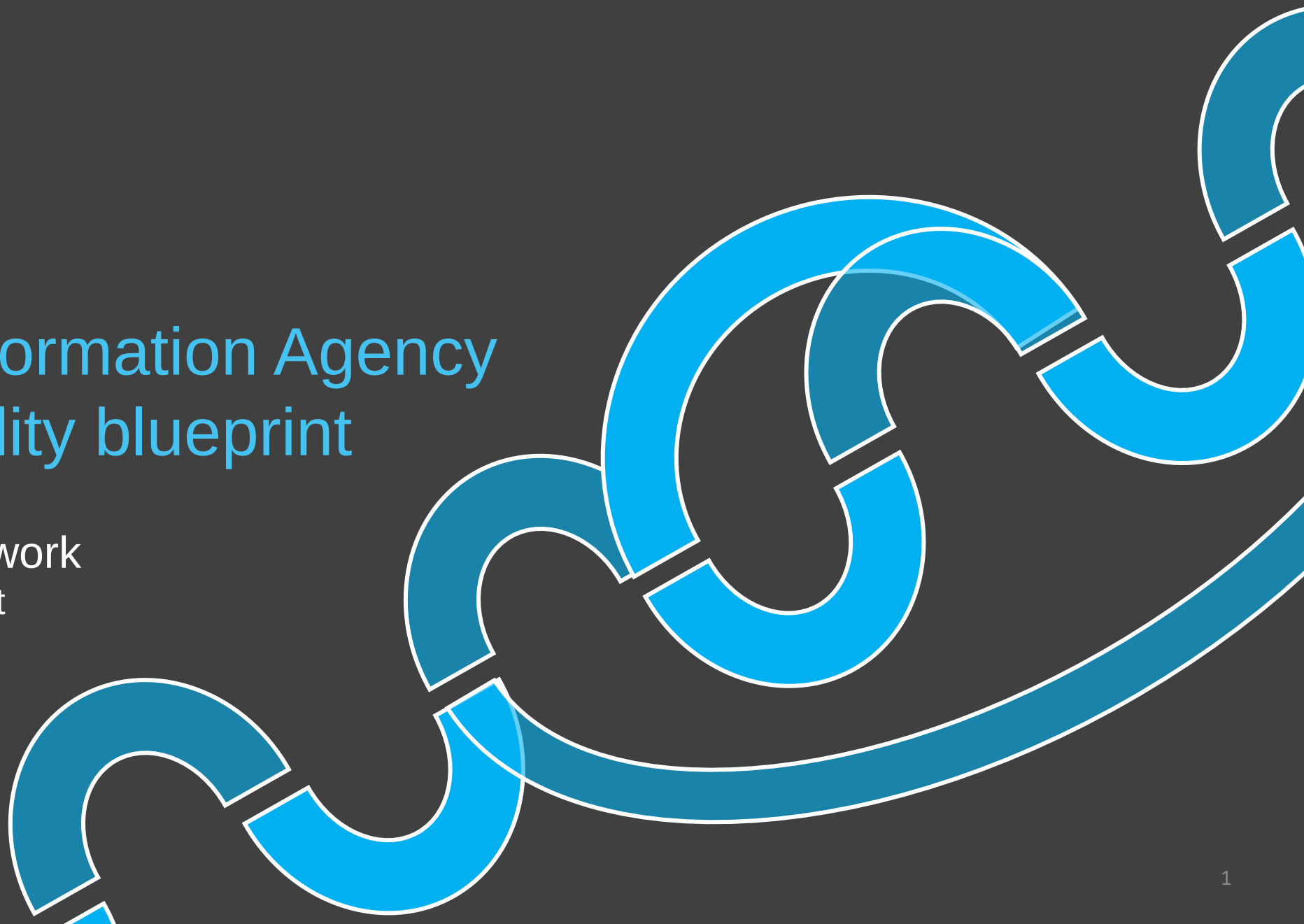
Digital Transformation Agency Protected Utility blueprint

Engagement framework
Risk Assessment Toolkit

FINAL

28 June 2021



Document Purpose

Purpose

The purpose of the risk assessment toolkit is to **provide APS agencies with detailed guidance on how to conduct a Risk Assessment.**

In this toolkit, we describe the detailed approach for conducting a risk assessment, including the steps that need to be undertaken to identify, rate and mitigate risks, to enable a successful adoption of the Protected Utility blueprint (the blueprint) by the end users within transitioning agencies.

