BANKING ON THE CLOUD

SUPERCHARGING COLLABORATION THROUGH CLOUD TECHNOLOGY

PUBLICATION DATE
August 2018

QUINLAN &ASSOCIATES

THE AUTHORS

BENJAMIN QUINLAN
CEO & MANAGING PARTNER
BCom (Hons 1) / LLB (Hons), *Macquarie*

HUGO CHENG
CONSULTANT
BA (Hons), *Cambridge*
MSc (Distinction), *Imperial*

SPECIAL THANKS

We would like to thank our summer intern, Joshua Tjie (BBA, Global Business and Finance at The Hong Kong University of Science and Technology), for his help in the preparation of this report.

CONTENTS

EXECUTIVE SUMMARY

Since the concept of FinTech gained mainstream popularity in 2014, the financial services industry has been actively developing or acquiring technology solutions to streamline its operations and enhance its customer service offerings. However, as with any investment in technology, system resources (such as RAM or storage space) are required, giving rise to additional hardware and labour overheads. As the industry continues to grapple with ongoing cost headwinds, especially in the wake of mounting regulatory hurdles, many banks are increasingly looking to cloud technology as a more efficient and cost-effective alternative to support their digital transformation programmes.

At its core, cloud technology enables the provision of system resources through the internet. Technological infrastructure is built and maintained by a third-party service provider, with system resources provided to customers on a pay-as-you-go basis. Due to the nature of this sharing economy, the outsourcing of technological infrastructure is generally much cheaper than the onsite development, maintenance, and operation of IT infrastructure.

Recognising the numerous benefits offered by cloud technology, including scalability, reliability, and cost-efficiency, banks have been increasingly adopting cloud-based solutions in areas such as data storage, application development, client servicing, and digitalisation. In fact, we estimate the global banking industry spent USD 8.5 billion on cloud services in 2017 and forecast this number to reach ~USD 32 billion by 2023.

The ability for cloud technology to drive cost savings in the banking industry is far from trivial. We believe that migration to the cloud has the potential to reduce bank technology spend by ~20% over the next five years, underpinned by a considerable reduction in hardware expenditure, as well as spend on in-house labour. With leading global banks allocating an average of 7-9% of their costs on technology, this translates to a ~1.6% reduction in overall costs for most players by 2023.

Whilst we recognise the progress many banks have made in leveraging the cloud for such endeavours, we believe cloud technology has been heavily underutilised in driving internal collaboration.

With the rise of the internet of things ("IoT"), connectivity and collaboration between diverse individuals are widely viewed as critical for sustained growth, especially given the many benefits they can bring to corporations, such as enhanced productivity, greater flexibility, and improved innovation. However, while "teamwork" and "collaboration" are touted as key corporate values by nearly all firms in the banking industry, banks are notorious for operating their businesses in an extremely siloed manner. This is exacerbated by a corporate culture in which employees are encouraged to compete against (and outperform) each other, instead of being incentivised to work together to contribute to a better overall result for the company. As a consequence, collaboration often ends up being more of a marketing strapline than an internal reality.

In addition, we believe cloud-based collaboration applications can meaningfully enhance collaboration efforts within many institutions, enabling employees to work together in a seamless manner by providing them with a host of functionalities, including centralised communication and file sharing, real-time synchronised file-editing capabilities,

and project management tools. Beyond this, we see considerable potential for cloud-based collaboration tools to streamline work efforts with external parties, such as lawyers and consultants, on major transformation projects.

Through the adoption and effective utilisation of cloud-based collaboration applications, we believe successful players can achieve an additional 1-2% uplift in revenues (stemming from increased cross- / up-selling and better client servicing) and a further 0.5% reduction in costs (driven by process streamlining and the elimination of duplicative procedures, allowing for considerably faster rollout timelines). Taken together, we believe cloud technology and related collaboration applications have the potential to reduce the cost-to-income ratios of leading global banks from ~85% to ~82% over the next five years.

There are, of course, several key obstacles facing the banking industry when it comes to the adoption of cloud technology, particularly around data security. Regulatory demands in certain jurisdictions with respect to data privacy and security (including data onshoring requirements) have created considerable industry reluctance around the use of public clouds. This problem is particularly acute in heterogenous regulatory environments like Asia Pacific, making it more challenging to adopt cloud-based solutions while addressing a plethora of non-standardised compliance requirements from multiple local regulators. To combat this, we believe banks and cloud providers will need to work closely together in coming years to lobby regulators into becoming more supportive of the use of public cloud technology, including pushing for greater international regulatory harmonisation. However, this education process will inevitably take some time.

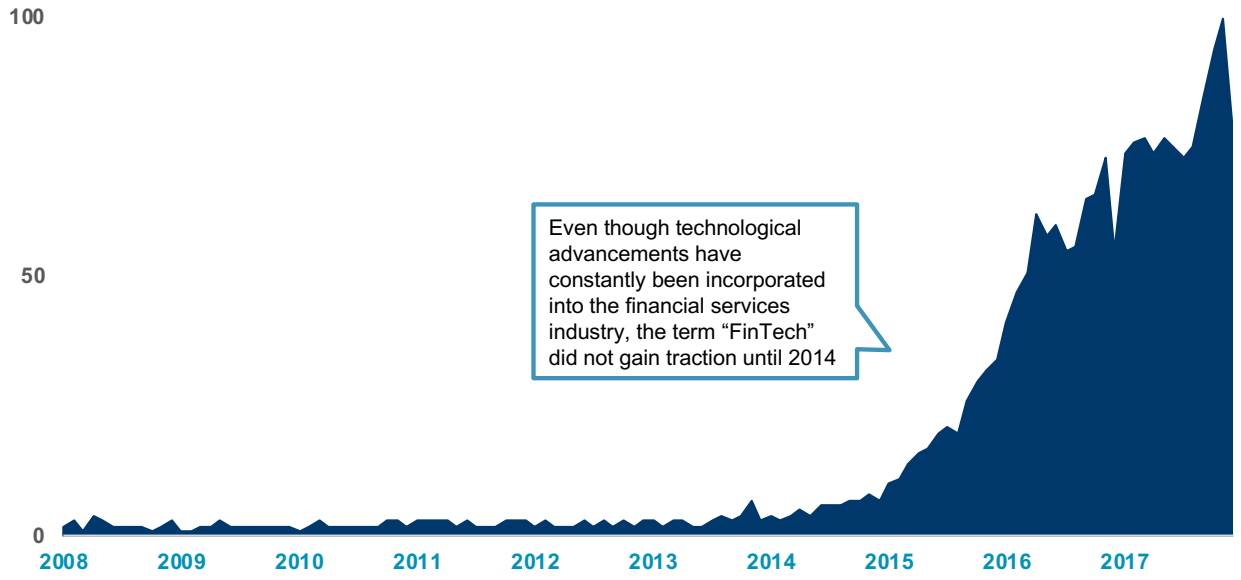
It is also important to note that technology alone will be unable to deliver our profit uplift forecasts. Cultural change is needed, which should include relevant policies and processes to support collaborative behaviour. In addition to utilising the most suitable collaboration systems and tools, banks need to design and implement appropriate incentive systems, governance structures, and communication strategies, in order to achieve a more fundamental shift in employee mindsets to fully reap the benefits of supporting technology.

Whilst we recognise that a technological overhaul and a substantial change in mindset requires significant time and upfront investment, we believe banking on the cloud is vital for firms looking to not only enhance their digital transformation programmes, but also supercharge their collaboration efforts.

SECTION 1
OUTLINE OF CLOUD TECHNOLOGY

Since financial technology ("FinTech") became a household term in 2014 (see Figure 1), the financial services industry has been actively developing or acquiring technology solutions to enhance its digital service offerings. Examples of key FinTech areas being actively pursued by banks include big data, robotic process automation, and blockchain.

FIGURE 1: GOOGLE SEARCHES FOR FINTECH (2008-17), INDEXED



Source: Google, Quinlan & Associates analysis

At its core, digital transformation allows banks to supercharge their client service proposition in a scalable fashion at a reduced cost. In our previous report, *Chasing The Tail*,[1] we argued that digitalisation can not only help banks service tail clients in a profitable manner, but also cut overall operating costs by up to 30%.

As with any investment in technology, there are two key elements that need to be considered: software and hardware.

In terms of software acquisition, banks can pursue three distinct strategies – namely, to buy (i.e. acquire a FinTech company or solution in the market), partner (i.e. work with FinTech companies to help them develop their products, typically through accelerator or incubator programmes), or build (i.e. invest in research and development to create proprietary FinTech solutions). Each avenue comes with its own unique merits and drawbacks.

[1] Quinlan & Associates, 'Chasing The Tail', June 2018, available at: https://www.quinlanandassociates.com/insights-chasing-the-tail/

The purchase of technological hardware infrastructure can be more problematic for banks, especially as the industry grapples with ongoing cost headwinds in the face of heightened regulatory scrutiny. First and foremost, the acquisition of hardware necessitates sizeable upfront investment. As banks continue to scale their digital offerings, these costs will continue to grow. Moreover, infrastructure maintenance requires banks to hire their own in-house talent. Taken together, the need for infrastructure and on-site technological expertise translates to significant costs. It is against the backdrop of such challenges that banks are increasingly turning to cloud technology as a potential solution.

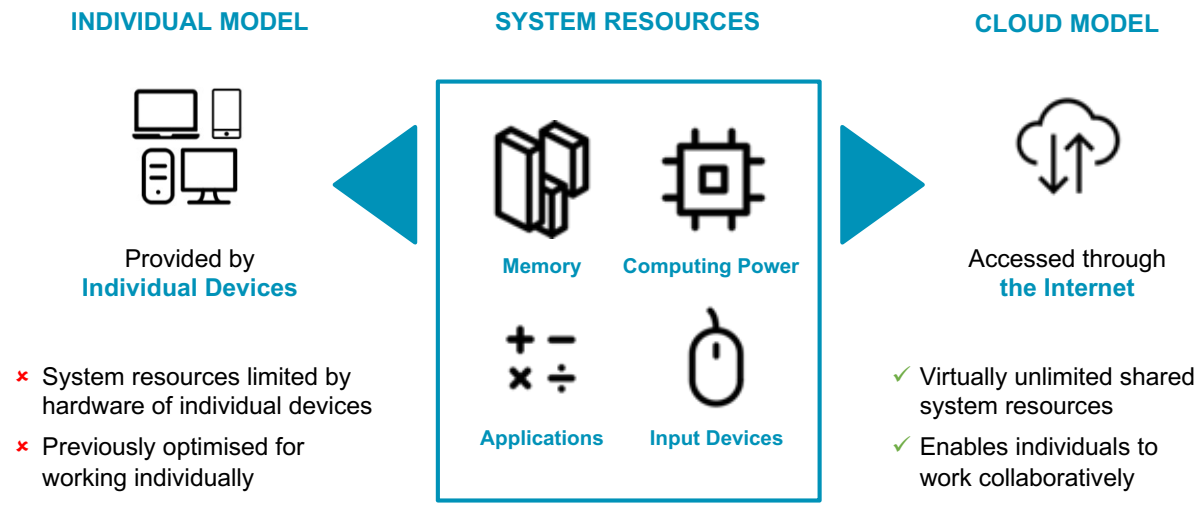
CLOUD TECHNOLOGY

Cloud technology allows users to utilise a pool of system resources through the internet, including remote access to a company's IT systems by its employees. System resources are assets within computer systems that enable them to carry out operations; examples include central processing unit ("CPU"), random access memory ("RAM"), and storage space.

Each computer is built from its component hardware, which provides a finite amount of system resources. As users or applications consume these limited assets, the performance of the computer declines. For example, when storage space is used up, users can no longer save extra files or applications, and when RAM is used up, applications cannot run smoothly, with users experiencing longer processing times.

The proliferation of applications and the rapid digitalisation of operations over the past decade have led to the demand for system resources growing at an exponential rate. As a result, individual computers no longer have the system resources necessary to keep pace with the demands of a techno-centric economy. This is the problem cloud technology seeks to resolve (see Figure 2).

FIGURE 2: ACCESS TO RESOURCES



Source: Quinlan & Associates research and analysis

Cloud computing was first conceived in the 1950s, with a model that allowed multiple employees to access a main, central computer, through "dumb terminals".[2] The high cost and impracticality of providing a computer to each employee meant access to a single, shared source of system resources was the logical solution.

The shared resource model evolved in tandem with technological innovation, underpinned by a strong emphasis on providing remote access to system resources. By sharing access to technological infrastructure and using system resources on an as-needed basis (or pay-as-you-go model), companies could attain their required computing capabilities at a relatively low cost. With growing demand for remote and real-time access, companies have been increasingly turning to cloud technology as a solution.

SERVICE MODELS

Building and maintaining a cloud system is relatively costly and requires considerable technological expertise. As such, companies typically engage with cloud service providers instead of developing their own cloud system. Some of the more well-known cloud service providers in the market include Amazon, Microsoft, IBM, Google, and Alibaba.

Cloud services are provided through three different models, being:

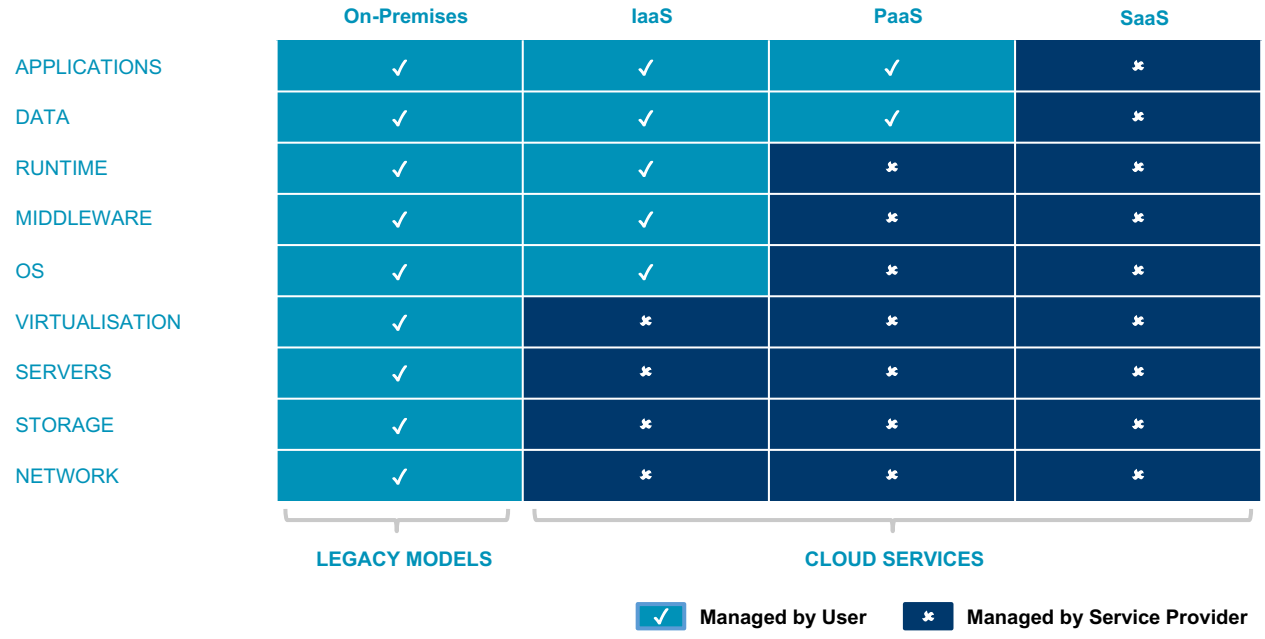
1. Infrastructure-as-a-Service ("IaaS");
2. Platform-as-a-Service ("PaaS"); and
3. Software-as-a-Service ("SaaS").

These three models are typically conceptualised as three layers, with IaaS on the bottom, PaaS in the middle, and SaaS at the top (see Figure 3).

[2] IBM, 'A brief history of cloud computing', 18 March 2014, available at: https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/

FIGURE 3: CLOUD SERVICE MODELS

	DESCRIPTION	USERS	COMPUTER EQUIVALENT	COMPLEXITY OF USE
SOFTWARE	• Provision of applications for end users, without the need for setting up or maintaining the underlying system	• Typically used by employees of the company	• Provision of software applications, which the customer uses right out of the box, without the need for technological expertise	LOWER
PLATFORM	• Provision of an environment for application development, testing, and deployment	• Typically used by software developers of the company	• Provision of an operating system, which enables the customer to develop and use different software applications	
INFRASTRUCTURE	• Provision of virtualised hardware (e.g. storage space and memory) on which a tailored platform can be built	• Typically managed by the system architects of the company	• Provision of just the hardware of a personal computer, on which the customer can install an operating system	HIGHER



Source: Quinlan & Associates research and analysis

The traditional model (i.e. on-premises solutions) typically requires the company to set up and manage all aspects of the cloud system. By using cloud service providers, some of this responsibility is taken away, allowing companies to focus on their core business.

INFRASTRUCTURE-AS-A-SERVICE

Infrastructure is the underlying hardware of the technology system, equivalent to the hardware of a personal computer (i.e. the actual machine itself, without any operating system installed). Cloud service providers are responsible for setting up the underlying hardware, with companies accessing system resources through the internet.

Under the IaaS model, companies have access to the skeleton of its IT infrastructure and are responsible for building their own platforms on it. Since cloud service providers only provide the simplest form of service in this model, IaaS solutions are typically the cheapest out of the three options. However, companies require technological expertise to build a suitable or customised platform of their own.

PLATFORM-AS-A-SERVICE

Platforms are built on top of the infrastructure, akin to operating systems being installed onto the hardware of a personal computer. The platform can be employed on top of any existing IaaS solution.

Cloud service providers typically set up a platform for companies to develop, test, and deploy their own software and applications. Software developers can focus their efforts on coding and developing applications for the company, instead of having to worry about the system or the environment on which the applications run. PaaS solutions require a lower level of technological expertise, but typically come with a higher price tag than IaaS solutions.

