RAIDIAM

CHECKLIST

Data sharing ecosystem checklist

Key questions to save you time and money

If you are thinking about creating your own data sharing ecosystem, regardless of why you need or want one, there are some key questions that it pays to consider upfront. Raidiam, the data sharing pioneers, have identified that your answers will significantly impact the design and implementation of any ecosystem.

Working through this list will not only save you time and money further down the line, it can also ensure you don't miss out on any opportunities to maximise your investment and avoid any unintended consequences.

Proven track record

Why trust us? Raidiam has unmatched technology and expertise developed whilst working on the world's most exciting data sharing ecosystems. From Open Banking in the UK and Open Banking and Open Insurance in Brazil, to delivering commercial ecosystems to individual enterprises, we have unparalleled experience.

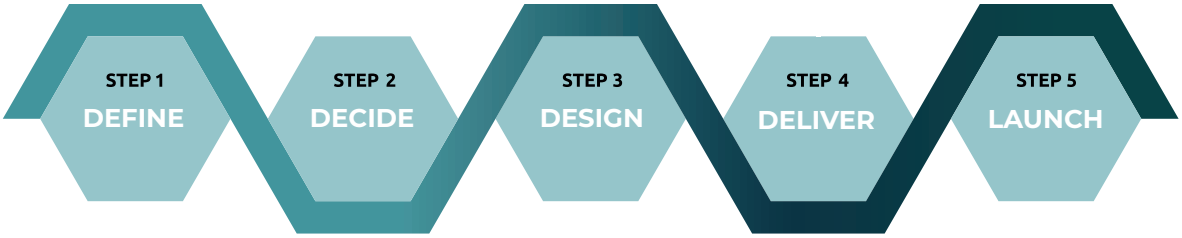
Although we started in finance, businesses from all sectors turn to us to help them excel in the API economy using our award winning, highly secure Raidiam Connect ecosystem-in-a-box technology to create and control their own ecosystem.

Over the years we've learnt that no matter whether the driver is commercial or regulatory, the fundamental principles of every ecosystem's Trust Framework are the same. This is why we have developed our Raidiam Connect technology to be sector and data agnostic. We have created this checklist to benefit anyone considering creating their own successful ecosystem.

How we can help

Raidiam provide everything needed to get an ecosystem designed and delivered from scratch, quickly and easily. If you would like to find out more about how we can help please get in touch at **sales@raidiam.com**.

A step by step guide to create an ecosystem



DEFINE & DECIDE

Start by going through the checklist. Define the purpose and objectives of your ecosystem and answer key 'who', 'what' and 'how' questions including if conformance is necessary to ensure adherence to ecosystem rules and regulations.

DESIGN & DELIVER

Raidiam team configure technology to meet your goals and get your highly secure ecosystem up and running quickly – often within a matter of weeks.

Ecosystem checklist	Questions	Considerations
Objective and outcome: defining the purpose of your ecosystem	**Why is it needed?**	What are the drivers for creating an ecosystem – consider what outcomes are sought and who it will serve. If you're building an ecosystem to meet regulatory requirements, consider how else it could be used to deliver commercial benefits.
	What do you want it to achieve?	Use cases need consideration and success criteria should be captured. Walk through use cases and customer journeys to help shape implementation decisions.
	How do you envisage it being used?	A valuable starting proposition can be developed by prioritising use cases and objectives. This can grow over time and be shared with participants to build confidence.
	How will the design, delivery, ongoing monitoring and development be funded?	Funding of the ecosystem build and ongoing costs needs consideration, e.g. maintaining an accreditation framework and Trust Framework. A funding model that splits costs fairly amongst different participants may be needed when multiple parties are involved. A cost-benefit analysis exercise can be useful to calculate the ROI and ensure a funding model exists to sustain your ecosystem into the future.
Key 'who', 'what' and 'how' questions	**Who**	
	Who is taking part? Participants in the data sharing chain need identifying and defining.	Define the parties whose data will be used - these are collectively known as the Data Owners. They may also be end users who are being provided with additional services based on their data. Define who will be 'exposing' the data for other parties to consume or use; what type of entities they are; and whether they are all providing the same or different types of data – these are collectively known as the Data Providers. Define who will be the entities that wish to use the data to provide products and services to the end users, and what types of propositions are envisaged – these are collectively known as the Service Providers. • Data Owners (consumers) need to know who the Data and Service Providers are. • Data Providers need to know who the Data Owners and Service Providers are. • Service Providers need to know who the Data Owners' Data Providers are.
	Who needs to be registered/ have membership?	Participants should be required to prove themselves fit and proper as eligible to participate in an ecosystem. They know the authority to whom they need to prove this and obtain accreditation.

