

Implementing 'Better Practice' Permissions

A Playbook for regulators to streamline permissions
and become digitally ready

Part B: Designing better practice processes and delivering change

Three parts of the Playbook

1 Overview

2 Part A: defining your ambition for reform

This section is targeted at 'Service Owners' – regulatory leaders or senior managers responsible for permissions. It includes guidance to understand baseline practices and processes and define your parameters and ambition for reform.

3 **Part B: designing better practice processes and delivering change**

This section is targeted at 'Reform officers' – responsible for designing and implementing regulatory improvements. It includes guidance for designing better practice permissions and implementing reform.



Contents

1	Design	Page 5
2	Implement	Page 21
	Inform	Page 23
	Apply	Page 29
	Review & Stream	Page 51
	Assess	Page 61
	Decide	Page 70
	Notify & issue	Page 78
	Other Processes	Page 88
3	Appendices	Page 99

Use this Playbook to develop an action plan for practice and process improvements and digital reform

Follow this four-step process to develop an action plan and related outputs (e.g., documented system requirements) to improve your permission processes and ensure they are 'digitally ready'. The Playbook is separated in two parts.

PART A

Primarily for Service Owners – you are a regulatory leader or senior manager responsible for administering the permission.

BASELINE

Understand your baseline process and practice

Gather baseline information on your current state practice and processes and identify pain points and challenges across the permission journey.

DEFINE

Define your parameters and ambitions

Understand your ambitions and constraints for reform. Identify your parameters for digital and non-digital improvements, guided by frameworks and criteria.

PART B

Primarily for Reform Officers – you are a reform officer or team member responsible for designing and implementing regulatory improvements.

DESIGN

Design 'better practice' processes

Work through the 'better practice' permission journey and use it to design an improved permission process.
Consider your requirements for digital reform, including through Service Victoria.

IMPLEMENT

Identify and implement improvements

Conduct an in-depth review of key stages and components to identify improvements.
Document and prioritise opportunities, actions, and enablers for reform and digitisation, developing an action plan.

Note: Going through this process might surface strategic questions related to the policy, role and design of your permission. Refer to Page 9 for other resources to help you with these broader considerations.

DESIGN

Better Practice Permission Journey | **The Better Practice Permission Journey explained**

The following sections of the Playbook focus on the Better Practice Permission Journey, which can be used to identify tangible actions to improve and digitise your permission process and practice.

What is the Better Practice Permission Journey?

- The Better Practice Permission Journey breaks down the end-to-end permission process into stages and activities or process components. It is comprehensive, identifying typical stages that might occur across both simple and complex permissions. **Not all permissions will include every stage or component in the journey.**
- The Better Practice Permission Journey will help you identify opportunities to administer permissions in a more effective and efficient way. The journey explores the digital enablers of a permission process to help you become 'digitally ready'.

How to use the Better Practice Permission Journey

- Explore each stage of the Better Practice Permission Journey. Review what 'better practice' looks like at each stage, the 'things to consider' and 'useful inputs' to improving the stage overall.
- Assess the individual components relevant to you that make up each stage, considering all potential process and digital improvements to each component. Once you have identified which components you want to improve, review the 'things to capture' and 'measures of success' to help you develop tangible actions for improvement.

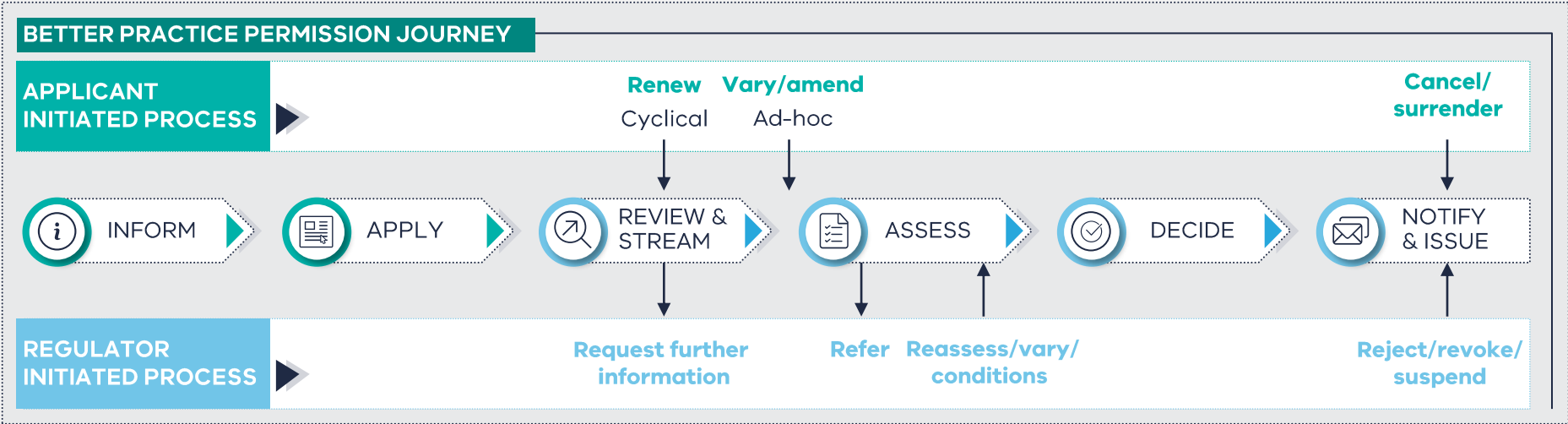
Considerations of the Better Practice Permission Journey

- The Better Practice Permission Journey covers a wide range of permissions types, from a simple or automated approvals to a more complex permits or licences requiring in-depth assessment. You should consider how your application and assessment processes can align with better practice.
- Not all components or stages might be relevant to your permission journey, so ensure you have a clear understanding of your current processes and focus on the parts that are most relevant for your permissions. Permissions vary in risk and complexity, and each permission should be reviewed separately.
- The Better Practice Permission Journey should be reviewed alongside other factors that might enable or constrain your permission such as legislation requirements, digital capabilities including automation potential, and project management requirements for each permission.

Better Practice Permission Journey Recap |

Permissions can be enabled by digital systems and platforms

The Better Practice Permission Journey is made up of six common stages. Additional processes are initiated by both businesses and regulators that input at different stages into the better practice permission journey (e.g., renewals or variations). While this is intended to cover all permissions, many don't need to touch every stage in detail (e.g., review and stream of simple applications with little variation). The journey can be enabled by digital reform.



DIGITAL ENABLERS

Systems and platforms enable the digitisation of permissions.

FRONT-END EXPERIENCE

Interface for applicants (including applicant profile dashboard, guest and log-in experience permits and licence applications, interaction history).

BACK-END SYSTEMS

Platforms for regulators to administer back-office system functionalities (including payments integration, inspection management).

INTEGRATION WITH OTHER SYSTEMS

Integration into other systems and platforms of other regulators / external bodies and agencies (including integration services API).

Better Practice Permission Journey recap |

A consistent way to design permissions for better practice

The six stages of the Better Practice Permission Journey can be considered common across permissions. **Better practice can be described at each stage, which each consist of a number of components.**

BETTER PRACTICE STAGES (1 of 2)



INFORM

The INFORM stage covers the information that you provide to applicants and regulated entities before, throughout and after the application and approvals process. It is outlined at the beginning of the permission journey for simplicity but should be considered throughout.

Information should be useful and accessible. It should include information about the regulatory scheme and requirements, provide meaningful guidance and set expectations.

Where requirements vary according to risk, the provision of information should be dynamic and surfaced at the right time.



APPLY

The APPLY stage covers the application process for applicants, who could be an individual, sole trader or company.

Information will vary across regulators. The application process should capture the minimum information required from applicants, often in a consistent way and through common components. Where useful and applications have different characteristics or risks, it should use conditional logic to stream applicants through the right pathway and level of assessment. Applicants should be able to pause and recommence applications.



REVIEW & STREAM

The REVIEW stage covers the review of application information, requests for further information and triaging based on risk.

Review of application information should be automated where possible, often through business rules in the APPLY stage. If required, it should determine whether the information is sufficient to make an assessment. Requests for further information should be limited and targeted. Where relevant, applications should be triaged against defined risk criteria to focus regulator effort on assessment.

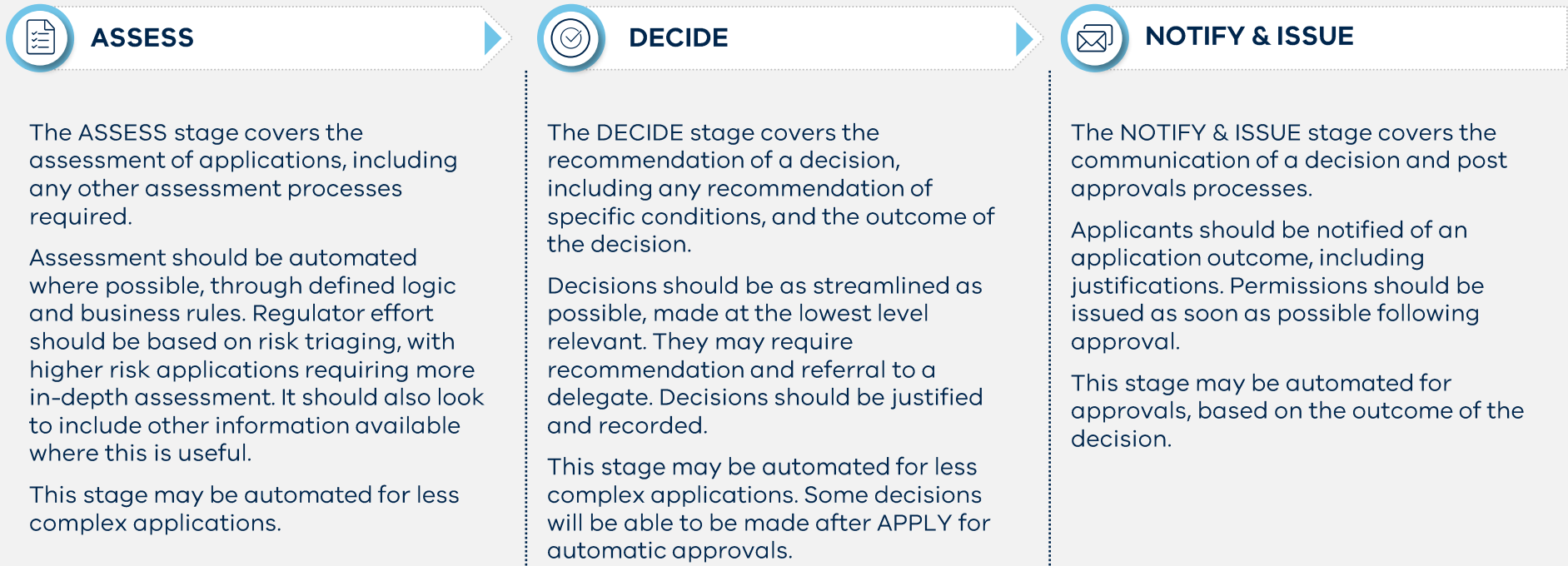
This stage may not be required or may concurrent with assessment for less complex applications or those that can be automated.

Better Practice Permission Journey recap |

A consistent way to design permissions for better practice

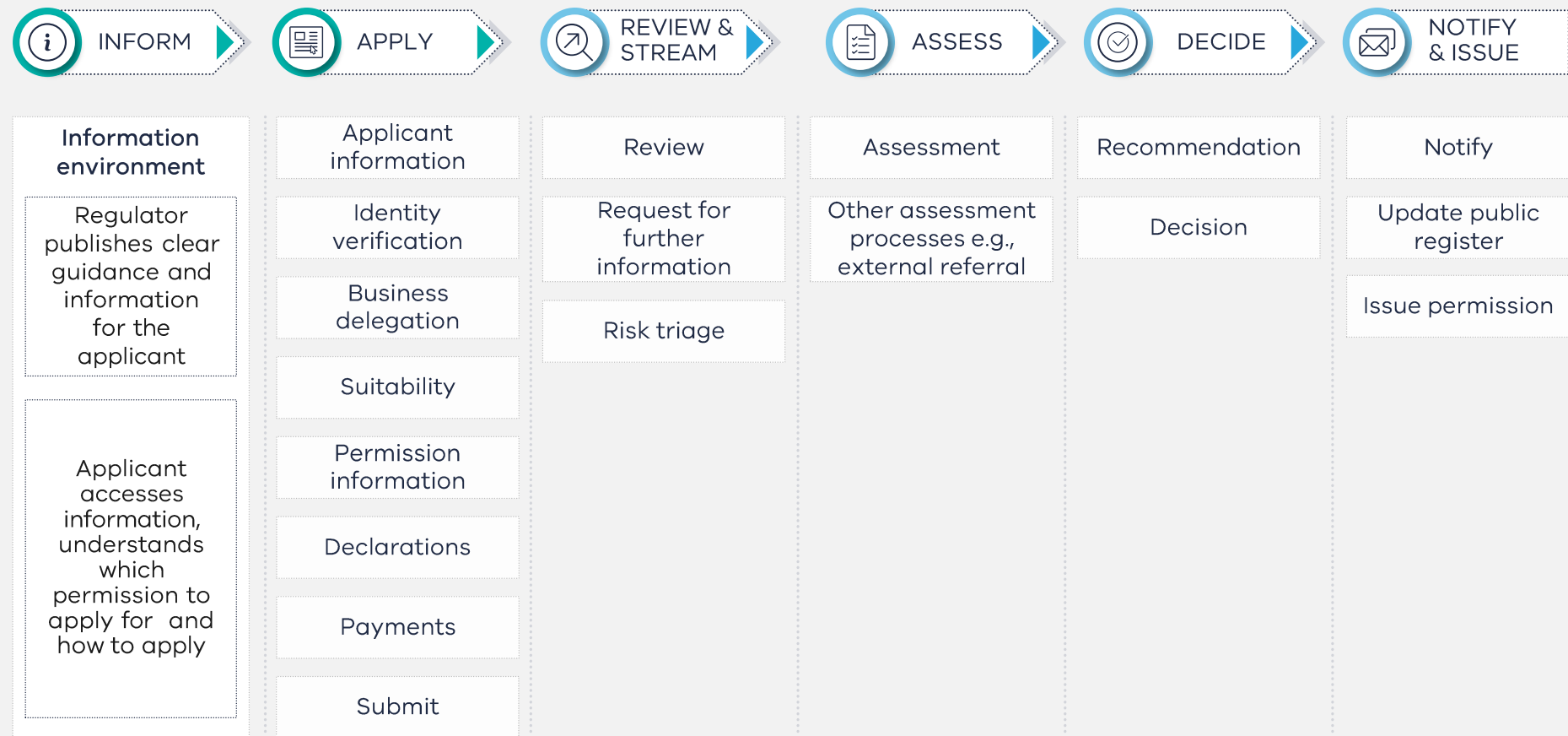
The six stages of the Better Practice Permission Journey can be considered common across permissions. **Better practice can be described at each stage, which each consist of a number of components.**

BETTER PRACTICE STAGES (2 of 2)



Better Practice Permission Journey | You can adopt common 'components' to improve permissions and make them more consistent

The Better Practice Permission Journey is made up of 'components' which represent common activities or processes undertaken by applicants and regulators. **The Playbook breaks down each of these components to provide a detailed view of what 'better practice' looks like** and how components could be enabled by digital reform. They are compatible with Service Victoria's offering.

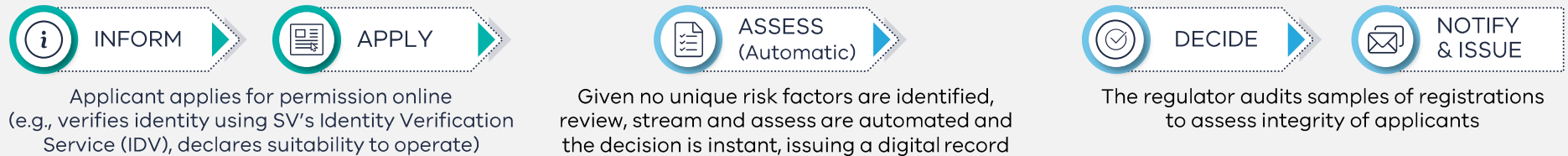


Note – this does not capture renewals, cancellations and other variations of the core process as they use the same components.

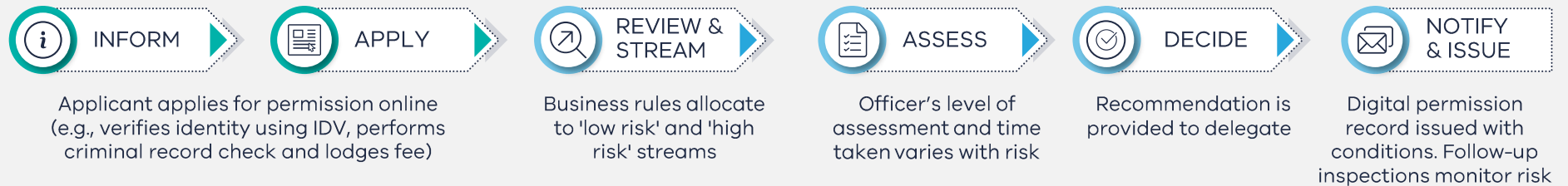
Better Practice Permission Journey | Examples of different permission through better practice

Different permissions will experience the stages and components of the journey differently. Many automatic or simple permissions may streamline review and stream and assess stages, while other more complex permissions may have a more intensive process.