SOFTWARE-AS-A-SERVICE

SaaS involves the provision of the actual application, so users do not have to worry about any technical aspects of the software. This is equivalent to software applications available for personal computers, such as Microsoft Office and computer games.

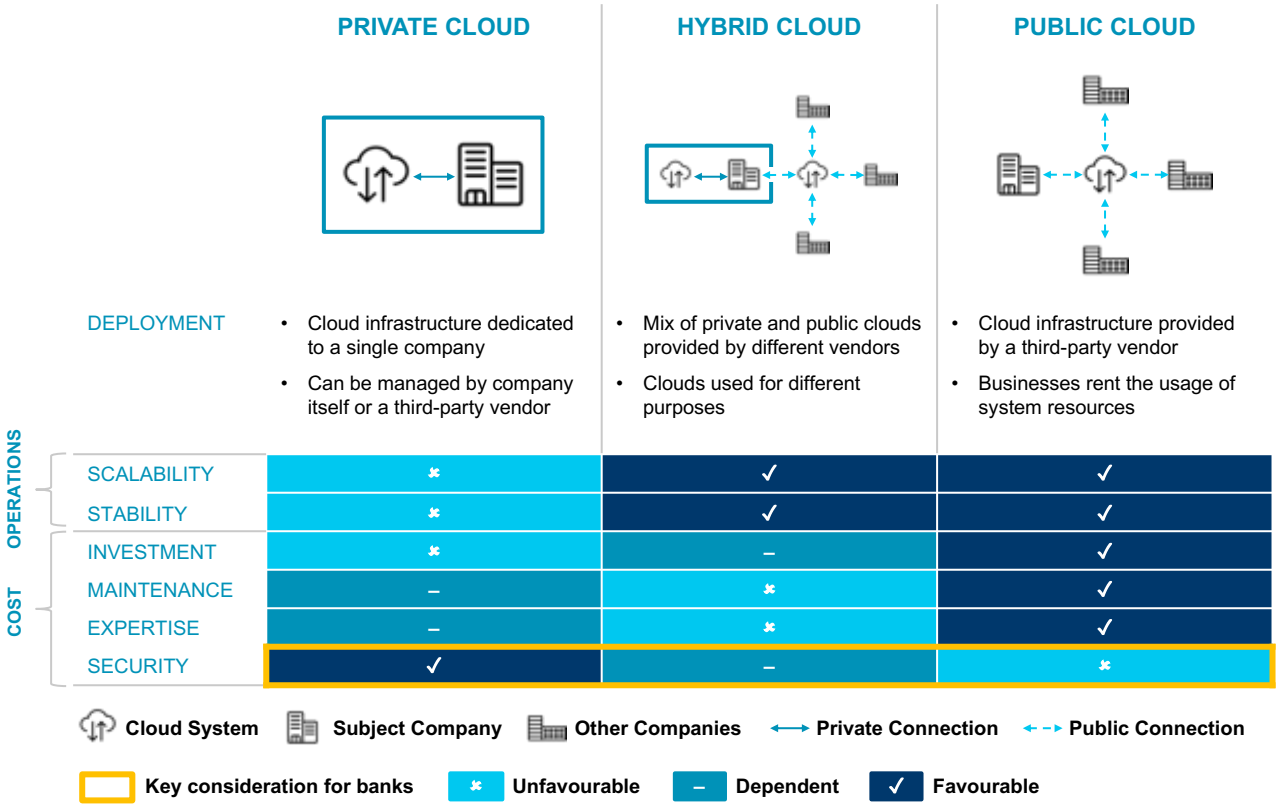
With this model, cloud service providers are responsible for setting up and maintaining all technical aspects of the application. Users simply run the application as a product right out of the box (i.e. a “plug and play” model). SaaS is preferred by companies lacking cloud expertise because service providers take care of all the underlying intricacies of the application. However, since the service providers are tasked with more responsibility, SaaS tends to be more expensive than the other service models.

DEPLOYMENT MODELS

Cloud services can also be categorised based on their deployment model, of which there are three types (see Figure 4):

1. **Private Clouds:** cloud infrastructure is solely devoted to a single company. The hardware itself can be stored and managed by either the company itself or by a third-party vendor, but the system resources are exclusively used by the single company (note that an on-premises solution is similar to a self-managed private cloud, with comparable benefits and drawbacks).
2. **Public Clouds:** cloud infrastructure is provided by third-party vendors and the system resources are accessible by any company or individual willing to pay for the usage. The system resources are typically rented on a pay-as-you-go basis. Examples of large public cloud services providers are Microsoft, Amazon, and Alibaba.
3. **Hybrid Clouds:** company uses both private and public clouds. Due to the nature of the setup, hybrid cloud model enables companies to select and benefit from the features from both private and public clouds.

FIGURE 4: CLOUD DEPLOYMENT



Source: Quinlan & Associates research and analysis

BENEFITS AND DRAWBACKS

SCALABILITY

The key benefit of cloud technology is the provision of system resources, which is limited by the capacity of the underlying cloud infrastructure.

To this end, private clouds are not as favoured as hybrid or public clouds. When companies invest in or employ a private cloud, the company chooses a set amount of hardware to acquire, which limits the level of system resources that can be accessed, limiting scalability. On the other hand, hybrid and public clouds both leverage public clouds, with hardware infrastructure provided by a service provider. Because they service a number of companies, these cloud service providers typically maintain a high level of system resources, along with significant buffer. Therefore, in times of heavy usage, companies employing hybrid or public clouds can easily gain access to extra system resources as needed.

STABILITY

Even though the physical infrastructure of private clouds can be located in multiple locations, companies typically only have a single facility of technological hardware. This means failure of the system can lead to a complete shutdown of the company's operations until the problem is resolved. In addition, even if companies host hardware in multiple locations, they typically do not have extra capacity to completely replace the operations of a single location in case of failure. Without access to extra system resources, private clouds are relatively unreliable and are susceptible to downtime.

By contrast, cloud service providers house their technological infrastructure in multiple locations and have significant buffers for system resources. Therefore, operations can be moved to other technological facilities if a single facility experiences difficulty, meaning public cloud users would not experience system-wide shutdowns. Similarly, for hybrid cloud users, if their private cloud malfunctions, relevant operations can temporarily be moved onto public clouds to continue operations.

INVESTMENT

Investment refers to the upfront cost of the cloud infrastructure.

As both private and hybrid clouds require the purchase of the private cloud infrastructure, these two deployment models require significant upfront cost. The cost required depends and varies significantly based on the capacity required by the company, ranging from buying a small server (priced at a few hundred dollars) to building a data centre, which could cost over USD 1 million depending on location.

However, in a private cloud model, the private cloud itself is responsible for the company's entire operations. As such, capacity requirements are significantly higher than in a hybrid cloud model, where operations are shared between the private and public clouds. Therefore, a purely private cloud model typically requires higher upfront investment than a hybrid cloud model.

On the other hand, because the cloud service provider invests in and provides the hardware to public cloud users, public clouds require essentially zero upfront investment.

MAINTENANCE

All hardware and software require ongoing updates and optimisation, with companies needing to spend both financial and operational resources to maintain private clouds. As all cloud infrastructure needs to be compatible, the private cloud must be adjusted after any changes to the public cloud, and vice versa. Therefore, hybrid clouds are typically more difficult to maintain than private clouds.

By contrast, public cloud infrastructure is operated by the service provider. As a result, users need not concern themselves with upgrading or maintaining the cloud. Even though users must take long-term leasing fees into consideration, public clouds should be less costly to maintain than private or hybrid clouds.

EXPERTISE

A dedicated team is required to supervise and monitor the technological infrastructure and system of a company.

For private clouds that are managed internally, specialised cloud talent is required. However, if the system is managed by a service provider, then essentially no in-house talent is needed. Hybrid clouds, whether internally or externally managed, require significant expertise because the company needs to ensure smooth communication between systems for operations. Finally, as public clouds are maintained by service providers, minimal in-house expertise is needed.

SECURITY

Security is arguably the most important consideration for banks when choosing an appropriate cloud deployment model, given that they store significant amounts of sensitive client information and any cybersecurity breaches could cause detrimental reputational and financial consequences.

Because all system resources are dedicated to a single company in a private cloud model, only the company has access to the resources. Therefore, private clouds are typically perceived to be the most secure out of the three deployment models. However, hybrid clouds also provide the same level of security for operations on the private cloud. Hybrid cloud users can choose whether to store information and run operations on the private cloud or public cloud, utilising the private cloud for confidential aspects of the business, and conducting less sensitive operations on the public cloud.

As system resources can be accessed by any entity willing to pay, public clouds are viewed as the least secure deployment model.

VERDICT

In terms of operational performance, hybrid clouds perform as well as public clouds, and by selectively allocating data and operations, hybrid clouds also benefit from the security provided by private clouds. Therefore, hybrid cloud deployment models that implement an appropriate allocation of system resources appear to be the most preferred option, enabling users to enjoy the operational benefits of both private and public clouds. However, they can be more expensive than purely public clouds.

RightScale reported that 63% of companies with over 1,000 employees (and 48% of companies with fewer than 1,000 employees) that use a multiple cloud system have either adopted or are considering adopting a hybrid cloud system.[3]

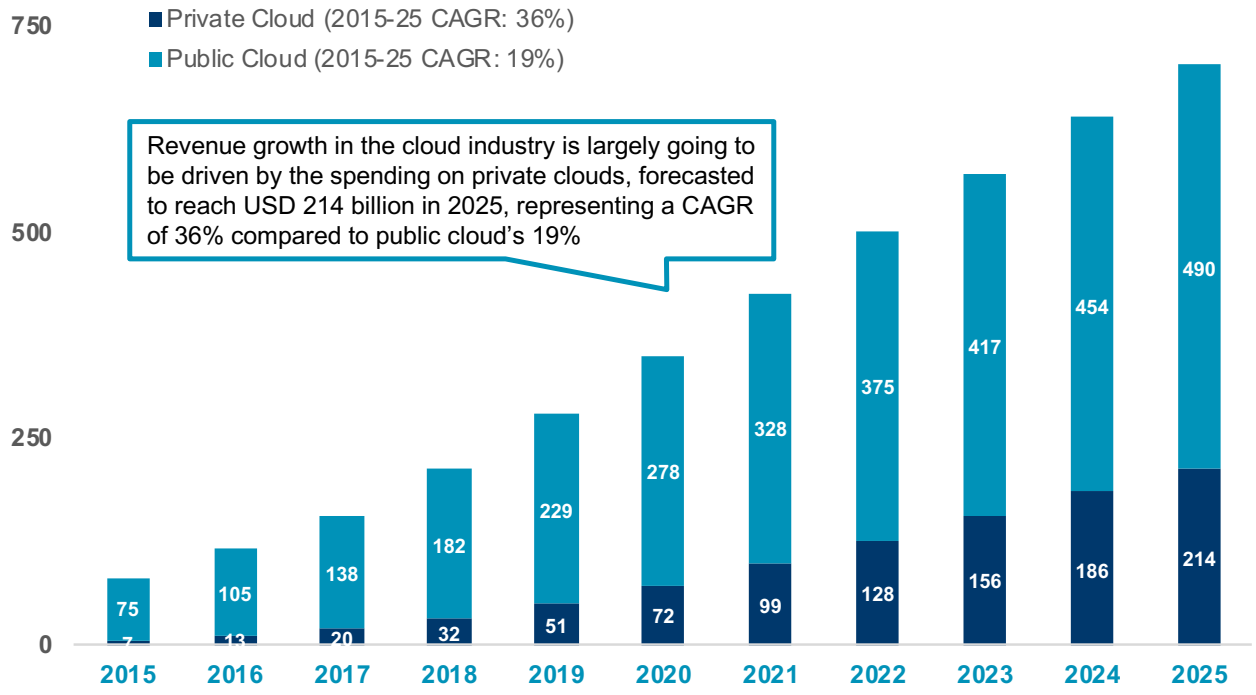
[3] RightScale, 'RIghtScale 2018 State of the Cloud Report', available at: http://www.rightscale.com/2018-cloud-report

SECTION 2
CLOUD INDUSTRY REVIEW

CLOUD INDUSTRY LANSCAPE

With increasing demand for cloud services, the industry is expected to witness tremendous growth, with global industry revenue estimated to grow by a CAGR of 24% from USD 82 billion in 2015 to over USD 700 billion by 2025 (see Figure 5).

FIGURE 5: CLOUD INUDSTRY REVENUE (2015-25), USD billion



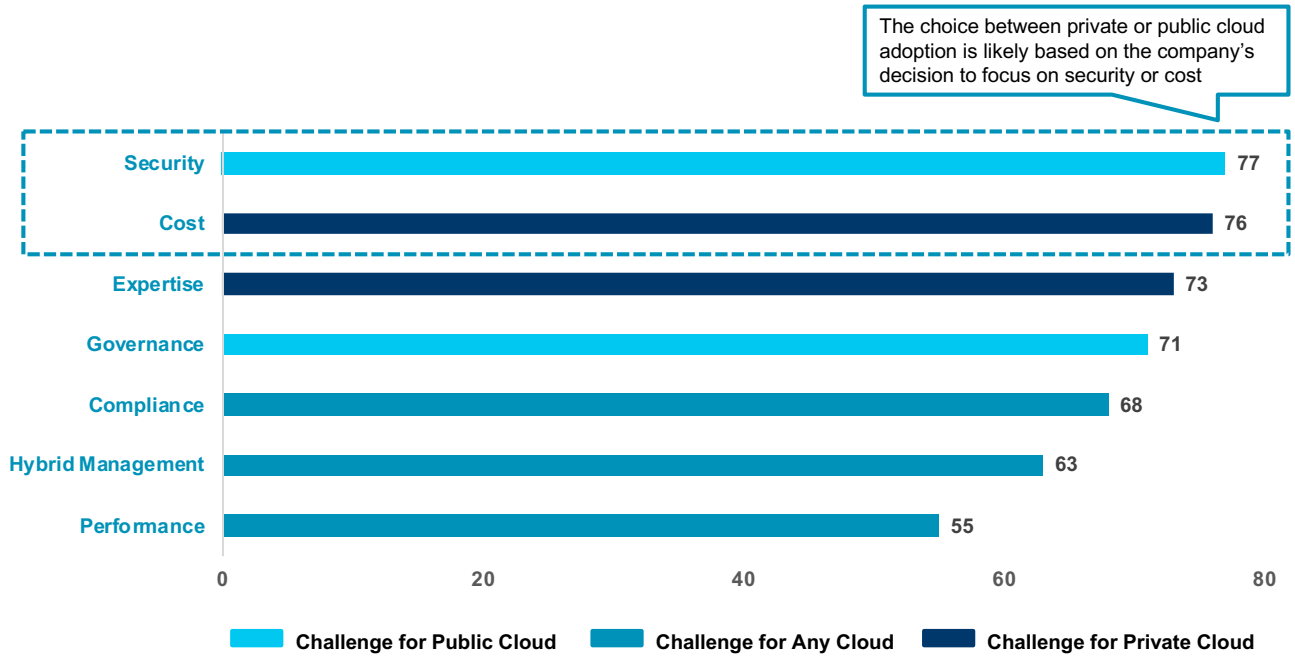
Note that revenue for hybrid clouds is separated and accounted for in the revenues for private and public clouds
Source: Statista, Quinlan & Associates analysis

It is unsurprising that public cloud revenues account for a large proportion of the total industry, given its lower cost and greater ease-of-use. In fact, it was reported that 38% of companies are currently focusing on public clouds, while only 17% place private clouds as their top priority (8% building the cloud internally and 9% sourcing externally hosted private clouds).[4] However, as private clouds are typically costlier, the growth in private cloud revenue outpaces that of public cloud despite the lower proportion of companies focusing on adopting private clouds.

[4] RightScale, 'RIghtScale 2018 State of the Cloud Report', available: http://www.rightscale.com/2018-cloud-report

Despite the high adoption and growth rate for the cloud industry, companies have identified a few key challenges regarding the usage of cloud technology (see Figure 6).

FIGURE 6: CHALLENGES FOR CLOUD ADOPTION (2018), %



Note that companies were allowed to identify multiple challenges for cloud adoption
Source: RightScale, Quinlan & Associates analysis

The top concern for companies considering cloud technology is security (particularly public clouds), followed by cost and expertise required. Because public clouds are provided and maintained by a third party through a shared infrastructure model and a pay-as-you-go cost structure, they address concerns around cost and expertise better than private clouds. By contrast, as private clouds provide better security and data governance, they cater much better to companies who see security as their key concern.

Large corporations, especially financial institutions and professional services companies (such as law firms and accounting firms) have the financial resources and reputation to invest in technology and attract specialised talent to manage their cloud infrastructure, meaning they are less concerned with cost and expertise. Additionally, as these firms collect and store large volumes of confidential client information and must comply with privacy and data security regulations, they see security and data governance as key priorities. As such, many of these companies are focused on adopting private clouds, driving industry growth rates.

CLOUD SERVICE PROVIDERS

As the cloud industry, especially the public cloud sector, is a sharing economy, service providers benefit significantly from economies of scale. It is therefore unsurprising to see the market being dominated by a handful of key players (see Figure 7).

FIGURE 7: PUBLIC CLOUD SECTOR MARKET SHARE (Q1 2018), %

Note that the listed companies are simply subscribers to cloud services, and are not necessarily users of public clouds (they may use hosted private clouds instead)
Source: KeyBanc, Amazon, Microsoft, Google, Quinlan & Associates analysis

Despite US cloud service providers dominating the market, their future growth may be stymied by government regulations, including the growing trend of data localisation which requires citizen data to be stored locally in servers located within the country. Examples of countries with data localisation regulations include China, South Korea, India, Australia, Russia, Germany, and Switzerland. Some countries such as China and Russia, essentially require all data to be stored locally, while others like Australia and South Korea only have such requirements for data collected within specific sectors, including healthcare and finance. In addition, increased regulatory scrutiny around the protection of personal data has made cross-border data transfers more problematic. Most recently, the European Union's ("EU's") General Data Protection Regulations ("GDPR") require the guarantee of a certain level of protection before personal data can be transferred to servers in a foreign country.

