iDP

INNOVATION
DATA PLATFORM

A next generation platform for ORX to launch high value risk applications

O.R.X

Contents

Introducing iDP

A next generation platform for ORX to launch high value risk applications

Standing for Innovation Data Platform, iDP is a first-of-a-kind digital platform on which ORX can launch a new generation of risk management and data visualization applications.

iDP brings these risk applications and your data together into one secure space. All apps on iDP are pre-validated and accredited, significantly reducing implementation time and cost. They all use a consistent data format, making it possible to ultimately create your own tailored, modular and integrated risk management ecosystem – the overall outcome being more powerful risk insights.

Connecting consistent data with various apps and services

iDP has been built to ease the effort of data upload and enable the sharing (only with member permission) of data across various applications and services. This means that structured data – mapped to ORX standards – can be used across different apps on iDP and across the various ORX services. For example, in the future, iDP opens up the potential for you to use loss and control data more seamlessly alongside data from ORX Scenarios or ORX News.

Secure by design

iDP is built on industry standard AWS componentry, is secure by design and delivers extra layers of trust to your data and risk application management.

Our layered security approach is built upon an industry grade infrastructure, industry standard certification, a user-controlled Locked Box security model, 24/7 monitoring and reporting, and application bench testing.

A platform to innovate on

iDP delivers on robust security and data standards but its purpose is neutral. It leaves the specifics of what apps are added to the platform and what they offer up to the users and app producers. To develop valuable solutions for our community, ORX will develop apps for iDP leveraging a growing library of industrial-grade tools and exploiting the advantages of operating on modern infrastructure. For example, on-demand cloud technology without physical servers allows low-cost app deployment.

Applications available on launch

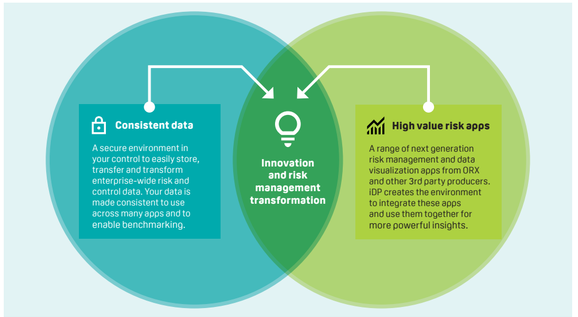
The first of ORX's applications for iDP – launching in Q4 2022 – is a risk control app, which shows visually where you have gaps compared to the ORX Reference Control Library (read more on page 6). Over 2023, ORX will then be exploring the requirements and timetable for bringing new ORX apps onto iDP.

In addition to ORX applications, iDP also provides the opportunity to deploy other apps from 3rd party risk and reg tech producers in a safe and consistent environment. See page 7 for details of apps available from Aylien and Elseware.