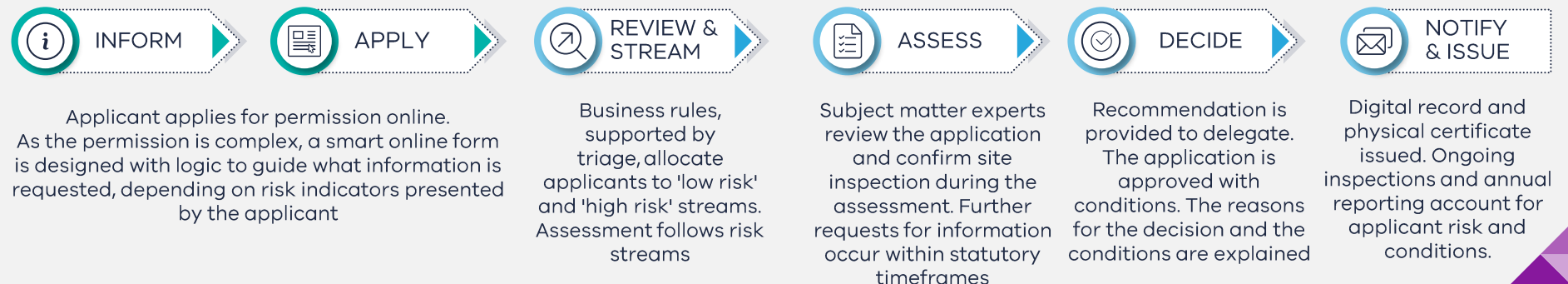
Example A: No cost registration, granted automatically on approval and lifecycle quality assurance



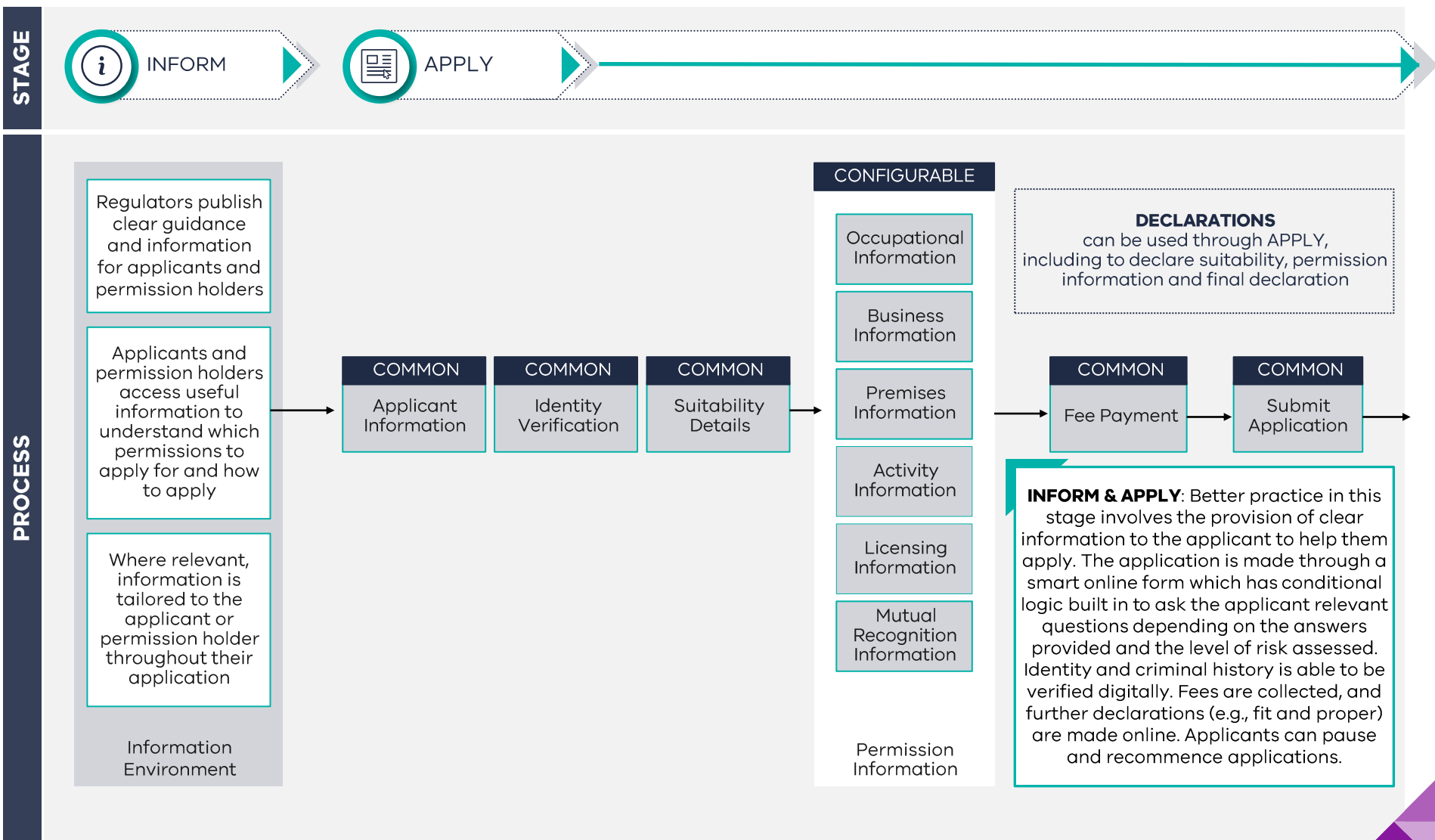
Example B: Low complexity permit review, supported by ongoing risk management



Example C: Complex licence with multiple risk factors and ongoing review



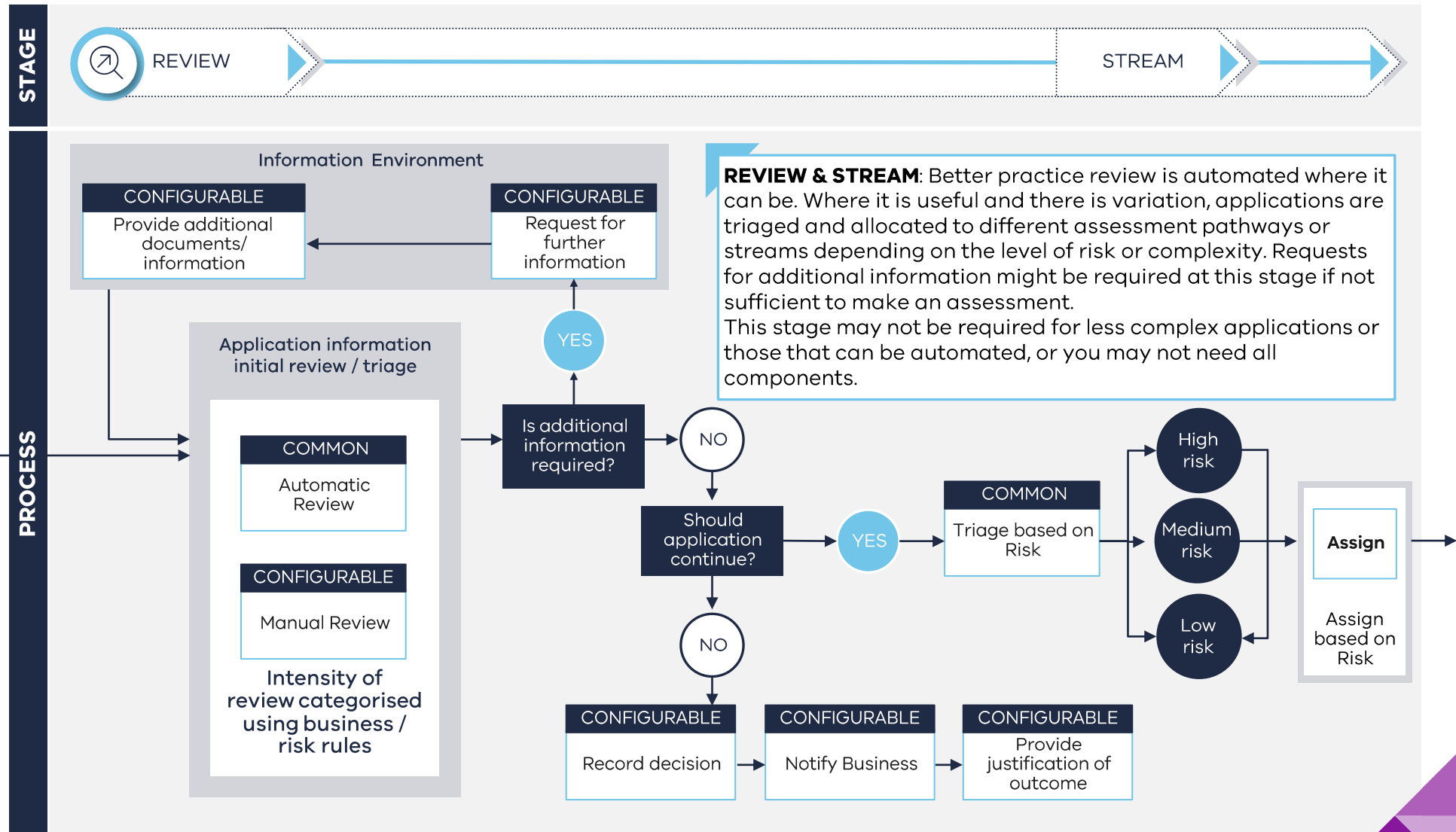
Better Practice Permission Journey | Inform and Apply



You may not need all components, refer only to those that are relevant for your permission. A digitised process might automate or bypass this stage if business rules are met and straightforward approval can be issued.

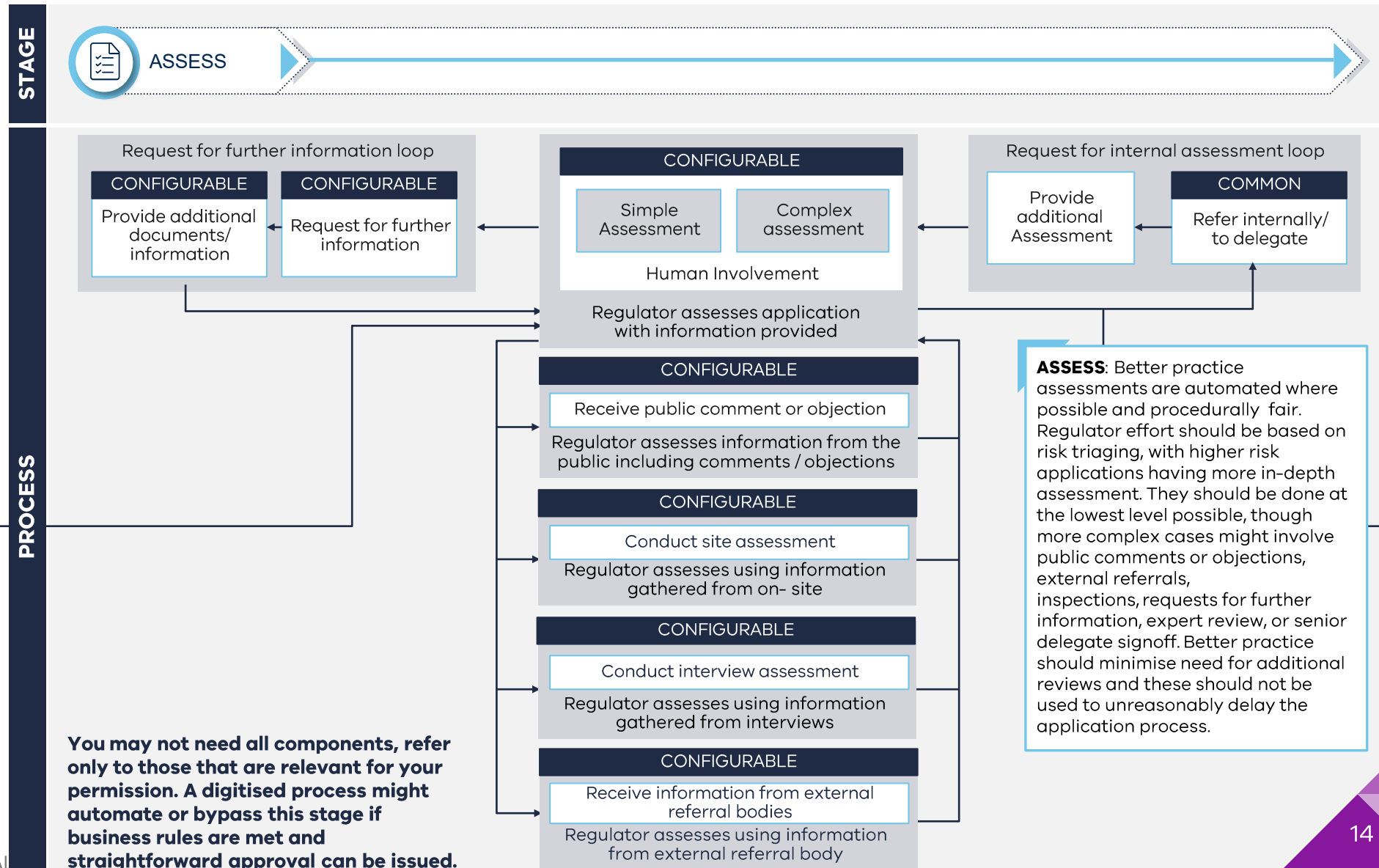
Better Practice Permission Journey

| Review and Stream



You may not need all components, refer only to those that are relevant for your permission. A digitised process might automate or bypass this stage if business rules are met and straightforward approval can be issued.

Better Practice Permission Journey | **Assess**



Better Practice Permission Journey | **Decide**



INFORM



APPLY



REVIEW &
STREAM



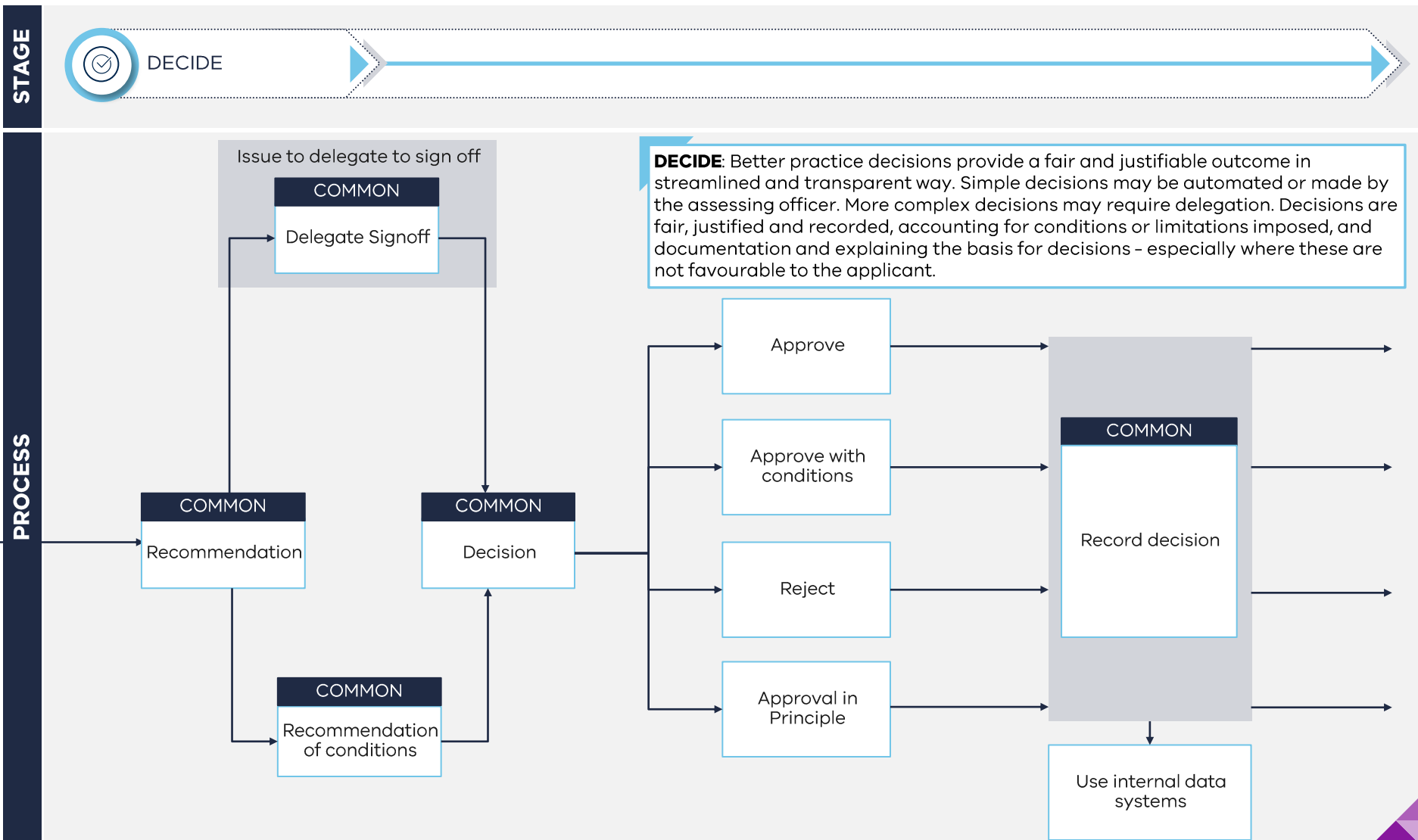
ASSESS



DECIDE

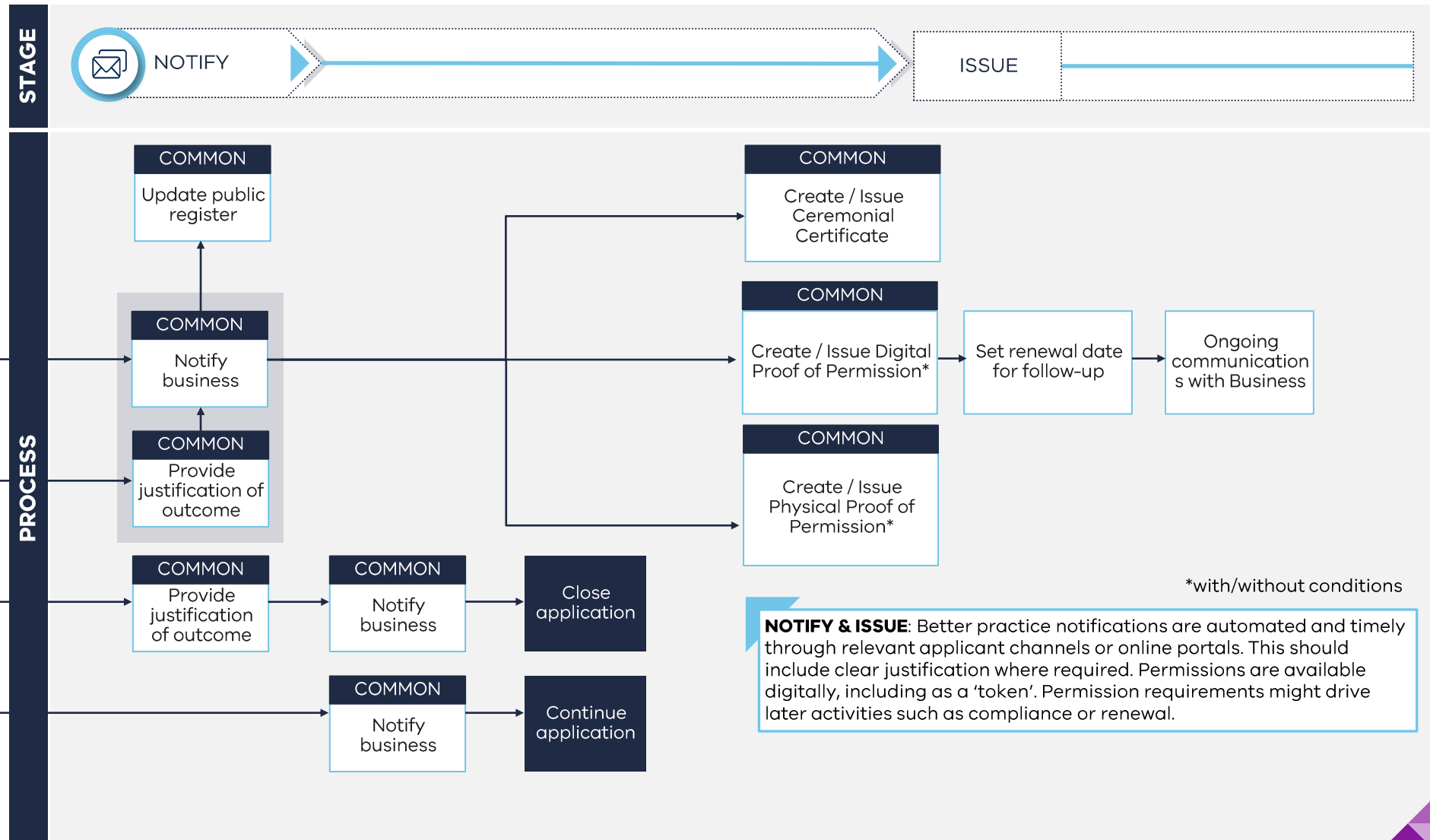


NOTIFY
& ISSUE



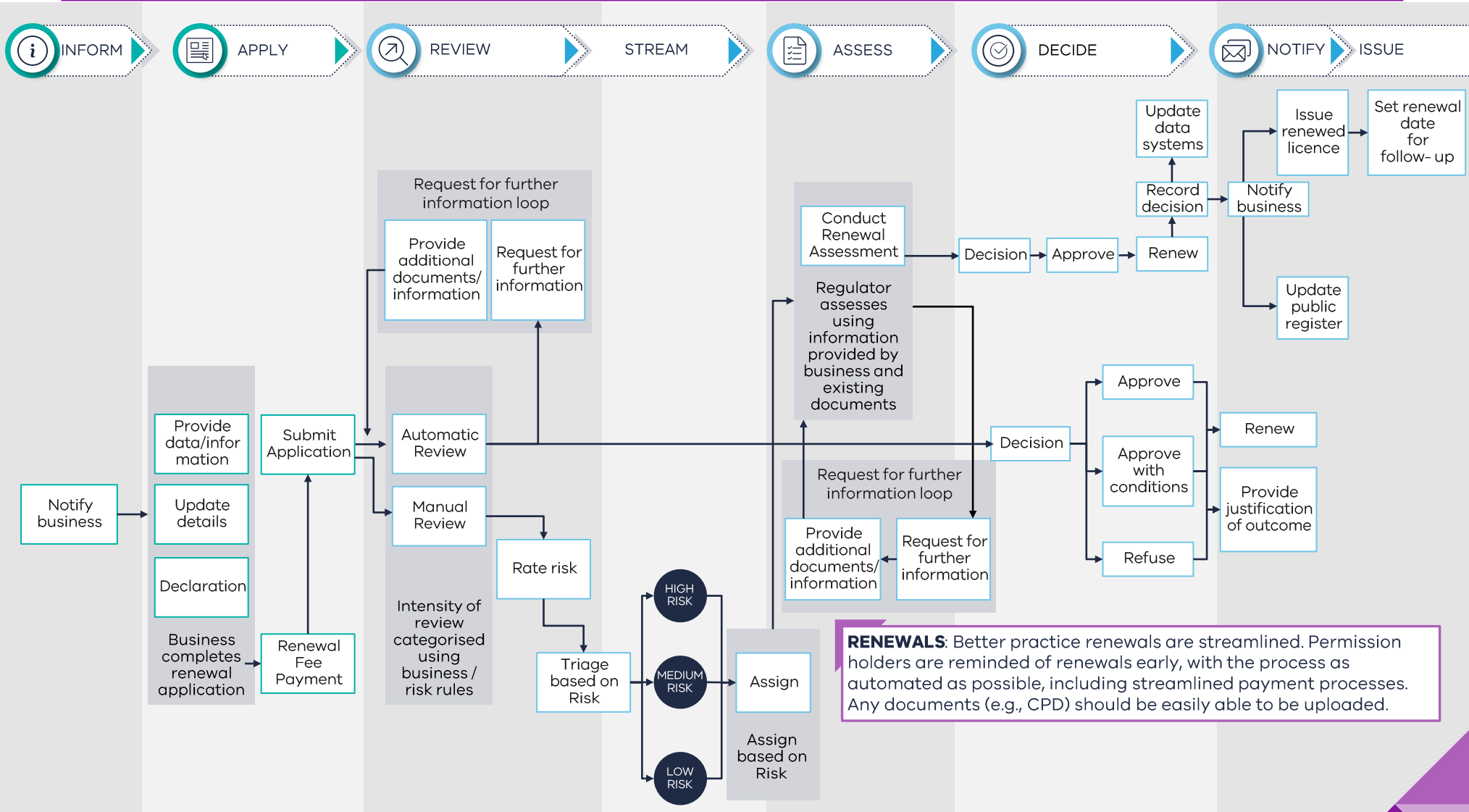
You may not need all components, refer only to those that are relevant for your permission. A digitised process might automate or bypass this stage if business rules are met and straightforward approval can be issued.