Due to such trends, dominant US cloud service providers will no longer be able to service overseas clients through their US infrastructure and must establish a physical presence within each country they intend to operate in, adding considerably to their costs. We see this as an opportunity for local or regional cloud service providers operating in Europe or Asia to compete against these giants for market share outside of the US. In fact, despite Amazon's leading position in the global cloud industry, it only had ~10% market share in China's cloud services market in 2017, significantly outsized by Alibaba's market share of over 30%.[5]

CLOUD SHORTFALLS

While cloud services have the potential to enhance operations, there are certain shortfalls that need to be considered, especially for companies looking to mitigate potential risks associated with cloud usage (see Figure 8).

FIGURE 8: CLOUD SHORTFALLS

CRITERIA	DESCRIPTION	MITIGATION
FLEXIBILITY	• Underlying infrastructure managed by service provider, and may not be tailored to specific needs	• Adopt private cloud solution, with the infrastructure tailored to specific requirements
DOWNTIME	• Server outage (or internet outage) may lead to suspension of service	• Use cloud infrastructure located in multiple locations to prevent simultaneous loss of all resources
SECURITY	• Reliance on competence of service provider to protect infrastructure and data	• Review all cybersecurity measures and implement advanced data access management
PRIVACY	• Data stored in third party-managed locations may lead to privacy concerns	• Store sensitive data on in-house or private clouds, and encrypt all externally-stored data
COST	• Pay-as-you-go model may incur significant expenses if prudence is not exercised	• Determine explicit quotas for system resource usage and implement continuous monitoring
INCOMPATIBILITY	• Applications may not be compatible with all cloud infrastructure	• Adopt applications developed with different cloud systems in mind or with sufficient technical support
DEPENDENCE	• Switching cloud service providers may be costly, especially if applications are not compatible	• Adopt a multi-cloud model and design systems according to best practice to streamline any integrations

Source: Quinlan & Associates research and analysis

FLEXIBILITY

While cloud service providers remove the responsibility of managing the cloud system from companies, this inevitably eliminates the flexibility of the underlying infrastructure. As the solution moves up the service model architecture – from on-premises to IaaS, to PaaS, and finally to SaaS – the cloud service providers manage more elements of the underlying system, and the company loses the flexibility to tailor the system to their specific requirements.

Companies can consider adopting private cloud solutions, which are typically costlier, but are optimised and tailored according to the companies' demands.

[5] The Economist, 'Chinese tech companies plan to steal American cloud firms' thunder', 18 January 2018, available at: https://www.economist.com/business/2018/01/18/chinese-tech-companies-plan-to-steal-american-cloud-firms-thunder

DOWNTIME

As cloud technology provides system resources through the internet, there are two potential vulnerabilities which may lead to a loss of service: (1) failure from the hardware; and (2) loss of access to the internet.

While cloud infrastructure can be managed by an experienced third party, reliability and consistency cannot always be guaranteed, and failures can arise due to unmanageable factors, such as natural disasters. Indeed, Amazon's S3 cloud storage system malfunctioned in March 2017, with the failure estimated to have cost companies on the S&P 500 over USD 150 million.[6] In addition, the company itself may lose access to the internet and fail to access the system resources needed.

Through adopting a mix of public clouds located in multiple locations, as well as on-premises private clouds, companies can significantly reduce the possibility of a complete service shutdown. If any part of the cloud infrastructure experiences a technical failure, other hardware can take over and continue providing the required system resources. In addition, if companies lose internet access, the on-premise private cloud may be able to provide a certain (albeit likely minimal) amount of system resources to continue operations until internet access issues are resolved.

SECURITY

Due to the vast amount of sensitive data and information processed through and stored on cloud services, public cloud infrastructure is often a key target for hackers. In fact, Microsoft stated that its cloud computing operations are constantly under attack, with 1.5 million hack attempts per day.[7]

While cloud service providers typically have measures in place, companies should review the cybersecurity budget and mechanisms to fully evaluate the cybersecurity risk. In addition, companies can employ their own cybersecurity policies to further protect their data, such as encryption and multi-factor authentication. Files can be encrypted, either by an in-house application or software from a third-party provider, prior to being uploaded and stored on public clouds. This further enhances the protection of sensitive information, even in the event of a cybersecurity breach. Multi-factor authentication also makes it considerably difficult for non-authorised personnel to access confidential data.

Alternatively, companies can adopt private clouds instead of public ones; while they are more expensive, private clouds are typically perceived to be safer.

[6] MIT Technology Review, 'Amazon's $150 Million Typo Is a Lightning Rod for a Big Cloud Problem', 3 March 2017, available at: https://www.technologyreview.com/s/603784/amazons-150-million-typo-is-a-lightning-rod-for-a-big-cloud-problem/
[7] Microsoft, 'SECURING THE CLOUD', available at: https://news.microsoft.com/stories/cloud-security/

PRIVACY

For public clouds and managed private clouds, data and information are stored within systems controlled and maintained by third parties, raising privacy concerns. This is especially relevant for the financial services industry as financial institutions collect, process, and store a vast amount of sensitive client information.

In addition to storing client data internally through self-managed private clouds or in-house data centres, companies should implement sufficient data protection policies such as encryption and data access management to eliminate the possibility of unauthorised personnel gaining access to such information. Regulators in regions or countries such as the EU and Singapore typically require companies to conduct due diligence on the data security and privacy policies of cloud service providers to ensure client data is protected and secured.

COST

While the pay-as-you-go model of public cloud services are viewed as cost-efficient with companies only paying for what is used, a variable rate can incur significantly higher expenses than a fixed rate if system resources are not being used prudently. This may happen during occasions or projects with significant resource usage, including an initial platform launch (where large volumes of clients may access the website) or during big data analyses (which require a significant amount of processing power).

Similar to any other budgeting policies, companies should set explicit usage restrictions and continuously monitor the consumption rate of system resources.

INCOMPATIBILITY

Cloud infrastructure provided by various service providers may be developed under different specifications or standards, such that applications may not be compatible with all infrastructures. This may not cause any problems if companies remain with the same cloud service providers, but significant migration costs may be incurred if a company chooses to switch cloud service providers in the future. In addition, cloud service providers may develop applications specially for their own infrastructure, and companies may lose access to the applications and related data when migrating to another service provider.

As there is currently no single cloud standard, companies should consider adopting applications which are developed to be functional on all major cloud infrastructures and hire cloud experts for any migration.

DEPENDENCE

Outsourcing a company's entire cloud operations to a single third party leads to dependence on an external party. Moreover, the incompatibility of applications may discourage companies from seeking other cloud service providers. This dependence on a third party may result in higher expenses and significant switching costs.

To address this, companies can employ a multi-cloud strategy from a number of service providers while developing or adopting applications that comply with industry best practices to minimise any dependence and reduce switching costs.

CONSIDERATIONS

As with any technology, the main decision for companies using cloud applications is whether to buy or build (i.e. to use a public or private cloud).

Developing applications internally ensures that the software is tailored to the bank's operations. However, software development requires significant expertise, with one cloud technology expert that we spoke to indicating that performance optimisation is the core challenge for cloud-based collaboration applications. As native applications (i.e. non-cloud-based tools) are directly executed in the terminal's operating system environment (providing for complete control), performance is relatively easy to optimise. However, as cloud-based applications are executed on browsers (i.e. subject to external influences), the applications need to be continuously optimised to attain an optimal level of performance.

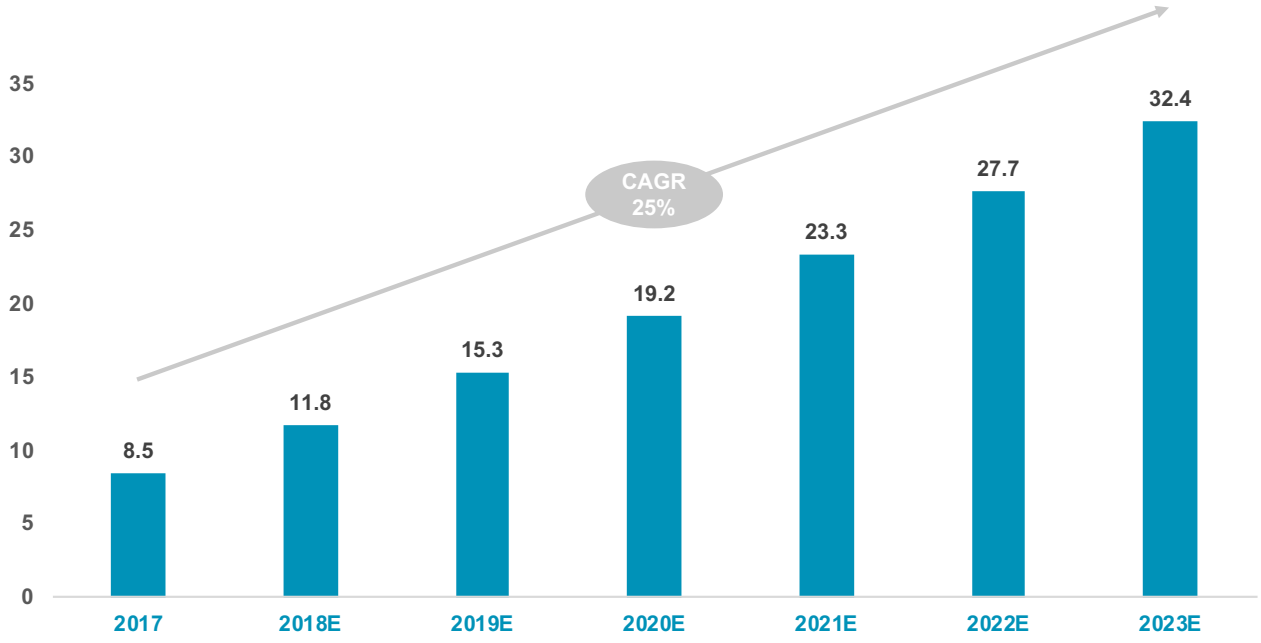
Sourcing external applications is much easier from a performance optimisation perspective, requiring companies to have significantly less technological expertise. However, the company will be reliant on the competency of the third-party service provider, whilst also having to worry about data privacy issues.

SECTION 3
CLOUD APPLICATIONS WITHIN BANKING

Cloud computing is by no means new to the banking industry. A number of well-established firms, including JP Morgan and Goldman Sachs, have already adopted public clouds.[8] Westpac is also the first bank in Australia to implement a hosted private cloud, built and managed by IBM, and is looking to move 70% of the bank's applications onto the cloud within three years.[9]

Based on a range of discussions with IT professionals working in the banking industry, we understand most banks currently spend 2-4% of their IT budgets on cloud technology, with larger firms typically spending towards the upper end of this range. Overall, we estimate that the global banking industry spent USD 8.5 billion in total on cloud technology in 2017. We predict banking cloud spend to grow by a CAGR of 25% over the next five years, topping USD 10 billion in 2018 and reaching just over USD 32 billion by 2023 (see Figure 9).

FIGURE 9: GLOBAL BANKING INDUSTRY CLOUD SPENDING (2017-23E), USD billion



Source: Quinlan & Associates proprietary estimates

[8] Fortune, 'U.S. Financial Firms Have Saved Billions by Embracing Shared Cloud Services', 17 March 2017, available at: http://fortune.com/2017/03/17/us-banks-shared-cloud-services/
[9] CIO, 'Westpac claims Australian banking first with offsite private cloud move', 5 June 2018, available at: https://www.cio.com.au/article/641944/westpac-claims-australian-banking-first-offsite-private-cloud-move/

There are a range of use cases of cloud technology in today's banking industry, including data storage, application development, client servicing, and digitalisation (see Figure 10).

FIGURE 10: USAGE OF CLOUDS IN THE BANKING INDUSTRY

	FUNCTION	EXAMPLE	DESCRIPTION	
1	DATA STORAGE	DBS	• Transformed a traditional data centre to cloud-optimised centre for future cloud operations	CURRENT USAGE
2	APPLICATION DEVELOPMENT	Westpac	• Migrated core banking applications, and associated developments, onto a cloud system managed by IBM	CURRENT USAGE
3	CLIENT SERVICING	Bank of America Merrill Lynch	• Adopted Microsoft Azure's service to support client-facing applications and services	CURRENT USAGE
4	DIGITALISATION	Goldman Sachs	• Approximately 85% of workload operated under a cloud framework in 2015	CURRENT USAGE
5	COLLABORATION		• Utilisation of cloud-based applications to both enable and enhance collaboration	PROPOSED USAGE

Source: DBS, Australian Financial Review, CloudPro, NetworkWorld, Quinlan & Associates analysis

CURRENT USAGE

At present, cloud technology is mainly being utilised by the banking industry to streamline operations and cut costs. Overall, we see banks leveraging cloud solutions for four key purposes, including: (1) data storage; (2) application development; (3) client servicing; and (4) digitalisation.

1. DATA STORAGE

Data storage is one of the most common uses of cloud technology in the banking industry. Storing data on the cloud allows employees to access the information through the internet, enabling them to work remotely. Banks typically choose private clouds for storage as they are considered to have a higher level of security than public clouds.

For example, DBS partnered with Equinix to optimise one of its data centres for cloud technology, as part of its overall cloud transformation process.[10] DBS stated that its cloud-based data centre is 75% cheaper than traditional data centres while being over 10 times more energy efficient.

[10] DBS, 'First bank in Singapore to launch new cloud-based data centre', 13 November 2017, available at: https://www.dbs.com/newsroom/First_bank_in_Singapore_to_launch_new_cloud_based_data_centre

Despite the numerous benefits that cloud services offer banks in terms of data storage, regulators remain wary of security risks, such as confidential data leakage. As we highlighted in Section 2, some regulators are taking a more conservative stance, requiring cloud service providers to maintain infrastructure within the country to become eligible for storing client data. For example, Indonesia's Ministry of Communication and Informatics (MOCI) requires that data localisation for "Strategic Electronic Data", which includes the bank account data of Indonesian citizens.[11] Similarly, China's 2016 Cybersecurity Law requires "personal information and important data collected and generated by critical information infrastructure operators" in the country to be stored domestically, with companies required to build data centres onshore. However, China is currently implementing changes to its cybersecurity laws, allowing some businesses to provide data outside the country, but only under state-defined measures and after security assessments.[12]

Other regulators are taking a different approach, allowing firms to operate in foreign domains under certain conditions. The EU's GDPR applies to any organisation in the world collecting EU citizen data, including banks and cloud providers. Individual organisations are accountable for the privacy and security of this data, which includes ensuring any data access is deliberate as well as restricted. GDPR also gives each EU citizen control over their data, such as the ability to request its deletion or modification.[13] However, these organisations are not prevented from operating from outside the EU, meaning data does not need to be stored locally.

On the other hand, regulators such as the Monetary Authority of Singapore ("MAS") place more of the onus on financial institutions themselves to ensure data is secure. Recognising the security infrastructure of cloud providers, the MAS simply recommends financial institutions to conduct appropriate quality checks (including audit) of their cloud service providers.[14]

Given the lack of global regulatory harmonisation around data privacy, certain markets are likely to be easier for banks to implement cloud-based data storage. A regional head of cloud technology we spoke to from a leading global investment bank said the heterogenous regulatory environment in Asia Pacific made the roll-out of cloud applications particularly challenging from a compliance perspective, especially when compared to markets such as the USA or the EU.

[11] Lexology, 'Indonesia – changes to data localization provisions for electronic system operators', 6 April 2018, available at: https://www.lexology.com/library/detail.aspx?g=a3b371a0-1b95-4ebc-86a1-2cbcda491eda
[12] Quartz, 'A key question is at the heart of China's new cybersecurity law: Where should data live?', 7 June 2018, available at: https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live
[13] Virtualization Review, 'GDPR and the Cloud: What You Need to Know', 14 March 2018, available at: https://virtualizationreview.com/articles/2018/03/14/gdpr-and-the-cloud-what-you-need-to-know.aspx
[14] Monetary Authority of Singapore, 'Guidelines on Outsourcing', 27 July 2016, available at: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

2. APPLICATION DEVELOPMENT

Because of the provision of essentially unlimited system resources, cloud technology streamlines the application development process; from development, to testing, to deployment. This enhances banks' agility by enabling them to design, launch, or upgrade applications swiftly in response to any changes in the market.

It was reported by Salesforce that companies experienced a 70% reduction in the time from application development to market launch from using the cloud.[15] In fact, Westpac expects to benefit from faster (up to 10 times) and cheaper (up to three times) development through migrating its core banking applications to the cloud.[16]

Westpac's cloud migration initiative is an example of banks trying to shift away from their legacy systems: outdated systems and technology plaguing modern banks with complex, inefficient, and costly procedures. Ironically, the challenge for many banks looking to move to the cloud involves the incompatibility of many of their legacy systems with cloud platforms. This sentiment was echoed by the global head of cloud technology at a global investment bank, who emphasised a number of specific risks, including failing to patch updates, run new applications, or view data due to incompatible system environments and features.

