Better Regulation Victoria

Implementing 'Better Practice' Permissions

A Playbook for regulators to streamline permissions and become digitally ready

Part A: Defining your ambition for reform

VICTORIA
State
Government

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.

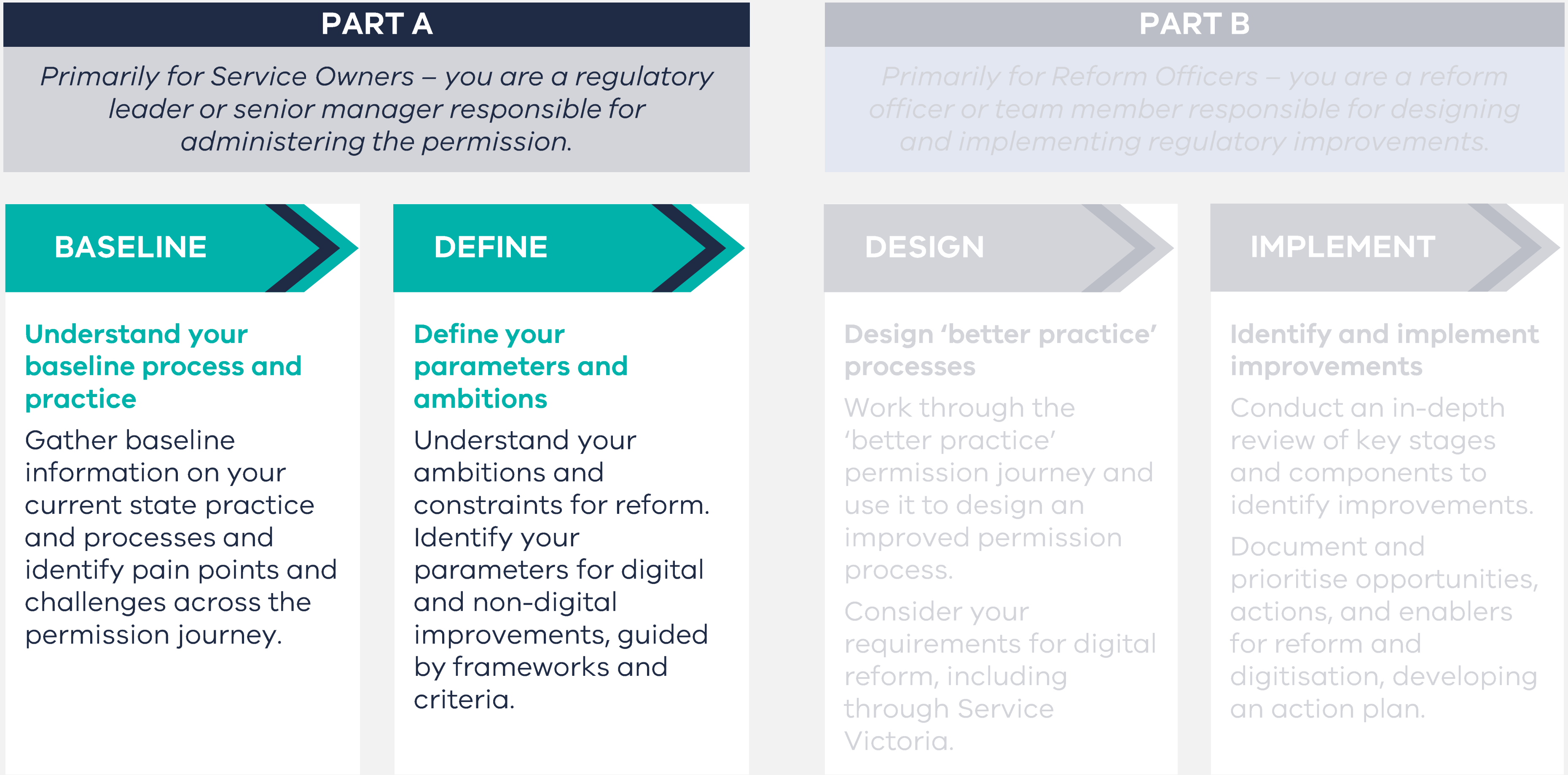
3 Part B: designing better practice processes and delivering change

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

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.

BASELINE

Baseline | **Start by bringing together your understanding of baseline practice and processes**

Understanding your baseline permission practice and processes, including what factors influence the way things are currently done, is important to defining the ambition for reform. Below are examples of useful information and analysis that you may already have to guide your baseline understanding.

What is the permission? What is the current process? Who uses it? How is it digitised? What is needed?

Legislative requirements

Understand how your permission requirements are dictated by legislation (e.g., what information must be gathered under legislation).

Current processes

Think about your current processes and collate any existing documents mapping the applicant and regulator journey.

Pain points and opportunities

Reflect on the key pain points and possible improvement opportunities across the application journey ideally using research undertaken with staff and applicants.

Information requirements

Understand what information is collected and assess what is necessary to be collected through the application process.

Applicants

Think about your applicants, their needs and common challenges going through the application process.

Digital systems and technology

Consider the strengths and limitations of your current technology and system capabilities (front and back-end) and how they could reduce manual practices.

Opportunities for digitisation

Have a sense of what technology opportunities might be available or emerging (e.g., through Service Victoria' Business Permit System).

Key measures of success

Think about what metrics are important to you and where you can improve (e.g., high number of RFIs at the review stage).

Pause and reflect | **Define your parameters and ambition for reform**

Reflect on key questions below to identify your ambition for improved practice and processes and digital reform, and what might constrain your improvement journey.