Better Practice Permission Journey | **Notify and Issue**



You may not need all components, refer only to those that are relevant for your permission. A digitised process might automate or bypass this stage if business rules are met and straightforward approval can be issued.

The Better Practice Permission Journey | **Renewals**



You may not need all components, refer only to those that are relevant for your permission. A digitised process might automate or bypass this stage if business rules are met and straightforward approval can be issued.

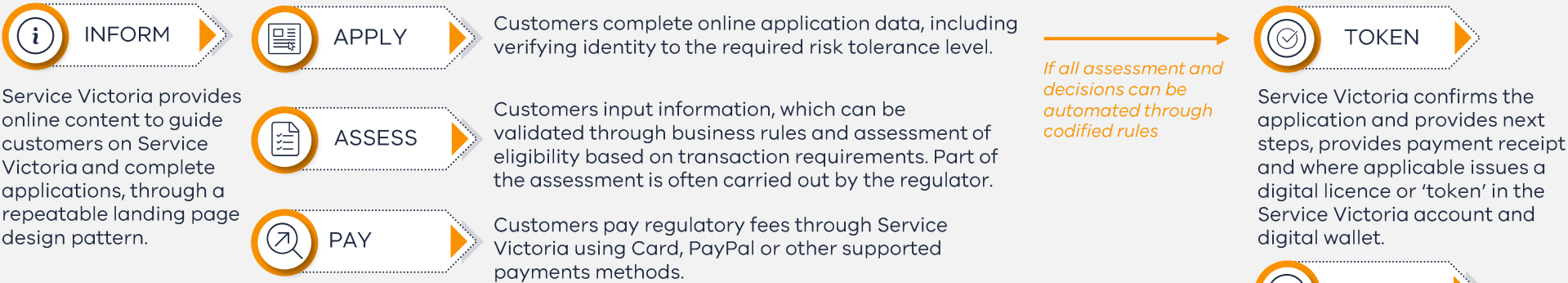
Digital and data | The Better Practice Permission Journey aligns with and complements Service Victoria’s digital reform ‘GRID’

Digitisation through Service Victoria’s is an option. **The Better Practice Permission Journey aligns and complements the Service Victoria digital reform GRID** across different permission types and complexities.

BETTER PRACTICE PERMISSION JOURNEY



SERVICE VICTORIA



REGULATOR



Regulators will need to provide more detailed information, including about regulatory requirements and technical information.

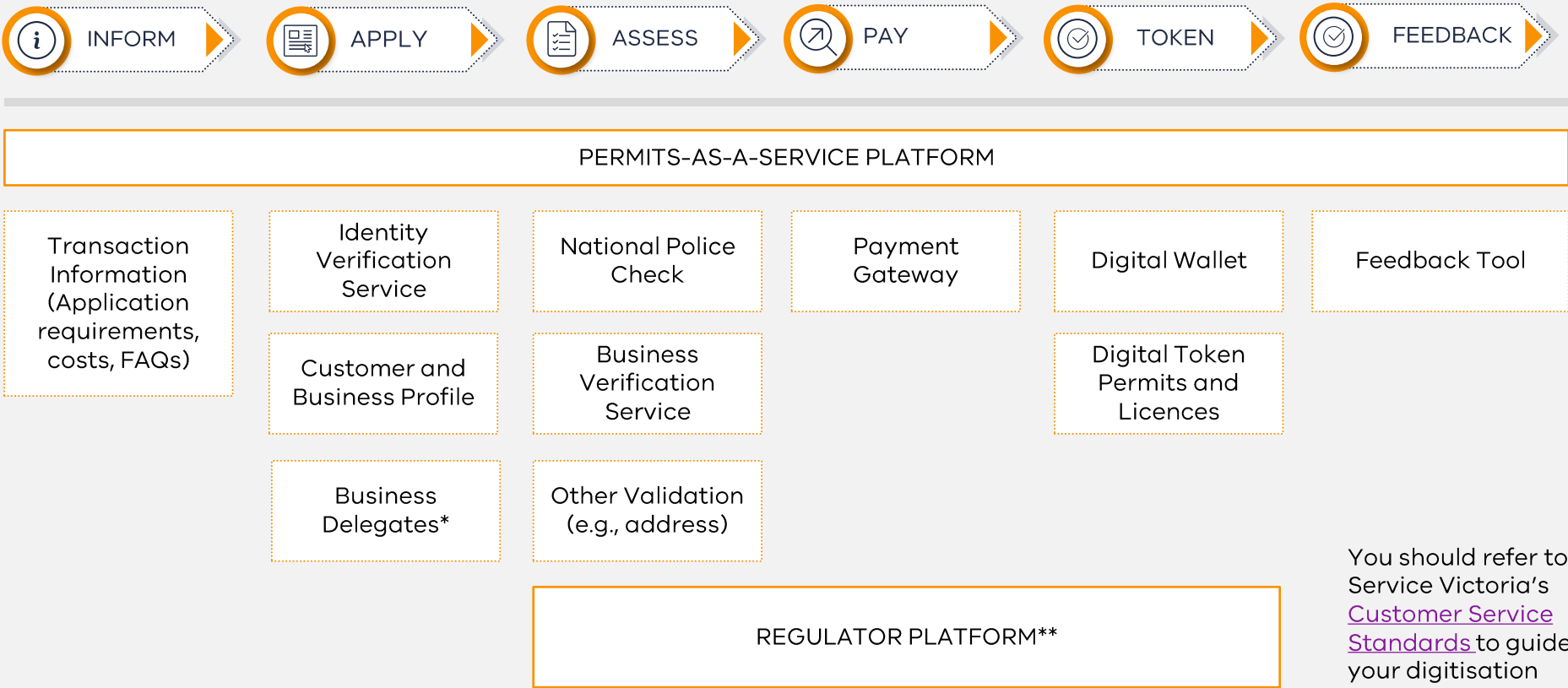
Regulators make justifiable assessment and decisions for more complex situations. Involves assessment that cannot be done automatically through codified business rules.

Regulators issue permissions and physical licences if required

Service Victoria | Service Victoria can support digitisation through common capabilities

Service Victoria offers common capabilities that can be used when digitising your permission journey, aligned with its digital reform GRID. These are aligned with the detailed components below. Consult with Service Victoria to understand more about common capabilities and digital reform opportunities.

SERVICE VICTORIA GRID



*The Business Delegates offering is not currently available but is in development.

** The Regulator Platform is shown here to highlight the parts of the customer journey (GRID) where there is interaction with customer frontend.

For action | **Work through the following stages and components to develop an action plan to improve your permission processes**







Work through the following stages and components to **identify improvement opportunities, then outline a set of implementation actions and identify enablers that support these improvements**. You should consider your key digital reform requirements, aligned to clear business outcomes.

OPPORTUNITIES	ACTIONS	ENABLERS
<p>Each stage and component provides guidance to:</p> <ul style="list-style-type: none"> Identify improvement opportunities at each stage and component of your permission journey (e.g. for better practice processes and/or digital systems). Clearly articulate the outcome you are seeking to achieve from each opportunity. Identify the benefits of implementing improvement opportunities and identify measures of success. 	<p>Each stage and component provides guidance to:</p> <ul style="list-style-type: none"> List the set of actions needed to investigate and implement the improvement opportunity (e.g. document processes, using <i>enablers</i>, update processes) Prioritise actions to implement improvements Identify timelines and key staff responsible for implementation 	<ul style="list-style-type: none"> Identify the key enablers needed to complete tasks. These could include: <ul style="list-style-type: none"> Key stakeholders – including from other departments, Service Victoria, or IT system providers Funding or investment Digital platforms / systems Data analytics Other resources
EXAMPLE	EXAMPLE	EXAMPLE
<ul style="list-style-type: none"> Improved triage of applications and allocation of effort based on an assessment of risk throughout the permission journey 	<ul style="list-style-type: none"> Codify and document risk assessment rules (e.g. risk assessment framework against different characteristics). 	<ul style="list-style-type: none"> Key reform officers who currently assess applications based on risk.

The complementary Better Practice Permission Process Manual template can be used to document opportunities, actions and enablers as you work through the following stages and components.

IMPLEMENT

Stages and Components | **Table of Contents**

 INFORM	 APPLY	 REVIEW & STREAM	 ASSESS	 DECIDE	 NOTIFY & ISSUE
Inform	Applicant information	Review	Assessment	Recommendation	Notify
	Identity verification	Request for further information	Other assessment processes e.g., external referral	Decision	Update public register
	Business delegation	Risk triage			Issue permission
	Suitability				
	Permission information				
	Declarations				
	Payments				
	Submit				



INFORM

The INFORM stage covers the information that you provide to applicants and regulated entities before, throughout and after the application and approvals process. It is outlined at the beginning of the permission journey for simplicity but should be considered throughout.

Where requirements vary according to risk, the provision of information should be dynamic and surfaced at the right time.

> INFORM

INFORM

THINGS TO CONSIDER

What information do you provide to help applicants understand what is required of them and to set their expectations (e.g., process, timing, cost)?

What information do you provide to help applicants submit higher quality applications, more consistently (e.g., guidance, templates, examples)?

Is the information you provide effective? Does it achieve what you want it to?

Do you provide information at the right time and in the right format for applicants?

Is the information you provide already available by you or other sources? Are you duplicating information that already exists?

Does the information you provide meet the accessibility requirements of *most* applicants (e.g., accessibility, readability, translation)?

How much pre-application engagement is needed, or will occur, for each permission and type or segment of applicant?

USEFUL INPUTS

Analysis of the common reasons that applicants contact you for information before and throughout the application and approvals process (e.g., through contact records, staff experience).

Analysis of the common requests for further information or where applications are below standard or fail to meet requirements (e.g., through common requests for further information).

Analysis of how effective your current information is at enabling more consistent applications (e.g., through website analytics) and reducing the number of 'outlier' applications.

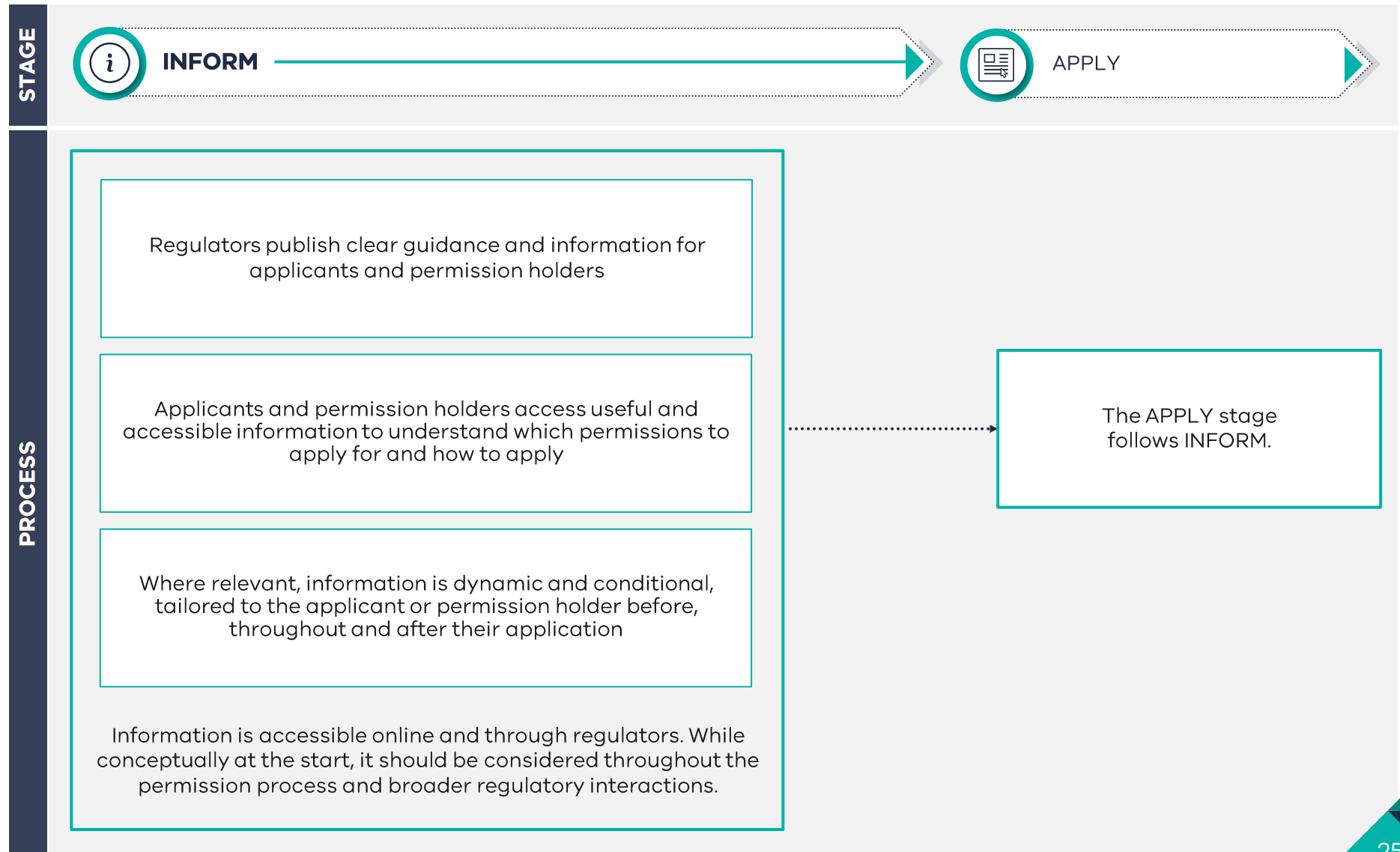
An understanding of the information that you are required to provide to applicants (e.g., defined in legislation, regulations).

An understanding of related information available through other sources (e.g., whole of government sources, other regulators).

An understanding of your applicants, how they access information and their requirements (e.g., accessibility, readability).

An understanding of your applicants and applicant segments, their specific information needs and requirements, and what interactions might be required prior to application.

Better Practice Permission Journey





DESCRIPTION

You should aim to provide useful and accessible information to applicants before, throughout and after the application and approvals process. This includes information to improve understanding, transparency and predictability of the application and approvals process, as well as information about the regulatory scheme and requirements, standard conditions that could be applied and what is required from applicants. This includes information provided within and outside the application form itself.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants have a clear understanding of the regulatory scheme and requirements, useful guidance to meet these requirements and expectations of the application and approval process. This can increase the quality of applications and reduce the number and complexity of contacts and requests for further information.

You should look for opportunities to:

- Improve and extend the information you already provide so that it is user-centric and meets the needs of applicants, including in response to feedback and available insights such as common contacts and requests for further information.
- Provide meaningful guidance for applicants, particularly for more complex requirements (e.g., templates and examples for more technical and complex documentation required, etc.).
- Clearly explain the application process and set expectations for its completion.
- Improve the readability, accessibility and language support of information so that it is useful for most applicants.
- Present information in relevant ways (e.g., content, dynamic tools and checklists, multimedia, FAQs, etc.) and surface it at the right time (e.g., guided by questions, conditional logic, etc.).
- Connect with external sources where information is already provided (e.g., other regulators, Business Victoria, etc.).

Information should be digital first, directing people to non-digital information or a point of contact where this is required.



DATA INPUTS

- N/A

DATA OUTPUTS

- N/A

DIGITAL CONSIDERATIONS

- Digital information should look to follow the Victorian Government Digital Guides, which outline best practice for Victorian Government digital information and services.
- General information should be accessible (e.g., WCAG 2.1 AA standards)¹, readable (e.g., to a Year 8 level)², and multilingual where relevant. More specialised and technical information should be readable and accessible for the relevant audience.
- Digital information should ideally be implemented through a Content Management System (CMS) or similar platform so that it can be easily updated and continuously improved. This should support multiple relevant formats. Search Engine Optimisation (SEO) can also help applicants find information.
- Any details captured about potential applicants (e.g., through proactive engagement and communications) should be captured in relevant systems.

Aligned WofG capability: Single Digital Presence. Service Victoria Permits-as-a-Service Platform. Aligns to Inform in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Information, both format and content, varies across regulators. Business Victoria and Service Victoria use a standard pattern for information.

² All Victorian Government digital information and services must comply with WCAG 2.1 AA accessibility standards as a minimum.

¹ A Year 8 level (age range 12 to 14 years) means around 83% of the Australian population is likely to understand content.

INFORM

THINGS TO CAPTURE

What are the common reasons that applicants contact you for information or where applications are below standard (e.g., you request further information from the applicant)?

What information could you update or develop to avoid these common reasons or where applications are below standard?

What other information could you update or develop to help applicants understand what is required of them and to set their expectations (e.g., process, timing, cost)?

What guidance, templates and examples could you develop to support applicants?

Is the information you provide accessible and understandable for *most* applicants?

What opportunities are there to continuously improve the information you already have?

INDICATIVE MEASURES OF SUCCESS

Improved applicant satisfaction.

Reduced number of contacts for common information.

Improved quality and reduced variation of applications.

Reduced number of requests for further information.

Improved readability and accessibility of information.

ACTION PLAN

Document and prioritise opportunities to update or develop useful and accessible information.

Identify segments of applicant types, their information needs, and tailor information provision on this basis.

Consider opportunities for proactive outreach and engagement with industry.



APPLY

The APPLY stage covers the application process for applicants, who could be an individual, sole trader or company.

Information will vary across regulators. The application process should capture the minimum information required from applicants, often in a consistent way and through common components. Where useful and applications have different characteristics or risks, it should use conditional logic to stream applicants through the right pathway and level of assessment. Applicants should be able to pause and recommence applications.