To address issues posed by legacy systems, banks are increasingly looking to leverage container environments. Containers allow software to run reliably after being moved from one computing environment to another (i.e. from a physical data centre to the cloud). They contain a whole runtime environment in one unit, consisting of an application, libraries, and the configuration files required for it to operate. With this feature, containers can isolate software from its surroundings, including differences in the infrastructure of where it was developed and where it will be used; in other words, containerisation standardises software for usage in other locations.[17] Moreover, containers provide various other advantages, including being compact in size and memory (allowing for more of them to be stored) and the ability to be started almost instantly (i.e. they can be generated as needed and removed after, allowing firms to save costs).[18]

[15] Salesforce, 'How Cloud Platforms Save IT Time and Money On App Development', 10 April 2014, available at: https://www.salesforce.com/blog/2014/04/cloud-platforms-it-app-development.html
[16] Australian Financial Review, 'Westpac claims advantage with cloud computing milestone', 4 June 2018, available at: https://www.afr.com/technology/cloud-computing/westpac-claims-advantage-with-cloud-computing-milestone-20180601-h10ueb
[17] Docker, 'What is a container', available at: https://www.docker.com/what-container
[18] CIO, 'What are containers and why do you need them?', 27 June 2017, available at: https://www.cio.com/article/2924995/software/what-are-containers-and-why-do-you-need-them.html

3. CLIENT SERVICING

Cloud computing can deliver significant improvements to digital platforms, which act as a critical service point for clients.

Cloud technology's flexibility in scaling enables banks to service clients during both peak and trough periods in a cost-effective manner. Using traditional systems, banks may be reluctant to invest in the technological infrastructure to service clients during peak periods, as extra capacity is essentially wasted during non-peak periods. As such, clients may experience significant lag and a deterioration in service levels during busy times. By contrast, leveraging cloud technology allows banks to rent the appropriate level of system resources from the service provider according to the level of client access on a pay-as-you-go basis, enabling a satisfactory level of service without incurring significant additional costs.

In addition, banks that employ a cloud system do not need to worry about potential server failures. Cloud service providers typically host the infrastructure in multiple locations. As such, the failure of one location has minimal – if not zero – impact on the other hardware, which means operations can easily migrate to functioning infrastructure. Cloud technology thus ensures system reliability via a decentralised infrastructure mechanism, as opposed to an on-premises model where the failure of a bank's infrastructure can lead to a breakdown of the entire client service platform.

Bank of America has reportedly adopted Microsoft's Azure to support its client-facing applications and services, providing clients with better wealth management tools in a more scalable and cost-efficient manner.[19]

[19] CloudPro, 'Bank of America turns to Microsoft Cloud to aid digital transformation', 3 October 2017, available at: http://www.cloudpro.co.uk/cloud-essentials/public-cloud/7080/bank-of-america-turns-to-microsoft-cloud-to-aid-digital

4. DIGITALISATION

Digitalisation is another key area where banks can utilise cloud technology.

Essentially, banks can migrate all internal operations onto a cloud-based system to take advantage of the scalability, virtually unlimited levels of system resources, accessibility, and reliability offered by cloud technology. Furthermore, by outsourcing the management and maintenance of technological infrastructure to cloud service providers, banks are able to achieve significant cost savings.

Goldman Sachs, for example, had already migrated 85% of the company's workload onto a cloud framework by the end of 2015. The ultimate goal of Goldman Sachs is to conduct application development, infrastructure management, and operations all in a single cloud environment.[20]

The provision of large amounts of system resources is particularly useful for product development. The connectivity of devices and the internet of things ("IoT") have enhanced the availability of big data, which is increasingly being used to better understand customer demands and preferences. However, for big data to have any use, it needs to be appropriately analysed. This typically requires sophisticated algorithms that run on a significant amount of computing power. By leveraging the flexible scalability of system resources through the cloud, banks can not only analyse client data at significantly reduced costs but also develop more appropriate products that are better tailored to each client, driving sales potential.

However, as everything connected to the internet is vulnerable to cyber-attacks, many institutions are still reluctant to migrate key operations onto cloud systems due to data security and privacy concerns. On the other hand, some have argued that migration onto the cloud can actually improve the systems' level of cybersecurity.

While bank hackings are rare, they are not unheard of. Examples include the Tesco Bank hack in Britain in November 2016, and the hack of Mexican banks in May 2018. By contrast, cloud service providers (especially dominant players such as Amazon, Microsoft, and Google) are inherently technology firms and operate the majority of their business online. In addition to their technological expertise, they invest significant amounts of money in cybersecurity. In fact, it was reported that Microsoft invests over USD 1 billion per year in cloud security technologies,[21] which is significantly higher than the cybersecurity spending of major banking institutions (such as J.P. Morgan Chase's 2015 cybersecurity budget of USD 500 million[22] and Citi's USD 300 million[23]). Moreover, Microsoft hires over 3,500 security engineers and utilises an A.I.-enabled security system to enhance the protection of its infrastructure. While banks should not completely rely on a third party for cybersecurity, they can reduce cybersecurity spend and reallocate the budget to other aspects of their technology systems.

[20] NetworkWorld, 'How Goldman Sachs and Bank of America use the cloud and containers', 9 December 2015, available at: https://www.networkworld.com/article/3013474/cloud-computing/how-goldman-sachs-and-bank-of-america-use-the-cloud-and-containers.html
[21] eWeek, 'Microsoft's Cloud Weathers 1.5 Million Hack Attempts Each Day', 6 June 2017, available at: http://www.eweek.com/security/microsoft-s-cloud-weathers-1.5-million-hack-attempts-each-day
[22] J.P. Morgan Chase, 'Annual Report 2015', available at: https://www.jpmorganchase.com/corporate/investor-relations/document/2015-annualreport.pdf
[23] Wall Street Journal, 'Financial Firms Bolster Cybersecurity Budgets', 17 November 2014, available at: https://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536

Q&A SAY…

OUTSOURCING SECURITY

Cybersecurity and data protection are of utmost importance to financial institutions, given their handling of extremely sensitive client information, including customer assets.

While concerns around data security continue to make regulators remain wary about the use of public cloud technology, we see their concerns as somewhat misguided. In short, we do not believe banks need to completely in-house their data storage and security, and that engaging a third party with sufficient expertise may in fact be a more secure option. To illustrate this point, an interesting parallel can be drawn with the storage of one's valuables.

Households take considerable steps to safeguard their personal assets. In-housing the security process means keeping valuables (e.g. cash, antiques, and jewellery) at home and instituting a variety of safekeeping measures, which may include fitting special locks on windows and doors, securing valuables in drawers / lockers / a safe, setting up security cameras, and purchasing a home alarm system. This is equivalent to banks protecting their IT system through various in-house cybersecurity measures, such as multi-factor authentication and access management. However, for both individuals and banks, this process is time-consuming and costly, while also being prone to individual implementation errors (e.g. forgetting to lock a window or activate the home alarm when leaving the house). Moreover, security practices across households (as well as banks) are not standardised to an industry "best-practice" and as a result, vary considerably in their application.

By contrast, individuals may choose to deposit their valuables in banks or third-party storage facilities (i.e. outsource the protection of their assets to an external vendor). While some individuals may be more comfortable protecting their own assets, it may in fact be safer to rely on a third party with considerable, specialised expertise in security. Banks, for example, have a range of proven safekeeping practices in place, including silent alarms, CCTV cameras, security shutters at cashier counters, on-site (and armed) security guards, biometric authentication, and vaults. Central banks, such as the US Federal Reserve, are even more difficult for unauthorised parties to access, due to extremely stringent security measures.

By the same token, as technology companies – especially well-established firms such as Microsoft, Amazon, and Google – have considerable experience and leading capabilities in the cybersecurity space (including continuous investment in their cybersecurity teams and research), their security measures are likely to be on par with, if not stronger than, those employed by banks. Moreover, the reputational fallout associated with any security breach is likely be much more damning to a third-party provider – for example, political data consultancy Cambridge Analytica filed for insolvency and shuttered its operations in May 2018 following revelations that it had inappropriately acquired and used the personal data of over 87 million Facebook users. As such, public cloud vendors have a vested interest in maintaining the highest standards of data security for their customers.

We are not suggesting that banks should ignore cybersecurity risks associated with the adoption of cloud infrastructure or rely solely on a third party to ensure security of the system. Nonetheless, we believe banks should stop seeing cybersecurity as a major roadblock to public cloud adoption, especially as cloud service providers continue to upgrade their cybersecurity measures. However, the banking and technology industries will need to work closely together in coming years to lobby regulators into becoming more supportive of the use of public cloud technology. This may include establishing clear regulatory guidelines for data privacy and security on public clouds, or relaxing data localisation requirements in certain jurisdictions.

PROPOSED USAGE

5. COLLABORATION

Collaboration is another key use case for cloud technology, with appropriate implementation of cloud-based collaboration tools having the potential to significantly enhance current workflow procedures within banks. Nonetheless, we believe cloud-based collaboration technology is currently heavily-underutilised by most institutions, likely due to its short history as well as compatibility issues with banks' legacy systems.

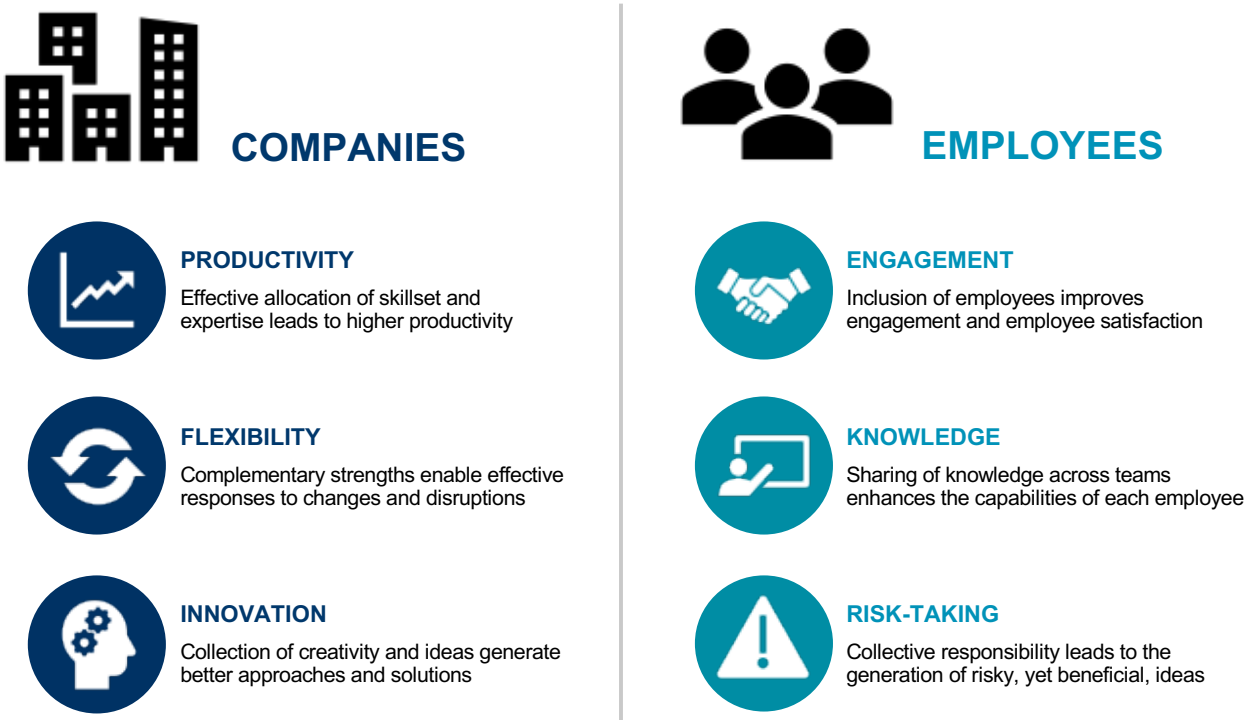
Before we discuss the applications and benefits of cloud-based collaboration tools, it is important to explore the merits of collaboration in the workplace more broadly, as well as some of the specific obstacles facing many banks in creating a truly collaborative working environment (see Section 4).

SECTION 4
COLLABORATION IN THE BANKING INDUSTRY

THE IMPORTANCE OF COLLABORATION IN THE WORKPLACE

With the advent of the internet and the proliferation of smartphones and other mobile devices, information has become ubiquitous, with access now largely free and instantaneous. Consequently, individual expertise is no longer considered sufficient for growth and development; collaboration between diverse individuals and groups is of critical importance, given the many benefits it can bring to both companies and their employees (see Figure 11).

FIGURE 11: BENEFITS OF COLLABORATION



Source: Quinlan & Associates research and analysis

At the company level, collaboration improves the allocation of complementary strengths and skillsets, enhancing productivity and enabling more effective responses to unexpected changes, such as business disruptions. In addition, a mix of diverse individuals generates a wider spectrum of ideas, driving creativity and innovation.

From an employee perspective, collaboration improves engagement by enabling staff members to contribute to projects they are interested in. By working with colleagues from different backgrounds with varied skillsets, employees can also gain new insights and expertise on specific subjects, enhancing their personal and career development. Moreover, employees tend to be risk averse. By working as a team, novel suggestions can be tested and challenged, and all members share the responsibility for the result, encouraging employees to take more measured risks, driving innovation.

There is a considerable amount of evidence indicating how companies that do not promote a culture of collaboration suffer from negative repercussions, including workplace failure and the loss of potential revenues. In fact, it was reported that 86% of employees identified a lack of collaboration or ineffective communication as a key reason for workplace failures.[24] Indirect consequences include lowered employee engagement and satisfaction, which can lead to higher turnover rates and associated replacement costs. Indeed, a lack of collaboration is a key driver behind millennials job-hopping, with 87% stating that they are unwilling to work without purpose and collaboration.[25]

[24] Fierce, '86 percent of employees cite lack of collaboration for workplace failures', 4 May 2011, available at: https://fierceinc.com/employees-cite-lack-of-collaboration-for-workplace-failures
[25] INQUIRER.net, 'Millennials job hop because of 'lack of purpose, collaboration' in workplace', 10 June 2018, available at: http://newsinfo.inquirer.net/999284/millennials-job-hop-because-of-lack-of-purpose-collaboration-in-workplace

COLLABORATION IN THE BANKING INDUSTRY

Given the importance of collaboration in the workplace, it is unsurprising to see it listed as a core value for many organisations. The financial services industry is no exception, with most major banks listing terms such as "Collaboration", "Partnership", and "Teamwork", as one of their core values or key business principles. Examples include Goldman Sachs' 'We stress teamwork in everything we do' and RBS's 'Working together' (see Figure 12).

FIGURE 12: COLLABORATION AS A VALUE

	COMPANY	PRINCIPLE / VALUE	STATEMENT
1	J.P. MORGAN	Business Principle	*A Great Team and Winning Culture*
2	GOLDMAN SACHS	Business Principle	*We stress teamwork in everything we do*
3	HSBC	Business Principle	*Connected to customers, communities, regulators and each other*
4	BANK OF AMERICA	Corporate Value	*Deliver together AND Trust the team*
5	BARCLAYS	Corporate Value	*Respect: Collaborate proactively with colleagues*
6	CREDIT SUISSE	Corporate Value	*A global community of over 40,000 individuals collaborating across 50 countries*
7	DEUTSCHE BANK	Corporate Value	*Partnership*
8	SOCIÉTÉ GÉNÉRALE	Corporate Value	*Team Spirit*
9	NOMURA	Corporate Value	*Teamwork*
10	RBS	Corporate Value	*Working Together*

Source: Company websites

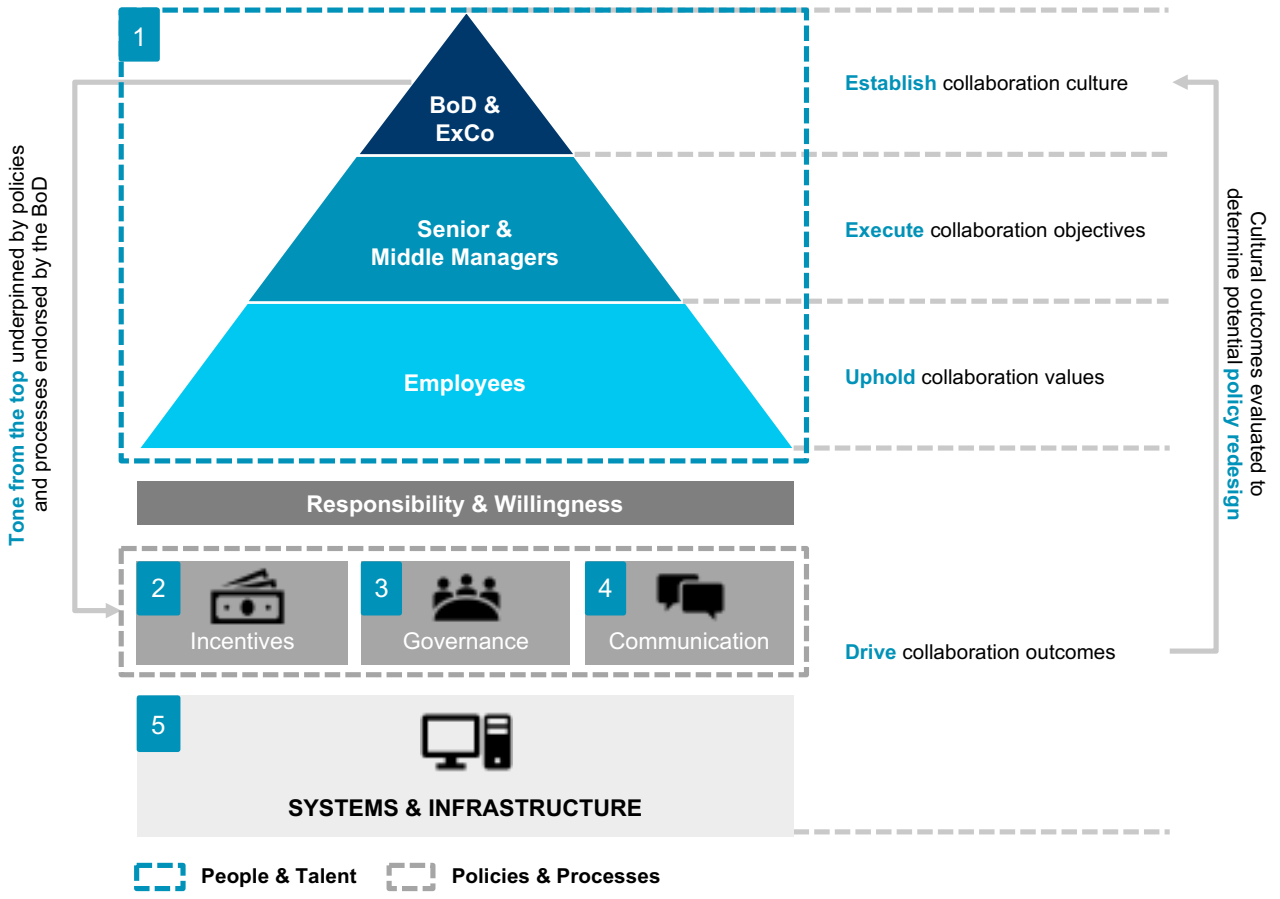
Despite advocating the merits of teamwork in most of their public communications, the internal reality at most banks is very different. A number of major obstacles continue to plague the industry, preventing many firms from creating a truly collaborative culture.

