

IFRS 17: Managing data to optimise cloud strategy

Contents

- 3 Building a data management framework
- 5 Data governance
- 7 Data usage and quality
- 9 Data management
- 11 IT architecture and alignment
- 13 Reason to push forward
- 14 Contacts

Introduction

Over the past five years, as insurers have prepared for the International Financial Reporting Standard issued in May 2017 (IFRS 17), which will dramatically affect finance — including underwriting pricing, and sales and marketing — they’ve steadily adopted cloud technologies and ramped up their investment in data engineering capabilities. More recently, to further prepare themselves for the new regulations and to modernise, insurers have also begun changing how they deploy these data applications and solutions. Instead of maintaining the installment of solutions onsite, insurers are choosing to concentrate on their core business and are beginning to adopt infrastructure provided by cloud services and software as a service.

This strategic redesign is a major undertaking, but insurers are realising they need to accelerate their transition. Making these changes will bring down expenses in the long term, and improve flexibility and focus on value-generated activities. Installing modern analytics will also enable better decision making and help insurers differentiate themselves from competitors.

This is crucial not just for delivering on IFRS 17, but for dealing with business-critical scenarios such as COVID-19 and the demands of the future in general. All these efforts require having the right data management framework in place, so building this framework should be insurers’ top priority right now.

Building a data management framework

Data is one of an organisation's most valuable assets. But the variety of technology platforms and applications that firms use to manage the data can make optimising it difficult. Disparate systems generate huge quantities of information, but in a siloed way that limits access. Because of these challenges, attempts to adopt cloud or multi-cloud strategies — such as moving all enterprise data into a cloud-hosted 'data lake,' or company-wide repository — are rarely successful.

To overcome these challenges, an organisation needs to build a data management framework that dictates enterprise-wide rules for how data is collected, stored, transformed, distributed and consumed. Consistency in how data is handled will help a company access it and use it to ensure regulatory compliance and develop business insights. A framework should include rules governing structured data formats, such as databases, and

unstructured and semi-structured formats. A framework also should describe how data connects with business processes to yield actionable information.

Because insurers vary widely in their go-to-market strategies, the complexity of their legacy systems and their IT capabilities, it's important that each company focuses on the specific issues that might hamper its own progress. There's no magic one-size-



fits-all solution. But every company's data and cloud strategy must address four core framework elements: data governance, data usage and quality, data management, and IT architecture and alignment (see exhibit, next page).

Exhibit

Data management framework

At PwC, we have a proven data management framework that helps to assess your business’s level of maturity and develop and build out your cloud strategy and enterprise-wide rules for how data should be collected, stored, transformed, distributed and consumed.

1 Data governance

Ownership and control

Security and data protection

System of record

Standards and policies

Processes and procedures

2 Data usage and quality

Internal and external reporting

Analytics and predictive modelling

Data visualization, querying and mining

Data quality standards

Usage controls

Profiling/analysis

Cleansing

Enhancements and enrichment

3 Data management

Metadata standards

Data movements

Enterprise service

Business rules

Master data management

Cloud architecture

Ontologies and taxonomies

Data dictionary and lineage

Design patterns and modelling

Big tables and unstructured data

Containerisation

Application service models

Infrastructure as a service (IaaS)

Platform as a service (PaaS)

Software as a service (SaaS)

4 IT architecture and alignment

Cloud deployment models

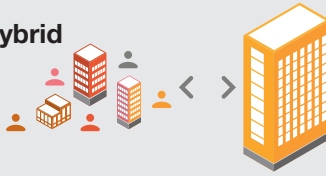
Public



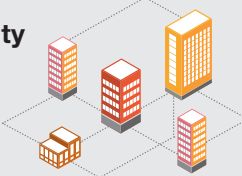
Private



Hybrid



Community





Data governance

A data governance plan puts the right processes and procedures in place to create, move, classify, use, store, retain and dispose of data. By improving data access and usage, governance empowers employees to ask more questions, get better answers quickly and innovate. And by moving data efficiently — i.e., moving only the data that's needed when it's needed — companies can save time and money.