> APPLICANT INFORMATION

> IDENTITY VERIFICATION

> BUSINESS DELEGATION

> SUITABILITY

> PERMISSION INFORMATION

> DECLARATIONS

> PAYMENTS

> SUBMIT

APPLY

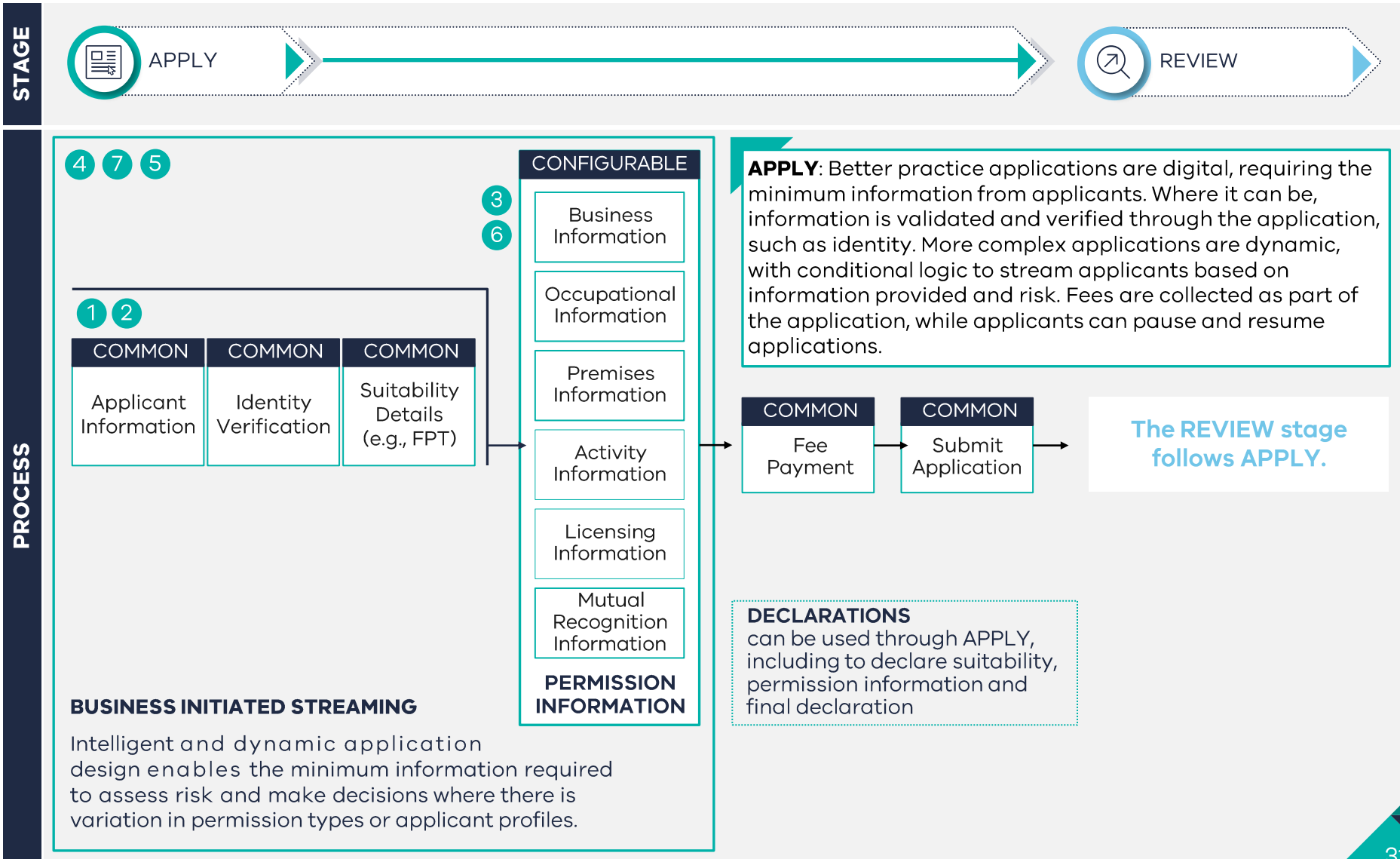
THINGS TO CONSIDER

- 1 How is your application process currently designed (e.g., organically changed over time, recently redesigned)?
- 2 Are you requesting the minimum information required from applicants (e.g., defined by legislation, required to assess risk or make a decision)? What additional information do you capture?
- 3 What are the key indicators of regulatory risk which you capture through the application process? Can you determine when an application is unlikely to receive approval?
- 4 What are the common reasons of lower quality applications (e.g., common reasons for requests for further information)?
- 5 How do you ensure that you reuse information you already hold (e.g., use existing information to pre-fill)?
- 6 Does your application process use conditional logic and stream based on risk, and does it auto-validate and verify information during the application?
- 7 Have you explored using digital capabilities to improve the application process and business experience (e.g., smart forms and portals, digital identity verification)?

USEFUL INPUTS

- An understanding of your current application process, including applicant journey and pain points.
- An understanding of the information that you are required to capture from applicants (e.g., defined in legislation, regulations) and additional information to achieve regulatory outcomes.
- Analysis of key indicators of regulatory risk.
- Analysis of the common requests for further information you require or where applications are below standard (e.g., through common requests for further information).
- Analysis of information available through reusable sources (e.g., existing records, whole of government sources).
- An understanding of your applicants, how they access information and their requirements (e.g., accessibility, readability).
- Analysis of digital opportunities (e.g., other regulators, Service Victoria).

Better Practice Permission Journey



You should consider the differences between types of applicants

Permission applications can be made by individuals, sole traders or companies

For many permissions, applicants can often be individuals, sole traders or companies. **You should consider which entities are likely to apply for your licences, the nature of the information they provide, and account for the implications of this on privacy, information retention and reusability requirements.** In some instances, the individual completing the application may be an applicant – in others they may differ.

1. Which entities can hold permissions?

2. What are the privacy requirements and safeguards for different entities?

3. How are you recording and retaining information from different entity types?

INDIVIDUAL	SOLE TRADER	COMPANY
<p>The applicant and permission holder is an individual as a natural person.</p> <p>The applicant and individual completing the application are likely to be the same individual.</p> <p>Permission information is more likely to include personal information (e.g., name, contact, etc) and therefore subject to OVIC Information Privacy Principles. In some cases, this information may be "sensitive information" and must be handled in accordance with OVIC IPP Principle 10 – Sensitive Information.</p>	<p>The applicant and permission holder is an individual acting in a business capacity.</p> <p>The applicant and individual completing the application are often the same individual.</p> <p>Permission information may be considered personal information, particularly when it is attributable to an individual capacity and therefore may be subject to the OVIC IPPs.</p>	<p>The applicant and permission holder is a company.</p> <p>The individual completing the application is on behalf of the business. This may be a Director or business representative.</p> <p>Permission information is less likely to be considered personal information, as it is generally about a company rather than an individual, and therefore may not be subject to the OVIC IPPs.</p>

Note: This is a general frameworks for different types of information. You should seek specific advice when applying this to a particular context.



APPLICANT INFORMATION

DESCRIPTION

Information is generally captured about the applicant for each permission, whether they are an individual, sole trader or company.

Applicant information incorporates a limited set of information about the applicant, including personal, company and contact information. The extent of information required will vary by applicant and permission type (e.g., occupation licences may require more personal information than company licences).

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants can provide a limited set of personal, company and contact information, with transparency over why it is required and how it is used. Where possible, this is pre-filled from an account or profile and validated through the application.

You should consider the minimum information generally required from each applicant type. This may be defined by legislation, but at minimum should be enough to establish an account and communicate with the applicant.

- Individual – name and contact information (e.g., email, contact number, address, etc.).
- Sole trader – name and contact information, plus simple company information (e.g., ABN, ACN, registered location, etc.).
- Company – name, contact and simple company information, plus business representative information where the individual completing the application is different from the applicant.

You should aim to provide guidance to applicants, why information is required and how it is used, including through a collection statement and privacy statement. Information should be the least sensitive required for the purpose (e.g., age or year of birth where required, rather than date of birth) or not captured (e.g., gender, rarely required for regulatory outcomes).

Individual information is more likely to be considered personal information (e.g., name, phone, address, as well as information like employee record, signature, photo, etc.) and therefore subject to OVIC Information Privacy Principles (IPPs). This should be minimised to what is required. Company information, including for representatives acting on behalf of a business, is less likely to be considered personal information (e.g., business phone number for company employees). **You should consider seeking legal advice on privacy requirements.**



APPLICANT INFORMATION

DATA INPUTS

FROM APPLICANT

- Information typically collected from applicants (name, email, contact number, address)
- Additional information typically collected from a sole trader or company (ABN, ACN, registered address, business representative information)
- Additional personal information (e.g., age, date of birth, gender, pronouns/preferred identification information) should only be collected with good reason and justification.

DIGITAL CONSIDERATIONS

- Applicant information should be pre-filled from an existing account or profile where possible. This may be from regulator systems or Service Victoria's Customer and Business Profile.
- Information should be validated through the application where it can be. This could include simple validation through common processes (e.g., email verification) or with external data sources (e.g., address lookup services, ASIC company lookup).
- Information should be captured in a consistent data structure and format, in a way that enables improved data quality, including restricted entry fields and options or lists rather than free text entry. Applicant information is generally captured against the permission holder account, to enable a holistic understanding of their history, performance and risk profile, particularly for information sharing and risk management.*

Aligned WofG capability: Service Victoria Customer and Business Profile. Aligns to Apply in the Service Victoria GRID.

DATA OUTPUTS

TO REGULATOR

- Applicant information for an individual, sole trader or company.

COMPONENT

COMMON COMPONENT

Applicant information should be common across applications.

Any variation should be supported by a clear justification and rationale.

CONFIGURABLE COMPONENT

*See slide 30 for more information on how to structure your data through data models

IDENTITY VERIFICATION



DESCRIPTION

Identity verification of applicants is required in many applications, whether they are an individual, sole trader or representative of a company. It varies between regulators, generally dependant on current processes and commensurate with risk, but often takes the form of a variation on the 100 points of identity check. It is a key enabler of the application and approvals process as a tool to mitigate risk.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants can verify their identity in a consistent and trusted way which enhances their privacy and minimises data. They are only required to provide the minimum amount of identity information necessary to meet identity requirements. It can apply to individuals, sole traders, representative of a company and other individuals as part of the application process.

You should consider the lowest level of identity assurance required from applicants, commensurate with risk. This can be aligned with Service Victoria's Identity Verification Standards (IDVS) and Levels of Assurance (LOA):

- No or limited level of assurance (e.g., where a declaration is enough or where an applicant is a business, recognising a business representative or delegate may need higher level of identity verification)
- Basic level of assurance (LOA 1)
- Medium level of assurance (LOA 2)
- High level of assurance (LOA 3)
- Very high level of assurance (LOA 4)

Regulators should use a risk-based approach for identity verification. Many permissions align up with to LOA2, some LOA3.

Identity verification information for individuals is generally considered personal information (e.g., identity documents such as drivers' licence, etc.) and therefore subject to OVIC Information Privacy Principles (IPPs). You should consider advice on privacy requirements. Identity information and documents should not be retained once identity is verified, or should be collected and retained securely and disposed as soon as feasible.



IDENTITY VERIFICATION

DATA INPUTS

FROM APPLICANT

- LOA1: One satisfactory¹ identity document
- LOA2: Two satisfactory identity documents
- LOA3: As in LOA2, plus photo bind and liveness.

The required LOA levels for permissions can be confirmed through IDV or aligned with regulator processes.

DATA OUTPUTS

TO REGULATOR

- From IDV: Identity verification outcome
- From applicant: Identity information (e.g., certified copies of satisfactory identity documents), to be verified by regulator

DIGITAL CONSIDERATIONS

- You should look to reuse common capabilities to verify identity, including reuse of Service Victoria's Identity Verification Service (IDV) and to issue Electronic Identity Credential (EIC) which applicants can choose to have ongoing and can be re-used for up to 10 years. This can be used for both digital and non-digital platforms, including those submitted outside the Service Victoria platform. Service Victoria retains the minimal amount of information needed to confirm an applicant's identity and applicant consent is required for use of the identity verification service.
- Where you are unable to reuse Service Victoria IDV and EIC, you should look to minimise identity verification requirements and the capture and storage of identity information.

Aligned WofG capability: Service Victoria IDV and EIC (Service Victoria currently supports LOA 2 and LOA 3). Aligns to Apply in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Identity verification should be common across applications.

Service Victoria IDVS provides a common risk-based framework for identity verification.

CONFIGURABLE COMPONENT

¹ Satisfactory identity documents include Commencement of Identity and Use in the Community documents.

BUSINESS DELEGATION



DESCRIPTION

Companies often require representatives to act on their behalf. Business delegations capture the relationships between companies and the representatives authorised to act on their behalf (generally individuals), as well as information about the delegate. These relationships can vary, including internal relationships (e.g., administrative roles within a business) and external relationships (e.g., agents or consultants), and are likely to be in addition to the primary applicant. The contact and personal information of business delegates are less likely to be considered personal information.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Representatives are able to act on the behalf of applicants and permission holders, with the relationship captured in a trusted way which enables integrity of the application and approvals process. In many cases, individuals are authorised to act on the behalf of companies, but business delegation can capture broader arrangements (e.g., individual to individual, individual to sole trader, etc.).

Applicants can have multiple representatives and for different purposes. You should aim to capture relevant information about delegations.

- Relationship between the applicant or permission holder and the representative (e.g., each side of the relationship). This should be captured as a relationship between the permission holder account and representative.
- Purpose and activities that are delegated (e.g., a specific activity, subset of total activities, overall delegation)
- Timeframe the delegation is active for (e.g., perpetual, time bound, activity bound).

You should aim to capture a limited set of information about representatives, aligned to applicant information. Identity verification requirements for representatives are likely to be aligned with those for applicants.

There are different models for business delegations, commensurate with risk. The relationship may be able to be established as part of the application (e.g., by the representative), or may be required to be established prior to the application (e.g., by the applicant).

BUSINESS DELEGATION



DATA INPUTS

FROM APPLICANT

- Business delegation (e.g., representative, relationship, purpose, activities and timeframe).
- Delegate information (aligned to applicant information)
- Delegate identity verification (if required, aligned to identity)

DATA OUTPUTS

TO REGULATORS

- Business delegation
- Delegate information
- Delegate identity verification

DIGITAL CONSIDERATIONS

- You should look to capture business delegation information digitally. Depending on requirements and commensurate with risk, this may be as part of the application or may be required prior to the application. Regulators should be clear about the level of identity verification required for business delegates, and the level of personal information required.
- There is currently limited reusable digital capability to capture and reuse business delegations. Service Victoria is designing a business delegates capability.

Aligned WofG capability: Service Victoria Business Delegates (TBC).

Service Victoria Customer and Business Profiles. Aligns to Apply in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Business delegations should be common across applications.

Service Victoria is developing a framework for reusable business delegations.

CONFIGURABLE COMPONENT



DESCRIPTION

Regulators often assess the suitability of applicants to hold a permission. The suitability of individuals may be assessed for applicants that are individuals or sole traders, while the suitability of a company (and indirectly of its directors and representatives) may be assessed more holistically. It varies significantly across regulators, from a declaration to a robust assessment of many information sources and can prevent applications or be used to capture further information and focus assessment. Suitability often consists of Fit and Proper Tests (FPTs) and other conduct and character information.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants can verify their suitability in a consistent and trusted way which enhances their privacy and minimises data collection. They should provide the minimum amount of information necessary to meet suitability requirements. Suitability can apply to individuals, sole traders, representative of a company and other individuals as part of the application process.

You should account for the impact of different suitability information on applications. It may prevent an application from progression (e.g. go or no-go), be used to capture additional information or be used to assess risk and focus assessment effort. You should look to assess whether suitability information is necessary and relevant to the assessment of an application, and how it is captured.

Different approaches may include:

- Declaration of suitability (e.g. declaration that an applicant is fit and proper against requirements with the ability to check and act against the information after the permission issues, etc.)
- Verification of standard suitability information (e.g. verification of relevant offences only through a National Police Check, verification of financial misconduct or bankruptcy, etc.)
- Verification of complex suitability information (e.g. letters of professional standing, character assessment, etc.).

Where there is variability between applications, you should look to stream applications based on defined business rules to adjust required suitability information based on risk. You should also look to broader intelligence and information sources.

Suitability is not always binary and you should consider if applicants should have the opportunity to provide further information or justification where they do not meet requirements (e.g. for a lower risk previous offence or instance of misconduct).

SUITABILITY



DATA INPUTS

FROM APPLICANT

- Declaration or demonstration of suitability
- Common suitability information (e.g., National Police Check)
- Additional suitability information (e.g., character reference)
- Additional information for any non-compliance against suitability criteria.

DATA OUTPUTS

TO REGULATOR

- Declaration of suitability
- Common suitability information (e.g., National Police Check)
- Additional suitability information (e.g., character reference)
- Additional information for any non-compliance against suitability criteria.

DIGITAL CONSIDERATIONS

- Digital channels should be used where possible to capture and verify suitability information (e.g., declarations enabled by identity, National Police Checks, and other common checks from reputable bodies). Where possible, you should reuse common capabilities to capture and verify suitability information, including reuse of Service Victoria National Police Check service.
- Digital systems should be used to automate the outcomes of suitability enabled by defined logic and business rules, including preventing an application from being submitted, dynamically asking for further information or as a input to risk assessment.
- Where you are unable to reuse Service Victoria National Police Check and other common capabilities, you should look to minimise suitability requirements. You should avoid capturing and storing suitability information. Any suitability information should be appropriately discarded once suitability is verified, or as soon as possible.

Aligned WofG capability: Service Victoria National Police Check. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Suitability should be common across many, if not most, applications.

DTF is developing a common framework for suitability, more specifically FPT.

CONFIGURABLE COMPONENT



PERMISSION INFORMATION

DESCRIPTION

Regulators capture detailed information about permissions to assess applications. This builds from information about the applicant (e.g., applicant information, identity, suitability, etc.) to incorporate a set of information specific to the permission being issued. Permission information can be considered in six components – *business information, occupational information, activity information, premises information, licensing information, and mutual recognition information.*

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants can provide the permission information required for a specific information component, with transparency over why it is required and how it is used. Where possible, this is pre-filled from an account or profile and validated through the application.

You should assess the minimum information generally required for each permission, likely correlated to the lowest risk applications, and the additional information required for higher risk applications. This may be defined by legislation, but at minimum should be enough to make an assessment about the permission. Different permission types generally require different permission information, for example:

- Occupation licence – occupation information (e.g., qualifications, etc.), often licensing and mutual recognition information.
- Business licence – business information (e.g., business structure, directors, etc.), often activity and premises information.
- Activity permit – business information, activity information, potential premises information.

You should look for opportunities to streamline the capture of permission information, such as through a declaration or capturing relevant extracts of information through the application form rather than uploading large documents.

Where there is variability between applications, you should look to stream applications based on defined business rules to adjust required permission information based on risk, generally more information for higher risk applications. You should also look to broader intelligence and information sources to assist regulators with their assessment.



PERMISSION INFORMATION

OCCUPATIONAL INFORMATION*	Information related to an applicant's qualifications and skills (e.g., formal higher education and VET qualifications, training, practical experience, etc.). Most relevant for occupational licensing.	Information should be sourced and verified from trusted data sources where available (e.g., My eQuals for higher education qualifications).
BUSINESS INFORMATION*	Information useful to identify and assess businesses (e.g., organisation and structure, financial viability, directors, etc.). Most relevant for business permissions and where businesses are applicants for other permissions.	Information should be sourced and verified from trusted data sources where available (e.g., ASIC for business information). Service Victoria's Business Verification Service verifies ABN and business registry information.
ACTIVITY INFORMATION*	Information regarding one-off or regular events and projects (e.g., time, location, and event specific details required to assess the feasibility, impact, and suitability of events, etc.). Most relevant for permits.	Information is variable to different activities. This can be configured to facilitate varying requirements.
LICENSING INFORMATION*	Information of the businesses' history with the regulator and other regulators (e.g., licences currently and previously held, outcomes, conditions, etc.). Relevant for many permissions.	Information should be pre-populated or automatically captured where possible. Service Victoria Business Profile and Customer Record will capture licensing information for many permissions.
MUTUAL RECOGNITION INFORMATION*	Information of the applicant's relevant history with other regulators (e.g., standing, compliance, character, etc.), in particular jurisdictions outside of Victoria. Most relevant for mutual recognition.	Information is generally available in different formats from other jurisdictions. Data structures should be designed to enable and ensure compatibility with other jurisdictions.
PREMISES INFORMATION**	Information about the premises or location relevant for a permission (e.g., address, location information, premises specifications and designs, tenure details, geospatial data etc.). Most relevant for premises permissions.	Information can be complex (e.g., architectural plans), which should only be used where required given increased burden. Site inspections should only be conducted where there is a clear rationale for doing so.