Similar to the approach we have outlined to establish an effective risk culture,[26] a collaborative culture cannot simply be regulated or governed into existence; the company's cultural identity must be created and fostered from within. In particular, the willingness of employees to collaborate with each other is the highest when there is an intrinsic motivation to do so, along with appropriate extrinsic incentives.

[26] For more information on risk culture in the financial services industry, please read our Thought Leadership Report, 'Value at Risk', available at: https://www.quinlanandassociates.com/insights-value-at-risk/

We believe an overhaul of the current cultural ecosystem is necessary to drive collaboration within most banks (see Figure 13). This must start with an appropriate cultural tone being set from the top of the organisation. This "tone from the top" must be endorsed by the board of directors and executive committee, communicated throughout the corporate pyramid, and supported by the institution's policies, systems, and processes. At its core, all programmes to drive collaboration must be designed to drive individual responsibility (i.e. an external influence, where employees feel like they "should" collaborate with each other) and willingness (i.e. an internal influence, where employees "want" to collaborate with each other). Appropriate systems and infrastructure are critical in facilitating this cultural transformation.

FIGURE 13: COLLABORATION CULTURE FRAMEWORK



Source: Quinlan & Associates proprietary framework

1. PEOPLE AND TALENT

Due to their visibility, the board of directors and executive committee must set an appropriate tone for the collaborative culture at the bank. They must "walk the talk" and demonstrate collaborative behaviours within the leadership ranks to encourage similar attitudes across the organisation. This strategy and vision must be supplemented with clear collaboration objectives and KPIs for the bank's senior management team.

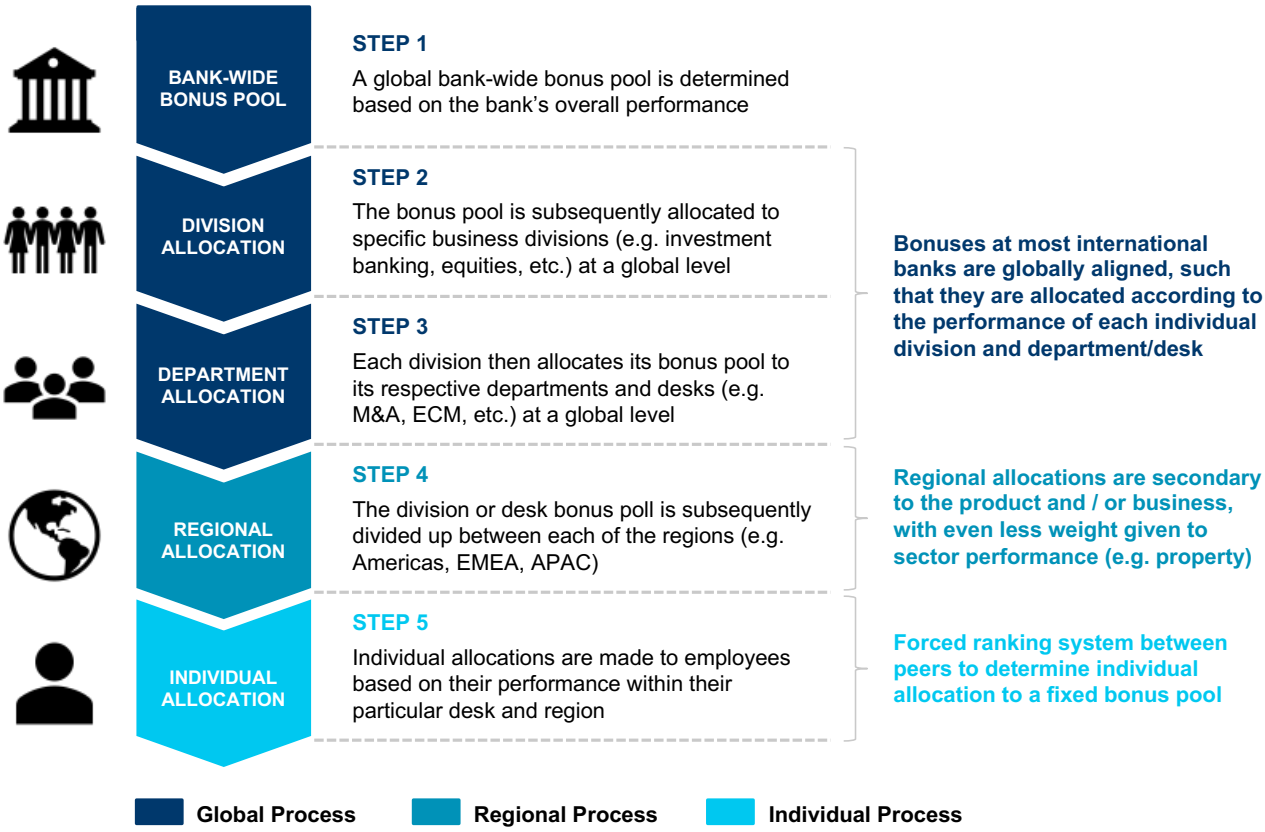
While collaboration is almost always articulated as a strategic objective by the board of most banks, we found that this "tone from the top" regularly fails to make its way to a bank's senior and middle management, who often have little responsibility (or incentive) to promote and execute collaboration targets – that is, if such targets even exist. Consequently, many banks are plagued by an innate silo mentality that is extremely difficult to change.

2. INCENTIVES

The banking industry is notoriously competitive. A key driver of this culture is employee incentive structures, particularly with respect to compensation.

While "bank-wide performance" is always factored into variable compensation schemes, annual bonuses are typically allocated to employees based on their individual and / or team performance (relative to team and / or individual targets). Regional or sector contributions are often a secondary priority (if at all), and little or no recognition is given to cross-business collaboration at most banks. Similarly, within teams, employees need to compete against each other for a larger share of a fixed bonus pool (see Figure 14). All of this can drive protective behaviour, in which employees are reluctant to share information or help each other.

FIGURE 14: TYPICAL BONUS ALLOCATION PROCESS OF GLOBAL BANKS



Source: Quinlan & Associates research and analysis

Similar dynamics are seen with the promotion process at many banks, given extremely limited promotion quotas in more recent years, especially at more senior ranks. Many junior bankers we interviewed feel that individual performance is emphasised and rewarded over teamwork. This is primarily a function of forced peer rankings, where analysts are bucketed into performance "quartiles", which in turn determines the quantum of their annual bonus payment and promotion prospects. Many analysts generally feel insecure about their place in the team and believe there is a lack of genuine collegiality – apart from spending long nights in the office together. Some interviewees felt this was reflective of the broader banking culture, and that voicing any concerns with their managers would be unwelcome and, in any event, futile. As such, instead of focusing on contributing to projects and / or creating value for clients, we often see employees placing a significant emphasis on outperforming each other.

3. GOVERNANCE

Most banks operate under highly siloed structures, where employees are typically aligned to specific departments and / or desks. This not only plays into compensation structures, but it is also reflected in bank governance models.

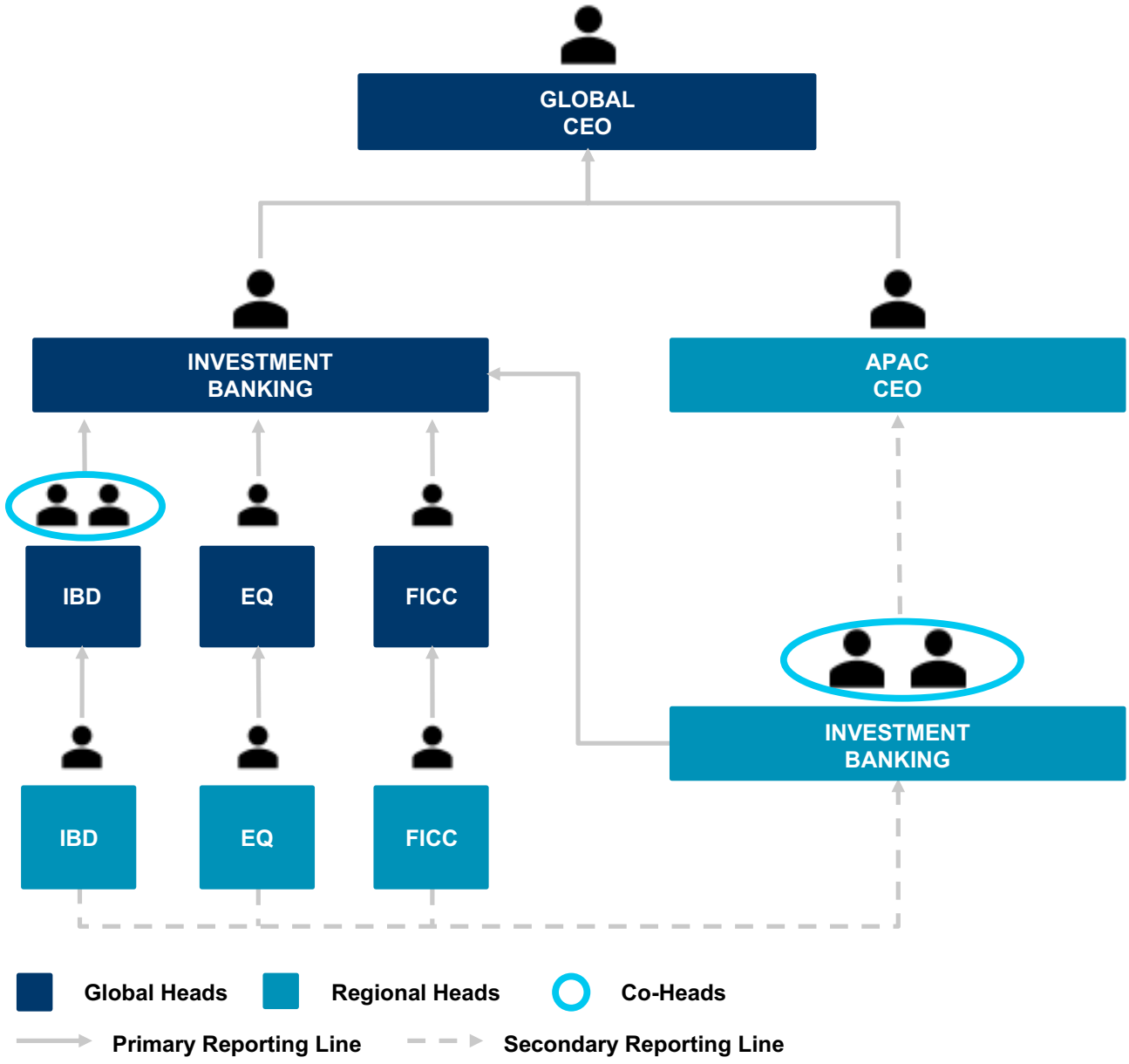
For most firms, reporting lines are dictated by an employee's product vertical (i.e. their division or department), with considerably less weight being given to their geographic or sector alignment. As such, regional department heads often end up with a hard reporting line into their global department heads, with a soft (or dotted) reporting line into their regional managers (see Figure 15). As a result, there is often very limited collaboration between departments or geographies (or even employees covering the same account), given it is a secondary priority to the product lines.

In-fighting among senior individuals has also become relatively common – and even encouraged – at some banks as a means to stimulate the workforce. Much of this is a function of loosely defined scopes of activities and target client universes, resulting in significant overlaps between departments. Competition within departments is even more pronounced in teams that are managed by co-heads, which frequently result in an inefficient and sometimes toxic power struggle. Many of these deliberate organisational constructs designed to promote competition have taken a heavy toll on promoting a more positive team dynamic, particularly in terms of encouraging collaboration and the free exchange of information.

Many bankers we interviewed working under co-head structures said that their business units were highly fragmented, with intense internal competition driving a breakdown in teamwork and collaboration. There was also an implicit understanding that employees would need to align themselves with one of the co-heads, as remaining impartial was often referred to as "no man's land". Such environments are highly counter-productive to collaboration.[27]

[27] Quinlan & Associates, 'Don't Bank On It', January 2017, available at: https://www.quinlanandassociates.com/insights-dont-bank-on-it/

FIGURE 15: TYPICAL REPORTING LINES IN GLOBAL BANKS



Source: Quinlan & Associates research and analysis

4. COMMUNICATION

While global and regional executive / management committees are typically comprised of a diverse group of senior individuals representing different parts of a bank (who are, in turn, supported by generally product-agnostic CEOs), these cross-business committees typically do not exist at the middle management or working level. As a result, inter-divisional communication among senior ranks often fails to cascade down throughout the wider organisation, impacting collaborative mindsets.

Training programmes at many banks are also extremely siloed in nature, focusing on developing the skillsets of their employees within specific business divisions. For example, graduates working in the investment banking department at most of the international firms spend their first weeks at work immersed in structured training programs, typically held in London (for European banks) or New York (for American banks). These programmes focus almost exclusively on bolstering an analyst's knowledge base on key corporate finance modules, including accounting, valuation, and financial modelling, together with some soft-skill training. Very little emphasis is given to educating new analysts on other business divisions, including identifying potential areas for collaboration such as cross-sell opportunities.

The lack of reliable communication systems, including the inability to produce and disseminate cross-sell data / Management Information Systems ("MIS"), also exacerbates this silo mentality. This is because employees are often unable to track (and hence prove) their contributions to other business units for the purposes of potential incentive payments (e.g. investment bankers referring their executives working at the corporations they advise to the private banking team).

5. SYSTEMS

While people, policies, and processes all have an important part to play in driving collaboration, a responsibility and willingness to work together is not enough; systems and infrastructure are critical in facilitating such behaviour. Furthermore, an intuitive collaboration platform with proven productivity-enhancement capabilities may naturally be adopted by employees, enabling an organic transition from a competitive culture to a collaborative one. In addition to a cultural and mindset overhaul, an effective collaboration system needs to be implemented in order to drive an institution-wide collaborative mindset.

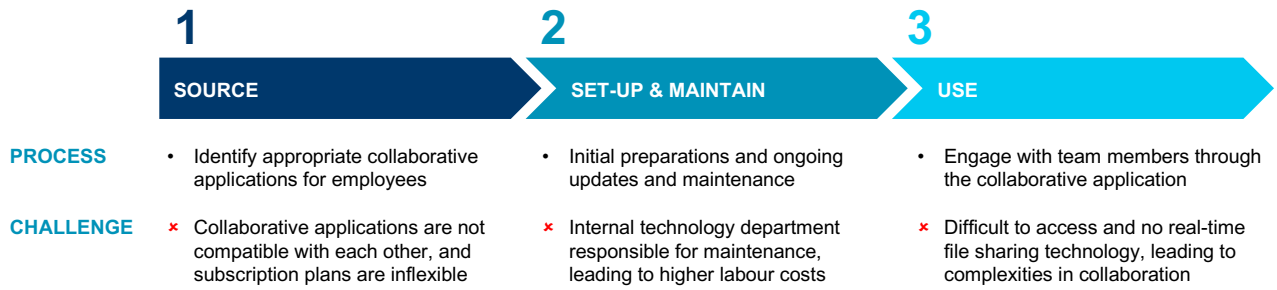
There are numerous applications in the market designed to enhance the collaboration process via the provision of a centralised platform on which employees can communicate with each other, share files and information, and make direct edits to documents. Nonetheless, many of these applications exhibit a number of shortfalls which impede effective collaboration, resulting not only in a reluctance by employees to use them, but also in the delivery of suboptimal outcomes.

SECTION 5
COLLABORATION THROUGH THE CLOUD

CLOUD-BASED COLLABORATION TOOLS

We believe the appropriate implementation of cloud-based collaboration tools has the potential to address shortfalls associated with existing collaboration applications while significantly enhancing current workflow procedures within banks (see Figure 16). Nonetheless, we believe such technology is currently heavily-underutilised by most institutions, likely due to its short history as well as compatibility issues with banks' legacy systems.

FIGURE 16: CLOUD TECHNOLOGY IN COLLABORATION



Source: Quinlan & Associates analysis

1. SOURCE

Most collaboration applications are developed with a specific function in mind, which means they are usually only compatible with specific legacy systems. As a result, banks need to source a host of collaboration applications to cater for different legacy systems running across their various businesses, adding to costs and operational complexity.

Traditional software is also typically sold through subscriptions based on the number of users, which can be inflexible. For example, there may be subscription license for 50, 100, 500, and 1,000 users, meaning that operating lines with 80 users must spend more than required to adopt the software, essentially wasting 20 units of quota.

As banks migrate toward cloud infrastructure (and develop applications on the cloud), new applications can be further standardised and developed to be more compatible, such that all future systems can operate on a single cloud-based collaboration platform. Furthermore, as cloud-based applications are used on a pay-as-you-go basis, there is potential for cloud-based collaboration applications to significantly reduce the cost of all future systems.

2. SET-UP & MAINTAIN

Software needs to be set-up prior to its use. While this is a one-off exercise, the complexity of a bank's technological infrastructure may hinder the process.

IT employees not only need to ensure that the new software application does not destabilise the system, but that it is compatible with other relevant systems and is secure. In addition, applications need to be constantly maintained and regularly updated, which can give rise to bugs and unforeseen issues, especially with respect to compatibility with other systems. As such, significant labour is needed to ensure that software applications run smoothly.

