comments

Our Office consulted with Legal Counsel and they advised that the use of this data could be viewed by customers and the media as a breach of trust where an apology would be more appropriate than a reactive media statement.

Residual Risk Impact

3_Moderate

Residual Risk Assessment Summary

If the mitigating actions are implemented, the Impact of the risk would be lowered thereby reducing the overall risk to moderate.

Important Fields	Guidance
Residual Risk Likelihood and Impact	Residual risk is the amount of risk that remains after controls are accounted for. Reference the Matrix to determine the likelihood and impact.
Residual Risk Level	Enter the likelihood and impact from the matrix.
Residual Risk Assessment Summary	Include a summary of your assessment to help the business understand how you have arrived at your rating.
Risk Owner	Enter the name(s) of the Director, VP, or ELT member who is responsible for signing off on the risk.

Tip: Please calibrate the risk with your peers. If applicable, leverage our various forums (Squad, EDC and EDS) to ensure that the risk is assessed correctly.

DEP | Assessment - how to

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Assessment

Inherent Risk Likelihood

3_Moderate

Inherent Risk Level

25

Impact: High (Significant)
Likelihood: Moderate (Possible)

Treatment Plan

1. Update the Agreement.
2. Present to the Enterprise Data Council.
3. De-identification (Increase radius).

See tasks for details.

Residual Risk Likelihood

3_Moderate

Residual Risk Level

14

Impact: Moderate
Likelihood: Moderate (Possible)

Risk Owners

Mohsin Khan

Inherent Risk Impact

4_High

Inherent Risk Assessment Summary

High impact and moderate likelihood render this a high risk overall. This is due due to the potential for media scrutiny which would include an erosion of trust with our customers, and the potential for a regulatory investigation. In addition, the X Agreement may not include the appropriate language for the use of the data.

Comments

Our Office consulted with Legal Counsel and they advised that the use of this data could be viewed by customers and the media as a breach of trust where an apology would be more appropriate than a reactive media statement.

Residual Risk Impact

3_Moderate

Residual Risk Assessment Summary

If the mitigating actions are implemented, the Impact of the risk would be lowered thereby reducing the overall risk to moderate.

Important Fields

Guidance

Inherent assessment represents the amount of

Go/DRMatrix to determine inherent risk level and describe it.

Summarize the treatment plan and any comments. If there are Tasks - [see next slide](#).

Go/DRMatrix to determine residual risk level and describe it.

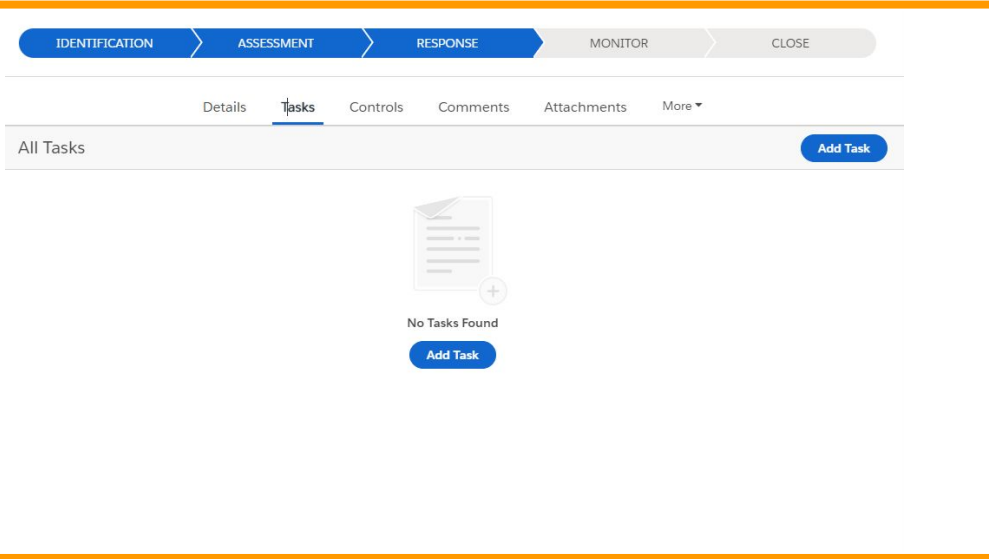
Add Risk Owner (who will sign off based on matrix) using policy from go/DataRisk

documented (i.e. consulted with Legal).

