Deloitte



Simplifying risk technology for deeper insights and lower cost Risk and regulatory data and technology insights





In this next article in our series of new insights on innovation in risk and regulatory data and technology, we examine how reshaping of risk technology could yield significantly better risk effectiveness, cost and flexibility for Australian financial institutions (FSIs).

Why the focus on Risk Technology?

Better use of technology to support Risk Functions is a fundamental enabler of risk effectiveness outcomes. Organisations need to look for ways to use technology to drive better value through simplification opportunities as well as increase in capability. Specifically, in **Financial Risk –** look to deliver significantly faster time to decision, increased approval rates through advanced AI models and reduced banker effort. In **Non-Financial Risk –** better understanding and integration of obligations and a shift from a manual controls' environment to a continuous and proactive data-driven, digitised approach. And finally, in **Modelling and Reporting –** enable aggregation of results for group-wide reporting, enable better and more timely business decisions. Better and more streamlined data use as well as moving to a service-oriented operating model are key enablers in Risk.

Significant opportunities exist to reduce operating costs, simplify and increase flexibility and speed in risk technology

What are the top three ways to use technology and improve effectiveness in risk management?

1

Cloud-adoption to remove layers of complexity and organic growth

Deciding to move to cloud can be daunting for risk leaders given the normally risk adverse nature of the business. However, many of the technologies underpinning cloud computing have been around for decades and have been proven to be extremely reliable. In addition, even the Australian regulators, with APRA at the forefront, encourage organisations to innovate around their technology. Yes, this must be done in a measured way, but using cloud is a well understood undertaking. Moving an application portfolio to cloud involves deciding which applications can be simply rehosted or re-platformed and which need deeper work by re-architecting them or converting them to softwareas-a-service models. By taking this measured approach, organisations can take most of the risk out of transformation and do so incrementally to minimise disruption.

2

Using cloud, automation and data-mesh for better speed and effectiveness

Modernising use of data and technology in Risk, specifically utilising data-mesh, cloud and automation approaches produces higher responsiveness and lower cost to serve – organisations that face challenges scaling data and technology reliably is where adopting data-mesh and the cloud makes most sense. With data-mesh, agility, lower cost and higher speed are achieved where domains within the organisation take on ownership of their data and build and publish their data products independently. The domains can take advantage of a common data and technology foundations built in cloud to remove the need to create their own infrastructure. This approach not only enables faster data availability, but also higher quality and speed to serve. The shift to cloud is also key to move away from an "asset" or "platform" language and instead implement more granular "services" where there is only one provider of each service. Implementing this model removes duplication, decreasing the technology footprint and operating costs.

3

Exposing Risk services for higher agility, control and business configuration

Moving to a service-oriented model across risk would increase agility and control the impact of change during faster implementation cycles - moving to a services-oriented model is about unbundling applications to expose key services that can be consumed independently and can satisfy much more granular interactions. For instance, individual services can fulfill specific steps within a credit decisioning workflow, thus adding a degree of automation in an otherwise highly manual process. The more services are implemented and exposed, the more automation is possible and the lower the overall cost to serve. Utilising the cloud for deploying services offers a significant benefit in being able to scale and manage services individually. What this means is that organisations no longer need to bring large sections of their technology landscape down for maintenance or upgrades. Instead, they can continuously work and deploy services without affecting other parts of their operating environment.

While the business and customer environment has changed it also became more complex, more volatile and more open. By more open, we mean that customers can transact with their banking from anywhere, anytime and through many more channels than has previously been possible. This flexibility has introduced the need for greater security and more encompassing monitoring to manage credit risk, fraud, sanctions and AML/CTF, market risk, operational risk as well as privacy and cyber issues.

This increase in activity is a two-edged sword. On the one hand, organisations benefit from more opportunity to capture new business. On the other, the supporting risk infrastructure has struggled to keep pace. Most banks suffer from overly complex risk architecture that drives slow customer response times, duplicate data siloes, complex and mostly static reporting and long lead times to implement changes.

Banks have been making new investments into their risk functions but in many cases, these investments have been bespoke and contribute to more complexity rather than holistic simplification of the risk architecture.

How can banks direct regulatory spend into achieving more strategic outcomes?

We would argue that bespoke approaches are unsustainable and would not deliver on key objectives for risk leaders, e.g., improving availability and resilience of systems and services, reduction of risk through new frameworks, practices and systems, improving delivery predictability, simplification and cloud-adoption and greater use of data through more integrated approaches.

