accenture consulting

IN THE CLOUD AND IN CONTROL

The Accenture Cloud Risk & Regulatory Compliance Framework

Moving data, managing risk, and keeping compliant.

RISK AND REGULATORY CHALLENGES TO CLOUD ADOPTION

In the current disruptive economic and competitive environment, banks and financial services organizations are challenged to run their business faster, cheaper and better than they have ever done before.

The cloud presents them with an array of opportunities related to cost savings, scaling and speed to market for managing their cost and growth agendas. At the same time, the financial services industry continues to operate in an ever-changing sphere of regulatory requirements, adding to the difficulty and complexity of making the right infrastructure and technology decisions.

Much of this complexity arises from the operational risks associated with moving, locating and accessing vast quantities of data. In this context, cloud conversations have evolved from "should we move to cloud" to "how do we deploy to the cloud in a way that is regulatory compliant and secure?" In this document, we will focus on reducing the risk around cloud deployment while touching on how our proposed approach can help address some of the key issues faced by banks and financial services firms which include:

- The increasing volume of security threats to critical business applications such as cyber attacks, data breaches, compromised and/or broken authentication and hacking, that are threatening organizations' ability to comply with new regulations;
- Lack of confidence in the ability of third-party cloud solutions to adhere to global regulatory frameworks or international standards, along with a lack of transparency into how data is handled;
- The generalized terms and conditions offered by cloud providers for the delivery of their services, rather than clear, tailored agreements; and
- Regulations and regulatory requirements that are largely territorial, creating difficulties with cross-jurisdictional aspects when moving or processing data. As there are no borders in the cloud, data governance and management is becoming more and more demanding.

THE COMPLEX GLOBAL REGULATORY ENVIRONMENT

Across the globe, banks and financial services firms are required to navigate numerous international standards and regional regimes, putting great stress on their people, capabilities and financial resources.

The more important standards and regimes include:

Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines

These guidelines for risk, compliance and outsourcing specifically touch upon FinTech advancements, and propose a control checklist for financial services to follow.

European Union Agency for Network and Information Security (ENISA)

The Agency, a center of expertise in cyber security, has published preferred practices for information security and certification for adherence to basic information security requirements.

European Commission (EC) Law

Data Protection Directive (95/46/EC) is being replaced by the General Data Protection Directive (GDPR) which broadens territorial effects and scope, increases individual rights, and prescribes enforcement penalties attached to breaches.

US Law and Country-Specific Laws

Some national laws are not fully aligned with regulations (such as the USA Patriot Act, Safe Harbor agreement, international data transfers, and GDPR, among others). This may lead to issues related to the global transfer of data, with firms having to review and/or act upon national legal provisions with greater diligence and care before transferring data to other jurisdictions.

Other Local Laws

Beyond data protection, there are other legal regimes such as banking secrecy, criminal law requirements (for example, law enforcement requests for data), as well as laws governing information barriers which have to be considered in conjunction with data protection laws.

ISO/IEC 27002-2013

Published by the International Organization for Standardization (ISO), this international information security standard provides guidance on risk controls and policies.

NIST SP800-53 Revision 4

This National Institute of Standards and Technology (NIST) Special Publication recommends US security controls for federal information systems and organizations, with broader coverage than ISO/IEC27002, or those from ENISA and MAS.

THE ACCENTURE CLOUD RISK & REGULATORY COMPLIANCE FRAMEWORK

As seen, banks and financial services firms face challenges and concerns related to available cloud-based solutions and accelerating security threats and breaches.

Yet, one of the most important areas of concern might be the evolving regulatory requirements, especially the need to answer regulators' questions about the organization's ability to properly assess operational risks before moving to the cloud.

In response to these issues, Accenture has developed the Accenture Cloud Risk & Regulatory Compliance Framework, a robust, cost-efficient, compliant and secure approach that:

- Focuses on eight dimensions of operational risk and 83 underlying risks to assess and identify gaps and design controls.
- Incorporates global and local jurisdictional restrictions such as banking secrecy, data residency and information barriers to plan the overall journey timeline.
- Provides a set of recommendations following the assessment results.