Calibrate the risk within the DTO to ensure agreement with the risk(s) and treatment plan.

Remember to save, and move to the next tab Response.

DEP | Assessment - how to



The screenshot displays the DEP Assessment interface. At the top, there is a navigation bar with five tabs: IDENTIFICATION, ASSESSMENT, RESPONSE, MONITOR, and CLOSE. The 'ASSESSMENT' tab is currently selected. Below the navigation bar, there is a sub-navigation bar with six options: Details, Tasks, Controls, Comments, Attachments, and More. The 'Tasks' tab is selected. The main content area shows 'All Tasks' with an 'Add Task' button. Below this, there is a message 'No Tasks Found' with a plus icon and another 'Add Task' button.

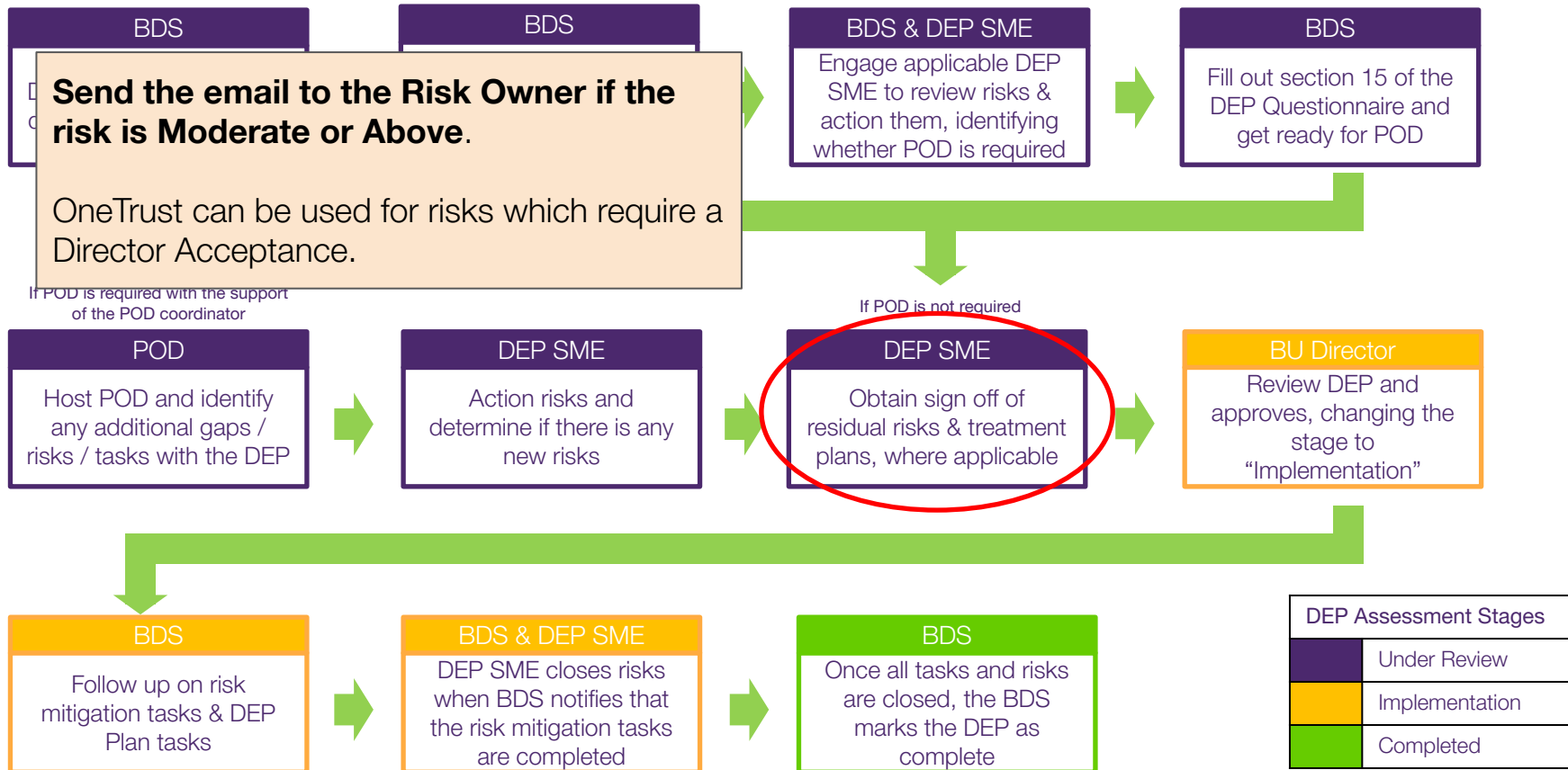
Add any Tasks required to mitigate the risks

