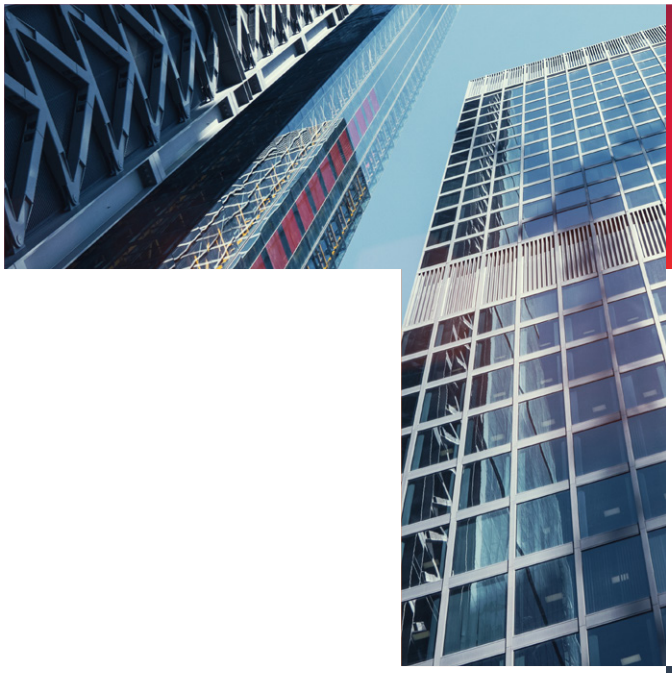

Banking in the cloud

Achieving strong compliance

CGI

Banks are increasingly accelerating their IT modernization and digital journeys through more strategic use of the cloud. The cloud provides an agile, scalable, and future-fit technology foundation for adapting to continuous market change, meeting fast-evolving customer expectations, reducing operational costs, and achieving many other strategic business objectives. Overall, it has become a key enabler of business transformation for banks.

Cloud environments, however, can be challenging to navigate due to their complexity, especially within a highly-regulated industry like banking. There are multiple internal and external stakeholders to manage, advanced technologies to oversee, and mounting regulatory and control requirements to meet—all of which demand extensive resources, including expertise, time and money.

In terms of compliance, there are a broad range of requirements that impact a bank's cloud journey—both globally and regionally. For example, within the European Union, banks must comply with the EBA Outsourcing Guidelines and the General Data Protection Regulation (GDPR). On a global scale, there also are numerous quality- and security-related standards that, while not mandatory, can help banks achieve greater compliance, such as quality standards issued by the International Organization for Standardization (ISO) and security standards within the CIS Benchmark and the NIST Cyber Security Framework.

Building a compliance culture

Typically, moving to the cloud begins with technological reflection. Among other initiatives, banks invest in a cloud strategy aligned closely with their business imperatives, conduct assessments of their current IT environment and cloud adoption requirements, develop a cloud roadmap and implementation plan for prioritized cloud initiatives, implement a cloud architecture, platform and security, and set up a cloud competence center for ongoing management.

However, often the most surprising aspect of cloud adoption is the amount and difficulty of work involved in achieving strong external and internal compliance. Compliance is the process of making sure your bank and its employees adhere to all applicable laws, regulations, standards, internal policies and ethical practices, as you operate within the cloud. It's often seen as an overhead cost but, if done right, it can be turned into a strategic asset for your cloud journey.

To achieve strong compliance in the cloud, we recommend building a compliance culture that delivers the following:

- Clear compliance policies and governance
- A well-defined compliance control framework
- Continuous compliance evaluation and monitoring
- Documentation of all evaluations and decisions

Such a compliance culture generates a wide range of benefits, including the following:

- Greater independence and flexibility in managing vendors
- Integrity and privacy when handling data
- More effective control over outsourcing through enhanced governance
- Reduced risk of lawsuits and financial liability
- Enhanced trust with customers, prospects, and vendors
- Protection of resources and reputation
- Greater agility in responding to change due to fewer compliance barriers

Identifying internal and external stakeholders

Building a strong compliance culture in the cloud begins with identifying all of the internal and external stakeholders that play a role in enforcing various laws, regulations, standards and policies. All of these stakeholders must be identified and managed to provide an enterprise-wide view and understanding of compliance requirements, risks and costs, ensure alignment, and support an enterprise-wide compliance approach and framework.