1 What primary outcomes do you want to achieve through practice and process improvements? (e.g., improved user experience overall, staff satisfaction, fewer RFIs).

2 What key pain points do you want to solve now vs. later?

3 What processes and decision points are not mandated by legislation that you might want to change?

4 Where is risk improperly managed across your process?

5 What information and record management standards are required and how does your current process compare?

6 What is your ambition for digital reform? (e.g., major digital transformation or minor improvements focusing on key processes).

7 What is your ambition for front end (e.g. user experience, portals) and back end (e.g. regulator systems) digital reform and how does this shape your priorities?

8 What is feasible for digital reform? (e.g., what are the emerging digital solutions and what investment do you have to implement these).

9 How does your vision align with the Victorian Government's vision for digitising regulatory services?

DEFINE

Permission Architecture Framework | **Consider your permissions in the broader regulatory context**

The Permission Architecture Framework

Permissions exist within a broader regulatory context that ensures appropriate compliance, accountability and oversight of regulated activities and industries.

The Permission Architecture Framework can help you to consider your permissions within the context of the broader regulatory system and your own regulatory practice.

This Playbook focuses on improving 'better practice' permissions.

The Permission Architecture Framework encourages you to consider your whole regulatory approach, and how permission improvements link to or are influenced by other factors (e.g., regulatory tools and practice, legislation).

It is worth considering these broader questions to avoid solving for challenges through practice and process improvements where there might be larger considerations at play that are better addressed in other ways.

Elements of the Permission Architecture Framework (see next page)

BROADER REGULATORY SCHEME & CONTEXT
(the legislation, regulations, standards, compliance, conduct provisions, related state and national schemes, co-regulatory systems)

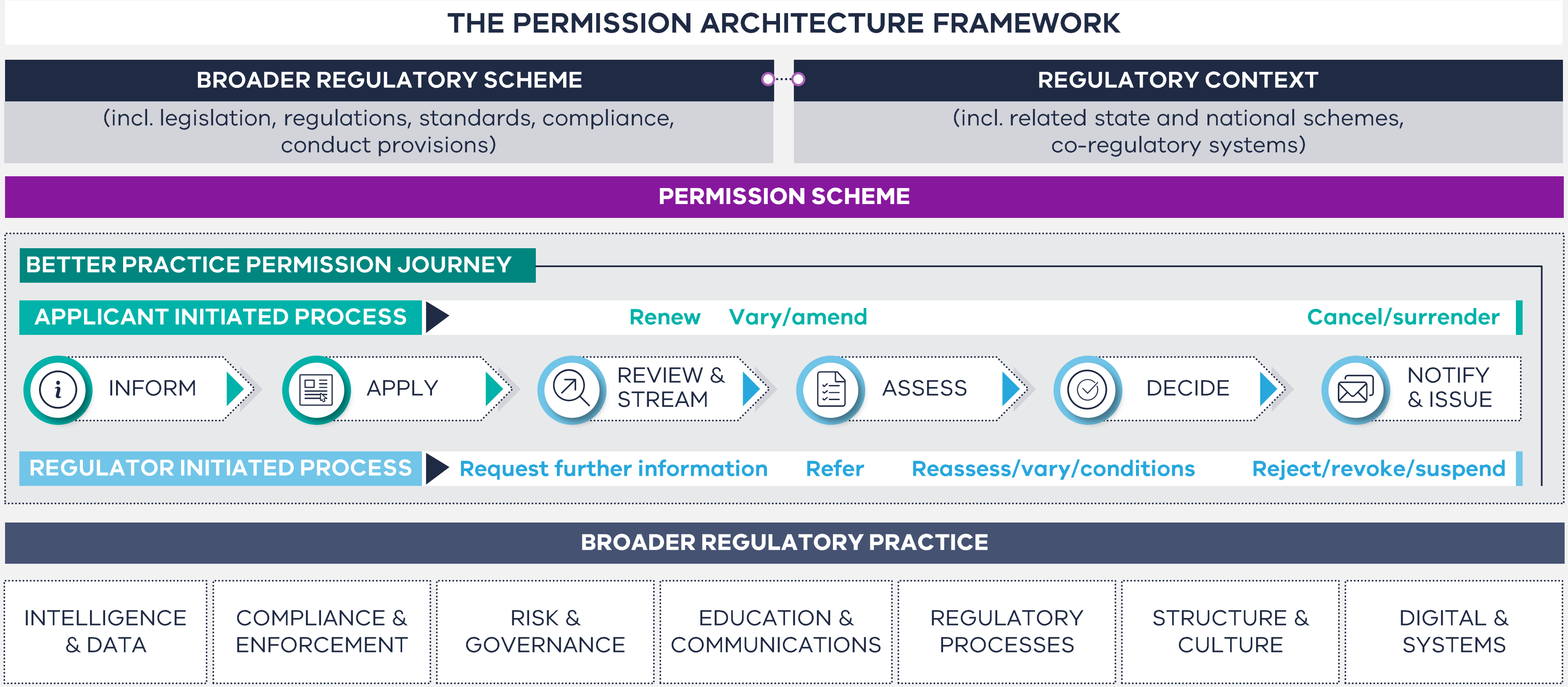
PERMISSION SCHEME
(the system or framework that governs the granting of permissions to individuals or entities within a specific context e.g., occupational licence scheme)

BETTER PRACTICE PERMISSION JOURNEY
(the key stages and processes of administering permissions from application to submission)

BROADER REGULATORY PRACTICE
(the structures and processes by which regulatory bodies carry out their regulatory functions and administer permissions e.g., governance, compliance and enforcement, supporting systems)

Permission Architecture Framework | **Orient your permissions within the broader regulatory context**

The Permission Architecture Framework is useful to help you orient your permissions within the broader regulator context and within your own organisation's regulatory practice and processes. It should help you to consider how your permissions and other regulatory activities work together and influence one another.