Then [return to Assessment](#) to update the Residual risk

Calibrate the risk within the DTO to ensure agreement with the risk(s) and treatment plan.

Remember to save!

DEP | High Level Process - Risk Management



DEP | Response (Risk Acceptance)

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Response (Risk Acceptance)

Risk Result (DEP only)

2_Mitigated

Date Signed off

06/30/2022

Implementation Date (DEP Only)

07/29/2022

Tips

- If there are multiple DTO risks (i.e. data ethics, records retention, etc.), send a consolidated email vs multiple emails.
- Ensure to cc the appropriate business Executive for awareness, including business Executives who own mitigating actions.
- Don't forget to cc the Business Data Steward as they will be responsible for following up on the mitigating actions (tasks).

Risk Level	Very Low	Low	Moderate	High	Very High
Business Leader	Director	Director	Vice President	Vice President	ELT
Executive Awareness	-	-	ELT	ELT	CEO

Important Fields	Guidance
Risk Result (DEP Only)	<ul style="list-style-type: none"> • Accepted: When a Director, VP or ELT member acknowledges the data risk, it consequences, and takes accountability for the risk in pursuit of their business goals. • Mitigated: Reduce the impact or likelihood of the risk by putting in place mitigating actions. • Shared: The risk and activity that introduces the risk is assigned or moved/transferred to a third party. • Avoided: The risk is completely eliminated or avoided by not pursuing the activity or developing an alternative strategy.
Risk Result (DEP Only) - Special Fields	<ul style="list-style-type: none"> • Not Applicable: When the risk is deemed not relevant based on the review of the initiative (i.e. risk was auto-triggered due to a response in the DEP). • Monitored by GRA: This is a special case for CSO to identify that it is being managed by GRA.
Date Signed Off	Enter the date the risk was signed-off.
Implementation Date (DEP Only)	Enter the date the initiative is going live.

DEP | Response (Risk Acceptance) - how to

IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Response (Risk Acceptance)

Risk Result (DEP only)

2_Mitigated

Date Signed off

06/30/2022

Implementation Date (DEP Only)

07/29/2022

Tips

- If there are multiple DTO risks (i.e. data ethics, records retention, etc.), send a consolidated email vs multiple emails.
- Ensure to cc the appropriate business Executive for awareness, including business Executives who own mitigating actions.
- Don't forget to cc the Business Data Steward as they will be responsible for following up on the mitigating actions (tasks).

If Risk is not Applicable: update **Risk Result (DEP Only)** SAVE, and then advance the stage to **Monitor & Close**.

Describe the Risk Result from the choices defined here. Attach the email to the record if the risk is Moderate or above see next slide.

Update the Date signed off by the Risk Owner and the date of the implementation.