Accenture uses a three-step process to help banks and financial services firms effectively assess their operational risk exposure.

The steps are:

STEP 1

Conduct an operational assessment across the firm for navigating to the cloud.

STEP 2

Review lower level controls, conduct analysis to identify gaps, and document solutions, including mitigating solutions and prioritizing quick wins.

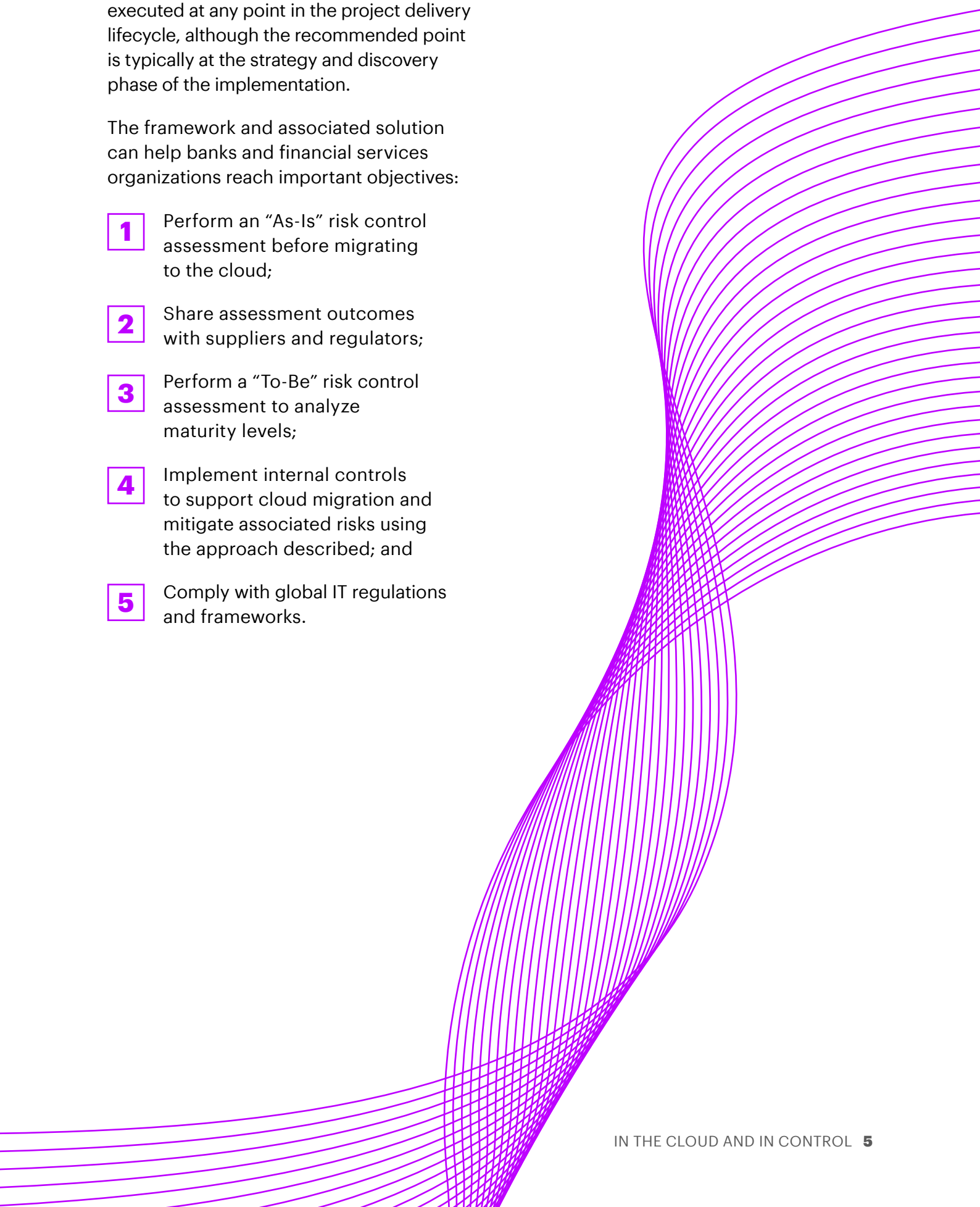
STEP 3

Create a roadmap for the overall journey with a focus on aligning with regulatory approval timelines and risk mitigation.