We would also argue that a new perspective is needed for risk functions where a focus on bringing fast, clean and high-quality data into risk and shifting to a services-oriented operating model drives far better customer decisioning. This would provide an up-to-date window into business performance and regulatory compliance.

Investing in automation, cloud-adoption and taking advantage of the data that organisations already own while also looking at simplification and cost take-out opportunities would result in a far more sustainable approach.

Cloud-adoption to remove layers of complexity and organic growth



In general, most banks have an operationally stable and functionally rich Risk portfolio. The richness reflects both increasing maturity of the Risk functions, and the ongoing series of regulatory investments in IFRS/9, Basel/2/3, AML/CTF, BCBS239 and APS220,221 & 113.

These investments have driven automation of activities that were previously manual or not undertaken. However, given the constant change and in many cases bespoke investment approach, there remain several gaps. Specifically:

- Creating consistent results and providing an integrated view across Risk portfolios and Basel III management information.
- Enhancing fraud case management and real-time fraud detection.
- Harmonising of processes across Risk and Finance.
- Providing a level of automation of risk processes.
- Functional coverage for stress testing, model/simulation and back-testing functionality.
- Alignment and consistency of applications across Risk and Finance.
- Strength and extent across the organisation of data governance and maintenance.
- Presence and consistency of golden data sources and risk-data.
- Real-time data capabilities.
- Meeting the regulatory reporting requirements for any future enhancements in time.
- Replacement of the existing risk infrastructure for calculation, data sourcing and reporting.

We acknowledge that several banks have recently embarked on or delivered significant operational risk transformations, and this has led to digitisation of large parts of the Risk landscape. However, the growth in the past few years has led to an "urban sprawl" of siloed systems for each specialty Risk function (e.g., Credit, IRRBB etc.). It comprises distinct "risk engines", often duplicated functionality, overlapping systems, sourcing data from multiple sources and a lack of integration with existing business systems, e.g., many Key Result Indicators used in the monitoring of Risk Management Performance are manually tracked and calculated and therefore prone to inconsistency or inaccuracy. This partly reflects the evolution of risk disciplines over the last 5+ years, pre-existing infrastructure, and the "specialist" approach of IT vendors as well as the evolution of our technology architecture thinking. Data sourcing is also exacerbated by overly complex business structures, product centric systems and use of spreadsheets that each drive the Group-wide view necessary for risk management.

There are several consequences of this environment. Specifically:

- Challenges in aggregation across the whole organisation, manual business processes, different IT architectures and systems and data sources.
- High cost of change due to the multiple systems and convoluted data flows.
- Increased operating cost due to multiple licenses and duplicate infrastructures.
- No single source of truth leading to extensive manual effort to identify/validate management information.
- Continuation of bespoke IT solutions to "patch" any issues as they are discovered.
- Difficulty in modernising Risk holistically simply because it's seen as too difficult and risky.

The key question here is, can organisations ignore the need to change and transform holistically for much longer?

Finally, it's worth noting that the base capabilities of each Risk area meet the specific current needs today, with a few exceptions. Most Risk functions have the right foundations, and their activities are focused on extensions rather that replacements. However, reflecting the journey to date, many systems are aging, and we are seeing the first evidence of this becoming a driver of change.

Across Risk domains, the major point of integration is at the source data level and via specifically developed environments predominantly contained to a Risk domain. This provides significant challenges to the reporting on risk exposures holistically. The provision of data is especially complex and found to have significant duplication. This has a direct impact on the cost and time required to facilitate change.

Modernising use of data and technology in Risk to tackle the challenges



We find that organisations that struggle with finding the right data or struggle with obtaining a holistic view of their portfolios tend to benefit the most from an integrated architecture and transformation.

In our experience, there are multiple dimensions to technology and data modernisation.

- Modernising the data architecture by re-architecting the data ingestion, storage, enrichment and data serving capabilities. This usually means transformation of the various data pipelines, which are usually separate, into a single metadatadriven pipeline to satisfy all primary ingestion patterns.
- Looking at moving application workloads into the cloud. This usually involves deciding on which applications can be re-platformed, re-hosted or where a more encompassing rearchitecture is required to create benefits
- 3. Lastly, the pathway to modern data and technology architecture cannot be done with a big-bang approach. Instead, a more thoughtful and incremental approach is needed where the architecture is designed with a 2–3-year transition in mind and one which can generate benefits from each incremental step on the roadmap.