THE PERMISSION ARCHITECTURE FRAMEWORK

BROADER REGULATORY SCHEME

(incl. legislation, regulations, standards, compliance, conduct provisions)

REGULATORY CONTEXT

(incl. related state and national schemes, co-regulatory systems)

PERMISSION SCHEME

BETTER PRACTICE PERMISSION JOURNEY

APPLICANT INITIATED PROCESS

Renew Vary/amend Cancel/surrender

INFORM → APPLY → REVIEW & STREAM → ASSESS → DECIDE → NOTIFY & ISSUE

REGULATOR INITIATED PROCESS

Request further information Refer Reassess/vary/conditions Reject/revoke/suspend

BROADER REGULATORY PRACTICE

INTELLIGENCE & DATA

COMPLIANCE & ENFORCEMENT

RISK & GOVERNANCE

EDUCATION & COMMUNICATIONS

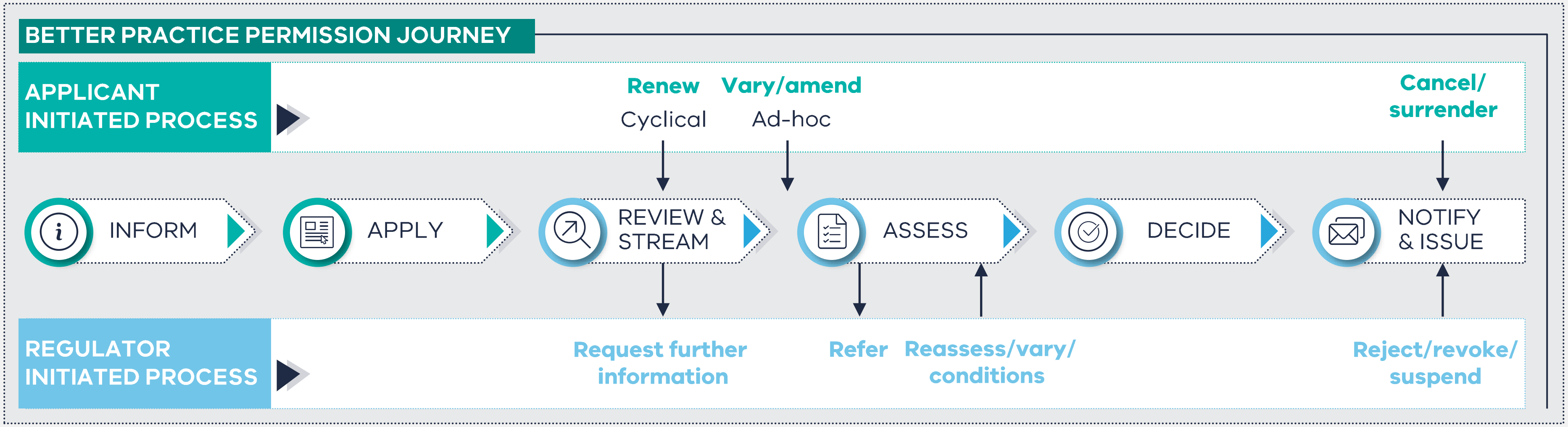
REGULATORY PROCESSES

STRUCTURE & CULTURE

DIGITAL & SYSTEMS

Better Practice Permission Journey | **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.



BETTER PRACTICE PERMISSION JOURNEY

APPLICANT INITIATED PROCESS

Renew Cyclical

Vary/amend Ad-hoc

Cancel/ surrender

INFORM

APPLY

REVIEW & STREAM

ASSESS

DECIDE

NOTIFY & ISSUE

REGULATOR INITIATED PROCESS

Request further information

Refer

Reassess/vary/ conditions

Reject/revoke/ suspend

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 | **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 | **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)

ASSESS

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

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.

This stage may be automated for less complex applications.

DECIDE

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

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.

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

NOTIFY & ISSUE

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

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

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

Permission processes do not exist in isolation. Other regulatory practices and activities may impact permissions, and vice versa.

Before improving permission practice and processes, account for key requirements and interactions that might influence your approach. You should also consult your colleagues who are responsible in these areas to see how improvements might have upstream and downstream effects.

Key consideration | **Consider how changes to your permission can impact other regulatory activities and vice versa (1/2)**

1 of 2

LEGISLATION

Permission processes can be dictated by legislation, and related regulations and rules. Consider how this enables and constrains changes to permission administration.

EDUCATION & COMMUNICATION

Education and communication is important for permissions and broader regulatory outcomes. Consider how you communicate to permission holders and tailor communications to different target audiences as necessary.

INTELLIGENCE & DATA

Permissions provide the foundation for data collection and analysis. Consider how your permission helps to collect data, while minimising burden, which can be analysed, alongside external intelligence, to target effort based on risk.

INSPECTIONS

Permissions can require inspections as part of the approval process. Inspections are also undertaken as part of compliance. Consider how inspection regimes are designed to target different permission holders depending on their risk.

Permission processes do not exist in isolation. Other regulatory practices and activities may impact permissions, and vice versa.

Before improving permission practice and processes, account for key requirements and interactions that might influence your approach. You should also consult your colleagues who are responsible in these areas to see how improvements might have upstream and downstream effects.

Key consideration | **Consider how changes to your permission can impact other regulatory activities and vice versa (2/2)**

2 of 2

COMPLAINTS AND INVESTIGATIONS

Regulators can receive complaints about permission holders which need to be investigated. Consider how outcomes of complaints and investigations can lead to necessary changes in the permission.