As it is technology agnostic, the framework can be used to assess risks across all cloud technologies and, more importantly, can be executed at any point in the project delivery lifecycle, although the recommended point is typically at the strategy and discovery phase of the implementation.

The framework and associated solution can help banks and financial services organizations reach important objectives:

1. Perform an "As-Is" risk control assessment before migrating to the cloud;
2. Share assessment outcomes with suppliers and regulators;
3. Perform a "To-Be" risk control assessment to analyze maturity levels;
4. Implement internal controls to support cloud migration and mitigate associated risks using the approach described; and
5. Comply with global IT regulations and frameworks.



HOW THE ACCENTURE CLOUD RISK & REGULATORY COMPLIANCE FRAMEWORK BENEFITS BANKS

The Accenture Cloud Risk & Regulatory Compliance Framework assesses a bank's operational risk along eight key dimensions, with each evaluated risk mapped to regulatory regimes, regulations and frameworks, including:

- Regulations and guidelines such as MAS Technology Risk Management Guidelines, GDPR and Cloud Security Alliance (CSA) Cloud Controls Matrix.
- Regulatory agencies and associations such as ENISA, Financial Conduct Authority (FCA) and Bank of Thailand (BOT).
- Frameworks such as ISO and NIST.

As a first step to assess and mitigate risks, we review the evidence provided by the cloud programs. This is done by mapping them to the regulatory control requirements. On the basis of the adequacy of evidence, the gaps are identified and the eight operational risk dimensions probed.

Underlying risks include:

Security

- Identity and access management
- Penetration testing
- Physical security
- Least privilege
- Information risk policy and control standards

Data

- Data location and cross-border access
- Data classification, segregation and flows
- Data backup
- Client consent
- Data encryption

Infrastructure

- Segregation of production and non-production environments
- Vulnerabilities
- Firewalls
- Scaling
- Patching

Regulatory

- Contractual security obligations
- Security due diligence
- Periodic assurance measures
- Continued compliance and adequate protection of data

Third party

- Exit strategy
- Contractual terms
- Commercial assessment
- Auditing
- Certification scope

Legal

- Material outsourcing
- Right to audit
- Customer contractual
- Data ownership
- Right to be forgotten
- Commercial protection and financial clauses

Service delivery failure

- Service-level agreement (SLA) and operational-level agreement (OLA) definition
- IT operations alignment
- Service recovery
- Service monitoring and alerting
- Service change notification

Business continuity

- Cloud-based disaster recovery process (DRP)
- Business impact analysis (BIA) assessment
- Business recovery time objectives (RTO) and recovery point objective (RPO) measurement
- Disaster recovery (DR) and business continuity management (BCM) testing
- Cyber attack planning

During the assessment phase, the following three areas should be reviewed for global implementation to the cloud:

1. **Local Regulatory Restrictions**
   Understand the impact of the local regulatory restrictions to design an approach that is compliant with these regulations.

2. **Client Consent**
   Confirm whether existing client consent suffice or if there is a need to plan a customer outreach; if client consent actions need to be taken, this may have an impact on the overall timeline of the program.

3. **Go-Live Timelines**
   Establish overall go-live approval timelines that consider the above and the time required to obtain regulatory approval.

The jurisdictional and regulatory restrictions that should be addressed when moving data include:

1. **Data Residency** – restricts cross border movement of data;

2. **Banking Secrecy** – restricts sharing of data outside borders or with third parties; and

3. **Information Barriers** – restricts different businesses and/or legal entities from sharing data with each other.

The contractual or documentary evidence gathered on the use of data is employed to validate the evidence on data usage by third parties as well as existing contracts.

If not available, client consent should be sought and contracts repapered to address data usage.