From a pure data perspective, Deloitte suggests that by creating a Risk Data Hub eco-system with a focus on data-mesh and data products (see figure 1 below), organisations can benefit from a modern data architecture by:

- Having improved access to and understanding of data.
- Having trusted and reliable information, managed through data quality and governance.
- Having better compliance with regulatory requirements.
- Reduced cost of finding and rectifying remediation issues.
- Risk effort focused on creating insights over managing data accuracy.
- Having much higher self-service for business users instead of relying on IT projects.
- Increasing self-serve capabilities.
- Enabling a heterogenous data environment that can be easily added to or updated without the need for major delivery disruptions.
- Compartmentilising change activities to deliver projects faster and with less risk.

It is worth explaining that the premise of data-mesh architecture needs more than just a focus on the technology and data-product creation level. Some industry professionals believe that data-mesh is just another substitute for data virtualisation. It is not. On top of the usual technical and data related capabilities, data-mesh requires organisations to:

- Create a distributed data culture where domains can operate independently on top of a common data infrastructure to create and publish data-products.
- Creating an appropriate model for accountability and data governance.

This approach looks at creating data products that are fit for purpose for specific use cases. For example, one data for serving Credit Risk needs, another for Financial Crime investigations and a third one for managing operational risk reporting and so on. Ultimately, it's the speed of serving decision-ready data that makes the difference. This approach is very much possible using object-based storage and modern technologies such as data-mesh to serve data in a variety of ways without having to worry about creation of bespoke warehouses for each scenario. Deloitte has created a blueprint for Risk Data Architecture (Figure 1 below) that highlights the kinds of requirements and features we look for.

We believe that consolidating capabilities along common themes, such as ingestion, enrichment and storage, data-mesh and dataproduct, reporting and analytics would provide key advantages. Consolidation does not mean loss of flexibility or speed. In fact, another key factor in our approach is the increase of self-service for Risk business professionals where the data as well as tooling becomes more accessible.

Figure 1: Deloitte Risk Data Architecture and Requirements



7

Data

Simplified & Flexible

- Shift to event/stream based source data ingestion reducing time of transaction data availability to close to transaction-time
- Central Integrated Risk Data Hub framework for increased flexibility
- Automated data preparation supporting downstream use
- Eliminate complexity & proliferation
- Dedicated consumption channels for Reporting, Analytics/Modelling and Decisioning

Well Managed

- Data Models tailored for key use cases and enforced governance
- Risk specific data models and definition of Risk entities
- Consistent provision of high quality, timely and trusted/accurate data
- Improved access to, and understanding of data
- Fully managed and governed platform

Risk Reporting

Efficient

- High level of automation
- Efficiency and industrialisation of reporting
- Fresh, Self-Serve Reporting Dashboards
- Risk effort focused on creating insights over managing data accuracy

Data Governance

Governed

- Data Catalogue driven by business metadata, lineage and data governance requirements to explain how each report is provisioned
- Fully integrated with data pipelines
- Capture of all metadata and transformations for a full picture of data lineage
- Self-serve

Risk Analytics

Simplified and governed

- Generate rapid insights, model, features and scenario analysis
- Single delivery base and analytical platform
- Full managed and governed platform

Flexible

- Leverage MLOps, DataOps and DevOps capabilities for quick deployment of productionised models and automation
- Ability to share insights, models and features to a wider audience
- Self-Serve

Innovation and time to market

- Ability to leverage the full capability of analytics, AI and ML
- Simplified landscape leveraging world class innovative technologies
- Drastically reduced deployment time into Production through MLOps, DataOps and DevOps.

Specifically, capabilities such as the following are incredibly important:

- Encryption
- Data product versioning & schema
- Data product discovery, catalogue registration and publishing
- Data governance & lineage
- Product monitoring
- Management of product quality metrics and usage

From a cloud-adoption perspective, we would look to taking advantage of cloud services to primarily achieve four things:

- 1. Establish a cloud-based data eco-system.
- 2. Establish a cloud-based self-serve reporting capability.
- 3. Establish cloud-based analytics.
- 4. Selectively cloud-enable Risk applications either via a replatform, re-host, re-architect path or convert to a SaaS model.

This tailored approach provides one of the best balances between flexibility, outcomes that can be achieved, lowest risk and optimal costs to implement the changes.

For example, at one large financial institution in the USA, Deloitte helped to deliver a significant digital transformation to migrate c. 2000 applications to AWS. Some of the improvements included better process and automation of machine learning model updates from months of elapsed time to just days, new virtual assistant service for fraud alerts, spend tracking for customers and selected loan pre-qualification service for customers.