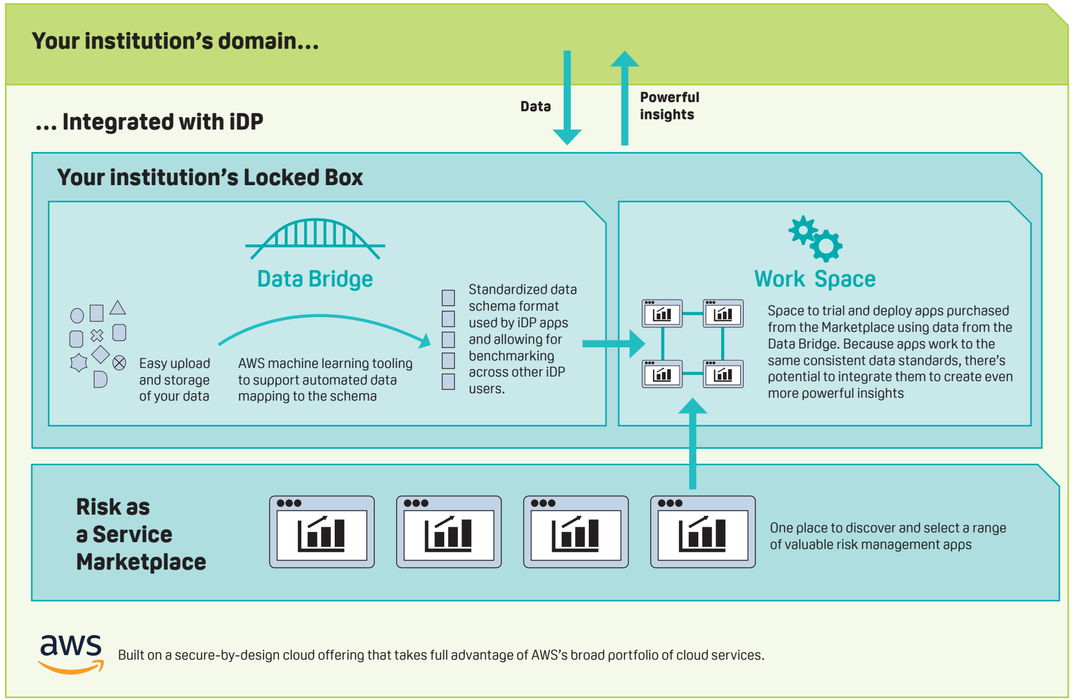
Future opportunities

iDP will unlock new opportunities for ORX and its members to advance operational risk – both for each individual institution using iDP and for the industry as a whole. These include:

- The functionality to create an overall iDP peer benchmarking service, whilst also allowing benchmarking to be built into specific apps
- Data pooling capabilities, meaning data from multiple institutions can be aggregated for powerful analytics and effective visualization
- The ability to perform complex federated analytics in a highly secure environment and without ORX or other app producers needing to access a financial institution's sensitive data.



The features of iDP



Risk as a Service Marketplace

The *'Risk as a Service'* Marketplace allows you to discover accredited risk solutions to enable you to innovate risk management more cost effectively.

All apps available are pre-validated and security-certified and all use consistent data standards. This not only reduces the time and effort required to adopt new apps, but it also means that they can potentially be used together to create richer insights.

As well as applications, in the longer term, we anticipate offering services such as enhanced validation and more 3rd party datasets to enrich your own data.

Locked Box

Built on secure by design AWS cloud technology, the Locked Box is a segregated zone specific to your institution for managing data and running apps in a consistent way.

The Locked Box is fully in control of your institution – essentially an extension of your own domain – but isolated from your systems and benefiting from iDP's robust security framework. iDP therefore offers a *'best of both'* situation.

The Locked Box contains two distinct areas – a **Data Bridge** and a **Work Space**.

Data Bridge

The Data Bridge is a secure place within the Locked Box for storage and easy management of your institution's risk and control data.

There is a standard iDP schema set available to map your own data to that the various apps on iDP will pull from. Data mapping to the schema can be an incremental process as and when particular data is required by an app you want to use. But once mapped, you can then use that same data across multiple apps – saving time and effort as opposed to working with 3rd party solutions that all require different data formats.

The data mapping process is further assisted by the iDP Data Mapper apps. These apps use AWS Natural Language Processing tooling and leverage industry data standards, such as those developed by ORX in conjunction with over one hundred of the world's leading banks and insurers. Over time, these machine learning apps will be able to identify similarities between your data and the schema used by iDP, mapping the majority of your data automatically and making the process far less manual and time consuming.

The Data Bridge is built on a data mesh concept, which enables the fusion of different data sources (both your data and external 3rd party data sets) and makes data accessible, available, discoverable, secure, and interoperable.

Work Space

The Work Space is where you will onboard and use any apps your institution has selected from the Risk as a Service Marketplace, accessing any data as required by particular apps. It contains enabling tools that support app deployment.

When you are interested in an app from the Marketplace, you can bring it into your Locked Box to trial before committing, making innovating easier with less risk and cost involved with purchasing a solution that isn't ultimately right for your organisation.

Once deployed, approved users from your institution can access the app via a secure web portal.

With iDP, you are in control

- You manage security and access to the Locked Box, and stored data is encrypted using user-controlled keys
- You manage what data you store and what apps you use
- You manage what data sharing and benchmarking you do with other users of iDP

The iDP layered security approach

What current issues with security does iDP solve?

Delays and risks are currently common when trying to integrate multiple 3rd party risk management solutions. The 3rd party producers of these solutions are rarely compliant with your institution-specific security and privacy requirements, so the process of onboarding them is often long and challenging.