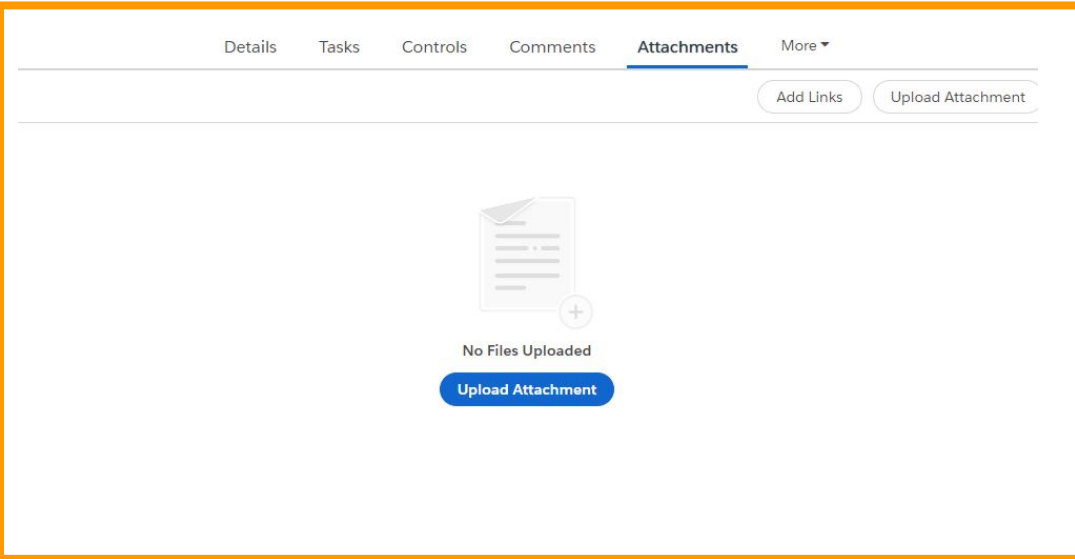
Only Special Fields

- **Monitored by GRA:** This is a special case for CSO to identify that it is being managed by GRA.

Risk Level	Very Low	Low	Moderate	High	Very High
Business Leader	Director	Director	Vice President	Vice President	ELT
Executive Awareness	-	-	ELT	ELT	CEO

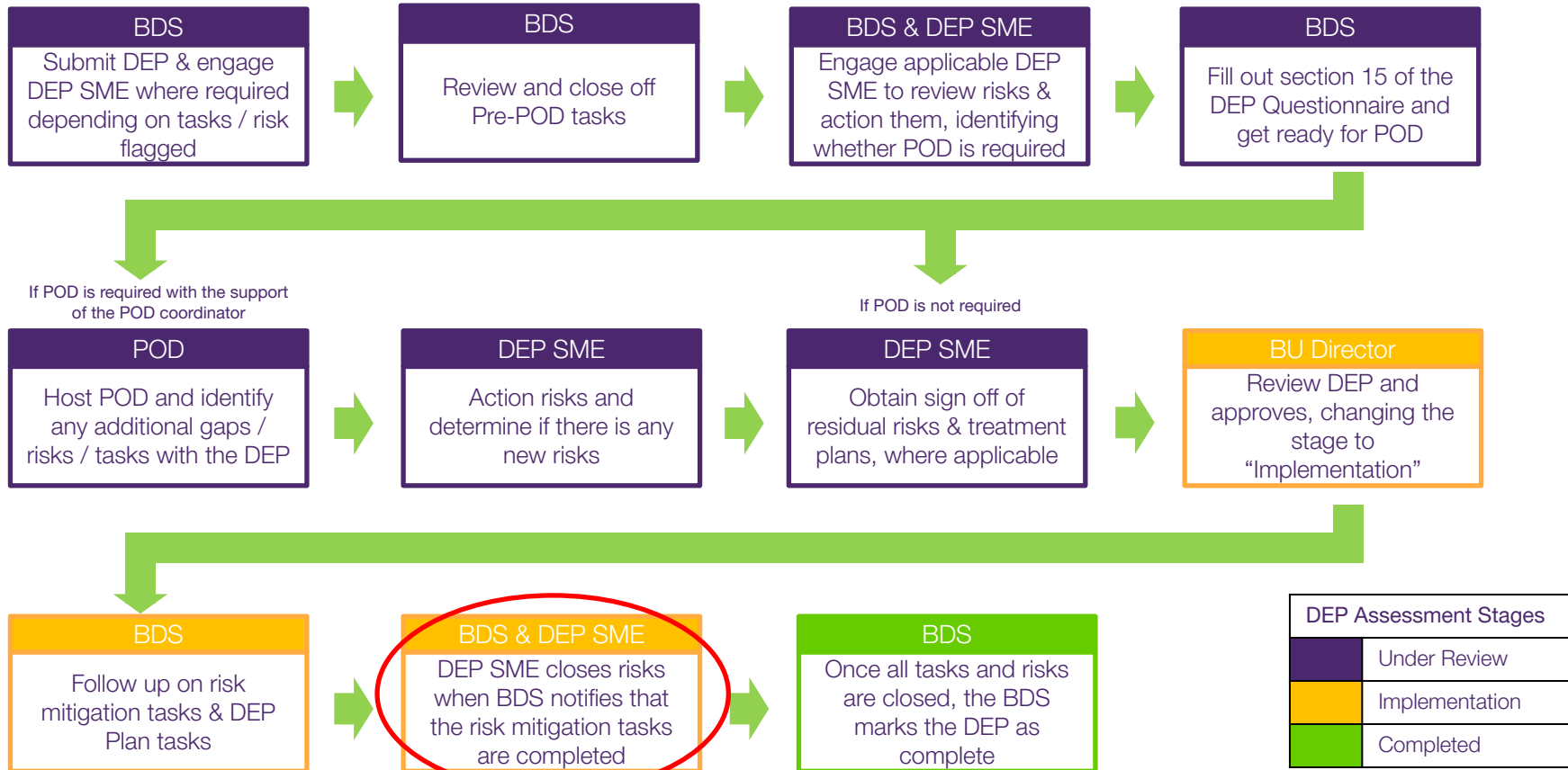
Remember to save, and move to the next tab Monitor.