The toolkit along with the risk assessment template (please see slide 14) provides the full suite of materials required to design and deliver risk assessment activities.

All APS agencies looking to operate under the blueprint are encouraged to use this toolkit and the risk assessment template. However, you may tailor the materials to suit your agency's specific needs.

Audience

The intended audience for this document are the agency team members responsible for implementing the blueprint services.

This may include:

- Blueprint project lead and team members
- Blueprint change team
- Blueprint communications and engagement team
- Blueprint training team
- Blueprint technical delivery team
- Agency technology and security team members and stakeholders

Table of contents

The Risk Assessment Toolkit comprises of three parts, outlined below:

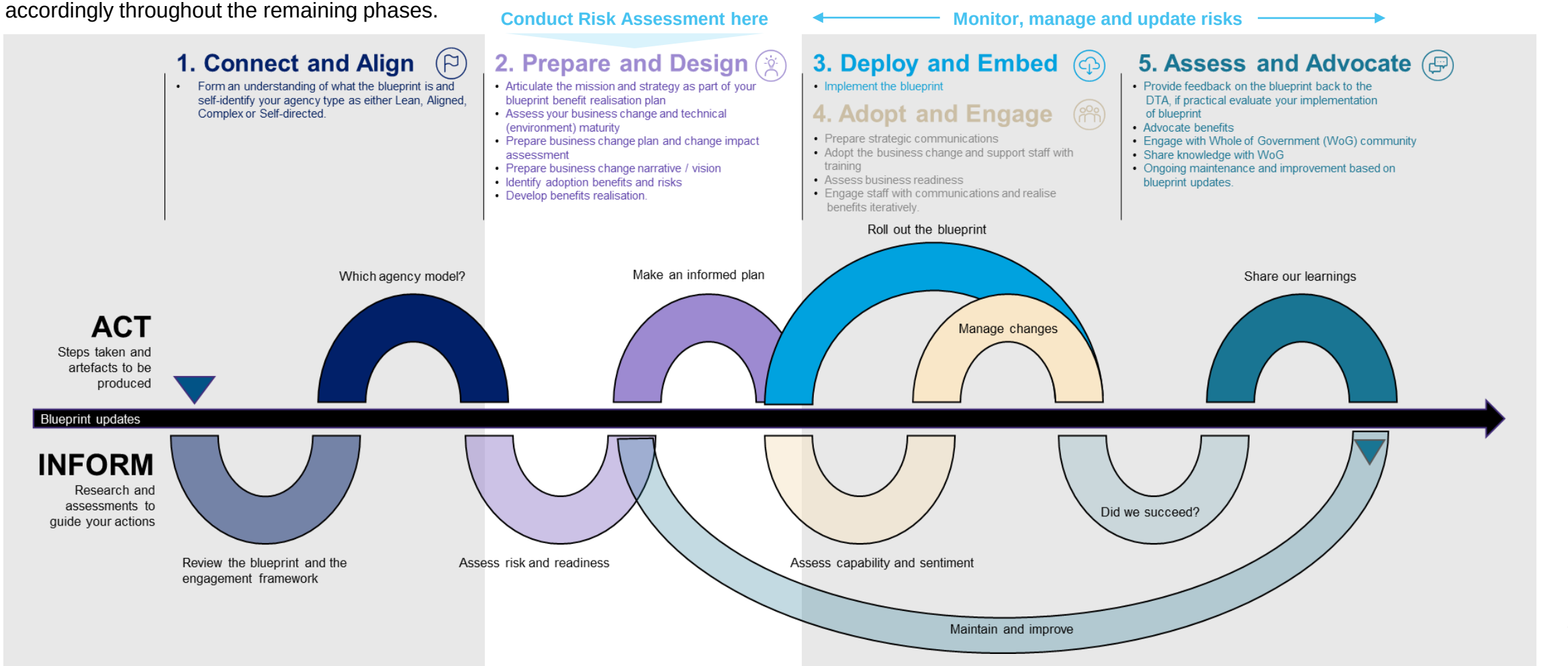
The Risk Assessment Toolkit is comprised of three parts:

Part 1:
Risk Assessment
Introduction

Protected Utility blueprint engagement framework

The DTA Protected Utility blueprint engagement framework defines how APS agencies access this program, and how they can maximise the use of the blueprint for modern desktop services.

It is recommended that agencies conduct the Risk Assessment during *Prepare and Design,* and then continue to monitor, manage and update the identified risks accordingly throughout the remaining phases.