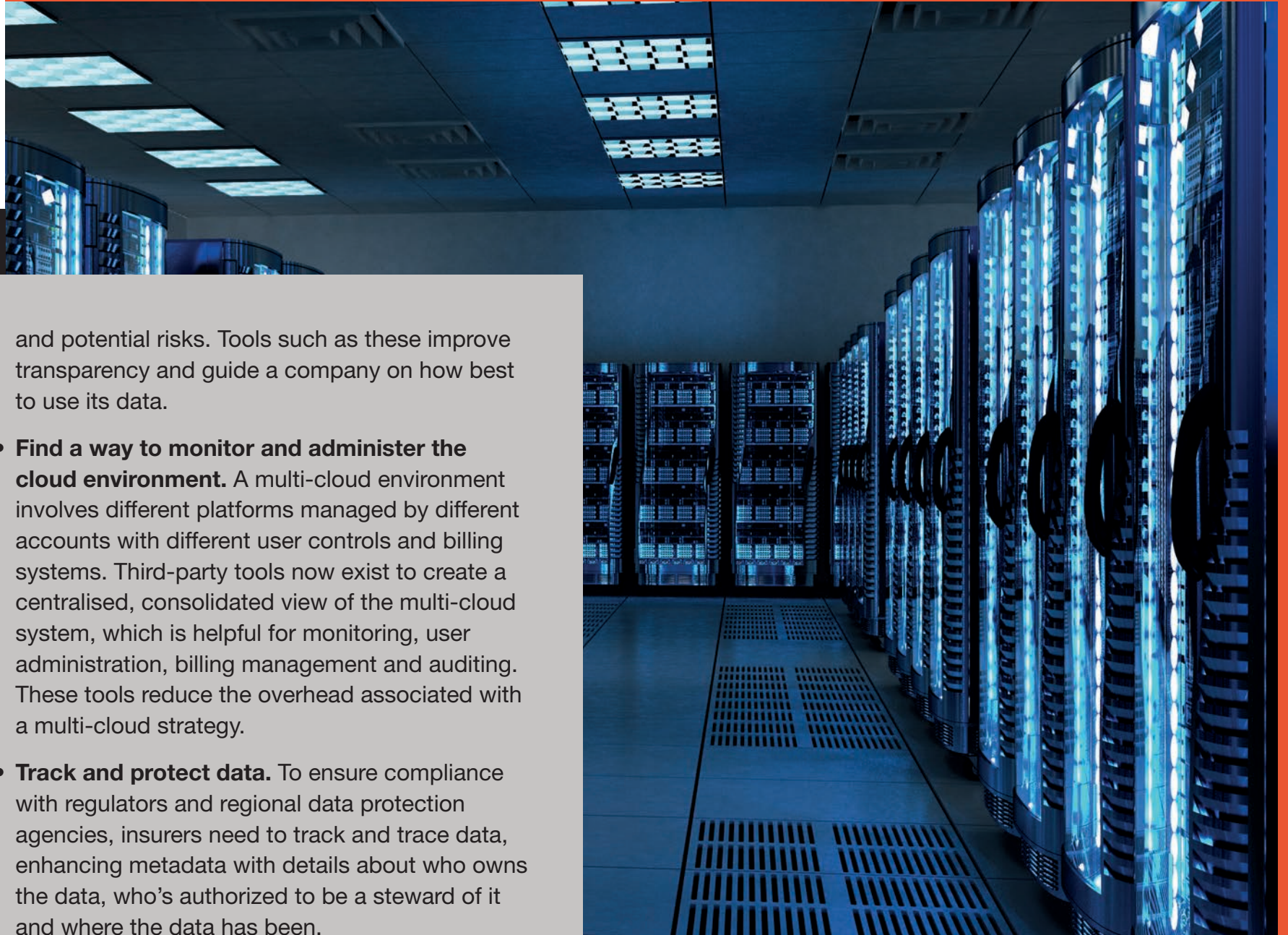
Companies can build the apps to govern data themselves, in-house, or they can use public cloud resources, including multi-cloud environments. But to make updates easier and avoid having to deal with underlying data, it's best for governance to be incorporated from the start, not after applications have been designed and implemented.

A senior leader such as chief data officer or business sponsor should be put in charge of defining all aspects of data governance, taking into account the needs of the business and the prevailing externally

imposed rules and regulations, and pulling in all of the right people to help. Rules around IFRS 17, for example, are intended to align insurance company reporting frameworks around the globe. Under the standards, insurance contract liabilities will be calculated as the present value of future insurance cash flows, with a provision for risk. Meanwhile, the general data protection regulation (GDPR) sets guidelines for collecting and processing European Union residents' personal information and imposes tough fines for violations.