In another example, Deloitte helped a large banking institution to consolidate their finance systems into one platform. This reduced infrastructure costs by 50% and removed manual compliance processes, rationalised profitability reporting from 600 to 100 reports, reduced month end processes by 25%, increased application speed by 33% and supported BCBS239 reporting use cases.

3 Re-defining Risk into a services-oriented model for higher agility, control and configuration



Moving to a service-based model requires a shift from "assets" or "platforms" where Risk capabilities are provided to consumers in a monolithic, or coarse-grained, manner, and re-define the Risk business as a set of business services. Once the business services are defined, they can then be linked to appropriate application services and subsequently to infrastructure services.

The whole point of moving to service-orientation is that organisations gain the ability to manage and operate the business functions in a much more flexible and visible manner. This ultimately results in much more control over how to execute each individual service, how to scale them, whether to automate them, how to monitor them etc. This approach offers one of the best approaches in business control and configurability and creates the ability for businesses to alter how they operate rapidly to match external demands.

For example, let's consider a simple reporting system. In a traditional architecture a reporting system would typically consist of a large data ETL (Extract, Transform, Load) platform, a large database platform (a data warehouse) and a large reporting platform where all the reports were coded and available to users. If one wanted to cloud-enable this reporting system, then the whole thing would need to be re-platformed in the cloud, causing potentially a lot of disruption while not really generating any significant benefits. Other than a change in infrastructure costs. On the other hand, in a service-oriented world, you could only take a small sub-section of the reports you're interested in, build and deploy only the needed data ingestion services, provision storage and then publish a live dashboard to users. Once this was done, a thin steel-thread for a new cloud-based reporting service is

> established, and you can iterate again later to do another slice of reports. Cloud offers many pre-built, pretested and production ready services that users can employ to compose their solutions. It's like working with highly configurable, scalable and secure Lego to create greater value for your business and it doesn't take months or years to do. Instead, technology solution can now be built in weeks or days.

> > One of the clear advantages with this approach is that organisation no longer need to purchase and pre-provision large amounts of infrastructure. For example, purchasing physical enterprise servers would require a multi-

million-dollar investment, plus time to host it in your data centre plus power costs to run it. Instead of doing that, cloud or data engineers can simply configure their requirements in the cloud console and provision the required resources within minutes and only be charged for the capacity they use. Gone is the need for lengthy contract negotiations and wait times until servers are shipped, installed and provisioned for use.



Roadmap for Risk Technology

Overall, we believe there are five factors that typically drive higher costs and pain points within Risk.

One, business users often can't find what they need. The complexity of the landscape means that it is often easier to respond to change with a tactical solution rather than a more strategic approach. Two, business users can't do what they want - the rate of change of business demand cannot be matched by the current landscape leading to unfulfilled demand or additional tactical solutions. Three, solutions can't adapt to change - it is problematic to easily determine which systems may have the data needed to fulfil a given business need.



Key pain points

Inadequate Data Controls for 2nd Line Systems – Users can't find or do what they need. Information is duplicated, incomplete, inconsistent, lacks standardisation and validation, and is inaccurate. Confidence in underlying data is low. Data ingestion flows into Risk via multiple and different mechanisms that need to be supported and maintained.

Inconsistent and delayed leverage of 1st Line data – Poor change agility, over reliance on either static data or significant delays to processing source system data within Risk. There is often a delay of one, two and sometimes three days between a customer transaction and this data being reflected in Risk.

Hindered by legacy technology – Non-sustainable, rigid legacy technology platforms with high running costs and unexpectedly high costs to upgrade. GRC solutions unable to support all elements of NFR (Non-Financial Risk) and drive required insight. Batch ingestion pipelines requiring careful maintenance often causing unintended issues in downstream dependencies.

Poor data insight and reporting – Lack of an integrated view of performance and Risk. Highly manual reporting process, retelling what is broadly already known. Selection and calibration of Key Risk Indicators (KRIs) not data driven. Static reporting and insights cause highly episodic view of Risk, portfolio performance and capital provisions required.

Poor data governance and controls overall – Siloed data sets that are managed in bespoke repositories without a holistic view of data lineage, metadata and data catalogues. This often leads to creation of "data squads" in many places to manually piece data controls together. Poor or at least not sustainable compliance to regulations such as BCBS239 and CPG235.

Four, non-sustainable platforms - end of life platforms, capacity and performance issues, mixed and aging technologies.