Based on the challenges created by local restrictions in each geography and the time it takes to get regulator approval, rollouts are typically planned in successive tranches as seen in Figure 1. This permits sufficient time to receive regulatory approvals as needed and prevents subsequent delays in going live afterwards.

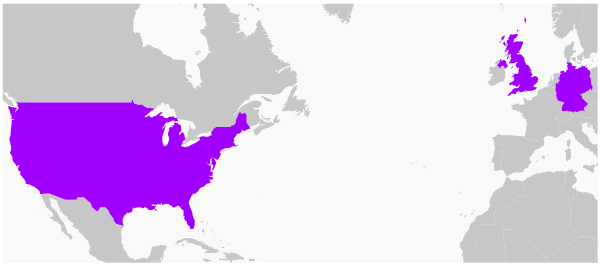
Figure 1. Rollout tranches

TRANCHE 1

Proposed Countries

United States, United Kingdom, Germany

*Some Tranche 2 countries may be brought forward

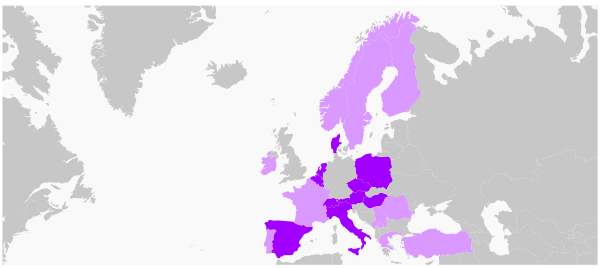


TRANCHE 2

Proposed Countries

EU/EEC Countries: Austria, Belgium, Czech Republic, Denmark, Finland, France, Greece, Guernsey, Hungary, Ireland, Italy, Jersey, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey

*Countries in Light Purple potentially in-scope for Tranche 1

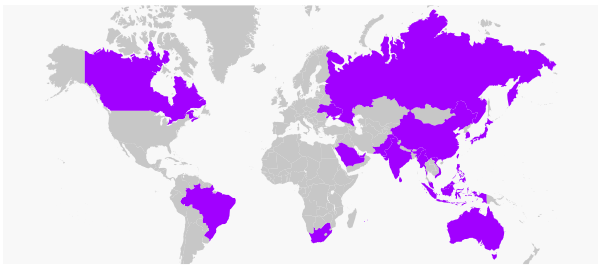


TRANCHE 3

Proposed Countries

Asia Pacific: Australia, China, India, Hong Kong, Indonesia, Japan, South Korea, Malaysia, Mauritius, Pakistan, Philippines, Russia, Singapore, Sri Lanka, Taiwan, Thailand, Vietnam

Other regions: Brazil, Canada, Saudi Arabia, South Africa, UAE, Ukraine



Source: Accenture, September 2018

Upon completing the assessment of the bank's operational risk, regulatory approvals should be obtained for the outsourcing of client data via third-party platforms in the cloud. Regulatory approval lead times vary and should be included in the go-live plan. In addition, depending upon the level of regulatory involvement, the timelines should consider staggered go-live dates across jurisdictions.

CALCULATE RISK EXPOSURE AND MITIGATE USING THE CLOUD OPERATIONAL RISK ASSESSMENT TOOL

Within the Accenture Cloud Risk & Regulatory Compliance Framework, the Cloud Operational Risk Assessment Tool helps banks and financial services firms conduct a structured operational risk assessment of their technology portfolio and migration workload, with the purpose of identifying risk gaps.