COMPLIANCE & ENFORCEMENT

Many permissions are underpinned by compliance and enforcement regimes. Consider how past concerns and outcomes can influence your approach to compliance and enforcement, including condition setting.

SECURITY & RECORD KEEPING

Permission applications collect important information. Consider how information is stored safely and in line with Public Record Office Victoria's (PROV) recordkeeping practices and requirements.

REPORTING

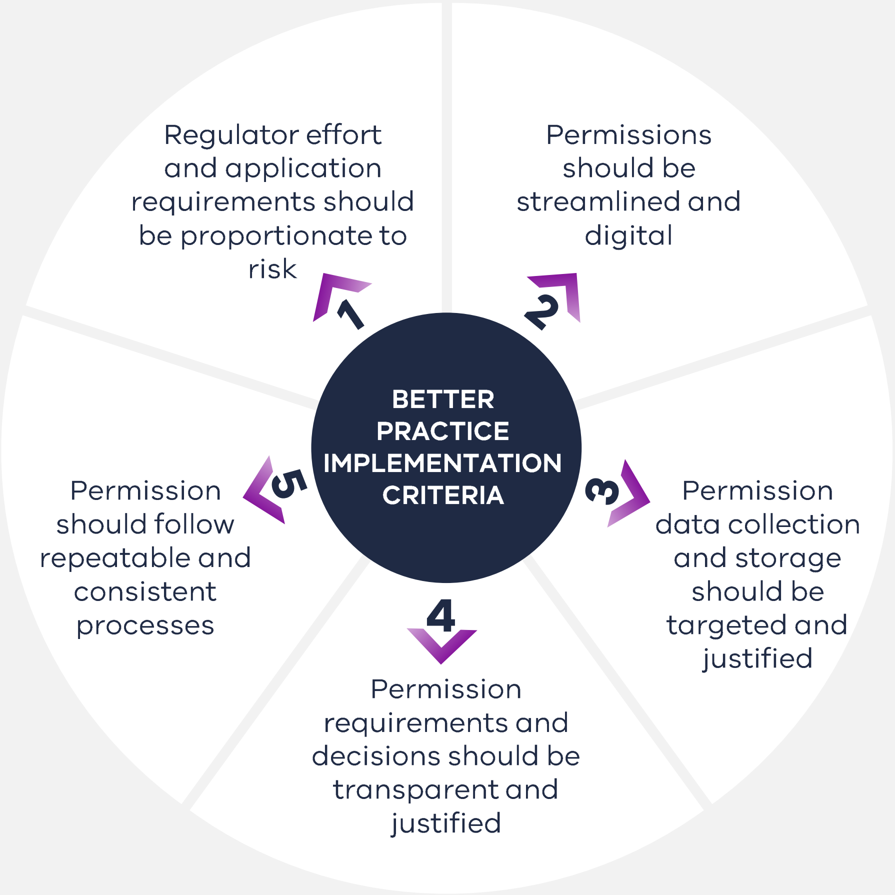
Permissions may drive reporting requirements for permission holders. Consider how these reports will be used in the ongoing management of the permission, such as risk analysis.

CONDITIONS

Permission conditions impacts compliance requirements. Conditions need to be clearly articulated and able to be enforced. Consider how a library of conditions (whether standard, common or bespoke) can be managed as an asset.

Implementation criteria | **Use implementation criteria to scope improvement opportunities**

There are five key implementation criteria:


BETTER PRACTICE IMPLEMENTATION CRITERIA
1
Regulator effort and application requirements should be proportionate to risk
2
Permissions should be streamlined and digital
3
Permission data collection and storage should be targeted and justified
4
Permission requirements and decisions should be transparent and justified
5
Permission should follow repeatable and consistent processes

Implementation criteria inform better practice

Implementation criteria can support you to identify, prioritise and test improvements to implement 'better practice' with a focus on good regulatory, administrative and user experience practices.

These implementation criteria are based on research across Victoria and comparable jurisdictions, including detailed analysis of over 20 permission schemes and engagement with BRV, regulators, Service Victoria and DTF. These criteria are aligned with BRV's principles for good regulatory practice.

How to use the implementation criteria:

- These implementation criteria can be used as a guide to interrogate your current state practice and processes and identify improvement opportunities.
- Sub-criteria outline practical implementation guidance for regulators.
- You should also consider and apply these as you work through the detailed permission journey and components. Key questions and considerations are provided at each stage of the process to help you apply these criteria.

Implementation criteria | **Five key implementation criteria are supported by sub-criteria for operational guidance (1/3)**

1. Regulator effort and application requirements should be proportionate to risk

Regulators are clear on the harm they are minimising through the permission; regulators design permission processes and apply effort based on an assessment of risk throughout the permission journey.

1.1 Regulators should be clear on what harm the permission addresses or policy objectives it achieves and how the permission aims to address it.

1.2 Regulators' assessment of risk across the permission journey should be considered in the context of the other regulatory risk management tools available (e.g., obligations on company officers).

1.3 Regulators should triage applications and allocate effort based on an assessment of risk throughout the permission journey

1.4 Regulators should design their processes to identify the risk profile of an application as early as feasible.

1.5 Accounting for risk, permissions durations and renewal processes should have the longest duration possible, and applicants should generally not need to go through a new approval process when renewing.*

2. Permissions should be streamlined and digital

Regulators make the permission practice and processes as straightforward and clear as possible for the applicant; permission information is easily accessible, and processes are digitised.

2.1 Permission processes should be streamlined for applicants, taking a 'user-centric' perspective to help applicants comply.

