HYBRID CLOUD GOVERNANCE & COMPLIANCE



As the cloud continues to fuel the digital transformation wave, companies around the world are grappling with a wave of new risks ranging from cyberattacks and privacy regulation to uncontrolled costs. The need for a rigorous approach to oversight on IT infrastructure, whether locally hosted or on the public cloud, remains paramount.

Hybrid cloud popularity

Deployment of hybrid clouds have become a major driver in digital transformation:

- The Flexera 2020 State of the Cloud Report reports that 87% of enterprises have a hybrid cloud strategy.
- The Nutanix 2019 Enterprise Cloud Index found that 85% of survey respondents selected hybrid cloud as their ideal IT operating model.

NIST defines hybrid cloud as a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Initially seen as a cautious stepping stone towards full cloud migration, hybrid clouds have gained preference on account of flexibility and choice. A recent independent study sponsored by OpenText found that organizations that adopted a hybrid cloud approach report:

- Improved flexibility

- Faster sales and service cycles
- Better collaboration and customer satisfaction

The video conferencing provider BlueJeans is one of the companies reported as benefiting a lot from flexibility in 2020: their traffic has switched from 80% on premise to 70% on cloud in the recent months. With the likes of AWS and Azure having the muscle to provide technical capabilities (such as security and support) well beyond most enterprises, it's a no brainer why an organization would go this route.

However, the previously mentioned risks mean that companies still want to hold onto their critical data especially in sectors where:

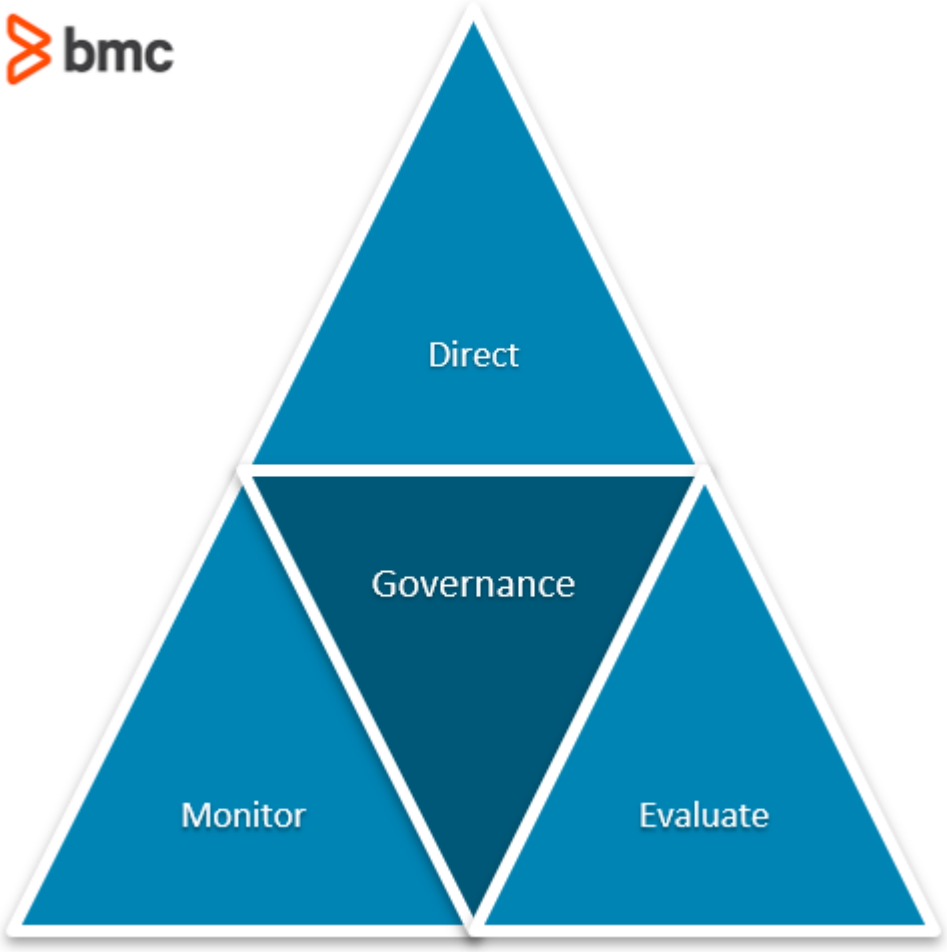
- Regulation is high.
- Intellectual property and personally identifiable information is concerned.