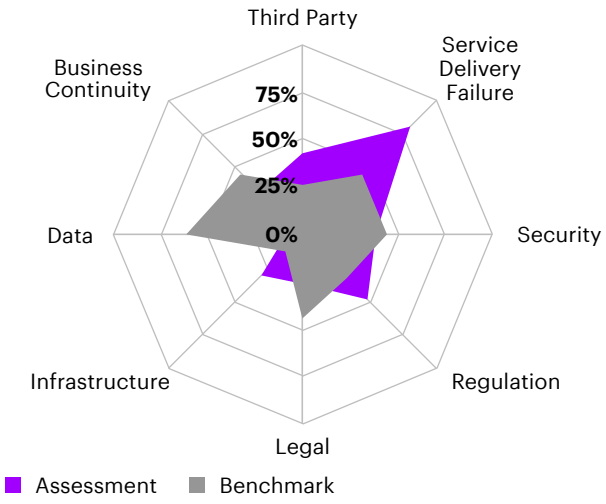
It looks at possible areas of improvement in addressing operational costs, increasing technology flexibility and scalability, and preventing and mitigating potential regulatory breaches and security threats. The assessment is conducted on the eight operational risk dimensions.

Figure 2 presents a sample distribution of risk exposures across the operational risk dimensions. This also gives banks the ability to benchmark against peers.

Figure 2. Example - Distribution of risk exposure

ASSESSMENT 1

Category	Exposure Score	Average Risk Rating	# of Risks
Business Continuity	31%	1.87	8
Data	7%	1.45	11
Infrastructure	30%	3.55	11
Legal	25%	3.33	9
Regulation	49%	3.22	9
Security	40%	2.67	12
Service Delivery Failure	80%	4	12
Third Party	42%	3	10



Source: Accenture, September 2018

For each of the operational risk dimensions, a set of risks is defined and mapped back to the technical and regulatory requirements and guidelines from bodies such as the FCA, MAS, ENISA, European Commission, BOT, ISO, NIST and CSA. Figure 3 shows the scoring approach used to calculate risk exposure.

Figure 3. Calculating risk exposure

RISK RATING

Banks have their own risk rating/impact parameters typically set from Low-High. The risks are reviewed with the stakeholders to agree on the risk rating to be used against the impact parameters.

CONTROL IMPLEMENTATION MATURITY LEVEL

Here we analyze the maturity level of controls by reviewing bank policies, cloud service provider controls evidence and implementation/planning evidence for the proposed solution. Each is rated on a scale from "Low" adoption to "Strong."

EXPOSURE SCORE

This is calculated based on the risk rating and control implementation level. The exposure score increases if the associated risk rating is high and control implementation maturity level is low.

PLANNING AND MANAGING THE JOURNEY

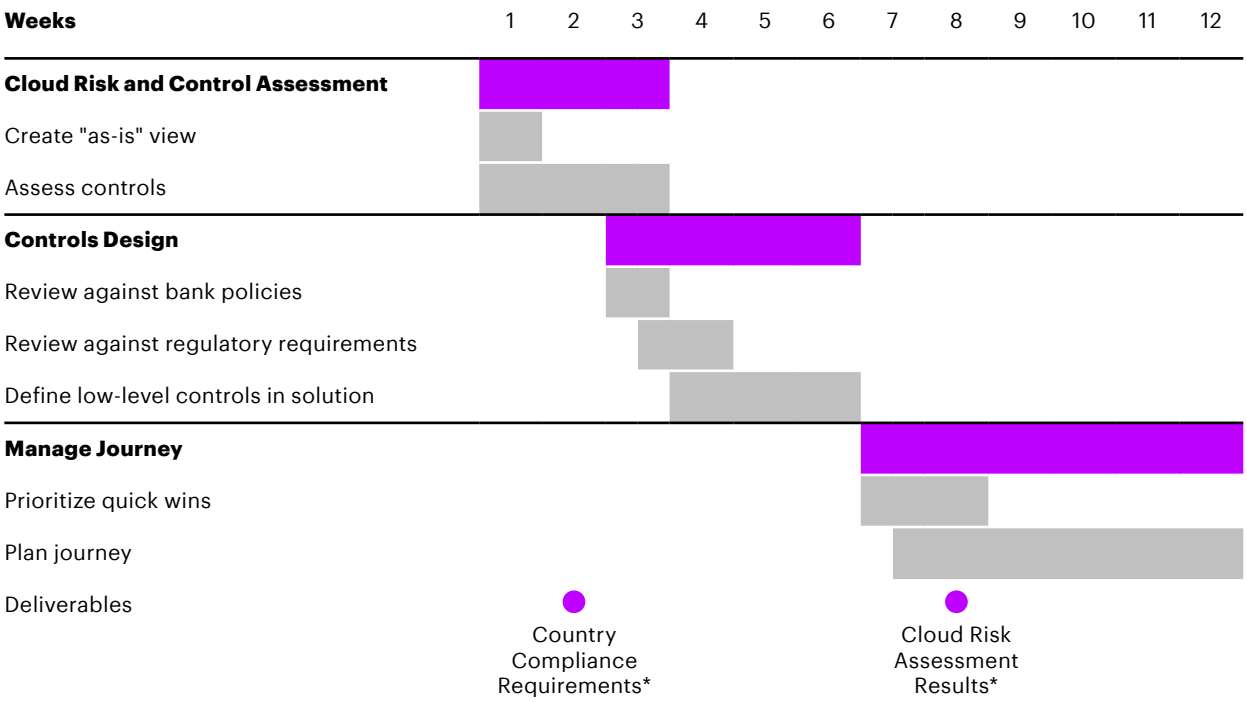
Our client experience indicates that it takes approximately 12 weeks to conduct the assessment, run the tool and develop a set of recommendations. Timelines can vary based on the scope of the assessment.