2.2 Permission processes should be taking a 'digital first' approach and be automated wherever feasible (e.g., considering applicant digital literacy or other important objectives such as procedural fairness).

2.3 Permission processes should adhere to digital accessibility guidelines, with situation-appropriate options for non-digital information, advice and support.

* Refer to the Victorian Permissions Framework for further guidance.

Implementation criteria | **Five key implementation criteria are supported by sub-criteria for operational guidance (2/3)**

3. Permission data collection and storage should be targeted and justified

Regulators collect the minimum information required and adopt a 'tell us once' approach to reuse information where possible; processes and supporting technology allow for the automatic verification of information and the integration of available data sources; any sensitive data that is collected is protected and/or deleted.

3.1 Regulators have substantiated reasons for asking for information from the applicants (beyond what is required under legislation), with requests limited to what is required to evaluate or manage risk, or to gather data for government that is not collected elsewhere.

3.2 Regulators should adopt a 'tell us once' experience and work with government to integrate with all available data sources where possible (e.g., pre-populated information, verified information from external trusted sources).

3.3 Regulators should uphold trust and be transparent with the applicant about how information is being reused (e.g., in line with consent and legislation.)

3.4 Regulators should protect the privacy and security of information and avoid collecting and retaining personal data unnecessarily (e.g., date of birth).

4. Permission requirements and decisions should be transparent and justified

Regulators provide the right amount of information at the right time to help the applicant comply as well as understand all decisions and outcomes; regulators provide accessible and transparent appeal mechanisms.

4.1 Information and guidance about the application process, what permissions are needed, what conditions might apply, and how to meet permission requirements should be readily available, timely and easily digestible.

4.2 Permissions should meet administrative law requirements including natural justice and procedural fairness requirements (e.g., by transparently explaining processes, providing justification and recording of decisions, ensuring appropriate delegations, and providing applicants the opportunity to query decisions).

4.3 Most conditions should be standardised, with bespoke conditions only applied to address unique harm or in response to other triggers (e.g., risks non-compliance and enforcement).

4.4 Regulators should consider the effort and burden associated with the applicant producing additional information (accounting for the number of entities impacted), and weigh this against the benefits to the regulator of acquiring this information.

Implementation criteria | **Five key implementation criteria are supported by sub-criteria for operational guidance (3/3)**

5. Permissions should follow repeatable and consistent processes

Regulators design all permissions in a repeatable and consistent way; permissions can be updated for continuous improvement and changes to policy and legislation.

5.1 Permission processes should be repeatable and consistent across permissions, as aligned to the better practice permission journey.

5.2. Variations from the standard permission process should be minimised by providing a straightforward application process, and variation should only be supported in exceptional circumstances where regulatory requirements and processes are necessarily distinct (e.g., in the Act or Regulations) or complex (e.g., complex assessment for high-risk permissions).

5.3 Permission processes should be underpinned by a consistent approach to managing interactions, so internal resources and requests for information are guided by predictable milestones, that streamline the applicant's experience.

5.4. Permission processes (while repeatable and consistent) should remain flexible and adaptable to respond to changes (e.g., policy, legislative changes) and allow business rules and system settings to be modified.

5.5 Permission processes should always be reviewed for continuous improvement, especially where current processes are inefficient or difficult for applicants to comply with.

Implementation criteria | **Account for 'better practice' essentials when reviewing your processes**

4.2: Australian administrative law requirements

Administrative law is the body of law related to government decision making in Australia and is important through the administration of permissions.[1] It accounts for:

- Decision making that is fair, high-quality, efficient and effective. Regulators follow procedural fairness and natural justice requirements, with decision-making fair and free from bias.
- Individual access to review of both the merits and lawfulness of decisions and conduct. Regulators ensure applicants have an avenue for decisions to be reviewed again on the facts.
- Accountability for government decisions and conduct. Regulators ensure they document clear reasons for decisions made.
- Public access to information about government decisions and processes, and individual access to personal information held by the government. Regulators facilitate relevant information requests and protect personal information.

You will need to ensure that any changes to your permission practice and processes uphold and promotes these attributes. You should also consider administrative law requirements through the design and implementation of business rules and automated decision making, ensuring this fits under your legislative framework, and is fair and justifiable.

4.3: Conditions

Conditions are commonly imposed on permissions and can take various forms depending on the application. This playbook considers three types of conditions:

- **Standard conditions:** Standard conditions across all permissions, generally communicated and accepted up front through the information and application.
- **Common conditions:** A set of common, standardised conditions that can be reused across permissions, such as those with common characteristics.
- **Bespoke conditions:** Conditions for certain circumstances to address unique harm or in response to other triggers (e.g., non-compliance and enforcement).

Conditions are often applied:

- At the registration or renewal stage
- When the regulator has no other tools to address risks
- When the regulator needs to address systemic issues facing the regulated system