A sample list of internal stakeholders might include the following entities within a bank:

- Board of Directors
- Executive management team
- Security and compliance
- Legal
- Communications and management secretariat
- Design authority
- Enterprise and platform architecture
- Infrastructure and operations
- Business owner group
- Business strategy board
- Internal systems auditors
- Sourcing and procurement

Examples of external stakeholders might include the following:

- Regional, national and local banking associations (e.g., European Banking Association)
- Regional, national and local standards organizations (e.g., International Organization for Standardization)
- Regional, national and local regulators (e.g., Data Protection Agency)

The cloud compliance process

Once internal and external stakeholders are identified, aligned, and managed, an efficient and ongoing cloud compliance process should be implemented with clearly defined business and IT steps and specific tasks for each step.

Potential steps might include the following:

1. **Procurement** – Identify a single point-of-contact for managing all commercial and legal issues arising from procurement contracts and conduct a contractual risk assessment.

2. **Technology and design** – Ensure the chosen cloud environment aligns with business requirements and the enterprise architecture model and follows IT strategies and decisions for approved vendors and tools. In addition, include a plan for cloud resiliency to minimize business risks.

3. **Security and regulations** – Ensure the cloud program aligns with IT security strategies and includes an exit strategy and plan.

4. **Audits** – Ensure all cloud services and resources are covered in the systems and organization controls (SOC) reporting process and comply with all internal and external auditing regulations.

5. **Sponsors** – Develop a clear cloud mandate and document executive approval of all required decisions.`

6. **Maintenance** – Ensure all compliance tasks and related controls (manual, semi-automated and fully automated) are documented and executed through an annual cycle of compliance work and integrated within IT operations.

Examples of compliance tasks performed for each step might include the following:

Compliance steps	Sample tasks
1 **Procurement**	• "Essentiality" assessment • Risk assessment and mitigation • Mapping regulatory compliance • Know your vendors (due dilligence)
2 **Technology & solution design**	• Software and tools verification • Know your services • Proof-of-concept • Operation checklist • Architecture verification
3 **Security and regulation**	• IT security evaluation • Exit strategy and plan • Regulation awareness chart • Regulation data flow diagram • Update contingency plan
4 **Audit**	• Services in scope • Internal audit • External vendor audit
5 **Sponsors**	• Technology mandate • Business mandate • Board mandate • Customer mandate
6 **Maintenance**	• Annual cycle of work • Operations • Exit plan testing • Re-visit risk assessments and mitigations

Partnering for success

Working as a trusted partner for leading banks across the globe, CGI has accrued deep knowledge and substantial experience from cloud-related compliance engagements. Based on this experience, we offer a compliance toolbox with guidelines, processes, templates, and checklists that help banks become compliant faster and with higher accuracy and overall quality.

We assess your compliance needs, define clear compliance objectives and steps, and lay out specific tasks for each step to help ensure the right compliance approach and framework for your organization. Both internal and external stakeholders are mapped to each step.

We also offer ready-made compliance templates and checklists that can be used at each step of the process to document requirements, activities and timeframes, saving your bank a significant amount of time and reducing your compliance risks based on lessons learned.

Finally, we provide concrete solutions for managing your most difficult compliance requirements, including issues related to exit strategies and data location.

This compliance expertise is combined with our broad cloud experience, including an end-to-end suite of cloud modernization services that organizations across industries and the globe are using to accelerate their cloud journeys.

Contact us today to learn more about our compliance services in the cloud for banks.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 88,500 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com