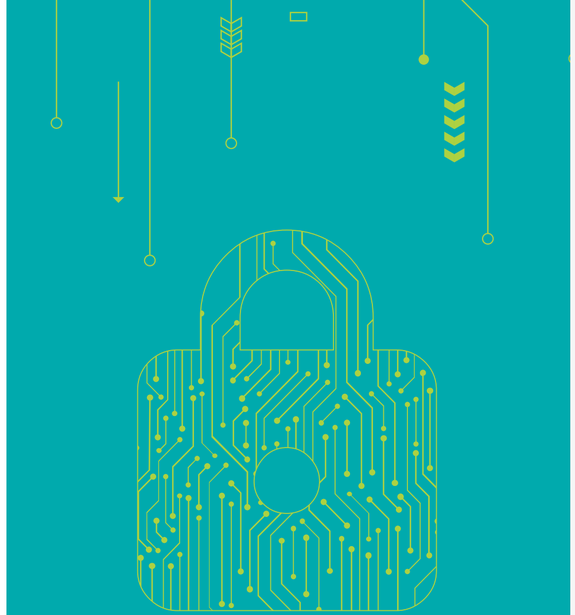
Before iDP, you either need to choose between handing over your sensitive data to a 3rd party supplier to use in their tech solution; or alternatively, you can choose to run a 3rd party solution in your own environment – both of which pose security issues.

What is the iDP vision?

iDP offers a third option: it allows you to access bench tested risk solutions through a single, industry-standard compliant and secure-by-design gateway that is frequently monitored and upgraded, while retaining control over your own security.

iDP addresses security pain points in 4 ways:

1. **Complying with industry standards:** iDP is on track to achieve high maturity against NIST CSF and region-specific privacy frameworks, migrating towards ISO 27001/02 compliance with longer-term build out towards NIST 800-53.
2. **Being secure by design:** iDP is secured through distributed computation (i.e., apps are run in isolated, 'Locked Box' instances), a multi-environment set-up (i.e., separate test and production environments) and an enterprise-grade AWS security model (i.e., 40+ guardrails, 10+ security solutions, and robust security design covering data ingress, processing, and egress) – with security assured through regular pen tests by a CREST-accredited 3rd party.
3. **Having 'Locked Box' instances that are controlled by each financial institution:** iDP provides you with control over all critical security aspects of your Locked Box, enabling you to adhere to organisation-specific requirements out of the box, whilst also benefiting from iDP oversight (e.g., security monitoring).
4. **Assuring the security of all applications:** All applications are bench tested before launch onto iDP, ensuring that they are compliant with relevant standards (e.g., OWASP), secure by design (e.g., enforced encryption at rest), and certified (e.g., CVE scan, independent pen test).



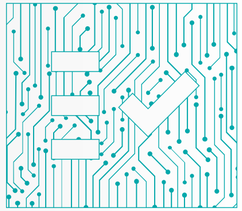
Faster innovation via pre-validated applications

What current issues with validation does iDP solve?

Validation processes to check that 3rd party solutions meet their intended purpose are often complex and resource-intensive, especially in the non-financial risk space.

What is the iDP vision?

iDP allows you to spend less time and effort validating, understanding and building confidence in 3rd party risk and reg tech solutions because apps available are all pre-validated by iDP before being allowed into the Risk as a Service Marketplace.



iDP addresses validation pain points through a 5-step proposition:

1. **Functional and non-functional bench testing and accreditation:** Functional and non-functional bench testing and accreditation ensure that applications deliver on their functionality, are properly configured to run on iDP, and are secure *(see security approach on the previous page).*
2. **Model risk assessment and pre-validation:** A foundational, comprehensive risk assessment of the application model using synthetic data is performed by iDP as a 'neutral' intermediary, outputs of which are shared with users. There is also potential for an optional enhanced, SR11-7 compliant pre-validation service in the future.
3. **Try before you buy:** *'Try before you buy'* trial licenses enable application testing in your Locked Box's Work Space before purchasing.
4. **Accelerated, context-specific validation:** Accelerated, context-specific validation modules are deployable on demand in your Locked Box to accelerate validation on your/context-specific data.
5. **Enhanced transparency through periodic review, continuous monitoring and peer intelligence:** iDP performs continuous platform-level monitoring enhanced by crowdsourced user feedback and pooled, user-level performance metrics (where applicable to a specific application).