By contrast, cloud-based applications are typically set-up and maintained by the service provider, so the bank's IT department is only responsible for the maintenance of internal systems and can partially rely on the vendor to ensure smooth operations of the collaboration platform. As a result, the bank can focus its efforts on optimising or standardising internal systems for maximising productivity.

3. USE

While IT departments may be able to provide an environment on which employees can collaborate, staff may find it difficult to work together on the platform due to inherent restrictions of the technological infrastructure. Key challenges include: (1) a lack of access; and (2) a lack of synchronisation.

Employees sometimes lose access to collaboration platforms, especially when they work remotely. By being kept out of the loop on the progress of a project (including document updates and / or changes), misalignment can ensue, impacting productivity. In addition, because files are not synchronised in real-time, edits need to be shared via e-mail or other file-sharing applications. Numerous banking employees we spoke to, especially those working in large project teams, commented on their email inbox being filled with countless different versions of the same file(s), from "Project – Version 1" to "Project – Version 10 Final", making it challenging for employees to work with each other seamlessly.

Most major banks utilise various forms of collaboration software, such as customer relationship management ("CRM") tools, and tend to use different systems across various business lines. As a result, there is often no golden source of customer information for clients who straddle multiple touchpoints at the bank. This is exacerbated by incompatibility issues associated with banks' many legacy systems. Some legacy CRM platforms also lack mobile or social media capabilities, severely impacting communication outside of office hours.

Because they can be accessed through the internet, cloud-based collaboration applications require no further installation of software. As files are stored on the cloud, all employees have access to the "master copy" of project files, and all edits or changes are updated immediately and synchronised in real-time. Moreover, all changes are shared and accessed by team members instantaneously, as if all members are working on the same file together at the same time, completely removing the need for constant file sharing with other team members after changes are made. This substantially decreases the complexity of collaboration and improves the user experience.

CONSIDERATIONS FOR CLOUD-BASED COLLABORATION APPLICATIONS

While some banks have already adopted a number of cloud-based collaboration applications currently available in the market, including Office 365 (Microsoft) and Google Docs, Google Sheets, and Google Slides (Google), these applications are typically task-specific and heavily siloed in nature (see Figure 17).

FIGURE 17: COLLABORATION TOOLS EXAMPLES

FUNCTION	G Suite	slack	Dropbox	Office 365	Wrike	HubSpot
COMMUNICATION	✓	✓	✗	✗	✗	✗
FILE STORAGE	✓	✓	✓	✓	✗	✗
FILE SHARING	✓	✓	✓	✓	✗	✗
FILE EDITING	✓	✗	✓	✓	✗	✗
PROJECT MANAGEMENT	✗	✗	✗	✗	✓	✗
CLIENT MANAGEMENT	✗	✗	✗	✗	✗	✓

No single application providing all functions

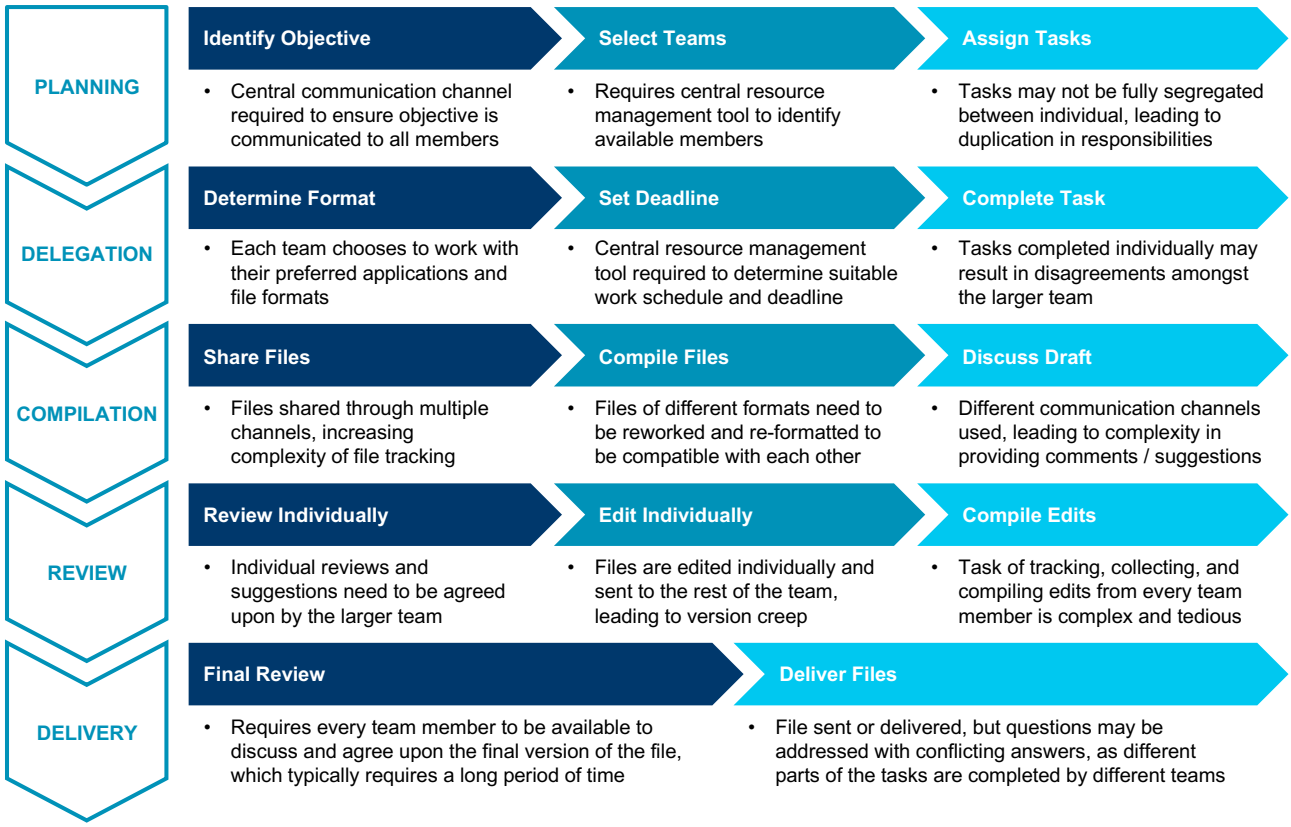
Source: Company websites, Quinlan & Associates analysis

Most collaboration applications are designed and optimised for their core functions. For example, HubSpot was developed to help companies manage customer relationships, while Slack is known for its communication capabilities. Some applications are also being developed to expand their functionalities, such as Dropbox, which now offers some file editing tools in addition to its core service of file storage and sharing.

One of the more extensive collaboration platforms is Google Drive, offering communication tools, file storage and sharing, and real-time file editing tools. Nonetheless, none of these collaboration tools currently offer a comprehensive set of functionalities. As a result, some have opted to integrate their capabilities with other platforms – for example, Wrike can be integrated with Office 365, Dropbox, and Google Drive.

Due to the specialised nature of current collaboration tools, banks cannot simply adopt one application for all operations. Instead, one or more collaboration applications is chosen for each specific task or function. As a result, the current collaboration process is relatively complex and requires significant effort in creating a final deliverable (see Figure 18).

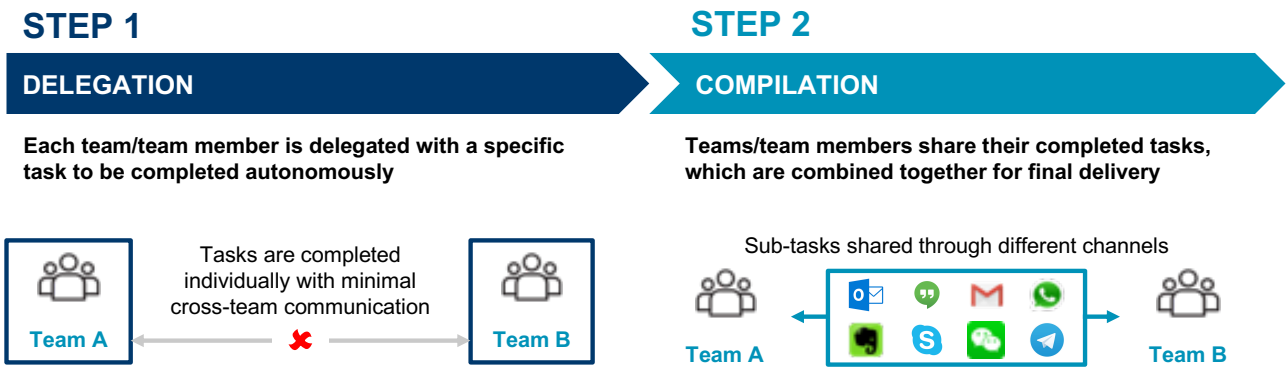
FIGURE 18: COLLABORATION PROCESS



Source: Quinlan & Associates research and analysis

In essence, because of the lack of a central collaboration platform on which all functions can be carried out, each collaboration project requires the team to utilise a mix of different applications to co-ordinate, communicate, and contribute to the project, during each stage from planning to delivery. The complexities are particularly relevant and represent significant challenges during the stages of delegation and compilation (see Figure 19).

FIGURE 19: DELEGATION AND COMPILATION



KEY ISSUES

1. Difficulties in defining independent tasks
2. Lack of communication
3. Lack of real-time updates or edits

RESULTS

1. Overlap of responsibilities and inability to collaborate on a larger scale
2. Potential misunderstandings and disagreements during compilation
3. Repeated work and wasted resources

KEY ISSUES

1. Files shared through third-party applications
2. Files edited with different applications
3. Individual reviews and edits of drafts

RESULTS

1. Data privacy concerns and reliance on third-party's cybersecurity measures
2. Complexity and compatibility issues
3. Potential disagreements and occurrence of version creep

Source: Quinlan & Associates research and analysis

1. DELEGATION

OVERVIEW

When a major project commences, the end-to-end project lifecycle is typically broken down into a mix of distinct workstreams and individual tasks are delegated to teams (and individual team members) to be completed. Each team will then employ their own collaboration tools to work on their tasks. While delegating discreet tasks to specialised teams enhances the overall productivity of the company, there are several issues caused by this model.

KEY ISSUES

Not all tasks can be broken down into fully independent sub-tasks, especially in the banking industry, where operations are complex and frequently spread across several products / functions, geographies and / or client segments. Sub-tasks may also depend on the progress or result of other sub-tasks, leading to an overlap of responsibilities. The complexity in defining independent sub-tasks increases with the size of the project – in other words, this collaboration model becomes increasingly inefficient as the project team grows.

Furthermore, due to the siloed nature of the individual tasks, there is typically little communication both within and between teams, leading to potential misunderstandings when inputs need to be compiled. And as tasks are typically only shared once they are completed, there is often no real-time understanding around the status of the overall project workflow, which could lead to a repetition of work and wasted resources.

2. COMPILATION

OVERVIEW

Following the completion of individual tasks, teams will come together and compile their work in order to produce the final deliverable. This is typically done by sharing individually completed files with each other via a host of communication or file sharing tools, such as e-mail, instant messaging tools, and online storage applications. After all sub-tasks are compiled, each team will then review and continue editing the draft until the final deliverable is approved and signed off on by every team. Again, there are a number of issues with this compilation process using current technological applications.

KEY ISSUES

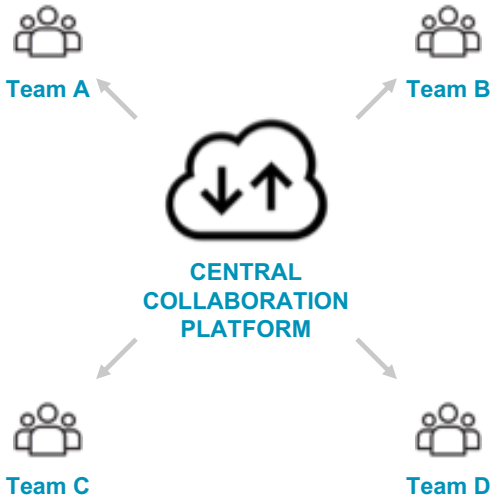
Files may be shared through third-party applications, which may lead to security or privacy concerns. Banks have to monitor the cybersecurity measures and review data privacy or protection policies of each application individually, increasing operational costs. In addition, the files may be edited using different applications, or different versions of the same application. This leads to the possibility of incompatibility, as certain applications may not be able to view or edit some files. For example, when a Word 2016 file (i.e. a .docx file) is saved in a Word 97-2003 format (i.e. as a .doc file), some features may be lost or behave differently. This means that all teams must not only be provided with all the necessary applications, but they must also have the same version of each application, increasing subscription or software costs.

Finally, document reviews typically involve each team editing draft documents on their own and subsequently sharing changes with the wider group. This can lead to disagreements between teams if there is insufficient communication during the editing process. Moreover, it increases the possibility of “version creep”, where teams are working on different versions of a document. We found this to be an extremely common occurrence within large project teams.

INTEGRATION OF COLLABORATION PLATFORMS

While incompatibility issues between applications are unlikely to be fully resolved in the short term, we believe further integration of collaboration and legacy systems via a centralised cloud platform can partially address the problems associated with the current collaboration model. Through the provision of a holistic, end-to-end collaboration platform on which applications and legacy systems can operate, employees can communicate with each other and work on all types of tasks and file formats within a single environment (see Figure 20).

FIGURE 20: PROPOSED COLLABORATION PROCESS



A centralised platform on which all tasks can be completed, stored, and shared

KEY FEATURES

1. Single communication and file sharing platform
2. Only one version of each file stored, which is updated in real-time
3. Tasks need not be fully segregated and siloed
4. Data and information can be stored on a single, internal server

POTENTIAL BENEFITS

1. Easier communications between teams reduces disagreements and misunderstandings
2. Elimination of redundant work and version creep
3. Collaboration model can be scaled upwards for projects requiring larger teams
4. Elimination of reliance on third-party around security and privacy policies

Source: Quinlan & Associates research and analysis

By fully migrating all collaboration applications onto a cloud-based platform, all files can be stored, shared, viewed, and edited in real-time in a single environment. As such, all team members have access to and can edit a single version of every file on the cloud platform on a real-time basis.

As all team members have access to a single, most updated version of every file, any repeated or overlapping work is eliminated. In addition, there is no need to wait for other teams to finish and share their tasks, as all progress is reflected immediately on the cloud. Furthermore, as teams are working on the same documents in the same environment, tasks need not be as strictly defined, allowing for more efficient scaling on larger projects.

By integrating communication tools onto one platform, conversations (including commenting history) can also be viewed by all team members, enhancing dialogue and encouraging the sharing of feedback and new ideas. To reduce the risk of cybersecurity breaches and provide a higher level of data control and governance, banks can opt to store files on a private cloud.

USE CASES

While we understand that cloud-based collaboration technology is largely utilised by back office teams, especially IT departments (e.g. developers, architects) for infrastructure management and application development purposes, we believe all employees, from front to back office, can benefit from the collaboration capabilities provided by cloud-based technology (see Figure 21).

FIGURE 21: EXAMPLE USE CASES IN BANKS

- Complete understanding of client preferences enhances application design
- Full knowledge of trade orders facilitates best execution procedures
- Single, shared client database for more efficient onboarding procedures
- Involvement in product development procedures to ensure compliance
- Information dissemination for product development and cross-selling
- External collaboration with other banks for underwriting syndications

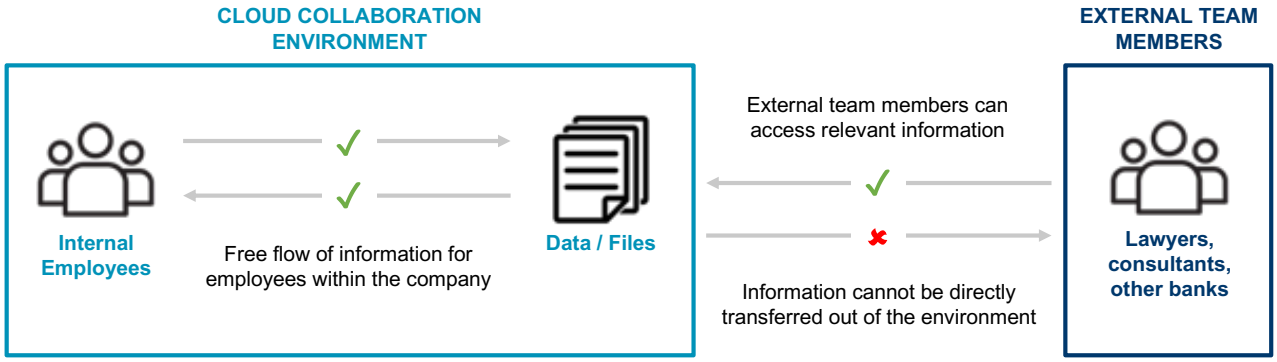
Source: Quinlan & Associates research and analysis

By working together on a single platform where all relevant information can be viewed (according to pre-defined access rights for security purposes), employees can rapidly enhance their knowledge of stakeholders within or across teams, driving productivity and streamlining operations.

In the back office, by gaining real-time insights on the full spectrum of client preferences across all front office communication channels, better client servicing applications or platforms can be designed to enhance customer experience. For the middle office, by accessing a single, shared client database, compliance teams can eliminate any redundant work during the onboarding process. Furthermore, direct involvement in product development can facilitate improved risk management and compliance procedures. Finally, in the front office, the instantaneous sharing of information or sales opportunities across product or client teams can significantly improve cross-sell and up-sell potential.

Finally, for larger projects which require collaboration with external advisors (e.g. lawyers, consultants) or other banks and / or financial institutions (e.g. syndicated lending or underwriting), a separate collaboration environment can be created where relevant information can be shared and stored in real time (see Figure 22).