Key actions to take involving data governance:

- **Establish a unified foundation for data governance and storage.** The enterprise-wide rules a company establishes around data and the environment it chooses for storing data — such as a data lake or data hub — can be referred to as the company's data architecture or data fabric. This is the foundation for data governance. As we've pointed out, when technologies and services run off of a unified architecture, it's easier and faster for a company to get a dashboard view of a lot of data assets, create central controls for the data, and consolidate, classify and curate the data. A unified data fabric also creates a strong foundation for progressive initiatives, such as implementing a global security framework.
- **Create a system for organising and finding data.** Scalable cloud tools support fast, detailed data profiling. These tools feed search metadata into a company's data catalogues and parse all content, determining its availability, usefulness and potential risks. Tools such as these improve transparency and guide a company on how best to use its data.
- **Find a way to monitor and administer the cloud environment.** A multi-cloud environment involves different platforms managed by different accounts with different user controls and billing systems. Third-party tools now exist to create a centralised, consolidated view of the multi-cloud system, which is helpful for monitoring, user administration, billing management and auditing. These tools reduce the overhead associated with a multi-cloud strategy.
- **Track and protect data.** To ensure compliance with regulators and regional data protection agencies, insurers need to track and trace data, enhancing metadata with details about who owns the data, who's authorized to be a steward of it and where the data has been.



Data usage and quality

Data never stops. It flows in ever more varied formats and is increasingly susceptible to delivery and quality issues. Organisations must be vigilant to ensure they stay in compliance with IFRS 17 and other regulations, constantly examining the completeness, validity, consistency, timeliness and accuracy of enterprise data as it moves from source to reporting and analytics.

Data enhancement initiatives, when data was not collected an optimal way to begin with, are also key to creating more informationally rich, high-quality data. Poor data quality taints new initiatives and kills attempts to use machine learning and AI for regulatory purposes and business insights.

So, insurers should consider very carefully which of the cloud tools and services they use. The cloud is a great enabler, but with its

ever-changing capabilities and features, it can also be a costly distraction. It's easy to use a service unnecessarily — for instance, to perform a data transfer — and run up a high bill. Avoid trying out all the new data processing tools. Remain focused on regulatory and business needs, and build accordingly. Ultimately, this will keep the organisation agile.



Key actions to take involving data usage and quality:

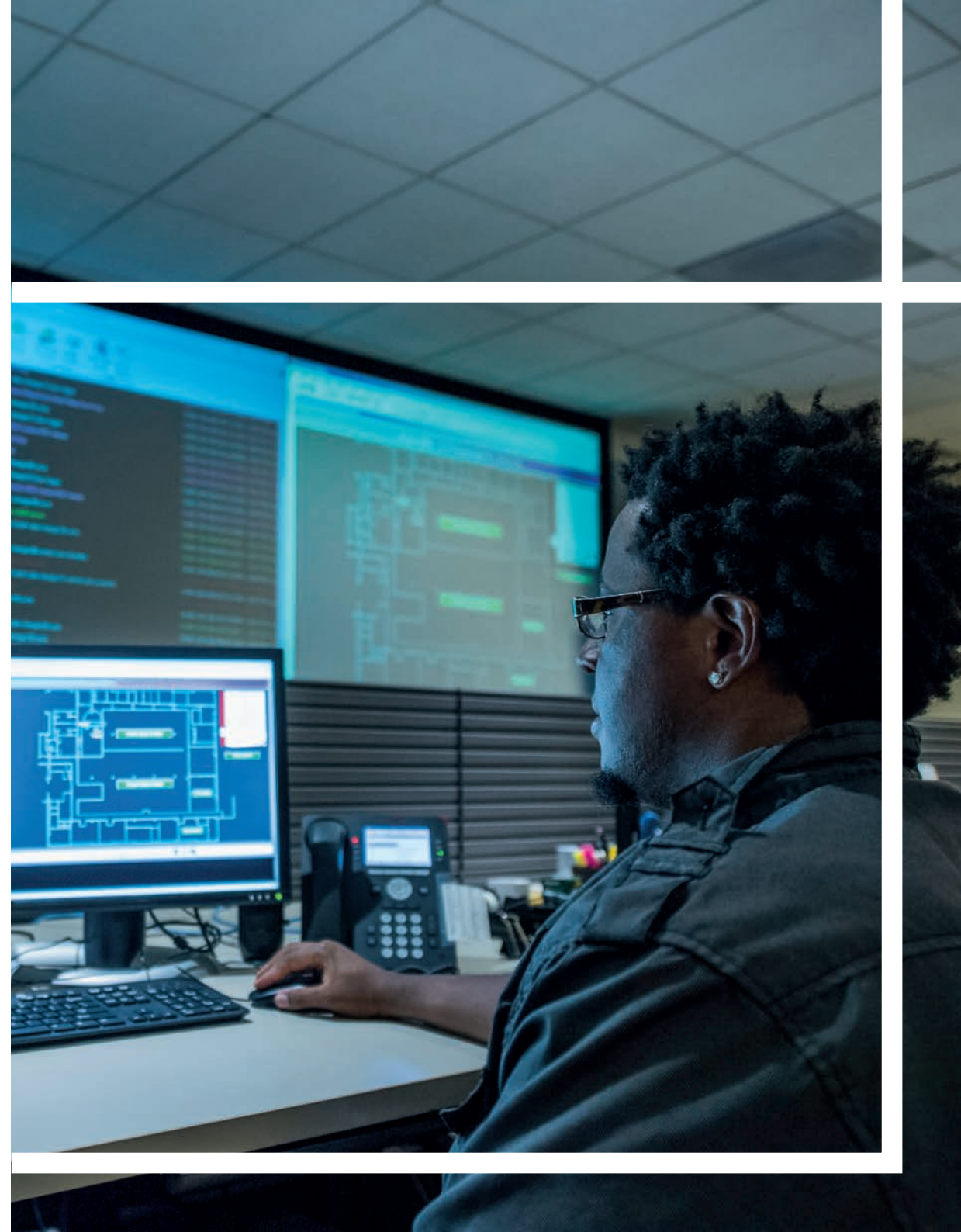
- **Automate data processing.** Tools exist that can source, cleanse, prepare and provision data automatically to help people across business and analytics functions use the data in their day-to-day work.
- **Assess and optimise data flows.** Use dynamic pipeline microservices, which enable your data architecture to be scaled up or down quickly, to manage data flows from different sources or between different services. Use technology to keep data moving, virtually, to save on the effort and costs of storing it.
- **Minimise cloud transfers.** To avoid charges incurred when data is transferred to and from the cloud, keep most business data in the cloud at all times. And because moving data between cloud providers also incurs charges, if your data architecture is set up to be multi-cloud, it's economical to keep data in the cloud where most processing will occur.
- **Use packaged data services to achieve these goals.** Cloud providers offer packaged services that can handle big data by offering low-cost, near-infinite storage and that can manage data flows, data processing and discrete data functions — for example, converting audio recordings to text or vice versa. These packaged services allow solution architects to use a building-block approach for multi-cloud adoption.
- **Report quality issues immediately.** Whenever a data problem is discovered, the insurer should notify the data supplier immediately to address the problem at the source, and should follow up to make sure the problem is resolved. A word of caution here. It's possible to fix these problems on your own, fast and on the fly, with today's cloud tools, but it's also important to take the time to fix the problem at the source. Otherwise, over time, these problems will repeat and add up, and the organisation will lose flexibility.
- **Adopt agile working policies.** The cloud's flexible characteristics align well with agile working. In most cases, organisations should take advantage of other companies' infrastructure-as-code offerings to launch services and resources quickly and easily as needed. The cloud also offers great flexibility and lower costs for testing new applications and evaluating new services.

Data management

Managing the volume of data that the cloud can hold with traditional IT is virtually impossible because traditional IT simply isn't set up to handle big data in a cost-effective way that is scalable, flexible and quick. Moreover, data management invariably involves many dependencies, some of which are at odds with one another.

Employees need as much access as possible, but not too much. They need freedom to use the data as they see fit for business purposes, but there must be proper access and security controls over exactly who can do what with the data. And regulatory changes such as IFRS 17 demand deeper data access and the application of new technical and business rules.

There's also the issue of security. Poor data management leads to security breaches. Although these have been less in the public eye of late, several damaging exposures occurred in 2018 and 2019. Even with the new cloud-based data security tools, managing and maintaining encryption across security domains requires enormous care.



Key actions to take involving data management:

- **Centralise data governance across silos.** Use governance catalogues to consistently enforce policies on data access and the data life cycle.
- **Optimise access to data.** Install identity and access management software across multiple cloud platforms by integrating with existing single sign-on or other computer-network authentication protocols. Broaden single sign-on access to data and applications.
- **Implement strong data security.** Configure or design service access points to share data and APIs and vice versa across cloud platforms. Make sure to use encryption, such as encryption key management and encryption key rotation, to keep data safe while accessing and transferring it.
- **Curate data.** Maintain a single source of input data that is catalogued — for example, from a data lake — and when retrieving it, automate data access to make consuming it easier and more scalable.
- **Enforce data quality standards.** Since data quality requirements and expectations vary across data sets — for example, the expectation for social media data quality is lower than for financial transaction data — companies should manage their standards by documenting data by sources and use cases.