Steps 1 & 2

Pre-validation:

iDP assures all applications through security bench testing and model risk assessment process using synthetic data.

Steps 3 & 4

Faster validation:

iDP equips you to do accelerated validation based on your own data.

Step 5

Sharing new insights:

iDP maintains ongoing quality controls and shares insights to increase transparency.

Applications available on launch of iDP

O.R.X

ORX's Risk Control app for iDP

The ORX Risk Control app builds on the recent industry-leading research with nearly 50 member firms to create a control standards library that provides a common representation of control systems by risk type across the enterprise.

The value of the risk control app comes from the ability to provide an interactive dashboard to explore how control systems are being used to manage specific risks across individual business lines and regions.

Key features and benefits

- Allows control systems to be analysed and compared, both within your firm and versus the industry norms in the library
- The application uses design and operating data from individual control instances to enable anomaly detection
- The application is supported by machine learning that automates the data set production
- Outputs can be provided through interactive digital dashboards, or via output files for custom analytics or incorporation into existing systems

How it can be used

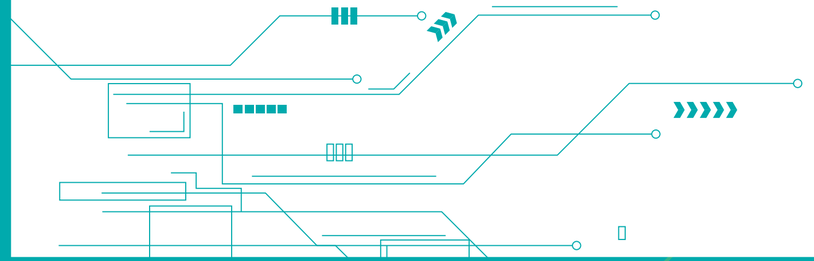
The solution delivers on demand insights to:

- Provide business line orientated risk intelligence over existing RCSA processes
- Support regulatory attestations over the adequacy of the control systems (e.g. Turnbull)
- Benchmark business line controls to industry practice, both for design and performance
- Allow anomaly detection across the enterprise, highlighting gaps or areas of excess controls

Using the app, 1LOD and 2LOD users can:

- Generate targeted alerts on control gaps or control performance trends across business lines
- Prepare analysis for control system assurance at oversight committees
- Perform ad hoc analysis on specific business lines or geographical locations.

Future versions will allow for dynamic benchmarking using anonymized peer data averages provided by ORX on iDP. Over time, ORX hopes to be able to combine this with its world-leading loss data service.



AYLIEN

AYLIEN'S Risk Signals app for iDP

AYLIEN provides risk and market intelligence solutions to a wide range of financial institutions, helping them identify risk events using unstructured data sources.

AYLIEN collects and processes millions of pieces of media content daily from across the globe and processes it using their proprietary Natural Language Processing models to provide analysts and data teams with actionable intelligence on their risk or market landscape.

AYLIEN's 'Risk Signals' solution for iDP acts as a discovery, investigation, and alerting tool for 2LOD professionals. Leveraging Machine Learning and Natural Language Processing, Risk Signals proactively detects risk events in the millions of new articles published online every day. Risk events are categorized by operational risk event type and enriched with a "risk score" based on severity, frequency, and impact. Risk events are then surfaced in real-time via a variety of dashboards, alerts, and RAG score matrices.

Outputs can then be graphically represented via a RAG score matrix, or alternate dashboard-style visualizations.

- Identify emerging risks related to counterparties and risk topics
- Leverage pre-built risk models or train your own
- Track anomalies across your entire risk landscape
- Configure risk dashboards to track signals across portfolios

How it can be used

Risk Signals transforms third-party monitoring processes by proactively identifying and scoring risks related to third parties and their impact on a financial institution's operational resilience. The tool also has applications in the broader operational risk space in areas such as ESG and reputational risk (e.g., understanding the impact of adverse reputational events on a financial institution or tracking ESG-related metrics and events of third-party suppliers).

elseware

Elseware's MSTAR app for iDP

'MSTAR' software allows for the design and simulation of structured scenarios for operational risk using the award-winning[1] XOI method[2]:

- Graphically design risk scenarios
- Quantify the dependencies within risk scenario design
- Run Monte Carlo simulations and what-if analysis
- Define correlations between scenarios
- Run enterprise risk models
- MSTAR provides a library of 35-40 predefined structures for operational risk scenarios in all risk categories (conduct, cyber, error, etc.)