What	
What data is each participant allowed to see and share?	• Data Owners need to be clear on what consent they are giving to Service Providers around the sharing and use of their data. • Service Providers need to obtain consent from the Data Owner to process their data. • Data Providers need to authorise the consent obtained by the Service Provider from the Data Owner by verifying it directly with the Data Owner.
What is the data sensitivity level?	Undertake a data classification and privacy impact assessment.
What level of security is needed for the data to be shared and how will authorisation be technically granted?	The data and its transmission need to be secured. The Data Owner must also have full control to give, see, monitor, change and/or revoke any consents granted.
What secures the exchange?	Any communication channel between the communicating parties must be secured, so any data transferred is received as sent, without being seen or manipulated by unauthorised parties. This is typically achieved by mutually authenticated transport-layer security (TLS).
What mechanisms exist for authentication?	Data Providers (and in some cases, Service Providers) must ensure that participants are authenticated before being granted access to the data.
What roles and responsibilities do different participants have and what must they be accredited for?	These should include: showing the Data Owner how their data has been aggregated and categorised; providing tools to enable Data Owner to control their data; and facilitating an easy point of complaint and access to redress.
What are the conduct requirements for participants?	For example, ensuring the fair treatment of consumers, especially the vulnerable.
What governance is needed? Is there a legislative or regulatory framework and how will the data sharing comply?	For example, for the accreditation and conformance testing.

How	
How will the data exchange be secured and how can all participants be sure?	• Data Owners need to know how their data will be provided and secured. • Data Providers need to know how to provide and secure the data. • Service Providers need to know how data will be provided and secured.
How will participants be defined and identified within the ecosystem?	The identification methods for use with Data Owners, Data Providers and Service Providers that allows their identity to be authenticated. These are the methods needed for providing the required consents and for ensuring that only the authorised data is provided, to the authorised Service Provider, for the authorised amount of time.
How should participants behave with regards to the data?	Setting clear rules on what participants can or cannot do with the data they access; what services they must provide to the Data Owner; and what responsibilities they have if/when something goes wrong – privacy policies and terms of use etc.
How do participants identify other participants, and communicate trust, e.g. have they met the 'fit and proper' requirements for accessing data (via a Trust Platform)?	Ensuring that appropriate and effective methods of identification, authentication and authorisation are in place and clearly sign-posted to participants. Authentication may differ for different types of data or sector requirements. The Trust Platform provides all the necessary capabilities.
How do participants conform to the standards, and communicate their conformance, both to other participants (via a Trust Platform) and to End Users/ consumers?	Ongoing conformance testing may be needed (for large ecosystems to ensure parity and consistency of implementation). A Software Development Kit (SDK) for participants is the best way to achieve this and Raidiam provides several open-source examples in different languages to get you started and on the right path. Also need to consider how technical accreditation conformance will be achieved. A Trustmark can be used to communicate to end users that participants meet the necessary requirements. Raidiam can offer ecosystem conformance and certification services as part of our Raidiam Assure service.

Developing an accreditation approach

Responsibility must be assigned to a specific authority for functional and supervisory elements including:

- Classification of data.
- Roles of participants who can provide, access and use data.
- Rights of access to data.
- Accreditation requirements participants need to meet to access data.
- Validation of the requirements having been met.
- Monitoring of accredited participants.
- Enforcement against participants who do not meet agreed accreditation standards.
- Reporting on the accreditation framework, market development and effectiveness.

Developing an accreditation approach, and confirming rights and roles, is a key part of the broader Trust Framework and an important pre-implementation exercise. This ensures a trusted and robust process is in place to control and protect who has access to an ecosystem and build confidence in it.

The use of a Directory API within a Trust Platform provides a scaling benefit for an ecosystem and reduces complexity. This securely communicates identity and authorisation attributes for all participants. Without a single centralised Directory API, each participant would need to agree, communicate and validate each and every other participant separately in order to guarantee security.

Voluntary accreditation
If no regulatory mandate exists on a Data Provider to share data (and therefore no right of access for a Service Provider), the agreement to share data must be agreed through voluntary consensus between Data and Service Providers. This can be achieved through a bi-lateral contract.

RAIDIAM

Contact us We would love to speak to you about how we could help make your data sharing ecosystem a reality.

sales@raidiam.com www.raidiam.com

December 2022