*Permission information will generally be captured at the Permission layer under your data model and linked to the Permission Entity account.

**Premises information will generally be captured alongside the Permission layer under your data model, linked to the Permission Entity account..

An example [data model](#) and [relationship model](#) are provided in the appendices.



PERMISSION INFORMATION

DATA INPUTS

FROM APPLICANT

- Permission information and documentation required across six configurable components – *occupational information, business information, activity information, premises information, licensing information, and mutual recognition information.*

DATA OUTPUTS

TO REGULATOR

- Permission information and documentation required to support eligibility, risk and application assessment.

DIGITAL CONSIDERATIONS

- Permission information should be pre-filled from an existing account or profile or related application where possible.
- Information should be validated through the application where it can be. This could include simple validation through common processes (e.g., premises and business lookup) or verification with external data sources (e.g., higher education qualification verification, related permissions, etc.) through integration or APIs.
- Applications should look to conditionally stream applicants based on defined business rules to adjust required information based on risk, where there is variance between applications or where permission information is only required in some circumstances.
- Information should be captured in a consistent data structure and format, in a way that enables improved data quality, including restricted entry fields or other formats (e.g., document upload). Permission information is generally captured against the permission, under the permission holder account.*

Aligned WofG capability: Service Victoria Customer and Business Profile, Business Verification Service, Customer Record. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Permission information requirements vary and are configurable across regulators.

Components should be consistent where possible, with configurable information.

*See slide 30 for more information on how to structure your data through data models

DECLARATIONS



DESCRIPTION

Declarations can be an important tool for applicants to attest to statements or that the information they have provided is true and correct. They are an enabler of better practice permissions and can be used at different points throughout the application, with a final declaration often required prior to submission.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants are able to provide declarations, rather than provide additional information and evidence, where possible and commensurate with risk. Declarations are clear and applicants understand what they are declaring.

You should consider the points in an application at which declarations can be used to make and confirm claims, in an accessible way. This may include a declaration of identity, suitability, or permission information (rather than providing further information), a declaration against certain criteria, additional information, conditions, or a final declaration of the application.

Declarations should account for scope of legislation and the level of risk involved with the information, as well as the availability of measures available to enquire, monitor, investigate and act on false, misleading or incomplete information after an application (e.g., inquiry powers, suspensions, revocations, penalties, etc.).

You should consider the different types of declaration that could be used.

- A simple declaration (e.g., tick a 'confirmation as true' box in the application) may be sufficient for many applications, particularly for lower risk information and applications and where your scheme allows for investigation and penalties.
- A statutory declaration may be required for higher risk applications, with additional controls and mechanisms for action under the *Oaths and Affirmations Act 2018*. These require external production and citation before being provided, which can add significant effort for applicants.

Declaration settings should be regularly reviewed and updated to ensure they are up to date with legislative requirements.



DECLARATIONS

DATA INPUTS

FROM APPLICANTS

- Declaration of compliance with stated criteria.
- Declaration of understanding and agreement with future conduct and compliance requirements.
- Additional information, where declarations are unable to be made by applicants, where relevant.

DATA OUTPUTS

TO REGULATOR

- Declarations.
- Additional information, where provided by applicants.

DIGITAL CONSIDERATIONS

- Depending on the circumstances, applications should design declarations that are either 'absolute' (e.g., declaration required to progress) or non-absolute (e.g., compliant or not compliant, declaration with criteria, with ability to provide further information if not complaint).
- Declarations should draw from a library of common declarations, developed by the regulator. Declarations should be designed into the application process depending on the information provided in each stage and should therefore be standard across similar applications.
- They should be automatically recorded in systems and provide a reliable record that can be used if required to verify declared content (e.g., for future compliance assurance or investigations).

Aligned WofG capability: N/A. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Declarations are often specific to the information required or legislation.

Declarations should look to follow consistent patterns.

PAYMENTS



DESCRIPTION

Most permissions require the associated fee to be paid with applications, as well as through renewals. Payments vary between regulators and permissions. Some have simple, set fee structures while others are calculated on fee units or on a pro-rata basis.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Applicants understand fees and how they are calculated, and are able to complete payments through common processes as part of the application process.

You should look for opportunities to make payments as streamlined and simple as possible for applicants.

- Provide information about estimated fees before and during the application, with transparency over how they are derived and calculated.
- Calculate fees automatically based on information provided through the application.
- Provide easy payment methods that applicants are familiar with and can pay as part of the application (e.g., credit cards, PayPal, etc.), with support for those who are less able to use those methods (e.g., less digitally able, disadvantaged applicants).
- Consider payment options that might be useful for applicants (e.g., different periods, instalments), providing this doesn't overcomplicate the payments process.
- Assess whether refunds may be required and how they are administered (e.g., through the same payment gateway or separately, recognising they are generally lower volume).

These considerations are based on the administration of payments being with your control. This is not always the case and you may have limited control over the design of pricing and fees and administration of payments.

PAYMENTS



DATA INPUTS

FROM APPLICANT

- Fee estimate and calculated amount
- Payment details (depending on payment method e.g., credit card details)

DATA OUTPUTS

TO REGULATOR

- Payment amount, reconciled with application
- Record of payment (e.g., transaction record)

TO APPLICANT

- Record of payment (e.g., receipt)

DIGITAL CONSIDERATIONS

- Payments should be made in the most convenient and relevant way that applicants are familiar with, supported by technology (e.g., online payments using credit card, payment gateways like PayPal, etc.). Service Victoria Payments Gateway can be reused*.
- Payments should be automatically calculated based on information provided by applicants, in line with regulatory requirements. Where possible, they should be completed as part of the application, not through a separate process (e.g., invoice and subsequent payment).
- Payments should be automatically reconciled with applications in regulator systems where this is possible.
- Payment reference number and receipt of payment should be automatically provided to applicants at the point of submission to provide security to the business.

Aligned WofG capability: Service Victoria Payment Gateway. Aligns to Pay in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Payments should be common across permissions and regulators.

Service Victoria Payments Gateway provides a common capability.

CONFIGURABLE COMPONENT

*Note - a Westpac Merchant ID is currently required to use the Service Victoria Payments Gateway.

SUBMIT



DESCRIPTION

Applications need to be submitted to enter the approvals process. Once submitted, applications are lodged with the regulator, attached with a reference number to commence the review and assessment process. Where this is automated, the application outcome should be provided.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Submission of applications is simple and streamlined. Applicants have confirmation of their submitted complete application, which has been lodged with the regulator.

You should look for opportunities to support applicants before and after submission.

- Design applications to not allow submission until complete, except in defined circumstances. Any areas requiring clarification or further information should be clearly identified to the applicant.
- You should allow applicants to save and resume an application prior to submission.
- Provide confirmation of submission, including a reference number where possible. This can be provided at the point in time (e.g., on the screen), as well as sent to the applicant (e.g., through email).
- Outline the next steps following submission, including guidance to set expectations around likely processing times and any further interactions. This should be connected to broader information and a point of contact.
- Seek feedback on the application experience, including satisfaction and areas for continuous improvement.

For lower risk permissions that can be automatically approved and issued following defined business rules, confirmation of outcome and issuance and any other relevant details should be provided straight after submission.

SUBMIT



DATA INPUTS

FROM APPLICANT

- Application is submitted with all required information

DATA OUTPUTS

TO APPLICANT

- Confirmation of submission, including reference number
- For automated applications, the application outcome

TO REGULATOR

- Submitted application
- For automated applications, the application outcome

DIGITAL CONSIDERATIONS

- Applicants should be able to save and resume their application at any point prior to submission. This can be captured as a draft application.
- Digital forms should ensure that required information is incorporated before an applicant can submit, with business rules for any (generally rare) circumstances where not all information is required (e.g., applicants experiencing disadvantage or technology limitations, where the applicant may be referred to the regulator).
- Applicants should receive a confirmation of submission. Where the digital application process is integrated with regulator systems, submission should automatically create a record and trigger the review process, including automated review steps based on the information provided.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Submit should be common across permissions and regulators.

CONFIGURABLE COMPONENT

APPLY

THINGS TO CAPTURE

What information do you capture that is not required (e.g., defined by legislation, to achieve regulatory outcomes)? Can you streamline or remove this from the application process?

What are the common reasons that applicants contact you for support or where applications are below standard (e.g., you send RFIs)? Is it clear what information applicants must provide?

How can you design your applications to be dynamically streamed, based on the key risk indicators (including where applicants are likely to be rejected)?

What are the opportunities to reduce information and preference declarations, commensurate with risk?

What are the opportunities to digitise the application process (e.g., end to end digitisation, reuse WoVG capability)?

What policies or business rules can be established to codify processes, including the measurement of risk and complexity in applications, or providing support to applicants?

INDICATIVE MEASURES OF SUCCESS

Improved applicant satisfaction, reduce number and complexity of contacts for information.

Improved quality of applications.

Reduced number of requests for further information.

Reduced time to complete applications.

Reduced requirements for businesses.

More consistent regulatory practice in the apply phase.

ACTION PLAN

Document and prioritise opportunities to update and design the application process.

Outline and investigate opportunities to digitise the application process (e.g., with Service Victoria).

Document requirements and specifications to digitise the application process.



REVIEW & STREAM

The REVIEW stage covers the review of application information, any requests for further information and triaging based on risk.

This stage may not be required or concurrent with assessment for less complex applications or those that can be automated, and triaging may not be required where there is little variation applications.

Review of application information should be automated where possible, often through business rules in the APPLY stage. If required, it should determine whether the information is sufficient to make an assessment. Requests for further information should be limited and targeted. Where relevant, applications should be triaged against defined risk criteria to focus regulator effort on assessment.

> [REVIEW](#)

> [REQUEST FOR FURTHER INFORMATION](#)

> [RISK TRIAGE](#)

REVIEW & STREAM

THINGS TO CONSIDER

- 1 How do you currently review application information?
What information requires more comprehensive review?
- 2 What are the common reasons of lower quality applications (e.g., common reasons for requests for further information)?
- 3 What are the key indicators of regulatory risk for the permission?
- 4 What information do you or can you use to assess risk, beyond application information (e.g., intelligence, other data sources)?
- 5 How do you currently assess risk of an applicant and triage applications?
- 6 How do these above considerations feed into business rules for streaming, and how are streaming decisions made and recorded?
- 7 Within determined streams, what level of effort is allocated to each application, and how is this quantified and managed in terms of resource allocation.

USEFUL INPUTS

- An understanding of your current review process, including process and pain points.
- Analysis of the common requests for further information you require or where applications are below standard.
- Analysis of key indicators of regulatory risk.
- An understanding of current risk assessment and triage approach.
- Analysis of current state processes for applicant triaging
- Codified business rules to stream based on risk and complexity
- Clear metrics for time and resource allocation based on streams, and level of decision-maker

Better Practice Permission Journey



INFORM



APPLY



REVIEW & STREAM



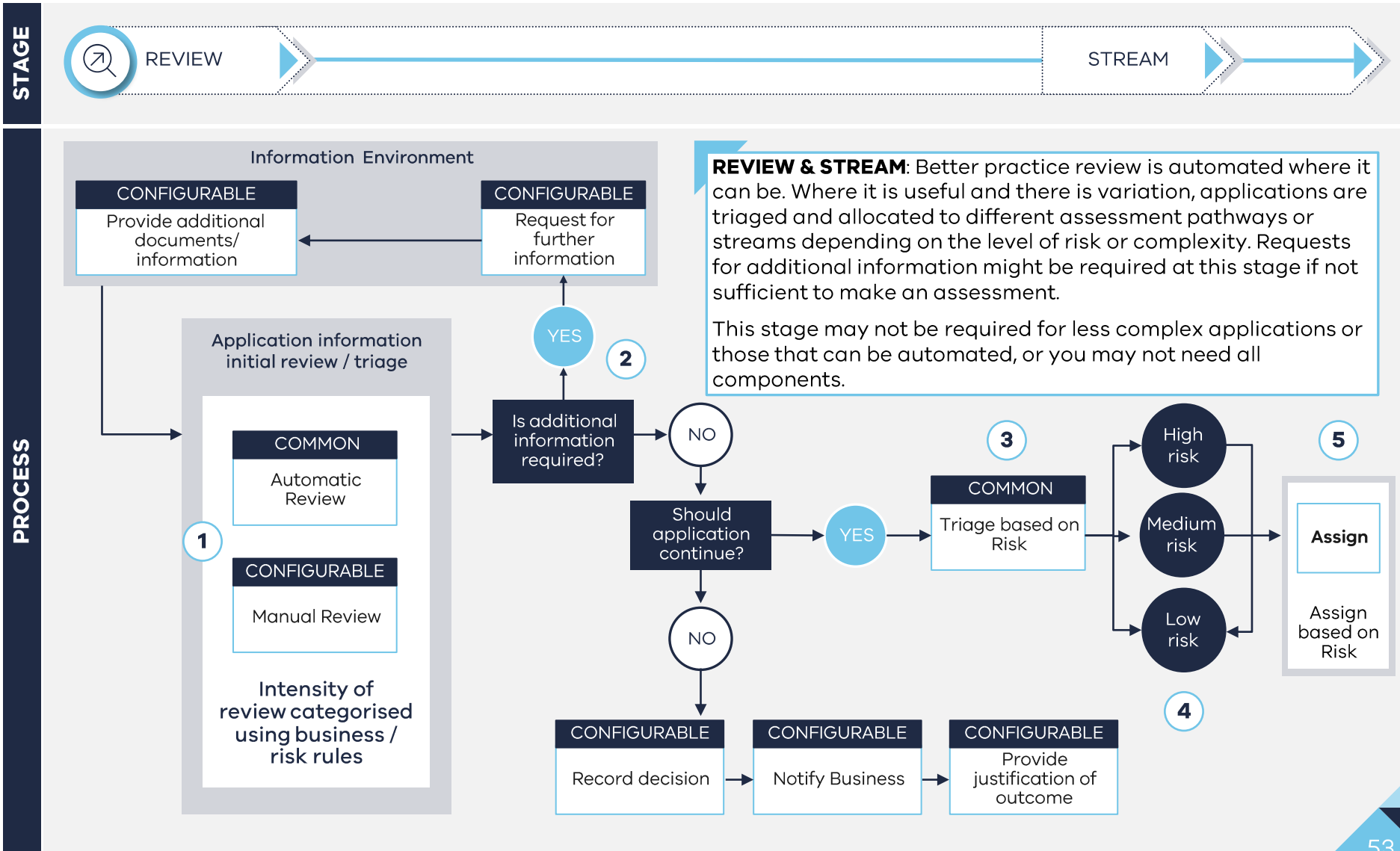
ASSESS



DECIDE



NOTIFY & ISSUE





DESCRIPTION

Application information should be reviewed before it is assessed, where this can streamline approvals. Application information can be reviewed to check that it meets requirements and is sufficient to make an assessment. This should be done as close to submission as possible to reduce any delays. It should be automated where possible, often through logic and business rules as part of the APPLY stage or may be concurrent with the ASSESS stage.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Application information is reviewed as soon as possible after submission to ensure that it meets requirements and is sufficient to make an assessment. This can streamline the process for applicants, particularly where further information is required.

- Automate review of information where possible. This can be done through logic and business rules as part of the APPLY stage (e.g. validation of information through business rules as part of the application form, verification of identity) or through verification with other information sources (e.g. verification of information with external information sources). This can be done for a subset of application information.
- Manual review should be done where this can streamline approvals and where it cannot be automated. Information may require manual review where this can reduce any delays for applicants (e.g. for more complex information or attached documents to ensure they meets requirements, for common sources of RFIs). This can also be done for a subset of application information.

Where information is insufficient to make an assessment (e.g. does not meet requirements or requires clarification), a request for further information is often made to the applicant. This should be done as close to submission as possible. Where an application is unlikely to receive approval following review, this should be rejected early, with appropriate justification and aligned with administrative law requirements.

REVIEW



DATA INPUTS

FROM APPLY:

- Application information, including information automatically reviewed and requiring manual review.

DATA OUTPUTS

TO NEXT STAGE:

- Reviewed application information, ready for triage and assessment, including identification of relevant next steps for application.
- Any requests for further information.

DIGITAL CONSIDERATIONS

- Reviews should be automated where possible, following clearly defined logic and business rules (which you should ensure are compliant with legislation, fair and justifiable). This can often be done through the application form itself as part of the APPLY stage. Identify which data sources can enable automated review.
- Front and back-end systems should identify and facilitate manual review of information (e.g. complex information, attached documents), record review conclusions and considerations for assessment and enable internal referral where relevant. They should also capture information to enable triaging based on risk.
- Where review is automated, previous applications could be audited in bulk or individually to ensure automated steps are functioning as intended to assure consistency and integrity.

Aligned WofG capability: Service Victoria Regulator Platform. Integration with data sources. Aligns to Assess in the Service Victoria GRID for both automated assessment (part of APPLY) and manual assessment (part of REVIEW and ASSESSMENT).

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Automated and manual review can be common across permissions and regulators.

The application information being reviewed will vary.



REQUEST FOR FURTHER INFORMATION

DESCRIPTION

Requests for further information (RFI) may be required when additional details are needed from the applicant. An RFI is generally triggered by insufficient, unclear or low-quality information during the application process or where the regulator believes additional details are necessary to evaluate application risk and make an effective permission decision.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Regulators make RFIs to applicants in instances where there is insufficient information to make an assessment. RFIs should be made as early as possible, though can also be used throughout the review and assessment process.

You should look for opportunities to support applicants through reducing the frequency and complexity of RFIs:

- You should limit the use of RFIs. They should not be used excessively or without rationale and should not be used as an instrument to delay or restart processing time frames for regulators. They should be supported by clear and limited business rules for when an RFI is acceptable (e.g. for unclear or subjective information that requires clarification).
- RFIs should be specific to distinct pieces of information, rather than entire sections or documents. Applicants should have a clear understanding of what information is required.
- RFIs should, in most instances, be made after the entire application has been reviewed, to limit the volume of RFIs.

Common RFIs are a useful source of feedback and intelligence. You should look for opportunities for continuous improvement based on common RFIs, including through improved information surfaced at the right time and design of the application process.

The RFI process can also be used for *requests for action*, which may involve the applicant having to action a request other than provide information (e.g., making alterations to a premise, proposing and agreeing conditions). These can be initiated following additional assessments, such as site inspections.



REQUEST FOR FURTHER INFORMATION

DATA INPUTS

FROM REGULATOR:

- RFI following review, with detail about what is required.
- Recording of RFI in systems.

The RFI process can also be used for requests for action and other interactions with applicants.

DATA OUTPUTS

TO APPLICANT:

- RFI to applicant, with detail about what is required, why and by when.

FROM APPLICANT:

- Required further information.

DIGITAL CONSIDERATIONS

- Front and back-end systems should be able to issue, receive, and record RFIs where possible. They should prioritise the channel of application or other common channels (e.g. email).
- RFIs should link to the original application and provide clear instructions on what is required and timeframes.
- Systems should manage and track RFIs, including through alerts or similar to ensure that regulators align to timeframes (e.g. statutory timeframes, service level agreements). Systems should also support reporting on RFIs against targets.

Aligned WofG capability: Service Victoria Regulator Platform, including through Service Victoria Permits-as-a-Service Platform and other common channels.

COMPONENT

COMMON COMPONENT

RFIs are common across permissions and regulators.

The information being requested will vary.

CONFIGURABLE COMPONENT



DESCRIPTION

Regulators should triage applications to ensure application of effort in assessment is aligned with risk, where there is sufficient variation between applications and aligned regulator processes. This includes the streaming of applications through defined logic and business rules based on the risk of the applicant and application, as well as the nature of the activities being regulated.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Risk triaging is used to allocate regulator effort based on the relative risk of applications. Applications with greater risk generally require a greater level of assessment effort to achieve regulatory outcomes. This can streamline processes for regulators, particularly where there is sufficient variation between applications and aligned regulator processes.

You should look for opportunities to triage applications to focus effort.