Protected Utility blueprint agency types

DTA classifies the program customer agencies into one of the four types described below:

1. Lean

Lean agencies are generally small (usually <100 employees). They are constrained in terms of workforce skills, resources and budget; limiting their ability to introduce new technology and manage the associated business change. They are likely to benefit from the blueprint services. However, they may not have the necessary funding or change management and technology capability. They would likely require procuring the services of a change or technology partner to successfully adopt the blueprint.

2. Aligned

Aligned agencies are best placed to benefit from using the blueprint services. These agencies have a desire to adopt cloud-based technology. However, they may encounter some challenges related to capability, funding and guidance on where to start. Additionally, Aligned agencies may not be aware of the complexity and scale of the business change required to fully realise the benefits of the technology.

3. Self-Directed

Self-directed agencies have complex and specific business requirements, and already have mature technical environments. Cloud services do not always meet the diversity of their needs, however, they may have some areas / use cases that could benefit from the blueprint services. Additionally, the change process to realise the benefits of the blueprint is typically challenging within Self-Directed agencies.

4. Complex

Complex agencies are open to cloud services but face a greater degree of implementation difficulty due to internal complexity, such as complex business processes and high levels of system integration. This makes the benefits more uncertain and the transition process a real challenge – factors that are likely to form a significant adoption barrier. Additionally, (as with Self-Directed agencies) the change process to realise the benefits of the blueprint is challenging within Complex agencies.

The value of the risk assessment template to each agency type has been described below:

Lean agencies need to consider their finite capability and resources against the complex requirements of implementing business technology and managing the associated delivery risks. They may wish to engage a service provider who has prior experience with implementing the blueprint and providing technology and change services to government.

Aligned agencies may not have a specified risk management process, and could consider this toolkit as a resource to understand their organisation's delivery risks with respect to the blueprint. Agencies should strive to use consistent risk assessment methods across the organisation.

Self-directed agencies have their own workforce capability, dependencies, technology and change services which suit their needs. As such, they will have their own methods and tools available for risk assessments. For these agencies, this toolkit may be useful as a comparison method, or to supplement their existing risk management processes.

Complex agencies often have multi-vendor, multi-product technical environments with either unplanned or conflicting implementation roadmaps. They will typically have their own methods for risk assessments. However, they could consider this toolkit as a reference to support and supplement their existing risk management processes.

Part 2:

Risk Assessment

Detailed Approach

Detailed Approach | Overview

A risk assessment assists in identifying, assessing and treating the delivery risks that may be encountered within agencies as a result of transitioning to the blueprint.

What is a delivery risk?

- A delivery risk is an adverse event that may impact a successful transition to the blueprint

What is a risk assessment?

- **A risk assessment will enable agencies to identify and self-assess* the likelihood, consequences and treatments of delivery risks relevant to the successful adoption of the blueprint.**
- The output of this assessment will frame the approach to successfully managing these delivery risks throughout transition.
- The outputs from the risk assessment will enable the agency to manage delivery risk.
- Additionally, outputs from the risk assessment can be used as inputs into transition activities, such as the transition and change management plans, security analysis, and the business case.
- Risks are rated based on very high, high, moderate, minor and low designations to inform risk treatment activities.