DEP | Response (Risk Acceptance) - how to



Upload the Attachment on the Attachments tab

DEP | High Level Process - Risk Management



IDENTIFICATION

ASSESSMENT

RESPONSE

MONITOR

CLOSED

Details

Tasks

Controls

Comments

Attachments

More

All Tasks

Add Task

Task Name	Assignee	Priority	Deadline
<div>✓</div> Agreement	Jesslyn Dymond	<div></div>	04/29/2022
<div>✓</div> Enterprise Data Council	Jesslyn Dymond	<div></div>	04/20/2022
<div>✓</div> Re-identification	Jesslyn Dymond	<div></div>	05/20/2022
<div>+ Add Task</div>			

- Once you have received an email response from the Risk Owner, PDF the email and attach it in the *Attachments* tab. You can then move the risk to the *Monitor* stage (when you click on the *Tasks*, you will see all of the activities that need to be completed to close the risk).
- The BDS is responsible for ensuring that tasks are completed. When you are comfortable that a task has been completed, you can add comments and mark the task as complete (if you have attachments or an email you would like to document, you can include it in the *Attachments* tab).
- Once all *Tasks* are completed, then can then move the risk to the *Closed* stage.

DEP | Asks for the DEP SME

Support the roll out of DEP within TELUS by advocating for the DEP; support BDS as they embark on their journey

Our ask

Access the [test environment](#) and create a test DEP, and action the risks and tasks associated to that DEP. Provide your [feedback here](#).

What's next?

1

Attend the next DEP training (Apr 18) where we will go through real life examples to help bridge the gap between theory and practice.

2

Review the Data Risk Management Policy and Framework [@go/datarisk](#), and the [DRM Job Aid](#).

3

Share your ideas and feedback with the project team early and often to help us (Jesslyn, Elena and Mohsin) quickly action any suggestions as roll-out continues in Q2 and Q3.

Visit [go/dep](#) for more information. Check out the [DEP Primer](#) slides for the basics.

let's make the future friendly™



Data Enablement Plan (DEP) SME Training Day 3

April 2022
DTO & CSO

Journey to Become a Data Enablement Plan Super Star!

Day 1 – Apr 7

Topic 1:
DEP & Process
Overview

Topic 2:
OneTrust
Navigation

Day 2 – Apr 11

Topic 3:
Process Deep
Dive

Day 3 – Apr 18

Topic 4:
Example
Walkthroughs

Outcome: Understanding your role in the Data Enablement Process





Questions?

let's make the future friendly™

DEP | Simplified Risk View Workflow

OG Slide