IT architecture and alignment

Companies that move data to the cloud must avoid the temptation to use the same traditional approaches and principles for IT that they've used in the past. Doing this instead of building a re-engineered IT capability in-house is a shortcut that never pays off. Savings will disappoint, integrations will be difficult, and overall performance will be poor. Instead, insurers need to commit to re-engineering the architecture to accommodate new ways of managing the enterprise data estate systems in the cloud.

Redesigning your IT architecture to accommodate the cloud environment isn't simple, but it comes with significant long-term benefits. These include eliminating the need for and operational cost of big computer infrastructures; reducing the need for technical research and development and IT tactical deployments, because the cloud providers focus on these; and enabling more agile regulatory compliance, the ability to focus efforts on business innovation, and more rapid development. Cloud computing is scalable and automatically adjusts day-

to-day to match the peaks and troughs of business. This ability to right-size the platform avoids the historic, money-wasting problem of over-engineering platforms to accommodate infrequent workload peaks.

All these benefits of re-engineering the IT architecture improve lifetime value and return on investment. They also mitigate obsolescence concerns, because cloud providers are focused on progress, innovating and creating new services.



Key actions to take involving IT architecture and alignment:

- **Accelerate adoption of new technologies.** Just as the cloud's flexibility makes it easier to be agile and test new insurance apps and services, cloud computing also makes it much easier to test and quickly adopt new IT technologies, methods and approaches with no locked-in commitment.
- **Leverage software as a service.** Cloud vendors offer fully hosted, secure, resilient, mainstream IT applications, with extensive integrations and user interfaces. Businesses just need to configure settings and upload data.
- **Use pre-packaged technology platforms.** There's no need to buy and deploy large, expensive computing clusters or hire teams of data engineers to use the applications. Instead, insurers can take advantage of ready-to-use implementations of big data technology platforms.
- **Embed machine learning and AI for business insights.** Software models using machine learning and AI can dynamically analyse the continuous data feeds to identify consumer behaviours, associations and causations. By spotting subtle changes in the data flow, the models can give insurers new business insights.
- **Pay by use.** Paying to run applications only when needed lowers costs. For this 'on-call' model, it's best to use 'containers' — which encapsulate the application, its APIs and its dependencies — to activate modular, stateless computing to do a burst of work quickly.
- **Use flexible microservices across clouds.** Computing in bursts is not just cost-effective, it's also more efficient. Instead of large, monolithic programs continually running on servers, a microservice-based system creates a mass of functional processes that run in bursts on small chunks of data. These bursts are triggered by events or other processes. Microservices are easily distributed across multiple cloud providers using APIs.

Reason to push forward

IFRS 17 requirements and the general advantages of migrating enterprise data to the cloud have been well known for years. But the COVID-19 pandemic has shown that these capabilities are an even more urgent business imperative than they already were. With a proactive and holistic data management framework and cloud strategy in place, insurers can accomplish this transition with reasonable speed and minimum disruption to achieve significant business benefits.



Contacts



Jim Bichard

Global Insurance Leader
Partner, PwC UK
+44 784 156 2560
jim.bichard@pwc.com



Alex Bertolotti

Global IFRS 17 Insurance
Leader and UK Insurance
Leader
Partner, PwC UK
+44 (0) 752 529 9263
alex.bertolotti@pwc.com



Ruud Sommerhalder

Partner, PwC Hong Kong
+852 5506 4004
ruud.s.sommerhalder@
hk.pwc.com



Alwin Sales

Partner, PwC UK
+44 207 212 2032
alwin.swales@pwc.com



Craig Skinner

Partner, PwC UK
+44 773 497 4406
craig.skinner@pwc.com



Diego Cervantes

Finance Transformation and
IFRS 17 Insurance
Director, PwC UK
+44 (0) 753 148 2175
diego.cervantes-knox@
pwc.com



Richard I. Hart

Director, PwC UK
+44 788 173 6872
richard.i.hart@pwc.com

We'd like to thank senior cloud architect and senior manager **Paul Groom**, IFRS 17 technology delivery senior manager **Rumeer Shah** and finance technology senior manager **Viswanathan Swaminathan** of PwC UK for their contributions to this report.

pwc.com/insurance



At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

© 2020 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.