FIGURE 22: COLLABORATION WITH EXTERNAL TEAMS



Source: Quinlan & Associates research and analysis

By establishing a ringfenced collaboration environment in which only relevant data and files are stored, companies can provide external team members with the appropriate resources for working together without jeopardising their own confidential information. Internal employees have full access and control over the information stored in the environment, enabling them to manage access and sharing rights.

On the other hand, external team members only have access to relevant files, but cannot directly transfer them out of the environment. This offers team members from different organisations the ability to work together efficiently while ensuring that confidential or sensitive information remains warehoused on site.

SUPPORTING PILLARS OF CULTURAL CHANGE

In addition to enabling the collaboration process, these collaboration platforms have the potential to enhance the cultural change process via supporting the three key pillars of the collaboration culture framework (i.e. incentives, governance, and communication).

In order to fairly and effectively incorporate collaboration KPIs into the incentive structure, employees' collaborative contributions need to be collected, quantified, and analysed. With a central collaboration platform in place, each employee's collaborative engagement can be monitored and tracked, providing a standardised measure for KPI evaluation.

While adjusting an organisation's governance structure in the real world in complex, this task is significantly simplified in the digital world. This is due to the fact that there are no geographical or functional restrictions on a virtual platform, and that all management structures and reporting lines can easily be changed and adapted according to the needs of each project.

Finally, through the provision of a centralised communication and information sharing platform, firm-wide communication is significantly simplified. By encouraging employees to communicate with each other on this centralised collaborative platform, all team members have access to relevant communication records and a single source of information, eliminating complexities such as miscommunications and multiple versions of the same file.

SECTION 6
CASE STUDY – PICOWORK

OVERVIEW

We had the opportunity to interview the team at Picowork, a Hong Kong-based cloud collaboration platform provider which enables employees to collaborate internally (with their colleagues) and externally (with their clients or other key stakeholders).

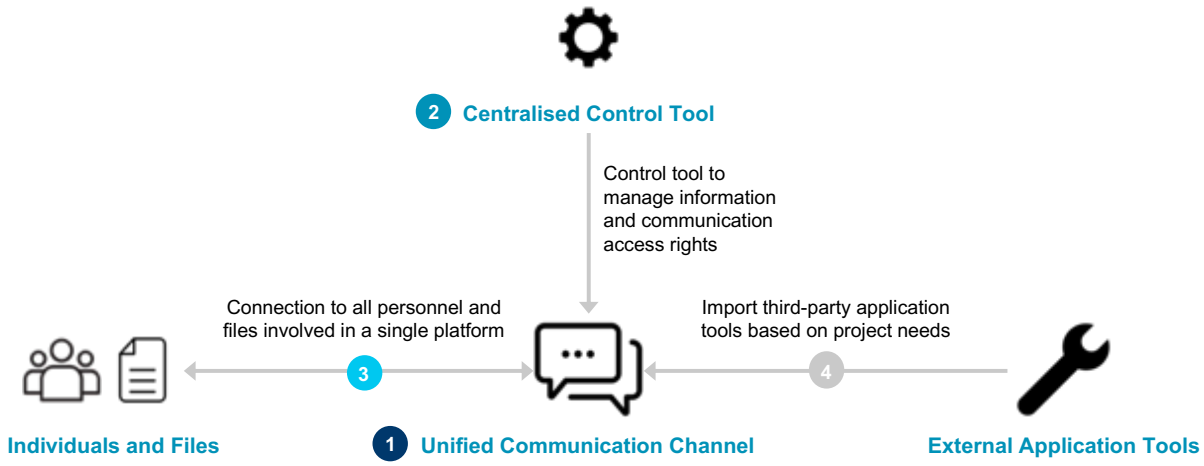
Picowork was founded in 2010, and has since expanded in the region, with offices in Hong Kong and Shanghai. The team at Picowork has developed a proprietary Collaborative Cloud Operating System ("CCOS") and Collaborative Cloud Computer ("CCC"), designed to facilitate a seamless, interconnected working environment through the cloud.

COMMUNICATION AND COLLABORATION

Current communication and collaboration applications exhibit a number of shortfalls, such as the lack of interaction between different users, the lack of connection to files or application tools, and the need for integration for communication between different systems or applications.

Understanding these limitations, Picowork identified four key requirements for an effective collaboration tool, being: (1) a unified communication channel; (2) centralised communication and content control tools; (3) connections to the individuals and files involved; and (4) ability to import additional application tools or content (see Figure 23).

FIGURE 23: REQUIREMENTS FOR AN EFFECTIVE COLLABORATION TOOL



Source: Picowork, Quinlan & Associates analysis

Picowork designed the CCOS platform with these four key features in mind, in order to enhance the current communication and collaboration process. In addition to the CCOS, Picowork also offers a "buy-and-play" CCC, a computer or server on which the CCOS is embedded.

KEY PRODUCT FEATURES

Picowork's key product features can be classified under three main categories: (1) technology, (2) procurement, and (3) use (see Figure 24).

FIGURE 24: KEY PRODUCT FEATURES

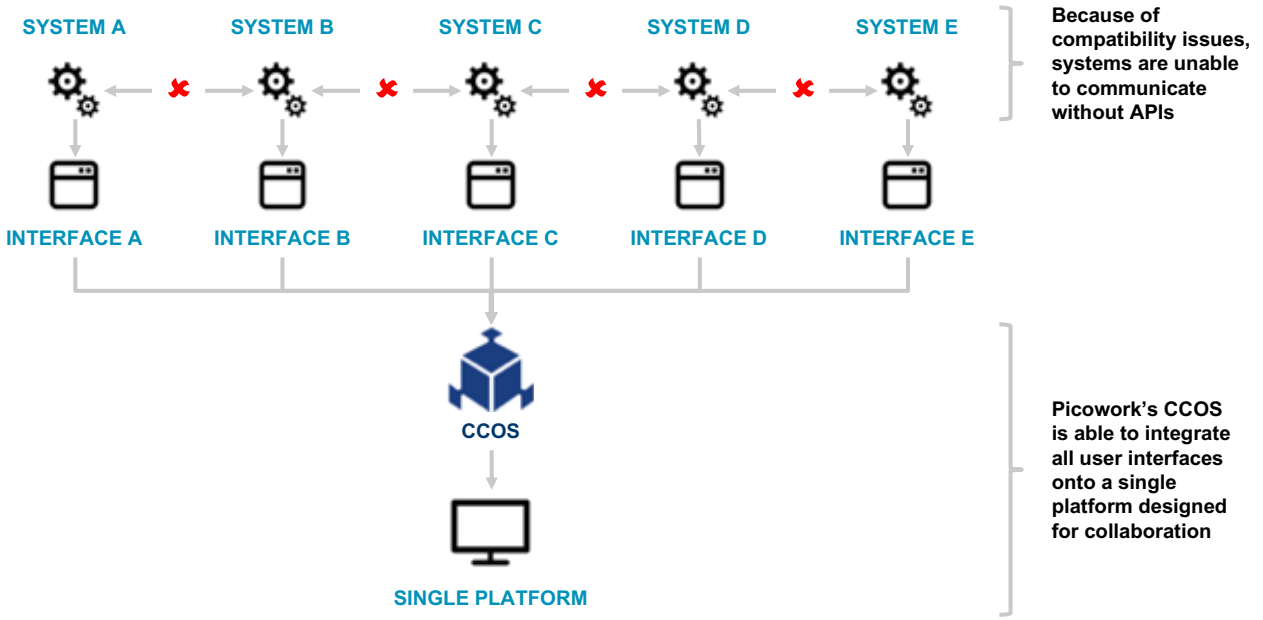
Source: Picowork, Quinlan & Associates analysis

TECHNOLOGY

Recognising that systems developed by different vendors are incompatible with each other, and the fact that large collaboration projects require the use of multiple applications and channels, Picowork wanted to develop a single platform on which all collaborative work could be conducted.

In order for certain systems to communicate with each other, an application programming interface ("API") may be required. This can be a tedious process and requires support from system developers. Understanding the difficulty and cost in integrating back-end systems, Picowork opted for a paradigm shift and instead focused on the integration of the front-end user interface ("UI") (see Figure 25).

FIGURE 25: SINGLE COLLABORATION PLATFORM



Source: Picowork, Quinlan & Associates analysis

The CCOS is a software solution that can be deployed on a company's existing hardware or virtual infrastructure. In fact, Picowork stated that the CCOS can be deployed on any technology infrastructure, including private clouds (both privately managed or outsourced), public clouds, and on-premises infrastructures. Furthermore, the CCOS platform is compatible with all application interfaces, allowing for their aggregation and integration onto a single web-based platform. To achieve Picowork's four requirements for an effective collaboration tool, CCOS was created to be compatible and interoperable with all legacy systems, third-party applications, and web-based resources, enabling easy set-up and smooth integration.

In addition, as the CCOS can be deployed in a company's private cloud or data centre, this provides the company with complete privacy and improved data governance. This is a particularly useful feature for companies that handle a large amount of customer information, including banks.

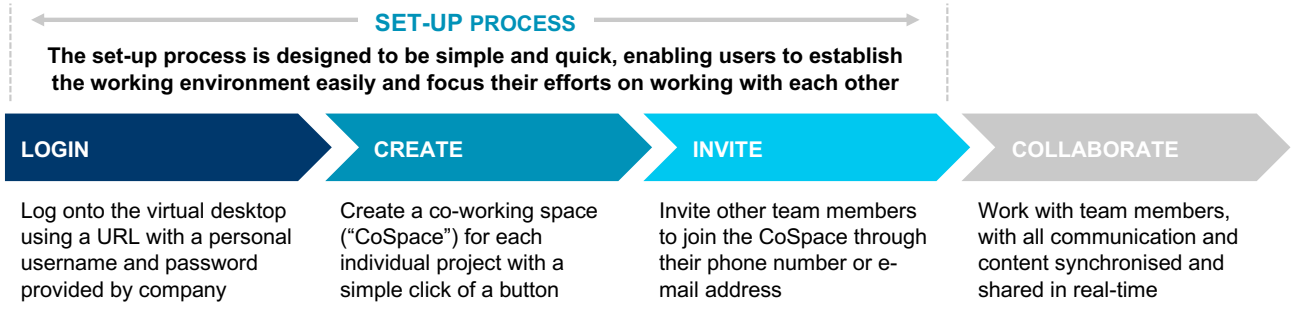
PROCUREMENT

Picowork's pricing structure is simple and flexible, charging companies a monthly subscription fee per user. With the flexible nature of cloud-based applications, companies can choose the most appropriate subscription plan and leverage the collaboration platform in a cost-effective manner.

USE

The CCOS is easy and intuitive to both set-up and use, allowing less technologically-savvy employees to navigate the platform with relative ease (see Figure 26).

FIGURE 26: CCOS USER JOURNEY



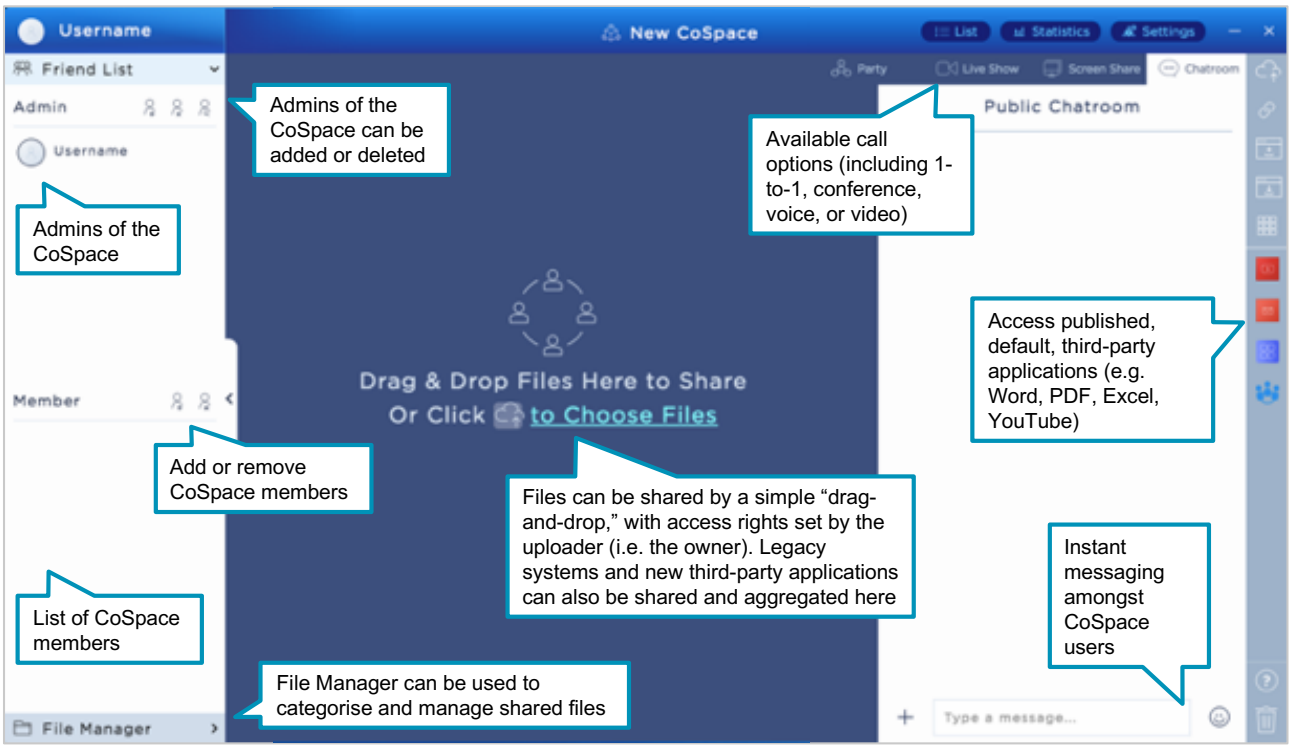
Source: Picowork, Quinlan & Associates analysis

The set-up process is designed to be extremely simple for users. A URL is used to access the CCOS, with a personal username and password being used to log in to the system. From there, a user can create a co-working space ("CoSpace") for each project. As CoSpaces are distinct and separated from each other, the user has greater levels of control around data and information sharing.

Invitations to other members of the group can be sent through e-mails or text messages. As the CCOS platform can be accessed through the internet, invitations can be sent to anyone, including those that do not have their own CCOS. This is a special feature which allows a company's employees to work seamlessly with external stakeholders, such as their advisors and their clients.

The platform itself is designed to be intuitive and easy to use, with users able to access familiar legacy applications through a single user interface (see Figure 27).

FIGURE 27: COSPACE INTERFACE



Source: Picowork, Quinlan & Associates analysis

The CoSpace provides a host of communication tools, including instant messaging, video calls, and conference calls. Files can be shared through a simple "drag-and-drop", and the uploader of the file can amend access rights (including the ability to download the file) for different users. This feature is particularly important when working with third parties and addressing compliance concerns relating to data privacy, given files can be viewed without the need for them to be transferred.

Any web-based applications of software available through the intranet can also be aggregated, published onto the platform, and accessed from the tool bar, without the need for changing existing codes. These applications can be launched in the CoSpace, enabling users to work on familiar legacy systems together using one UI. All files are continuously updated and synchronised. Together with native communication tools, the CCOS allows teams to remotely discuss and edit files in real-time.

Through the provision of a centralised platform on which all files can be stored, shared, and edited, the complexity of collaboration is significantly reduced. The CCOS can also easily be accessed through the internet on any devices, including laptops and smartphones, via a URL.

USE CASES

Picowork's product has already established several successful use cases.

1. HEALTHCARE

One of Picowork's key clients is a major China-based medical foundation.

Through the CCOS, patients located in even the most remote parts of China have access to the services of doctors with more sophisticated expertise who are located in tier-1 cities. Doctors from different hospitals can also collaborate by sharing a patient's data without transferring any patient files.

For example, if doctors at a less advanced hospital do not have the relevant knowledge or expertise to treat a patient, a CoSpace can be created specifically for the patient, with all relevant files uploaded to the platform. Doctors with relevant expertise can then be invited to join the CoSpace, gaining access to the information without the need to transfer any files. In this way, external doctors can collaborate directly with doctors at the patient's original hospital to provide the most appropriate treatment plan, while the patient's sensitive information remains stored within the infrastructure of the hospital. This enables better diagnosis and treatment for the patient in a compliant and cost-effective manner.

2. RETAIL

Another client of Picowork is a major international jewellery chain.

Through the CCOS, designers can share jewellery concepts and designs with clients, receiving feedback and making edits in real-time, improving the customer experience. Through the provision of direct communication channels with real-time editing capabilities, designers can better understand the customers' ideal products and can design their jewellery accordingly.

Picowork also stated that the collaboration platform enabled the client to expand its service offering, broadcast announcements and notifications, and enhance internal communication, leading to reductions in the need for physical store branches and lower communication costs. Through leveraging its native communication tools, employees in Hong Kong and China were also able to communicate with each other in a seamless fashion via the CCOS. This was able to address specific communication barriers linked to certain messaging applications being widely used in Hong Kong that are banned in China (e.g. WhatsApp).

ADDRESSING THE PILLARS OF COLLABORATION THROUGH THE CCOS

Picowork has stated that its clients have successfully implemented the CCOS to enhance the three pillars of collaboration culture: (1) incentives; (2) governance; and (3) communication.

1. INCENTIVES

In the case of the jewellery retailer, the CCOS helped the retailer collect various user statistics, including project participation and overall contribution levels on the collaboration platform. Using this data, the client was able to generate a "co-operative contribution ranking" for each employee, indicating their willingness to collaborate and contribute to team projects. Through the collection of use of data from the CCOS platform, the client was able to incorporate collaboration KPIs into its decision-making process around employee incentives.

2. GOVERNANCE

As a multinational organisation, each project conducted by Picowork's client employed a different project management structure to maximise efficiency and productivity. Treating each CoSpace as a separate organisational sandbox, the virtual management structure and reporting lines could be adjusted and adapted to the project's specific requirements, enabling teams to be highly flexible in designing and implementing different project governance structures.