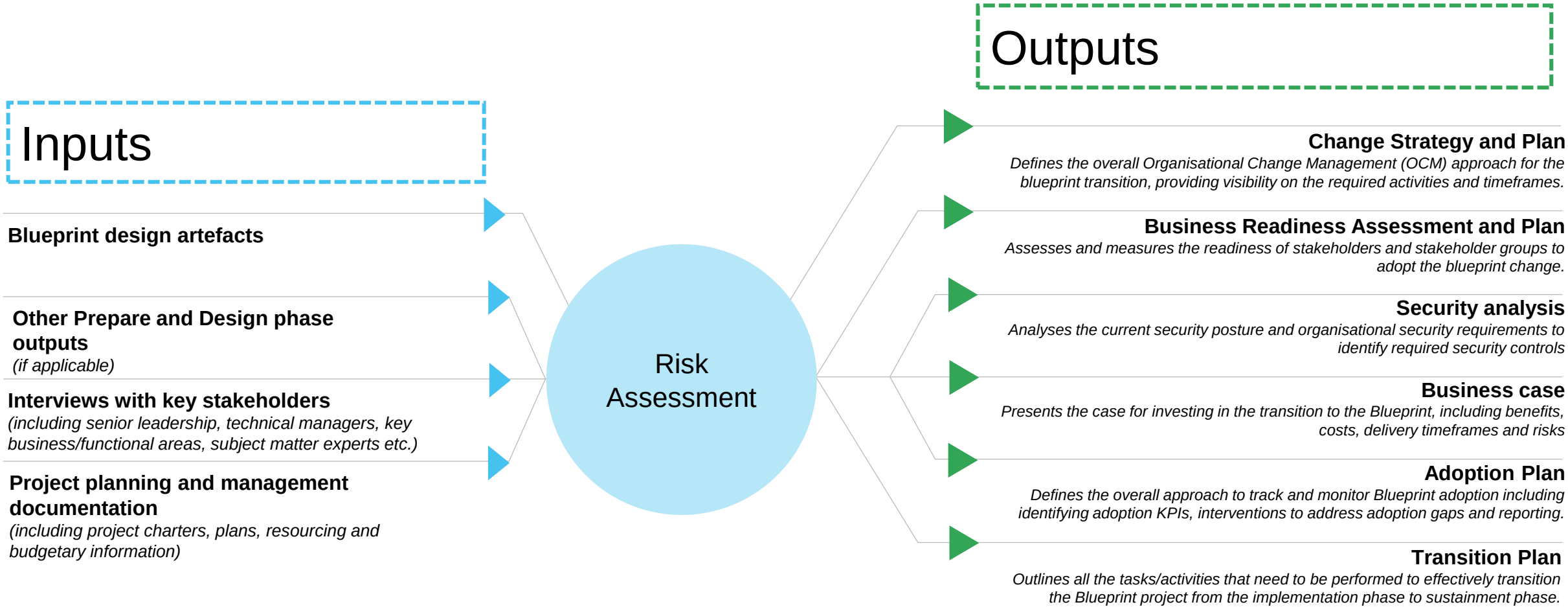
How will a risk assessment help manage delivery risks for your organisation?

- The risk assessment will:
    - Enable agencies to identify and manage* the most pertinent risks associated with transitioning to the blueprint services
    - Support the project team to develop suitable treatment plans for risks
    - Provide a formal tracking mechanism for the identified risks.

***** For some agencies, particularly those that identify with the Lean archetype, this identification and management may be conducted by a service provider engaged by them.

Detailed Approach | Risk Assessment inputs and outputs

Various inputs will be required to assist develop the Risk Assessment. Once developed, the assessment informs various transition activities. Inputs and outputs are identified below:



Detailed Approach | Sources of risks

The risk sources described below may be used to assist the identification of delivery risks. Considering each of these sources ensures that a pragmatic and holistic approach is developed when identifying and assessing risks.

	Risk source				
	Project management	**Technology**	**Security & compliance**	**Organisational**	**People**
Description	Risks that concern transition to the blueprint within defined time, cost and quality constraints. These risks often encompass project management activities such as planning, budgeting and resourcing.	Risks that concern technology requirements, gaps, issues, or decisions which may impact the agency's ability to implement the blueprint services. These risks can often be aligned to phases within the software delivery lifecycle: analysis, design, implementation, testing, maintain.	Risks that concern the agency's ability to comply with security, legislative and regulatory requirements. These risks may relate to either the controls used to meet requirements, or the requirements themselves.	Risks relating to organisational constructs and how they support transition to the blueprint. These risks can include both internal organisational constructs and considerations for external organisations, such as vendors and partner agencies.	Risks related to the agency's people and how the blueprint will be delivered to them. These risks can cover both the capability and resourcing of those involved in delivering the blueprint services themselves, and the people who will make use of the services once delivered.
Relevant examples of risks	• There may not be sufficient time in the delivery plan to transition to the blueprint successfully • Limited contingency within the project's budget may negatively impact the project's ability to respond to unexpected changes to organisational requirements	• Requirements may not be sufficiently understood to support design and implementation • Design may not be completed to an acceptable level of detail to inform implementation • Dependencies on legacy technology solutions may not be fully understood • Sufficient testing may not be completed	• Regulatory change may lead to new requirements which cannot be met • Existing controls may not be sufficient to meet legislative requirements	• Significant organisational changes may occur during transition • Licensing and/or procurement activities may not be completed in time to support implementation • Organisational requirements may change during implementation	• Insufficient resources may not have been made available to deliver the blueprint successfully • The scale of change in transitioning to the blueprint from current ways of working may be beyond the workforce's current capacity for change

Detailed Approach | How to assess risks

The following table is used within the risk assessment to rate the severity of risks, based upon their likelihood and impact of being materialised. The impact and likelihood scales are further defined within the template itself (please see slide 14).