Governance in the hybrid cloud

ISACA defines governance as the method by which an enterprise ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives are achieved. Governance involves:

- Setting *direction* through prioritization and decision making.
- *Monitoring* and *evaluating* performance and compliance against agreed-on direction and objectives.

Cloud governance ensures that an organization's cloud capability supports and enables the organization's current and future strategies and objectives and is aligned to IT governance.



There are five key decisions in IT governance which we can cascade towards management of hybrid cloud infrastructure:

1. ## IT Principle Decisions

   This involves making high level decisions about the strategic role of IT within the organization. From a hybrid cloud perspective, consider how best to support business strategy using the right combination of on-premise and cloud services:

   - Does the business require services to be available at a global scale, with fast, high levels of availability and performance?
   - What are the business risks around data access due to regulation or sensitivity considerations?

   Answers to these questions will ensure that the hybrid cloud approach is consistent with the direction that the company is taking.

2. ## IT Architecture

   This involves making decisions on an integrated set of technical choices and aligning them to meet business needs and objectives. Architecting for hybrid cloud, particularly where multiple providers are involved, is not an easy undertaking when you consider workload management, orchestration, and integration.

   Governance must focus on ensuring consistency in planning, tooling, and resource management; otherwise the hybrid cloud can end up being a significant source of pain down

the road arising from redundancies, manual rekeying of data, and complexity.

3. ## IT Investments

   This involves prioritizing investment and determining where best to invest in IT aligned to the strategic needs of the organization. (Cost management is one of the biggest headaches in adopting the cloud, and is listed as one of the five disciplines of cloud governance by Microsoft.)

   Economic decisions will be driven by your strategy and architecture, defining what data needs to reside on-premise vs cloud, while also considering transfer and other factors. To prevent waste and overruns, be sure to consider different types of costs such as:

   - Integration
   - Storage
   - Compliance
   - Customization
   - Platform costs

4. ## IT Infrastructure

   This involves making choices and decisions regarding centrally coordinated and shared IT services. Here, hybrid cloud governance will address issues around choice of hardware, software, and licences as guided by the first three decisions.

   Security and continuity will be heavily considered at this point. Consistency and standardizations are key to ensure configurations, resources, and tools work seamlessly to deliver the required quality at the right cost.

5. ## Business Applications

   This step involves making decisions on application architectures and business requirements for internal and external applications.

   Sudden shifts in application demand is one of the major challenges that affect service performance and thus are a key consideration for architecture. Cloud governance must provide direction to ensure the right hybrid cloud mix is used to provide quality for both public facing and internal applications, while protecting data (especially PII, personally identifiable information) in line with regulations.

Compliance in the hybrid cloud

Compliance is the act of ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed.

When it comes to hybrid cloud, compliance drives a lot of decisions around:

- What should be maintained on-premise
- What should go on the public cloud

Depending on the sector, a company may find itself facing a myriad of legal, industry, and regulatory requirements such as:

- SOX
- PCI-DSS
- ISO
- HIPAA
- GDPR
- And more

For this reason, there must be a concerted effort to manage the hybrid cloud through appropriate policies to ensure that the right decisions on what data needs to be on what infrastructure are made.

Compliance must be supported by relevant governance actions around monitoring and evaluation which includes regular risk assessments, audits, and status reports on data management in hybrid environments. The governance body instituted by the company must:

- Ensure all stakeholders, especially employees, are constantly aware of the requirements that the organization is subject to.
- Institute policies to ensure that inventory of data is kept including relevant security mechanisms, guidelines for transfer across on-premise and public clouds are clear, and measures to be taken in case of violation of these policies are understood.

Additional resources

For more on this topic, explore these resources:

- BMC Multi-Cloud Blog
- BMC Security & Compliance Blog
- Top 5 Cloud Security Trends of 2020
- How to Reduce Risks of Shadow IT by Applying Governance to Public Clouds
- Homogeneous vs. Heterogeneous Clouds: How to Choose Your Hybrid Cloud