- Outline the pathways for different applications and assessment based on risk, including regulator processes and workflows.
- Define clear and consistent logic and business rules aligned to these pathways that account for the permission type and the risk of the applicant, application and the activity being regulated. These should be codified, generally from low to high, based on application information (e.g. suitability, location, activity) and available intelligence and information (e.g. previous interactions and conduct). Most applications will generally be lower risk, focusing regulator effort on fewer and higher risk applications. The rationale should be clear and transparent, justified and consistently applied.
- Develop common guidance and processes about the level of assessment required for different applications based on risk.
- Set measures (e.g. time per application, level of approval required) aligned to risk to ensure that time and effort is spent where it is most valuable.

Applications should be triaged primarily by risk, and to a lesser degree complexity. Non-regulatory controls that monitor and oversee business operations should be considered when determining risk ratings (e.g. contractual agreements, industry guidelines).

RISK TRIAGE



DATA INPUTS

FROM REVIEW:

- Application information.

FROM REGULATOR:

- Defined and codified risk triage assessment.
- Broader information sources (e.g., intelligence)

DATA OUTPUTS

TO ASSESSMENT:

- Application triaged based on risk, assigned to appropriate person to assess.
- Identified stream for an application, including expected timeframe, allocated level of effort

DIGITAL CONSIDERATIONS

- Risk triage should be considered through the application process to ensure that application information required to assess risk is captured.
- Front and back-end systems should facilitate risk triage based on defined logic and business rules (which you should ensure are compliant with legislation, fair and justifiable). This should be automated where possible, based on application information and input through the REVIEW process.
- Systems should automatically assign applications to the right assessment workflow and assessor, based on the defined pathways.
- Where risk triage is automated, previous applications could be audited in bulk or individually to ensure automated steps are functioning as intended to assure consistency and integrity.

Aligned WofG capability: Service Victoria Regulator System, including defined logic and business rules.

COMPONENT

COMMON COMPONENT

Risk triage can be common across permissions and regulators.

The business rules for risk triaging will vary.

CONFIGURABLE COMPONENT

REVIEW & STREAM

THINGS TO CAPTURE

What information requires manual review and what can you automatically review (e.g., through the application process, other data sources)?

What are the common reasons that applicants contact you for information or where applications are below standard (e.g., you request further information)?

What information fields impact application risk levels for a permission?

What other sources (i.e., external or other data sources) can be used to assess risk for an application?

What business rules can you develop to review and triage applications based on risk?

What level of effort and time should be expected and allocated to an application based on its stream and risk assessment?

INDICATIVE MEASURES OF SUCCESS

Reduce time taken for reviews.

Reduced delays and review times from requests for further information.

Reduced number of requests for further information.

Reduced duration of approvals process, and better allocation of effort and time.

Consistent risk assessment and triage.

Improved staff experience.

ACTION PLAN

Document the review workflow, including opportunities for automatic and manual review.

Document the RFI workflow, including opportunities to streamline and target processes.

Develop business rules and policies to consistently review and triage applications based on risk.



ASSESS

The ASSESS stage covers the assessment of applications, including any other assessment processes required.

This stage may be automated for less complex applications.

Assessment should be automated where possible, through defined logic and business rules. Regulator effort should be based on risk triaging, with higher risk applications requiring more in-depth assessment. It should also look to include other information available where this is useful.

> [ASSESSMENT](#)

> [OTHER ASSESSMENT PROCESSES](#)

ASSESS

THINGS TO CONSIDER

1

How do you currently assess applications? What information requires more manual and complex assessment?

2

What are the common pain points for your regulator in the assessment process? What are the common reasons you need to communicate with applicants?

3

What current business rules and criteria are being used to assess applications?

4

What other information do you use through the assessment process (e.g., intelligence, compliance information)?

5

What other processes are required (e.g., external referrals)?

6

Are officers supported by guidance and aware of what does or doesn't have to be assessed according to risk levels?

USEFUL INPUTS

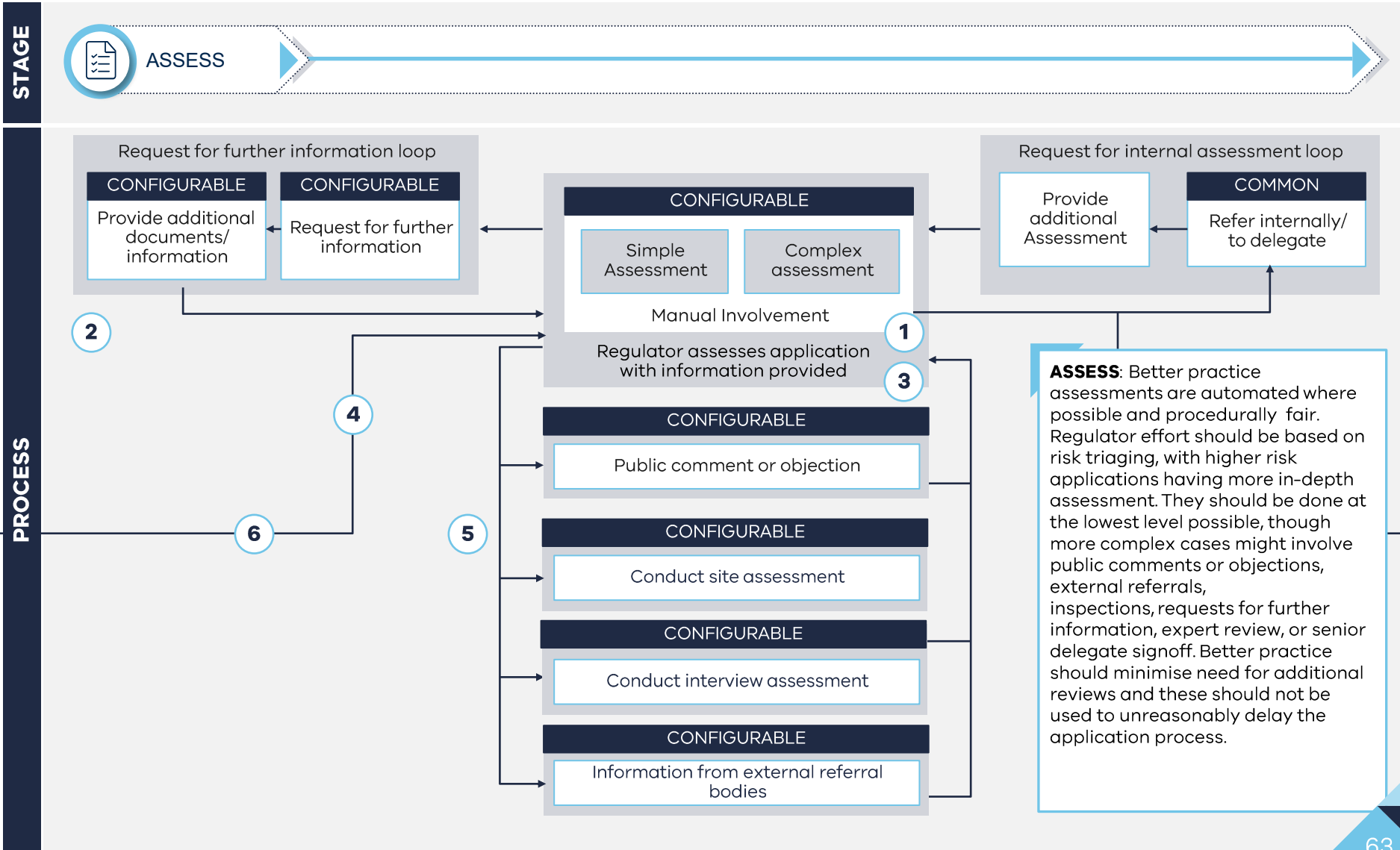
.....
An understanding of your current assessment process, including process and pain points.

.....
Analysis of the common requests for further information you require or where applications are below standard (e.g., through common requests for further information).

.....
An understanding of the other information used through the assessment process.

.....
Knowledge of any assessment process or business rules that are set out by legislation.

Better Practice Permission Journey





DESCRIPTION

Assessment determines whether an application should receive approval. It should consider application information and other information sources relevant to assess whether the permission should be approved. Effort should align with the risk of each application. It should be automated where possible, often through logic and business rules, and may be concurrent with the REVIEW & STREAM stage.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Assessment is focused based on risk triaging, following defined logic and business rules which result in transparent and justifiable outcomes.

You should account for assessment to ensure consistency and fairness.

- Define clear and consistent logic and business rules for assessment (e.g. defined thorough a checklist or criteria) to focus regulator effort. Where possible, you should look to make this transparent to applicants.
- Develop common guidance and processes about the level and focus of assessment required for different applications based on risk. Internal referral or escalation may be required, particularly where assessments are more complex.
- Capture clear and justified reasoning for assessment outcomes, aligned to administrative law requirements.
- Incorporate other information sources relevant as part of assessment (e.g. intelligence, complaints).

Assessments should be completed within well-defined timeframes that are predictable for applicants and regularly monitored and re-evaluated, including for cost-recovery considerations. For longer assessments, the process should be broken down into steps that are guided by timeframes. You should avoid requests for further information unless necessary.

Automate the assessment of information where possible. This can be done through logic and business rules and may be for a subset of or all information. Manual assessment should be as simple as possible (e.g. simple verification of information) but may be complex (e.g. requiring a more in depth, interpretive or specialist assessment).

ASSESSMENT



DATA INPUTS

FROM REVIEW & STREAM:

- Reviewed application information.
- Risk triaging and any flags for attention.

FROM REGULATOR:

- Broader information sources (e.g. intelligence, compliance).

DATA OUTPUTS

TO DECIDE:

- Outcomes of assessment.
- Reasoning for assessment outcomes to justify decisions made.

DIGITAL CONSIDERATIONS

- Assessment should be automated where possible, following clearly defined logic and business rules (which you should ensure are compliant with legislation, fair and justifiable). This may be for a subset of or all information.
- Front and back-end systems should identify and facilitate manual assessment of information where required, record assessment conclusions and justifications and enable internal referral where relevant. This may vary between simple (e.g., defined outcome, yes or no) and complex (e.g., specialist analysis) assessments.
- Systems should keep records of assessment processes and support information availability. This will enhance integrity, quality assurance and continuous improvement of workflows.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Assess in the Service Victoria GRID for both automated assessment (part of APPLY) and manual assessment (part of REVIEW and ASSESSMENT).

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Automated, simple and complex assessments can be common across permissions and regulators.

The application information being assessed will vary.



OTHER ASSESSMENT PROCESSES

DESCRIPTION

You may require alternative methods of assessment. Other assessment processes can be used to meet specific requirements generally in addition to internal assessment, often outside of the permissions team to provide specialist input or engagement as part of the approvals process. These processes include *external referral*, *conduct site assessment*, *conduct interview assessment*, and *public comment or objection*.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Other assessment processes should only be used when required. This includes when specialist input is required for higher-risk applications, to accommodate accessibility needs, or where required under legislation.

You should ensure that your use of other assessment processes is consistent and efficient.

- Other assessment processes have defined circumstances when they should be used, supported by logic and business rules. They have a clear purpose, objective and influence on your internal assessment processes. The outcome of any external or specialist input should be incorporated into your decisions.
- Service level agreements and processes should be defined to support the approvals process. They are predictable and reliable.
- Applicants are aware of external interactions, and third parties provide all information available with any resulting decisions justified by clear reasonings that can be relayed to applicants. Additional consent may be required from applicants for external referrals.
- Account for the relevance of external input and conduct further assessment where appropriate.

Consider if applicants should be notified of any comments or objections of concern from other assessment processes and how it may affect their application.



OTHER ASSESSMENT PROCESSES

Other assessment processes include three configurable components. One or more components may be used to assess a permission application depending on the applicant and regulatory requirements.

EXTERNAL REFERRAL

You may need to seek external involvement (e.g., licenced architects) to use their expertise when specialist knowledge is required to appropriately measure risk on non-standard or complex applications.

You should use verified and trusted external bodies to provide fair, thorough assessment and protect sensitive information. External bodies may not be on the same platform, so you will have to communicate through other methods.

CONDUCT SITE INSPECTION

You may conduct site assessments to verify or gather premises information and assess risk. Site inspections evaluate the state of a location, building, or area against criteria to assess whether it is safe and suitable for operations.

You use a set of criteria and checklist to conduct site inspections. Businesses know what is expected during a site inspection and can prepare premises to meet standards. Businesses are notified well in advance and can propose an alternative time if appropriate.

CONDUCT INTERVIEW

You might conduct interviews with applicants or relevant stakeholders (e.g., supervisors or references) to assess the suitability of applicants, evaluate risk, or gain additional information for assessments.

You should have firm reasons for conducting interviews which are made clear to the applicant. Questions should be targeted to the information required. Interviewers use appropriate communication techniques to facilitate discussions.

PUBLIC COMMENT OR OBJECTION

You might have to open applications to public comment or objection as part of the permission process. This ensures that the public have an avenue to provide input on decisions that will impact their day-to-day lives and community.

You listen and respond to public concerns where appropriate, reassuring stakeholders they have been heard. You create an accessible platform where public right to privacy is upheld. You provide all relevant information and guidance on when the public can object.



OTHER ASSESSMENT PROCESSES

DATA INPUTS

FROM ASSESSMENT:

- Relevant application information, with initial assessment.
- Areas of focus for other assessment processes (dependant on process).

DATA OUTPUTS

TO ASSESSMENT AND DECIDE:

- Outcomes from other assessments including supporting justifications.
- Any areas for further investigation or risk assessment.
- Needs for request for further action if required.

DIGITAL CONSIDERATIONS

- Digital systems should enable automated trigger of other assessment processes where required, in addition to manual triggers. Assessors should be notified when other assessment processes are complete to continue their assessment.
- Other assessors should be able to view relevant application information (e.g. permission information, attached documents) and capture assessment outcomes. They should be completed in digital systems where possible. Where not, they should be connected (e.g. as email workflow). Public comment should be delivered through accessible digital interfaces.
- Systems should manage and track other assessment processes, including through alerts or similar to ensure that regulators align to timeframes (e.g. service level agreements). Systems should also support reporting on RFIs against targets.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Other assessment processes can be common across permissions and regulators.

The application information being assessed will vary.

ASSESS

THINGS TO CAPTURE

What information requires manual assessment? What information requires simple or complex assessment?

What are the opportunities to streamline your assessment process, including other assessment processes?

What business rules and criteria can you develop to consistently assess applications? What information can you automatically assess?

What other information sources should you incorporate in assessment process?

How can other processes be better incorporated into the assessment process?

What additional guidance can be given to officers?

INDICATIVE MEASURES OF SUCCESS

..... Reduced time for assessment.

..... Reduced duration of approvals process.

..... Consistent assessment and outcomes.

..... Improved staff experience.

..... Increased productivity.

ACTION PLAN

Document assessment workflow, including opportunities for automatic, simple and complex assessment.

Develop business rules and criteria to consistently assess applications.

Detail policies for staff to follow in their assessment approach.



DECIDE

The DECIDE stage covers the recommendation of a decision, including any recommendation of specific conditions, and the outcome of the decision.

This stage may be automated for less complex applications. Some decisions will be able to be made after SUBMIT for automatic approvals.

Decisions should be as streamlined as possible, made at the lowest level relevant. They may require recommendation and referral to a delegate. Decisions should be justified and recorded.

> RECOMMENDATION

> DECISION

DECIDE

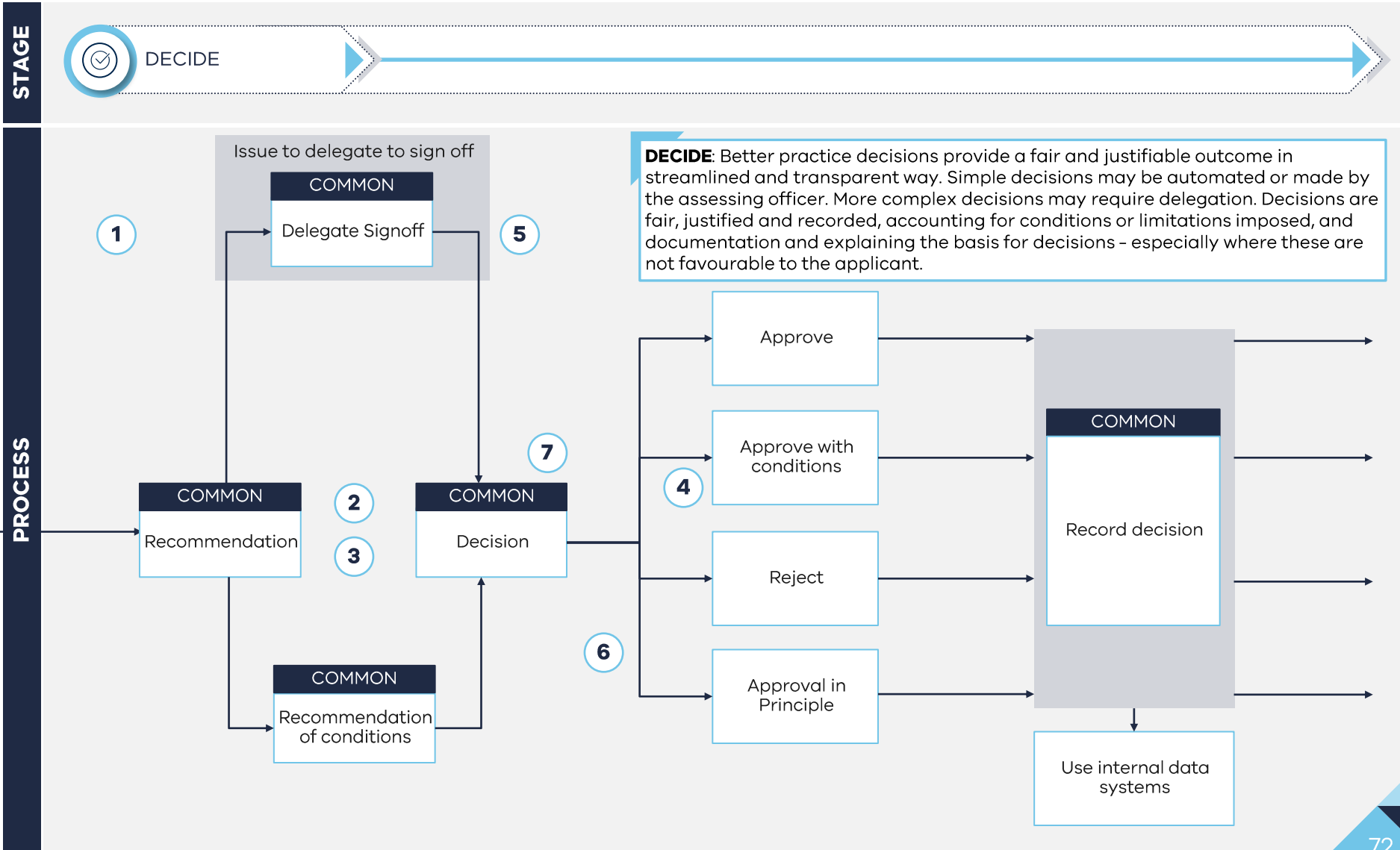
THINGS TO CONSIDER

- 1 How are recommendations and decisions currently made (e.g., made by assessor, provided to delegate)?
- 2 What is the current process to make recommendations and decisions (e.g., prepare memo, minute)?
- 3 How are decisions currently recorded?
- 4 What are the common conditions and bespoke or tailored conditions that are recommended across applications?
- 5 What external decisions are being made (e.g., board decisions), if any, and what is the current process?
- 6 What are your legislative and administrative law requirements around recommendations and decisions (e.g., processes, justifications)?
- 7 How are staff supported to make the right decisions? Do you have documented decision making materials and/or staff training?

USEFUL INPUTS

- An understanding of your current recommendation and decision process, including process and pain points.
- Analysis of the common and bespoke conditions that are recommended across applications.
- An understanding of the legislative and administrative law requirements around recommendations and decisions.

Better Practice Permission Journey



RECOMMENDATION



DESCRIPTION

A recommendation for an application outcome will be formed through assessment. This may include a recommendation on whether to approve or reject an application once all provided information has been reviewed and assessed. You may recommend conditions that stipulate restrictions or additional requirements on an applicant, which may need to be agreed by the applicant. It should be automated where possible, often through logic and business rules following assessment.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Recommendations should be in line with defined logic and business rules and can be clearly justified to permission applicants. Similar applications should tend to have similar recommendations, to support consistency and fairness.

Account for the requirements for recommendations.