And lastly, five, diluted IP creates a knowledge gap - unsupported systems for which there is limited documentation or knowledge create lock-in where it is extremely difficult to replace or modernise those systems.

These five factors translate into 5 key pain points for Risk Technology.



What you can do

- Create an enterprise & data architecture
- Design a roadmap
- Establish data governance and controls
- Simplify, centralise & digitise
- Adopt cloud architecture
- Shift to event-based data ingestion
- Adopt cloud architecture
- Simplify data pipelines
- Create data products and shift to more selfservice
- Create an enterprise & data architecture
- Design a roadmap
- · Simplify, centralise and digitise
- Automate manual processes
- Adopt cloud architecture
- Modernise reporting from static reports to dynamic dashboards
- Create data products and increase self-service
- Adopt cloud architecture
- Create group-wide stress testing capability
- Establish a data architecture
- Create a data governance capability including people, processes and technology
- Automate data lineage gathering
- Establish a data catalogue

Key use cases

In the table below, we have identified several use cases of varying levels of complexity. There is no one size fits all approach here.

Instead, we focus on engaging our clients in pro-active conversations to learn how ready each organisation is to transform and then select the right approach to help with modernisation.

	\bigcirc	
Key Use Case	From	То
Data ingestion – Ability to bring fast, clean and high-quality data into Risk within minutes of it being created by customer behaviour	 Batch driven. Data delayed by 2-3 days 	• Event driven. Data available in minutes
	Multiple, hard coded pipelines	Single pipeline
	Multiple ingestion technologies	Metadata driven
	No or little metadata	Single technology stack
Integrated/Live Reporting – Ability to utilise live, dynamic reporting dashboards for increased flexibility, reporting and analysis of insights – e.g., home loan delinquency reporting	Static reports	• Fewer, live dashboards in cloud
	• Little or lack of group wide view	 Aggregated views across group or divisions
	• 1000s of reports that are hard to	
	interpret	Fresh data within minutes
	Data often delayed and not fresh	Modern reporting technology
Analytics – Ability to design, build, execute and monitor risk analytics at scale – e.g., LGD capital calculations	Traditional/monolithic platforms	• Executed in cloud
	Bespoke, small & slow data	Open-source frameworks for analytics
	Manual data preparation	
	 Manual model lifecycle and 	Super large data sets
	execution	• Data within minutes of creation
	Hard to monitor	 Robust model lifecycle with KPI monitoring and feedback loop
Enterprise-wide integration for Risk – Ability to have Risk measures and results embedded in key enterprise-wide processes to drive performance	Bespoke and manual	Integrated Performance management
	Multiple disconnected models	
	 Little ability to do integrated stress testing Little ability to run different scenarios Integrated stress testing Scenario analysis and risk profiling Integrated view of customer 	 Integrated stress testing
		 Scenario analysis and risk profiling
		Integrated view of customer
	 Little or no integration between Risk, Finance, Treasury and Customer 	
	Fragmented customer view	

How we can help

In the current climate, organisations need to be smarter in how they design their roadmaps. It is prudent to spend the time upfront on designing the right architecture, operating models and a holistic roadmap which can then be used to prioritise new initiatives. Incremental delivery and a steady progression to the desired goals is far more doable than a traditional, big-bang transformation.

We have the experience and the accelerators to support our clients through a range of delivery models.



- Integrated risk and regulatory reporting operating model design
- Data risk management framework refresh and maturity assessment
- Data capability assessment
- Risk technology simplification assessment



- Regulatory reporting readiness and remediation
- Re-imagined Reporting implementation
- Risk and regulatory data and technology architecture enablement
- Data risk management capability uplift
- Risk and compliance automation
- Risk analytics in cloud enablement
- Data governance and controls digitisation





Scaled delivery model

- Data risk management monitoring and oversight managed service
- Risk and regulatory reporting as a service
- Financial model management



Contacts



Simon Crisp Partner, Data Risk & Technology simoncrisp@deloitte.com.au +61 421 788 737



Vicky Poon Director, Data Risk & Technology vipoon@deloitte.com.au +61 434 602 006



Mike Szalinski Principal, Data Risk & Technology mszalinski@deloitte.com.au +61 407 625 875



Chris Topple Principal, Data Risk and Technology ctopple@deloitte.com.au +61 412 125 031



About Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu.

As one of Australia's leading professional firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2022 Deloitte Touche Tohmatsu.

Designed by CoRe Creative Services. RITM1029198.