1 Risk.net Industry Initiative of the Year for the use of MSTAR to model Cyber risk with the American Bankers Association.

2 Operational Risk Modeling in Financial Services: The Exposure, Occurrence, Impact Method, Wiley 2019.

An MSTAR iDP app subscriber will be able to:

- Define all the assumptions and data related to a scenario model, via a wizard
- Access the MSTAR risk knowledge base with up-to-date drivers on risks such as fine-to-revenue ratio distribution, probability of natural events, duration of a cyber attack, etc.
- Store and retrieve different versions and scopes (firmwide, legal entity) of assumptions
- Improve these assumptions iteratively and collaboratively
- Perform what-if analysis (new controls, climate stress, etc.)

How it can be used

Key applications are in the scenario space, with the tool assisting the 2LOD scenario function with desktop reviews/workshopping around risk types. The tool will support collaboration between different users, allowing teams to better manage and facilitate risk assessments. Assumptions and outputs will be graphically represented, simplifying reporting to more senior functions.

The iDP roadmap

2021 – MAY 2022

Validated iDP

- iDP design & standards developed with 7 ORX member pathfinders

JUNE 2022

Working iDP

- Initial working version of iDP developed on AWS toolset that demonstrates how it works
- Detailed iDP roadmap devised

Q3 & Q4 2022

Live iDP

- In-production version of the platform is live
- 3 producers available in the Risk as a Service Marketplace: ORX controls, Elsware, Aylien
- Pathfinder & early adopter onboarding

2023

Benchmarking

- ORX exploring the requirements and timetable for bringing new ORX apps onto iDP
- Benchmarking functionality, enhancing solutions already on iDP and allowing for other future benchmarking possibilities as part of apps in the Marketplace

Validated iDP

- Data pooling functionality, allowing data from multiple institutions to be aggregated for powerful analytics and effective visualization
- Develop the platform for existing ORX services such as loss data and scenarios

2023 – 2026

Scale iDP

- Federated analytics functionality, allowing complex analytics to be performed in a highly secure environment
- Scaling iDP as more users and apps onboarded, in addition to expanded solution offering across more risk types

What's involved with using iDP?

Step 1

Sign up to iDP

Following consultation and confirmation with ORX of your intention to access iDP, you will need to sign up and subscribe to iDP.

Step 2

Configure Locked Box

Your institution's Locked Box is set up as an extension of your own operating environment. You are in full control to apply and manage encryption keys and configure relevant user access. This is a one-time process to access all iDP apps.

Step 3

Upload data required

You can then upload data required, e.g., for the ORX ORX Risk Control app, to your Data Bridge. This can be as simple as uploading a CSV file extracted from your GRC platform.

Step 4

Transform data

Once your data has been uploaded, you can transform it into the format needed by the relevant app(s) you wish to use. Advanced AI-powered tools in the Data Bridge automate data cleansing, sorting and augmentation.

Step 5

Find apps & subscribe

You can easily find, click and subscribe to ORX and other 3rd party apps within the Risk as a Service Marketplace. This automatically installs the app within your Locked Box's Work Space, pre-configured to use your data.

Step 5

Trial & deploy apps

Once an app is in your Work Space, you can trial it to ensure it is suited to your needs. If it is, you can use the app via a secure web portal, controlling who from your institution has access.

Step 5

Integrate & benchmark

Now you have a single view of your risk and control data – which is more consistent thanks to iDP's tools – you can more easily achieve internal and external benchmarking, as well as integrate apps to deliver your risk management needs all in one safe place.

iDP
INNOVATION
DATA PLATFORM

A next generation platform for ORX to launch high value risk applications

For more information about iDP, contact:

Mark Cooke

mark.cooke@orx.org

Simon Wills

simon.wills@orx.org

O.R.X