- Automate recommendations where possible. This should be done through logic and business rules as an outcome of the ASSESS stage. Manual recommendation may be required for more complex applications or where they follow delegated or structured decision making processes (e.g. through a board).
- Consider legislative and administrative law requirements when providing recommendations. Most applicants have the opportunity to refute decisions placed on them if they believe they've been unfairly or unjustly considered or provide any further input to support their application.
- Regulators can impose restrictions or conditions to mitigate risk. You should aim to maintain a set of defined business rules for when standard conditions are recommended. Recommended conditions should be justified and draw from a library of standard conditions. Bespoke, tailored conditions should only be recommended where necessary, to support consistency across similar applications and ease of compliance.

You should strive to be objective to make fair recommendations based on information available. Reasons for recommendations should be documented. You should be able to trace the information and input that led to a recommendation.

RECOMMENDATION



DATA INPUTS

FROM ASSESS:

- Assessment outcomes to inform recommendation.

DATA OUTPUTS

TO APPLICANT:

- Notice of recommended rejection, with opportunity to provide further information. Recommended conditions, with opportunity to contest if needed.

TO DECISION:

- Recommendation of approval outcome with justification.

DIGITAL CONSIDERATIONS

- Digital systems should enable automated recommendations based on assessment outcomes where possible using defined logic and business rules.
- Manual recommendations should be able to be made and tracked in digital systems where possible (e.g. when provided to a delegate). Where not, they should be connected (e.g. as email workflow when provided to a board).
- Where the recommendation is to reject an application or impose conditions, consider if applicants should have an opportunity to provide further information or respond. This should be done through digital systems.
- Digital systems should support a standard conditions library and templates to select and autofill recommended conditions and their justification.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Recommendation can be common across permissions and regulators.

The recommendation information and conditions being recommended will vary.

CONFIGURABLE COMPONENT



DESCRIPTION

Every application requires a decision to reach an outcome. A decision is generally a result of the assessment outcomes and recommendation. Regulators may require an internal delegate to make a decision based a recommendation. Decision is generally the culmination of all assessments and recommendations where the regulator chooses to approve, approve with conditions, or reject an application. This is a common component of most, if not all, applications and decision are often required under the relevant Act or Regulations.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Decisions are based on assessment outcome and recommendations, taking into account all information available.

- Decisions should align with assessment outcomes and recommendation wherever possible. There should be clear justification for any variance between decisions and recommendations.
- Decisions made should be clearly justified in line with defined logic and business rules, which draw from past similar applications. They should meet all legislative and administrative law requirements, including avenues for review and appeal where required.

Where a delegate signoff is required, decision processes are managed in a way where delegate decisions are as quick and frequent as possible to shorten timeframes.

- Delegates should have access to all the information required to make a decision.
- You should consider whether external decision makers have access to digital systems (e.g. board members).
- All communications and information transfer with delegates should be clearly recorded.

Regulators who have provided approvals in principle (AIPs) and are now considering granting a full permission, will need to once again undertake inform, apply and assessment processes. This may need to be prompted by the system.

DECISION



DATA INPUTS

FROM RECOMMENDATION:

- Assessment outcomes and recommendation.
- Any recommended conditions.

DATA OUTPUTS

TO NOTIFY:

- Decision outcome (approved, approved with conditions, rejected).
- Clear and documented justification of the decision outcome and any conditions applied.

DIGITAL CONSIDERATIONS

- Digital systems should enable automated decisions based on assessment outcomes and recommendation where possible using defined logic and business rules. This may be able to be done at the point of submission if assessment can be automated.
- Manual decisions should be able to be made and tracked in digital systems where possible (e.g. when provided to a delegate). Where not, they should be connected (e.g. as email workflow when provided to board members). This includes access to all relevant information to make a decision.
- Digital systems should automatically record decision outcomes and clear justifications that can be used for notifying and issuing application outcomes.
- Where the recommendation is to reject an application or impose conditions, consider if applicants should have an opportunity to provide further information or respond. This should be done through digital systems.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Assess in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Decision can be common across permissions and regulators.

The decision and conditions will vary.

CONFIGURABLE COMPONENT

DECIDE

THINGS TO CAPTURE

What are the opportunities to streamline your recommendations and decisions process?

What business rules and criteria can you develop to consistently make recommendations and decisions?

Can your recommendations and decisions process be automated for any applications (e.g., based on assessment outcomes)?

What common conditions can be included in a standard condition library? Can bespoke conditions be standardised?

How can external decisions be made quickly and reduce timeframes?

Are you meeting all your legislative and administrative law requirements when making recommendations and decisions?

INDICATIVE MEASURES OF SUCCESS

..... Reduced time for assessment.

..... Reduced duration of approvals process.

..... Consistent recommendations and decisions.

..... Streamlined conditions.

..... Improved staff experience.

..... Reduced decision-making bottlenecks and delays.

ACTION PLAN

Document recommendations and decision workflow, including opportunities for improvement.

Develop business rules and criteria to consistently make recommendations and decisions.

Develop standard conditions and policies that explain their application.



NOTIFY & ISSUE

The NOTIFY & ISSUE stage covers the communication of a decision and post approvals processes.

This stage may be automated for approvals, based on the outcome of the decision.

Applicants should be notified of an application outcome, including justifications. Permissions should be issued as soon as possible following approval.

> NOTIFY

> UPDATE PUBLIC REGISTER

> ISSUE PERMISSION

NOTIFY & ISSUE

THINGS TO CONSIDER

- 1 What are your current notification processes?
How do you currently communicate with businesses?
What are the legislative requirements?
- 2 How do you currently issue permissions? What are the legislative requirements?
- 3 What current accessibility measures are you taking to support applicants of varying abilities?
- 4 What templates can you develop, improve or consolidate across your notifications?
- 5 Do you have a public register? How does your public register currently work? What database do you work with?
- 6 What third parties, if any, need to be notified of application outcomes?
- 7 How sensitive is the information you share in notifications? How do you keep this information secure?

USEFUL INPUTS

..... An understanding of your notifications and issue permission process, including process and pain points.

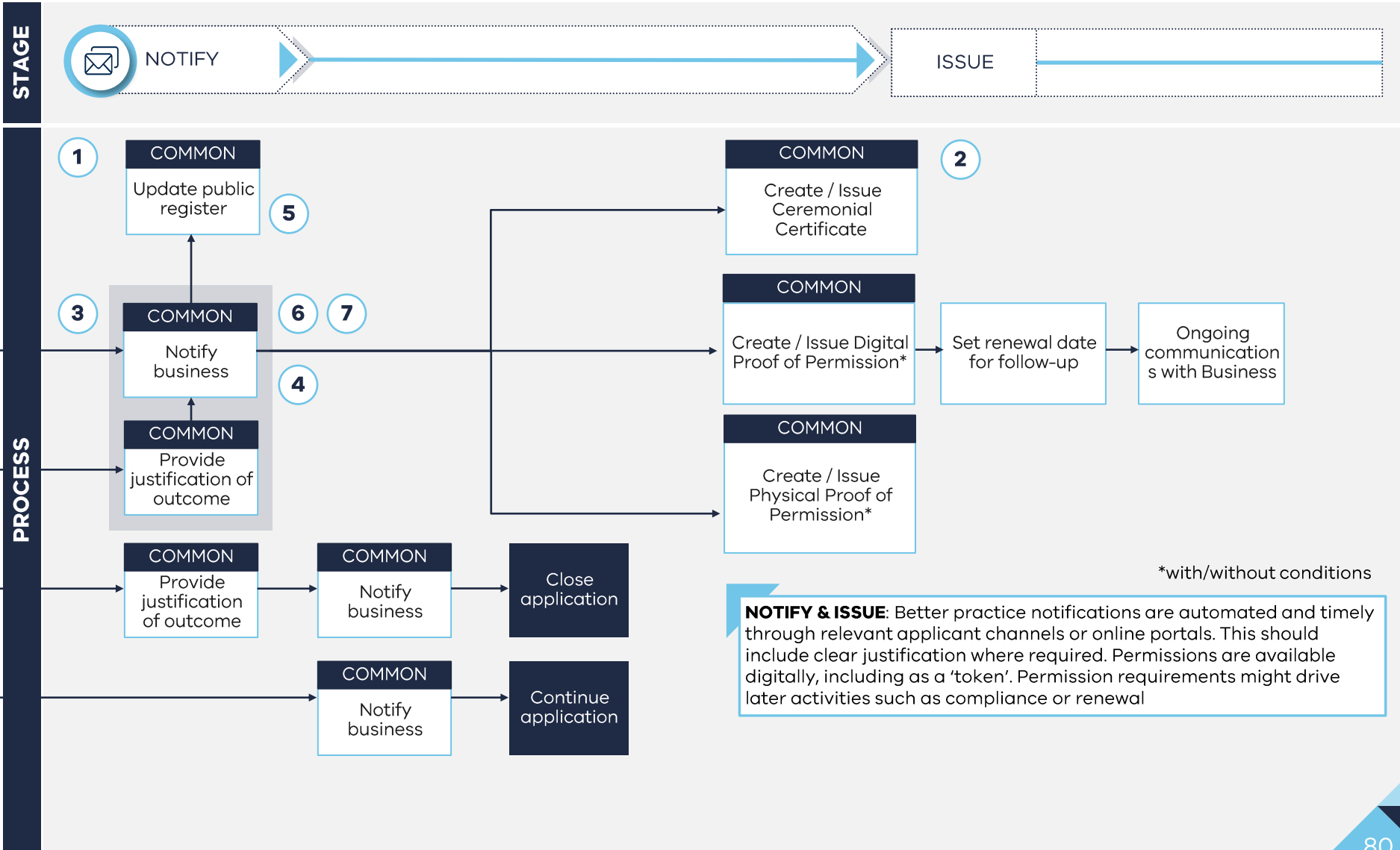
..... Analysis of the common contacts and clarifications arising from notifications.

..... An understanding of the legislative and administrative law requirements around notifications, public registers and permissions.

..... An understanding of the legislative and administrative law requirements around issuing permissions including licence details and the form it takes (i.e., physical or digital).

..... An understanding of opportunities to use Service Victoria offerings for electronic records and 'tokens' for digital permissions.

Better Practice Permission Journey





DESCRIPTION

Applicants should be notified of their application outcome as soon as possible. This includes the justification of an outcome, as well as any next steps. While important for application outcomes, notify should be a pattern of communication between regulators and applicants across regulatory interactions.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Notification is provided to applicants as soon as possible after an outcome. It justifies any outcomes, decisions and next steps, including options for review and appeal. Notifications should meet all legislative and administrative law requirements, and sufficient steps should be taken to ensure sensitive information is protected and included only when possible.

You should look for opportunities to improve the accessibility and efficiency of your notifications:

- Automate notifications where possible. Notification of application outcomes may be concurrent with the issue of a digital licence or 'token' which can be used to commence activity. Common notifications should be templated.
- Notifications should be accessible for applicants and only sent where required or relevant. They incorporate clear instructions with all necessary information and clearly outline the implications of the notification. Notifications to third parties beyond the permission holder or representative should be limited.
- Notifications should be timely and proactive, to ensure that the application and approvals process is not delayed. They are sent through the most appropriate channel, accounting for any security requirements with information.

Notifications should provide an opportunity for applicants to give feedback to identify opportunities for improvement.

NOTIFY



DATA INPUTS

FROM APPLICANT:

- Contact information

FROM DECIDE:

- Application outcomes and justification.
- Notification template.

DATA OUTPUTS

TO APPLICANT:

- Notification.

DIGITAL CONSIDERATIONS

- Digital systems should enable automated notification based defined logic and business rules as part of common workflows. Templates should be created in digital systems for common notifications and draw from account or permission information.
- Digital systems should send notifications directly from systems using stored contact information. Applicants should be able to respond to these notifications directly (e.g. as an integrated email workflow) and update information with ease through digital systems. All communications in and out should be recorded within the system.
- Notification may be sent concurrently with digital permissions or 'tokens' which are electronic representations of permissions in digital systems, as part of the ISSUE stage.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Token and Feedback in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Notify can be common across permissions and regulators.

The content of notifications will vary.

CONFIGURABLE COMPONENT



UPDATE PUBLIC REGISTER

DESCRIPTION

You may need to update public registers with details of permission holders and permission information. Updating registers ensure the public has access to relevant up-to-date information on licence holders to support transparency and allow consumers to make informed decisions. Public register information may include full business/personal name, registration number, licence status including conditions, and any other relevant details. This is not required for most permissions.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Public registers should be up to date and include all information required for members of the community to make informed decisions when hiring or working with licence holders.

- You should look to hold your register on a publicly accessible platform such as a website, directly integrated with digital systems to ensure it is up to date with the most current information.
- You should consider legislative requirements and ensure you provide all information required in an appropriate manner. A public register will not require all account and permission information so you should consider what information is relevant.
- Where appropriate, conditions or variations as part of the business licence should be outlined on the public platform, to promote transparency.

You should ensure the public is able to raise concerns or complaints using the information publicly available on the register.

UPDATE PUBLIC REGISTER



DATA INPUTS

FROM PERMISSION:

- Permission details from regulator records.

DATA OUTPUTS

TO PUBLIC:

- Up to date public register with all required information.

A public register is not required for many, if not most permissions.

DIGITAL CONSIDERATIONS

- Digital systems should enable automated update of public registers in response to approvals and triggers related to permissions. This should be integrated with the public register. to ensure registered information is up to date and accurate
- Not all information is required on public registers. Business rules should clearly define the elements required are published to public records.

Aligned WofG capability: UPDATE PUBLIC REGISTER can be incorporated as part of Service Victoria Business Permit System (BPS), including integration with website.

COMPONENT

COMMON COMPONENT

Update public register can be common across permissions and regulators.

The content of the public register will vary.

CONFIGURABLE COMPONENT



ISSUE PERMISSION

DESCRIPTION

Most regulators issue a proof of permission. This may be a digital permission or 'token', or a physical permission. This authenticates the duty holder's right to operate. Proof of permission should be issued as soon as possible following approval. Some may also offer or require a ceremonial certificate for licence holders.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Digital permissions or 'tokens' are issued as soon as an approval is made. This is an electronic representation of a permission which can be trusted and verified. This can reuse existing capabilities (e.g. Service Victoria Digital Wallet). Physical permissions should only be used where required.

You should ensure as little time as possible is taken for a permission holder to receive their proof of permission to allow businesses to commence operations.

- If licences are physical or will take time to issue to the business, you should provide a temporary permission. This may be in the form of a digital permission or 'token'.
- Physical permissions may need to be created and issued by third parties (e.g., licence cards), this should be effectively managed to reduce time taken.

Proof of permissions and certificates are made in a way that prevents falsification and ensures authenticity. This includes seals or other modern techniques to prevent against fraud. Only details that are required by legislation and are necessary to uphold the legitimacy of a licence or verify the permission holder's identity are included.

Ceremonial certificates are often issued by occupational licensing authorities. These should follow a similar process.



ISSUE PERMISSION

DATA INPUTS

FROM PERMISSION:

- Permission details from regulator records.

DATA OUTPUTS

TO APPLICANT:

- Digital and/or physical permission.
- Ceremonial certificate (if required).

DIGITAL CONSIDERATIONS

- Digital systems should enable automated issue of digital permissions or 'tokens' as an electronic representation of a permission. This should be done as soon as an approval is made, often concurrent with NOTIFY. This should be enabled by templates and standard data elements, including for attributes and conditions, to issue permissions and 'tokens'.
- The status of a permission (i.e., active, inactive) should be recorded digitally and integrated with relevant systems. Digital systems should be able to update permission status and other attributes, this can be supported by digital permissions.
- Digital and physical permissions should link back to regulator records to ensure consistency and allow for automated updates of digital permission, including for variations such as name changes or regular updates such as renewal date.

Aligned WofG capability: Service Victoria Regulator Platform. Aligns to Token in the Service Victoria GRID.

COMPONENT

COMMON COMPONENT

Issue permission can be common across permissions and regulators.

The content of the permission will vary.

CONFIGURABLE COMPONENT

NOTIFY & ISSUE

THINGS TO CAPTURE

INDICATIVE MEASURES OF SUCCESS

What are the opportunities to streamline your notifications process? How could you improve your notifications for applicants?

Improved applicant satisfaction.

What are the opportunities to streamline your issue permission process? Is there an opportunity to issue digital permissions?

Reduced number and complexity of contacts for information.

Is the information you provide accessible and understandable for *most* applicants?

Up to date public register.

Is there an opportunity to automate notifications using templates and auto-filled data?

Streamlined issue permissions.

What are the opportunities to streamline your public register process? Can you integrate this with your records?

Improved staff experience.

How can you automate third party notifications? How can you make this process more efficient?

ACTION PLAN

Develop opportunities to improve notifications.

Document requirements to update the public register.

Develop opportunities to streamline the issue permission process.



OTHER PROCESSES

The OTHER PROCESSES stage covers the other processes that are aligned to the permissions process.

Other processes should reuse components of the better practice permission journey. They may be triggered outside this process, but should feed into the journey.

> [RENEWALS](#)

> [APPLICANT INITIATED TRIGGERS](#)

> [REGULATOR INITIATED TRIGGERS](#)

RENEWALS

THINGS TO CONSIDER

- 1 What information and guidance is provided to permission holders prior to the renewal period?
- 2 How much information is required from permission holders as part of the renewal process? Is there a clear rationale for this information to be captured?
- 3 How does the regulator receive, assess, and approve renewals?
- 4 Are renewals processed in an efficient way? Do regulator systems and process allow for streaming and automation?
- 5 Are there guidelines and business rules for a renewal decision? How are decisions made and recorded?
- 6 What avenues are available for permission holders to appeal renewal decisions?

THINGS TO CAPTURE

- What common user errors cause problems in renewals? What guidance could be provided to avert this?
- Is the minimum amount of information required to make a renewal decision being requested?
- What are the current state processes for renewals, and what pain points and barriers to improvement exist?
- What inputs can be automatically reviewed and assessed, and how might risk levels and triaging be implemented?
- What factors are considered in making a renewal decision? Are these factors recorded in an accessible and retrievable medium?
- Are admin law requirements understood and adhered to by the regulator in communicating a renewal decision?

ACTION PLAN

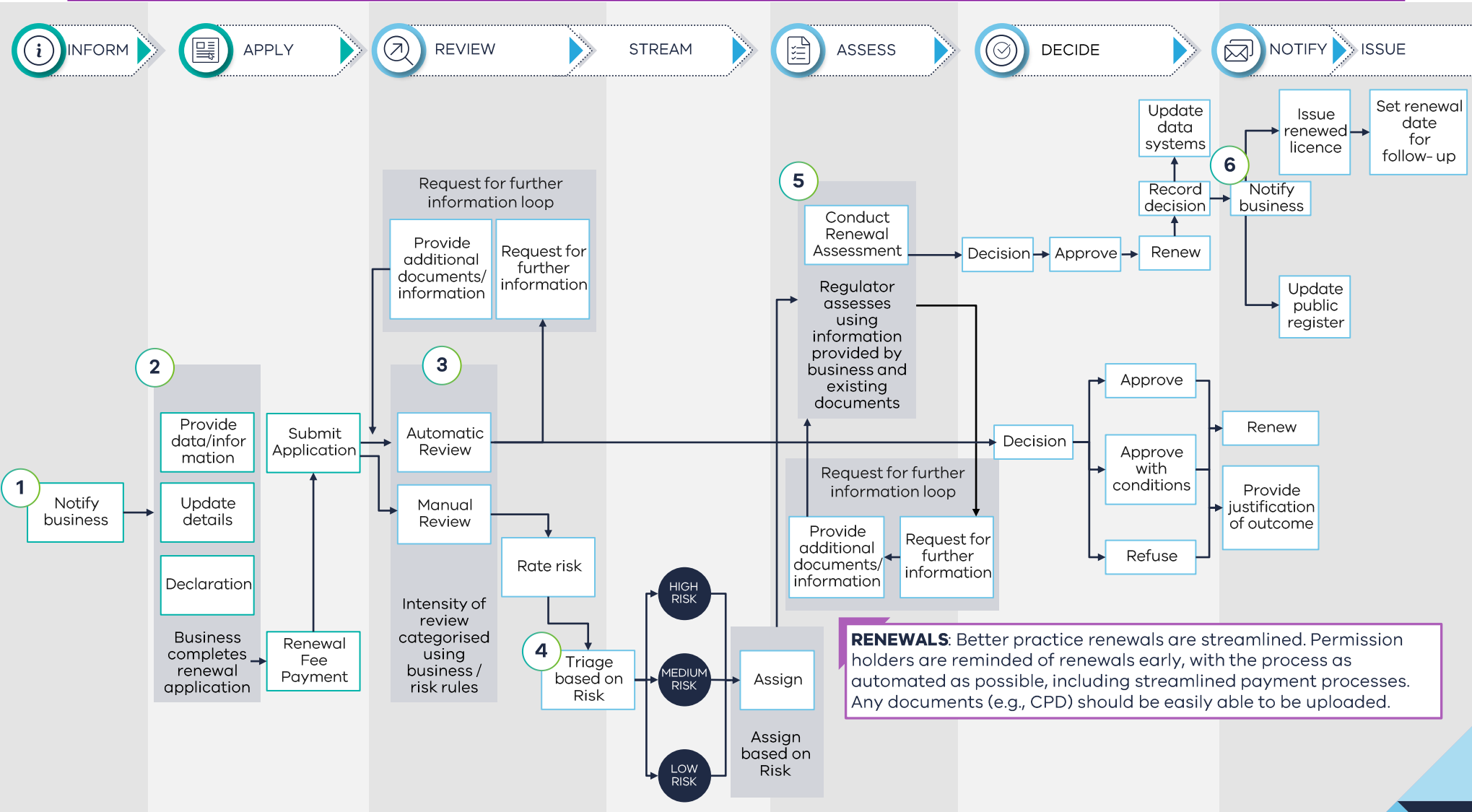
Capture pain points and problems in the current state renewals process.