Likelihood	Impact				
	Insignificant	Minimal	Medium	Major	Severe
Almost Certain	Minor	Moderate	High	Very high	Very high
Likely	Low	Minor	Moderate	High	Very high
Possible	Low	Minor	Moderate	High	Very high
Unlikely	Low	Minor	Moderate	Moderate	High
Rare	Low	Low	Minor	Moderate	High

Once a risk is rated, its treatment should be determined. One of the following treatments should be chosen for each risk, informed by its risk rating.

	Risk treatment		
	Accept	**Mitigate**	**Avoid**
Treatment description	The risk is accepted as is with no actions, mitigations or controls planned.	Actions and/or activities are planned to either reduce the likelihood or the impact of the risk being materialised.	Actions and/or activities are planned to entirely avoid the risk i.e. eliminate its likelihood and/or impact.
Applicable risk characteristics	It is advised that only risks that have a low risk rating should be accepted.	Risks that have a rating higher than low should be mitigated unless it is feasible to avoid them. It is likely that a mitigation treatment will be applied to most risks.	Using an avoid treatment risks that have a high or very high rating should be considered, however the feasibility of doing so should be tested, and may result in a mitigation treatment being preferred.
Appropriate next steps	• Document the risk treatment • Continue to monitor the likelihood and impact of the risk to ensure it is still appropriate to accept it	• Document the risk treatment, including an appropriate mitigation plan • Execute the mitigation plan and continue to monitor the risk to ensure this plan remains appropriate and is effective.	• Test the feasibility of avoiding the risk and document the plan to do so if deemed feasible • Execute the avoidance plan and continue to monitor the risk to ensure this plans remains appropriate and is effective.

Detailed Approach | Risk Assessment steps

The steps to undertake a blueprint risk assessment are presented below. It describes what activities should be undertaken at each phase, along with providing an indicative view of the outcomes expected.

	1. Data gathering	2. Validation	3. Consolidation and approval	4. Reporting and next steps
Purpose	**This phase involves gathering current state information and data to inform the risk assessment.**	**Once the initial risk assessment has been captured and documented, this phase involves validating it with relevant business/functional areas and key stakeholders.**	**After validation, this phase involves finalising the assessment and sharing with relevant leaders for approval.**	**This phase involves using the results from the risk assessment to inform onwards delivery of the blueprint services.**

Key Activities	• Gather and review data from existing documentation, assessment reports etc. (please refer to slide 9 for input resources).
	• Meet with technology, change and other relevant functional teams to gather inputs
	• Capture the findings within a risk assessment template and complete other key information in relation to this (please refer to slide 14)
		• Meet with technology and other relevant functional teams to validate the draft risk assessment and address questions and gaps.
		• Validate the risk treatments and identified actions within the assessment.
			• Perform final review and validation with technology SMEs and leaders
			• Modify risk assessment report as needed
			• E-mail assessment to leads and obtain sign-off
			• Leads may also request to meet in person before final signoff.
				• Analyse the risk information and insights gathered, focussing on different categories.
				• Use the risk information and insights to develop and/or inform customised action plans:
				  ○ Transition Plan
				  ○ Business case
				  ○ Security analysis
				  ○ Change Plan
				  ○ Business readiness plan
				• Continuously monitor risks throughout transition and update action plans accordingly

Responsible individuals / teams	• Agency blueprint project team • Relevant agency stakeholders	• Agency blueprint project team • Relevant agency stakeholders	• Agency blueprint project team • Agency project sponsor and other senior leadership • Relevant agency stakeholders	• Agency blueprint technology team • Agency blueprint project lead • Agency blueprint change team • Agency blueprint security team • Agency project sponsor
Expected Outcomes	• Initial risk assessment drafted	• Final risk assessment report completed	• Final risk assessment report completed.	• Action plans which include identified mitigations and actions against risks

Part 3:
Risk Assessment
Template

Template | Access

The risk assessment template will provide a mechanism to capture and consolidate all the risk information. Based on the inputs, the tool will analyse and summarise the risk ratings (low, minor, moderate, high, very high).

The risk assessment template can be accessed by clicking the icon:

Note: Further information regarding how to complete the template has been included within the template itself. An example has also been included to further clarify how to use the template.

Thank you!