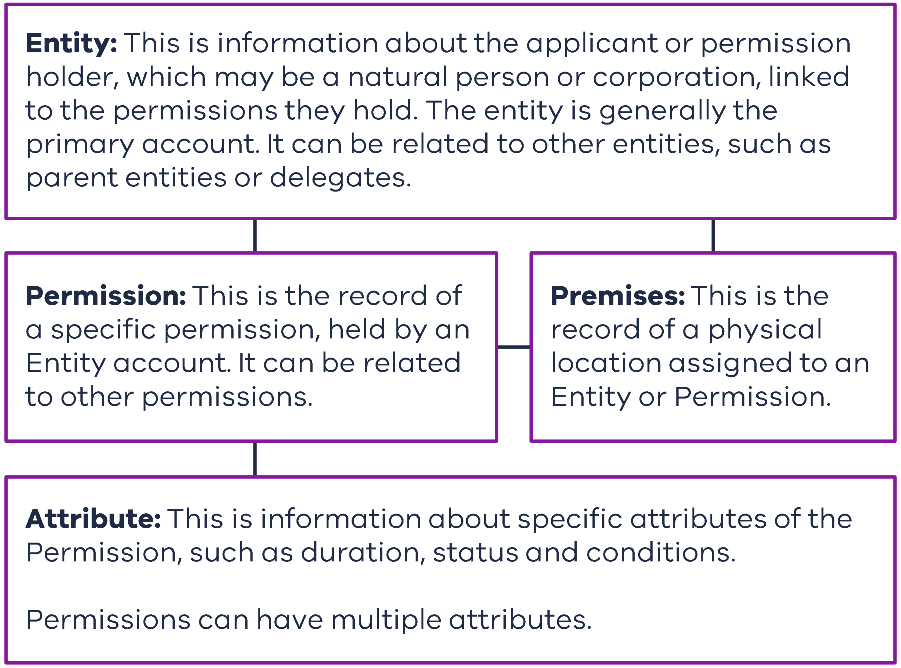
You will need to carefully consider when and how conditions are applied across your permissions (e.g., up front or after assessment)[2] and the level of prescription or flexibility they provide. You may choose to test conditions with applicants through a draft permission to ensure requirements are properly understood.

[1] Australian Administrative Law Policy Guide, Australian Government, Attorney-General's Department, 2011
[2] Refer to the Victorian Permissions Framework for further guidance.

Digital and data | **Consider your permission data model**

You should consider your data model and structure to ensure your data is collected, retained and used in the most effective way. Identify what information should be stored against the entity, permission, or attribute.

3 DATA MODEL LAYERS



Entity: This is information about the applicant or permission holder, which may be a natural person or corporation, linked to the permissions they hold. The entity is generally the primary account. It can be related to other entities, such as parent entities or delegates.

Permission: This is the record of a specific permission, held by an Entity account. It can be related to other permissions.

Premises: This is the record of a physical location assigned to an Entity or Permission.

Attribute: This is information about specific attributes of the Permission, such as duration, status and conditions.

Permissions can have multiple attributes.

An example **data model** and **relationship model** are provided in the appendices.

A data model outlines how information is collected, organised, and retained during the permission process. It captures the relationships between different kinds of data.

This Playbook considers three 'layers' of permission data that work together – the Entity which is the applicant or permission holder (generally the primary account), the Permission and Premises, and Attributes of the permission. These are often captured as separate records that are linked to each other.

You should look for opportunities to consider your data model.

- Understand how your data is currently organised and retained, at what layer and what data is linked
- Consider how your permission information enables your broader regulatory outcomes, including risk assessment and intelligence, compliance management and reporting.
- Identify opportunities to realise greater value from your data or what other data sources would be valuable.

You should also consider the relationships between data and information, the differences between personal and business information, and how data migration or conversion could be used to support your data processes.

Digital and data | **Permission components can be digitised by regulators, aligned with Service Victoria's offering**

Digital reform can be enabled through better practice and this Playbook

The Playbook outlines considerations for how you can prepare to digitise your processes and practice, considering Service Victoria and other whole of Victorian Government products where this is relevant.

Practice and processes should be improved before or in parallel to digitisation. It does not have to be achieved all at once but can be focused on where it is most valuable. Digital reform can be a significant change and you should also consider and plan to manage the impact of change on regulated entities and your people.

Permissions can be made of common and configurable digital components

Permissions can be broken into 'common' and 'configurable' digital components.

Common components will have processes and collect information that can be made consistent. This allows for common components to be copied and easily incorporated into digital workflows when using the same systems.

Configurable components can also have consistent processes but require varying information fields. These components will need to be tailored to your processes as needed/

This aligns with Service Victoria's view of how 'components' (i.e. digital processes and information capture) can be made consistent and where variation is likely to occur.

COMMON COMPONENTS	**Standardised process / standardised information** *For example, the same applicant information (i.e. name, address) should be captured in the same way across all permissions.*
CONFIGURABLE COMPONENTS	**Standardised process / variable information** *For example, information specific to a permission will vary depending on the activity being regulated and requirements.*

Digital considerations | **There are important broader considerations for information and digitisation**

1 of 2

PRIVACY

You should consider the privacy of information collected through the permission process.

Some information may be 'personal information' under the Privacy and Data Protection Act 2014, particularly when about an individual as a natural person, and therefore must be managed and protected to align with the Office of the Victorian Information Commissioner (OVIC) Information Privacy Principles (IPPs).

Some personal information may also be 'sensitive information' which has additional requirements, as outlined in OVIC IPP-10.

You should seek advice for the privacy requirements of information collected.

SECURITY

You should take a risk-based approach to implement security controls commensurate with the sensitivity of the information and security risks, and regularly assess those controls.

You should consult with relevant agencies, including OVIC, and monitor potential cyber security risks. Information should be minimised by default, only collected and retained as necessary.

Some information collected may need to comply with the Public Record Office Victoria (PROV) standards framework, which outlines requirements such as retention, storage and disposal.

You could complete a Privacy Impact Assessment to identify all systems where the personal information is collected, stored, processed, transferred and/or archived.

Digital considerations | **There are important broader considerations for information and digitisation**

2 of 2

CONSENT

You should identify where consent is required and consider how this information will be used.

Information used within a permission may not require consent or may require implied consent, such as captured through completion and declaration of the application and declaration process and supported by a collection statement, as outlined in OVIC IPP-1.3.