Streamline requested information to ensure only information necessary for a renewal decision is requested.

Codify business rules for automated and manual review, risk triaging, and decision-making.

The Better Practice Permission Journey - Renewals

Numbers correlate to 'Things to Consider' and 'Things to Capture' at each stage.





DESCRIPTION

Renewals are generally required on a cyclical basis, often directed by legislation. Regulators conduct renewals at varying intervals to maintain the permission and make sure holders are still fit to operate, generally collecting payments. Fees will vary between regulators and permissions. Information can be captured through the renewals process as a primary contact with permission holders. Review and assessment should only occur where information is consequential to the permission.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Renewals should be done in the simplest way possible to minimise the burden placed on the permission holder and regulator.

You should consider automatic renewal payments if information can be collected separately and a payment is all that is required. This will significantly reduce regulator workload and burden.

- You should only ask for information necessary for renewals and where possible request additional information separately.
- Payment instructions and amounts are clear so permission holders are informed and able to pay for renewals easily.
- If authentication is required for renewals, this should be aligned with identity verification and be made as simple as possible.

You should look to set renewal periods to the longest duration possible, commensurate with risk. Renewal periods could be configurable and differ between permission holders, generally where risk varies.

Permission holders should be given sufficient notice before their licence is expired to either renew or surrender their permission. Any late lodgement fees or other consequences for licence holders that pass their renewal date are clearly defined for permission holders.

Internal records and proof of permissions are updated as soon as possible following renewal payment and acceptance.

RENEWAL



DATA INPUTS

TO REGULATOR:

- Compliance history from permission holder file.

TO PERMISSION HOLDER:

- Notification for renewal.
- Calculated fee amount.

DATA OUTPUTS

FROM PERMISSION HOLDER:

- Submission and payment of renewal.
- Any additional information required.

TO PERMISSION HOLDER:

- Record of submission and payment.
- Renewed permission.

DIGITAL CONSIDERATIONS

- Digital systems should look to enable automated renewals to be triggered based on permission dates and renewal periods. This should be configured for each permission and automatically updated after renewals have been completed.
- Renewals should reflect a streamlined application process, reusing relevant components (e.g., applicant information, permission information where required, declarations, payments, submit).
- Where information is not consequential for the permission, they should be automatically processed and approved. Review & stream, Assess and Decide should only not be automated by exception.

Aligned WofG capability: Aligned with other components.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Renewals should be consistent with the application process.

APPLICANT INITIATED

THINGS TO CONSIDER

What is the current process for applicants notify you of changes to their situation and operations?

When must a permission holder provide updates? How are they informed of this and is it clear?

How do you respond and interact with applicants following notifications?

What assessment or review, if any, do you take for applicant initiated processes?

What other actions do you take in response to applicant initiated processes (e.g., updating records, issuing new licences, etc)?

THINGS TO CAPTURE

How can you make it easier for permission holders to notify you of variations? Can this be digitised?

Where is more information required and how can you make this clearer for permission holders?

Are there any issues with your current process? What are the opportunities to solve these, including digital solutions?

Should you do less assessment? More? How can you automate this process?

Are these additional actions required/adding value? How can you automate these processes?

ACTION PLAN

Develop opportunities to improve applicant experience when providing updates.

Detail plans to digitise and automate applicant-initiated processes.

Outline method of responding to applicant initiated processes.



APPLICANT INITIATED TRIGGERS

DESCRIPTION

Businesses may initiate some processes that the regulator will need to either implement or respond to. Applicant initiated triggers could include variations such as name changes, transfer of licence holder, change to services or operations, surrender of licence, etc. Due to their nature, applicant-initiated processes are driven by the unique needs and situation of permission holders.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Permission holders are able to easily submit any variations. There should be few barriers for permission holders such as negative incentives and accessibility issues.

You should look for opportunities to improve applicant initiated processes.

- Communicate when updates and variations are required from permission holders, through clear and predictable processes. Permission holders should be aware of any information or documents they need to provide in order to successfully submit an applicant initiated trigger. Requests for further information should be limited.
- Applicant initiated processes are defined and enabled through digital systems. They should also be flexible to respond to changing inputs from unique permission holder situations.
- Requests to surrender a licence should be granted provided there are no legislative restrictions or community impacts.

Regulator records should be up to date because permission holders are encouraged to notify the regulator of any variations before or immediately after they occur. Where required, basic declarations should be used to confirm the permission holder's identity and authority to make variations.



APPLICANT INITIATED TRIGGERS

DATA INPUTS

FROM PERMISSION HOLDER:

- Applicant initiated trigger information and reasoning.
- Declaration of authority to provide variation.
- Any further information or proof of variation required, including s defined by legislation.

DATA OUTPUTS

TO REGULATOR:

- Updated permission holder information in internal systems, on public registers, and with any third parties.
- Process for change to proof of permission documents.
- Deactivate licence where required.

DIGITAL CONSIDERATIONS

- Digital systems should look to enable automated applicant initiated processes, particularly where information is non-consequential (e.g. update contact details).
- Applicant initiated triggers should reflect a streamlined application process, reusing relevant components (e.g., applicant information, permission information where required, declarations, payments, submit).

Aligned WofG capability: Aligned with other components.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Applicant initiated triggers should be consistent with the application and approvals process.

REGULATOR INITIATED

THINGS TO CONSIDER

Under what circumstances might a regulator look to initiate an amendment to an individual or business' permission?

What powers are available to the regulator to amend an individual or business' permission? Is the power to issue, amend, revoke, or suspend permissions legislated?

Are there policies or guidelines that outline whether a regulator-initiated amendment is appropriate and justified?

What regulator processes must occur in order for a regulator-initiated amendment to occur?

Are the reasons and justifications for a regulator-initiated amendment clearly communicated to the permission holder, in addition to what avenues for appeal are available?

THINGS TO CAPTURE

What are common reasons why permissions have been amended in the past? What happened, and why was action taken?

What powers are granted to the regulator through legislative, regulations, etc.,?

What criteria and considerations should be applied to assess the appropriateness of each regulator-initiated amendment?

What is the regulator required to do (by legislation or by policies) in order to action a regulator-initiated amendment?

Are admin law requirements adhered to in regulator-initiated applications?

ACTION PLAN

Codified guidelines and policies for appropriate and reasonable regulator-initiated amendments.

Examine legislation to ensure regulatory powers are granted and sufficient.

Ensure that admin law requirements are understood and adhered to.



REGULATOR INITIATED TRIGGERS

DESCRIPTION

Regulators may initiate some processes outside of the standard application and renewals process that are important to the overall permission journey. New information or assessments can trigger regulator-initiated processes. These may often come as compliance outcomes such as suspending, revoking, or imposing conditions to a permission.

WHAT 'BETTER PRACTICE' LOOKS LIKE

Regulators should only choose to revoke a licence when required. This decision is made in line with risk and clearly defined rules that determine when a permission holder is no longer suitable to operate. Where appropriate, suspension or conditions should be used as an alternative to revoking a licence. Regulators should consider the seriousness of compliance breaches and whether they are capable of proving their suitability to hold a permission in the future.

Regulators should clearly outline why permission changes have been imposed and permission holders understand what they must do to operate normally. Where appropriate, permission holders are given clear, achievable benchmarks that fairly represent when they are fit to have conditions or changes removed. Permissions should be suspended, revoked or have conditions imposed as soon as a compliance breach has been substantiated to prevent any further risk or damage. Regulators should conduct further assessment and investigation to ensure permission holders have made improvements and are meeting all compliance requirements. Regulators should ensure that conditions or suspensions are removed when requirements have been met and risk has been mitigated so permission holders do not lose any operating time.

When appropriate, permission holders should be given the opportunity to respond to decisions that will negatively affect their business.

Regulators should use a standardised set list of conditions that can be applied across permissions with similar risk. Regulators should only apply unique, tailored conditions where necessary, to support consistency and ease of compliance. Regulators should impose conditions or other changes where required rather than whenever possible.



REGULATOR INITIATED TRIGGERS

DATA INPUTS

TO REGULATOR:

- Compliance outcomes, intelligence etc. that triggers regulator initiated process.
- Existing permission holder compliance history and application information used for assessment.

DATA OUTPUTS

TO PERMISSION HOLDER:

- Updates to permission status and conditions.

DIGITAL CONSIDERATIONS

- Digital systems should look to enable automated regulator initiated processes to be triggered based on compliance or enforcement outcomes, relevant intelligence, etc. with all information to be used in regulator initiated triggers made accessible to decision-makers.
- Regulator initiated triggers should reflect a streamlined application process, reusing relevant components, particularly for non-consequential information (e.g. applicant information, permission information where required, declarations, payments, submit).
- Regulator initiated processes should trigger attributes and outcomes through digital systems. Digital systems should be used to flag repeating compliance issues or feedback to identify greater changes required, such as legislative or broader processes, and which groups they apply to.

Aligned WofG capability: REGULATOR INITIATED TRIGGERS can be incorporated as part of the better practice permission components.

COMPONENT

COMMON COMPONENT

CONFIGURABLE COMPONENT

Regulator initiated triggers should be consistent with the application and approvals process.

Appendices

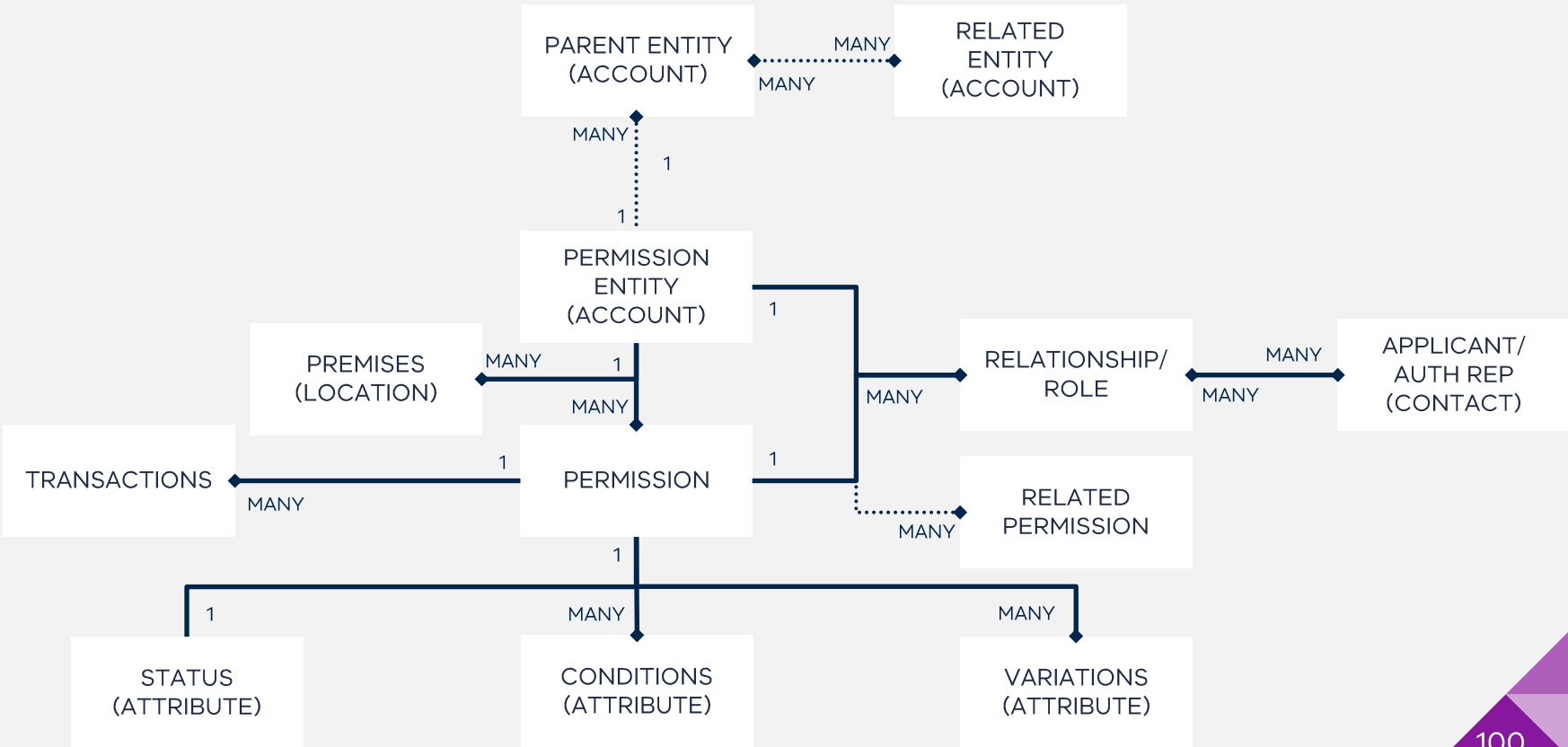
An example data structure for permissions, with defined relationship between the entity, permission and attributes

What is this for?

This is an example data structure for common permissions. You can use this as a reference or starting point for your data structure, including to map your data fields to the different components (e.g., business information to the permission entity) and to support your broader regulatory outcomes (e.g., how this enables compliance and enforcement processes).

Who should use this?

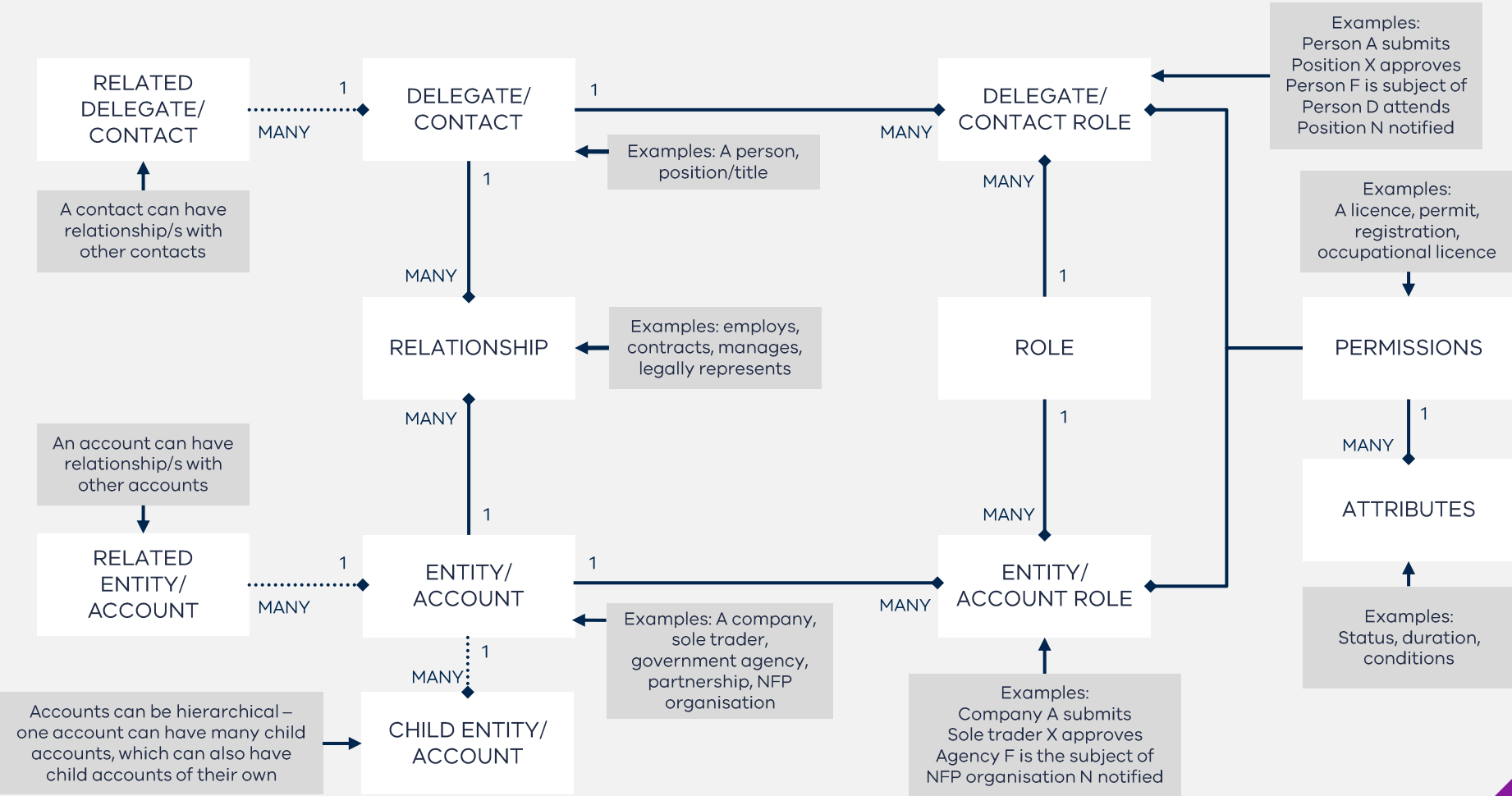
It is likely that your digital and data team will consider the data structure and model through detailed design, but it is something that is valuable to be familiar with. A senior regulatory leader will often be the data steward of a regulator.



An example data model for permissions, visualising how entities and roles connect with activities

What is this used for?

You can use this as an example and reference to develop your data flow between components and the actions involved, aligned with the data structure above.



Glossary

TERM	DEFINITION
Applicant	An entity applying for a permission. This could be an individual, sole trader or company.
User	An individual who uses the regulator’s platforms or systems. This is a general term that can refer to an applicant, representative, permission holder or regulated entity. When applying for a permission through digital services, a user can be considered a ‘customer’ of government services.
Delegate	A role that that undertakes activities due to their expertise or position. This could include more senior regulator officers involved in more complex assessment or approval decisions or representatives with the authority to act on behalf of a business. Delegates can be either in a regulator or regulated entity.
Permission	The right to engage in specific activities or conduct specified actions as granted by a regulatory authority. This can take the form of a licence, registration, permit, or other approval administered by a regulatory authority.
Permission holder	The entity that holds a permission from a regulatory authority and can undertake activities as defined through the permission. This could be an individual, sole trader or company.
Regulated entity	A business or individual that holds a permission, and whose conduct and activity is regulated by the regulatory authority. Regulated entities are considered a duty holder.
Service owner	A role within the regulator, generally a more senior manager or leader, that is responsible for the improvement and administration of a permission and how it is experienced as a service by applicants.
Reform officer	A role within the regulator, generally an officer or manager, that is responsible for designing and implementing improvements to regulatory practices and permission process.



© State of Victoria 2023

You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Department of Treasury and Finance) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos.

Copyright queries may be directed to IPpolicy@dtf.vic.gov.au