3. COMMUNICATION

Internal communications typically involve a significant amount of sensitive or confidential information. Using third-party communication software or telecommunications solutions are typically costly and involve surrendering control of such information to the service provider. As the CCOS can be deployed on an on-premises infrastructure or in-house data centre, the client was able to communicate through an inexpensive channel while retaining control of all communication data and information. This feature has been particularly useful Picowork's healthcare client, given the importance of protecting personal medical data.

FUTURE PLANS

We understand that Picowork is focusing its initial expansion efforts on the Greater China market and is actively exploring opportunities across a number of industries, including retail, professional services, financial services, and real estate. In addition, the company is seeking partnerships with government entities and will be driving a retail version of the CCC.

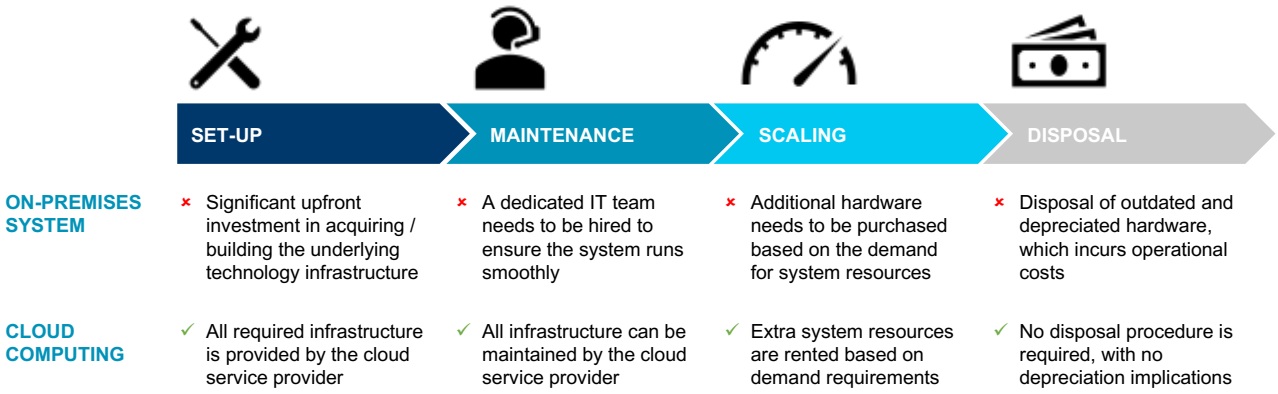
Picowork aims to establish a smart, collaborative society through the interaction between the government, enterprises, and households via their collaboration platform.

SECTION 7
CONCLUSION

TECHNOLOGY COST SAVINGS

Cloud services have the potential to significantly reduce the cost of a bank's technology system throughout its entire useful life, from set up through to disposal (see Figure 28).

FIGURE 28: USEFUL LIFE OF TECHNOLOGY SYSTEM



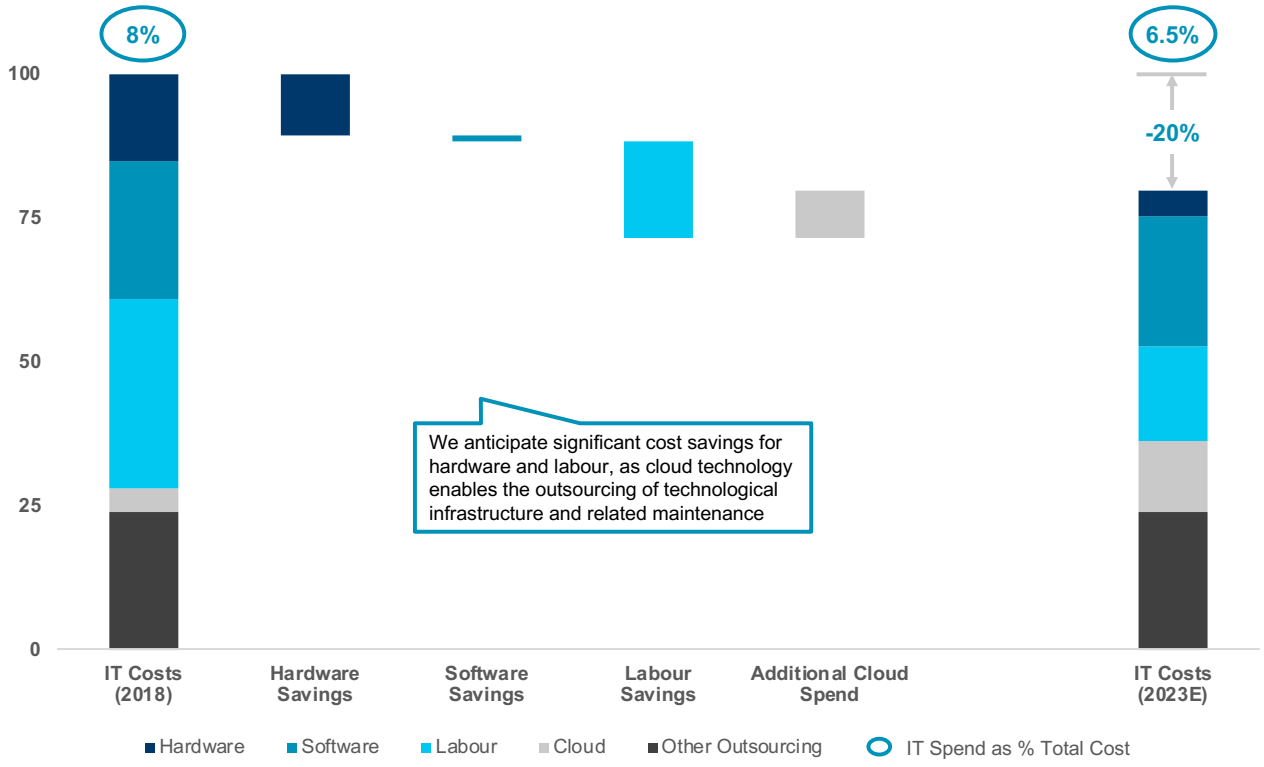
Source: Quinlan & Associates analysis

A traditional, on-premises model requires banks to make significant upfront hardware investments to provide the underlying infrastructure for the IT system. Banks also need to hire a permanent IT team for ongoing system maintenance. Moreover, if operations expand beyond the capacity of available hardware, investment in additional hardware is needed to acquire the necessarily system resources. And if operations subsequently slow down, extra capacity remains unused, leading to system underutilisation. Finally, the hardware will inevitably become obsolete, with banks incurring costs from asset depreciation and the disposal process itself.

By contrast, under a cloud computing model, the underlying hardware and infrastructure is provided and maintained by the service provider, significantly reducing upfront investments and ongoing maintenance costs. The cloud service provider typically has a dedicated team to support the operations of – and resolve any queries relating to – the system, allowing the bank to hire a smaller internal IT team. Public clouds also offer a virtually unlimited amount of system resources that can be rented on a pay-as-you-go basis, enabling cheap upscaling and addressing the issue of under-utilisation during down times. There is no need for physical disposal of hardware; the bank can simply stop renting extra system resources.

By outsourcing the technological infrastructure (and large segments of its maintenance) to a cloud service provider, banks can save a significant portion of their technology spending (see Figure 29).

FIGURE 29: TECHNOLOGY COST SAVINGS (2018-23E), %



Source: Gartner, Quinlan & Associates analysis

We estimate that the top 15 global banks allocate, on average, between 7-9% of their total costs to technology spend (though this can range from as low as 3% to as high as 15%, depending on the specific firm). According to analyses from market intelligence firm Gartner, 15% of this is spent on hardware, 24% on software, 33% on labour, 4% on cloud infrastructure, and 24% on other outsourcing.[28]

As explained earlier, outsourcing the technological infrastructure and its maintenance to a cloud service provider can significantly reduce technology-related spending. The bulk of these cost savings will come from reduced spending on hardware and labour. Based on our conversations with industry professionals and our proprietary analysis, we believe banks can reduce their current hardware costs by 70% and labour costs by 50%. Furthermore, by migrating to the cloud and eliminating redundant software (or by further standardising / integrating existing software), 5% of software costs can potentially be eliminated.

[28] CenterState Bank, 'Where Banks Are Spending Their Technology Dollars', 3 January 2018, available at: https://csbcorrespondent.com/blog/where-banks-are-spending-their-technology-dollars

Factoring in our expectation that the average banks' cloud expenditure increases in line with our forecasts for the industry over the next five years (i.e. a CAGR of 25%), we estimate overall IT costs have the potential to be reduced by ~20% from current levels by 2023. This would translate to a ~1.6% reduction in total costs for most global banks.

COLLABORATION IMPLICATIONS

By encouraging a cultural change to drive employees from a siloed mindset to one where team members actively work with each other, and providing the appropriate cloud-based collaborative tools to do so, we believe banks will experience higher levels of productivity (see Figure 30).

FIGURE 30: COLLABORATION IN THE CLIENT SERVICING VALUE CHAIN

	CLIENT IDENTIFICATION	CLIENT ONBOARDING	PROUCT DEVELOPMENT	SALES	EXECUTION	MONITORING & REPORTING
Process	• Identify suitable clients and deliver targeted marketing material	• Review clients' documents and understand the clients' profile	• Understand clients' needs and develop tailored products and services	• Sales through campaigns and relationship managers	• Take orders from clients and complete with best execution in mind	• Monitor and review performance, and identify new sales opportunities
Collaboration	• Single, shared client identification procedure, with targeted marketing and messaging, improving acquisition rates	• Single, shared client onboarding procedure, eliminating any repetition in document review or profiling	• Seamless approval process and sharing provides complete view of client's profile, enabling the development of tailored products	• Cross-selling enabled through understanding all needs of the client and real-time collaboration around sales opportunities	• Transparent communication between teams leads to best execution and higher operational efficiency	• Deeper understanding of client can be shared to tailor and enhance customer experience for future opportunities
Revenue Uplift	✓	-	✓	✓	✓	✓
Cost Reduction	✓	✓	-	-	-	-

Acquisition Monetisation Maintenance

Source: Quinlan & Associates analysis

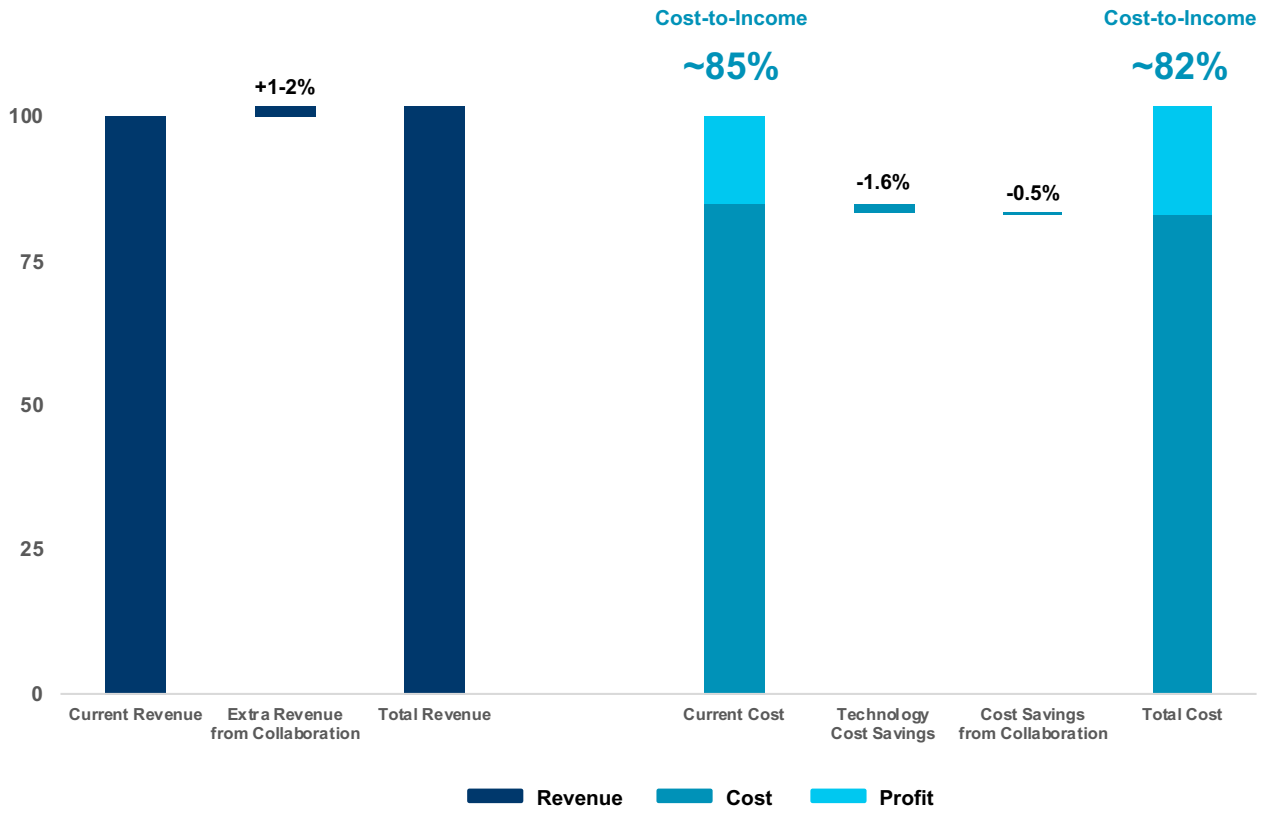
Collaboration improves banks' productivity in two key ways: (1) elimination of duplicative processes and (2) better understanding of clients' needs. By sharing all information and documents, labour-intensive processes such as client identification, onboarding, and profiling can be standardised and streamlined, and labour costs can be cut down. In addition, by sharing information and expertise in a seamless fashion, employees gain a better understanding of the clients' specific needs, enabling the development of tailored products, increasing product uptake (including cross-selling) and hence providing revenue potential.

We anticipate a revenue uplift of 1-2% (from improved opportunity identification and cross- / up-selling) and a further 0.5% reduction in total costs (from streamlining processes and improving efficiency across the bank, including expediting digital transformation efforts) by leveraging cloud-based collaboration tools.

PROFITABILITY IMPLICATIONS

Combining the revenue and cost implications from cloud technology and cloud-based collaboration applications, we see potential for cost-to-income ratios of leading global banks to fall from ~85% at present to ~82% (see Figure 31).

FIGURE 31: PROFITABILITY IMPLICATIONS, %



Note that the cost-to-income ratio is based on the average of the top 15 bulge bracket banks, and the extra revenue and cost savings are anticipated results for banks that appropriately adopt cloud technology, a change in collaborative mindset, and cloud-based collaboration applications, and are not actual performance results
Source: Bank annual reports, Quinlan & Associates analysis

Nonetheless, this increase in profits cannot be driven by technology alone. As highlighted in Section 2, cultural change is needed, along with appropriate policies and processes. In addition to utilising the most relevant collaboration systems and tools, banks need to design and implement supporting incentive policies, governance structures, and communication strategies, in order to fully reap the benefits of collaboration.

While we recognise that a technological overhaul and a substantial cultural shift require significant upfront investments and time, we believe banking on the cloud is not only vital for firms looking to supercharge their digitalisation efforts, but also fundamentally transform their collaborative culture.

SECTION 8
HOW CAN WE HELP?

Our consultants have worked with a number of regional and global banks / financial institutions on implementing a shift in the collaborative mindset and procedures. Our experience is further enhanced by our expertise in areas such as talent, culture, and FinTech.

CULTURAL CHANGE

As outlined in Section 3, suitable incentive policies, governance structure, and communication strategies are required for a successful change towards the desired collaborative mindset. Examples of what we can do include:

- Analyse incentive structures to identify policies that support collaborative behaviour, and subsequently designing appropriate policies (and suitable KPIs) to drive collaborative outcomes
- Review cross-business governance structures to determine oversight and accountability framework for collaboration across the entire organisation
- Develop an effective communication strategy, from the top of the corporate pyramid to the bottom, to drive bank-wide engagement and augment employee mindsets

TECHNOLOGY IMPLEMENTATION

Collaboration is encouraged through a change in mindset, but is enabled via the adoption of the appropriate systems and applications. Examples of what we can do include:

- Review the current technology infrastructure to identify key pain points and bottlenecks, and determine areas most appropriate for upgrading and / or cloud migration
- Evaluate and select suitable vendor and solutions to be adopted, based on the institutions' own capabilities, technological infrastructure, and constraints
- Design implementation strategy and roadmap to migrate the current technology system onto the cloud, and adopt appropriate systems / applications to enhance the existing infrastructure

REGULATION AND COMPLIANCE

With cybersecurity and data privacy remaining key issues in the adoption of third-party solutions and cloud technology, banks need to take regulations and compliance into account when designing their migration strategy. Examples of what we can do include:

- Conduct regulatory due diligence to identify actions / strategies that are allowed or restricted, helping the bank understand the flexibility in adopting cloud technology
- Benchmark operations against industry best practices to identify operations that are suitable to adopt new technology and those that should wait for further regulatory clarification
- Design a technology implementation / migration strategy compliant with local / international regulations, especially with respect to data storage, transfer, and sharing requirements

QUINLAN
&ASSOCIATES

STRATEGY WITH A DIFFERENCE

ABOUT US

Quinlan & Associates is a leading independent strategy consulting firm specialising in the financial services industry.

We are the first firm to offer end-to-end strategy consulting services. From strategy formulation to execution, to ongoing reporting and communications, we translate cutting-edge advice into commercially executable solutions.

With our team of top-tier financial services and strategy consulting professionals and our global network of alliance partners, we give you the most up-to-date industry insights from around the world, putting you an essential step ahead of your competitors.

Quinlan & Associates. Strategy with a Difference.

CONTACT US

info@quinlanandassociates.com | www.quinlanandassociates.com | +852 2618 5000

Level 19, Two International Finance Centre, 8 Finance Street, Central, Hong Kong SAR