Information shared and used more broadly may require more explicit and informed consent, such as for identity verification and police checks.

ACCESSIBILITY

You should ensure that all information is readily available and understandable.

The Victorian Digital Guides provides guidance. You should aim for content to be accessible to meet Web Content Accessibility Guidelines (WCAG) 2.1 (AA) standards and is understandable for your audiences, at a Grade 8 reading level for general information.

Translation services can also be used to communicate more effectively with culturally and linguistically diverse (CALD) communities.

INTEROPERABILITY

You should consider required uses for information, what systems will be used, and how these systems will communicate information between each other.

Understand how your different front and back-end systems work together to identify any issues and where new options, such as new platforms or APIs, can be used to support your data model.

Pause and reflect | **Think about how you are going to effectively deliver reform**

Reflect on the ambition and parameters to guide reform. It is important to think about the people running the process and those who are impacted, the process of running the project itself and what you want to get out of the project.

PEOPLE

- Who will run the reform project and who is responsible for the outcome (ownership might be shared where it involves cross-cutting data sets and interactions)?
- What staff capabilities are needed to run and work on the project? How will you manage change?
- How will endorsement and executive sign-off be obtained, including project funding?
- How will the benefits of the reform product will be communicated to staff?
- What is the governance?

PROCESS

- What level of investment is needed for the reform project?
- What are the user expectations of the reform?
- What your engagement or project management strategy is with staff beyond user testing for the transitional period
- What are the key actions that need to be taken before starting the reform project (e.g., data quality/cleaning, research into systems, compliance with records requirements)?

PROJECT

- What do you want to get out of the project? Have you got a clear idea about what your minimum viable product is at the end of the process?
- How can you preference off-the-shelf solutions vs. designing bespoke solutions? How can you challenge your processes where there might be unnecessary customisation?
- How will new processes and products be tested (at a minimum by staff but ideally by applicants)?
- How will you account for data hygiene and quality practices as enablers and constraints?

Better Regulation Victoria

Appendices

VICTORIA
State
Government

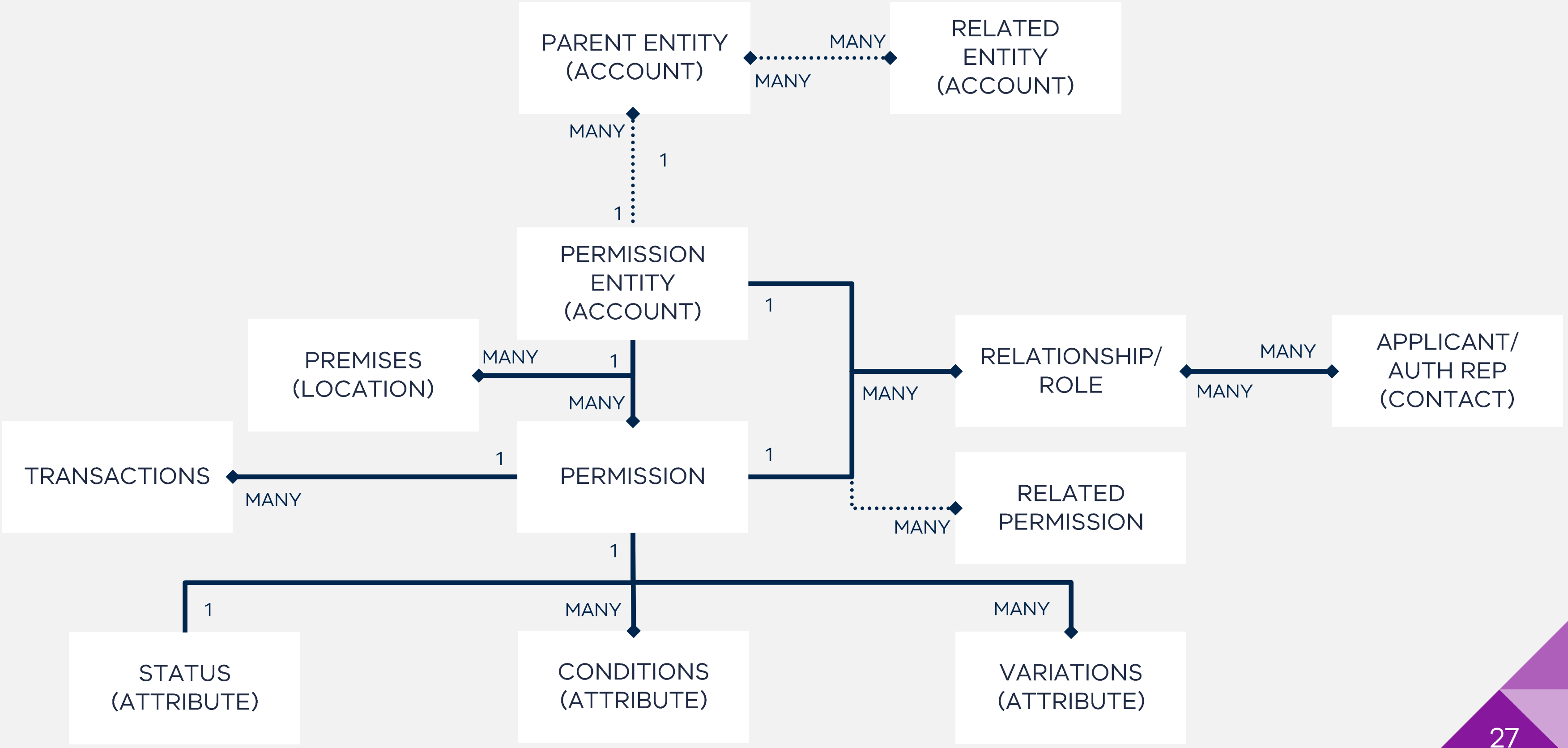
An example data structure for permissions, with defined relationship between the entity, permission and attributes

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?