As seen in Figure 4 below, this covers:

- Set-up of cross-functional governance with first and second-line functions;
- Assessing the risks related to contractual arrangements, cloud service provider controls, bank policies and implementation documents; and
- Creating lower level controls to mitigate risk, along with a plan to address prioritized areas.

This review could be provided along with a cloud delivery of core areas, but would need to be accounted for in the overall project timelines.

Figure 4. Typical delivery timeline



*Note: Deliverables finalized via sprints and in sequence
Source: Accenture, September 2018

Key program deliverables include:

1. Set-up a Cloud Risk & Regulatory Compliance working group to enable cross-functional governance.

2. Conduct the operational risk assessment and provide results, quick wins and mitigation controls to help the bank effectively manage risks and reduce risk exposure.

3. In collaboration with the bank, we engage with regulator and advisory on local regulatory restrictions that need to be built into proposed solution.

Accenture has worked with clients across the globe to plan and manage cloud rollouts to be compliant with local regulations, assessing, mitigating operational risks and helping gain regulator approval.

Among our typical engagements:

- UK Bank – Using the Accenture Cloud Risk & Regulatory Compliance Framework, we assessed the key operational risks and gaps. This permitted the rollout of a public cloud platform, facilitating compliance with regional and national data protection requirements. The framework's solid risk-based decision-making platform offers strong evidencing to the regulator.

- UK Banking Group – Accenture delivered up-to-date customer relationship management (CRM) systems in the cloud, including defining the delivery approach in accordance with regional and national regulatory requirements.

- Large European Bank – Accenture assessed regulatory requirements for a global rollout. We evaluated operational risks related to a move to the cloud and designed teaming and collaboration models that would address local data protection requirements and information security barriers.

- Asia-Pacific Bank – For this institution we helped them setup their cloud governance capabilities and regulator engagement. We also assessed operational risks and advised on a service provider solution for their compliance needs.

KEY TAKEAWAYS

When moving to the cloud it is important to exercise caution and adhere to all legal, risk and compliance requirements. This means addressing operational risks.

For regulators, the key question is whether the bank has identified the operational risks associated with the move and the process to manage them. Using a structured and comprehensive approach, the Accenture Cloud Risk & Regulatory Compliance Framework helps quickly identify the risk gaps and develop a set of corrective actions that respond to the regulator's expectations.

The approach is flexible and the assessment and delivery of core components of the solution could be delivered at any point in the roadmap, although our recommendation is to incorporate this during the strategy and discovery phase.

CONTACT US

Preetha Bedi
Financial Services, Technology Advisory,
Cloud Risk & Regulatory Compliance Lead
Preetha.bedi@accenture.com

Elodie de Fontenay
Financial Services, Technology Advisory,
Offering Development Lead
Elodie.b.de.fontenay@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

181503