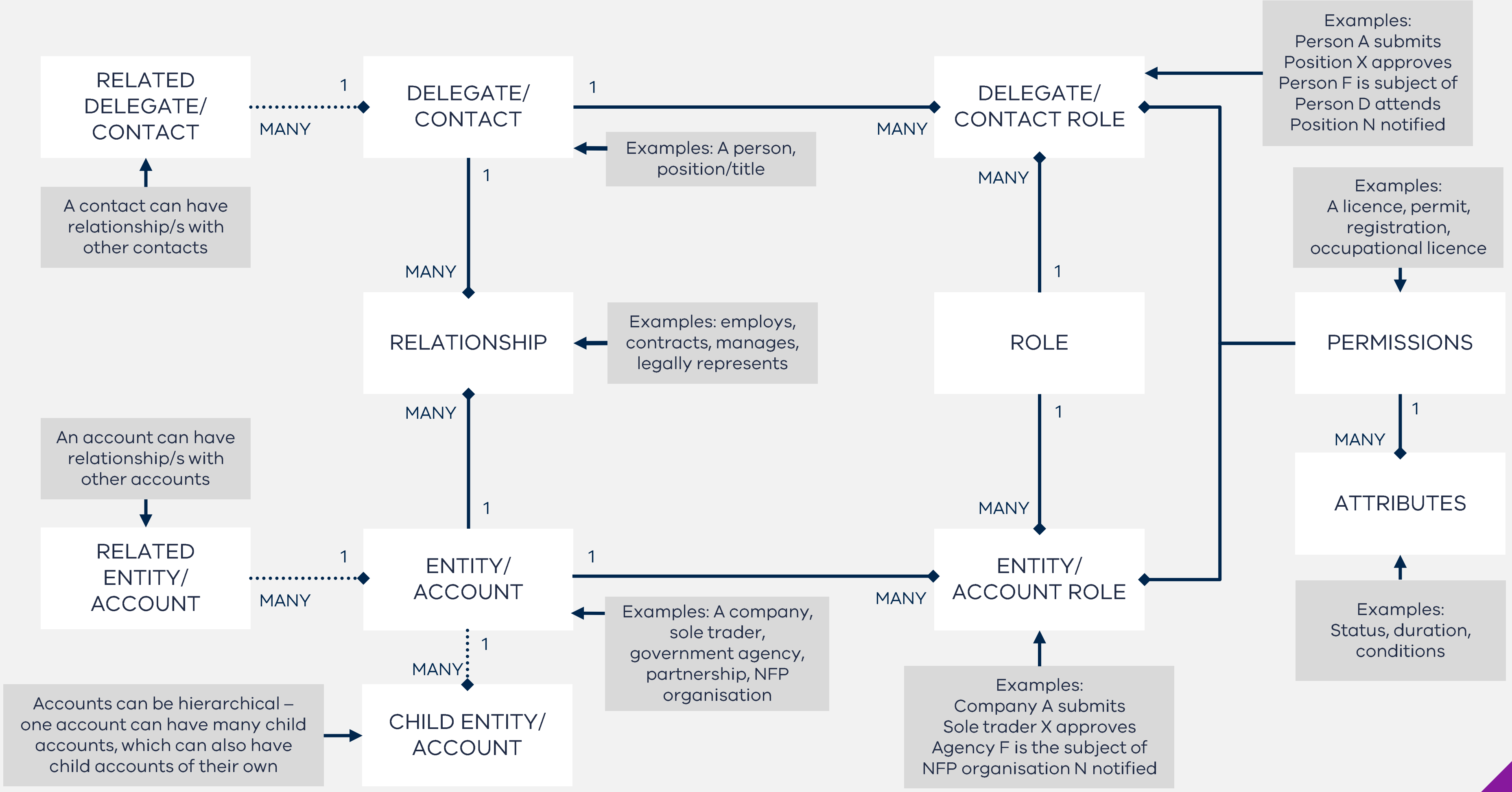
It is likely that your digital and data team will consider the data structure and model through detailed design, but it is something that is valuable to be familiar with. A senior regulatory leader will often be the data steward of a regulator.



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.


RELATED DELEGATE/ CONTACT
1
MANY
DELEGATE/ CONTACT
1
MANY
DELEGATE/ CONTACT ROLE
Examples:
Person A submits
Position X approves
Person F is subject of
Person D attends
Position N notified
Examples: A person, position/title
A contact can have relationship/s with other contacts
1
MANY
MANY
1
Examples:
A licence, permit, registration, occupational licence
RELATIONSHIP
Examples: employs, contracts, manages, legally represents
ROLE
PERMISSIONS
MANY
1
1
MANY
An account can have relationship/s with other accounts
1
MANY
ATTRIBUTES
RELATED ENTITY/ ACCOUNT
1
MANY
ENTITY/ ACCOUNT
1
MANY
ENTITY/ ACCOUNT ROLE
Examples: A company, sole trader, government agency, partnership, NFP organisation
1
MANY
Examples:
Status, duration, conditions
Accounts can be hierarchical – one account can have many child accounts, which can also have child accounts of their own
CHILD ENTITY/ ACCOUNT
Examples:
Company A submits
Sole trader X approves
Agency F is the subject of
NFP organisation N notified

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.

VICTORIA
State
Government

Better Regulation
Victoria