

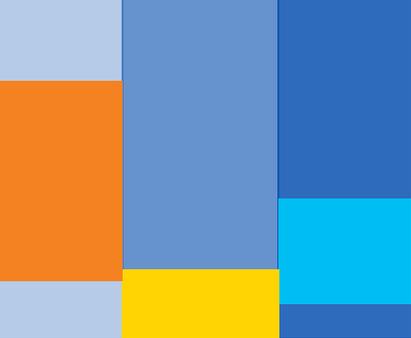
Automating the Cloud Governance

Inside

- Cloud and Beyond - What lies Ahead?
- Cruising Towards a Promising Cloud Future
- Attributes of a Cloud Governance Automated Tool
- Modernizing Governance Through Technology
- The Right Way to Good Governance
- Salient Features of Governance Automation
- Conclusion

Written by
Supriya Balaiya,
Business Analyst

Contributor
Kartikaya Sinha,
Chief Product Architect



Cloud and Beyond - What Lies Ahead?

The global cloud computing market is anticipated to witness a compound annual growth rate (CAGR) of 17.5% by 2025 with a significant surge in the usage of cloud automation tools.

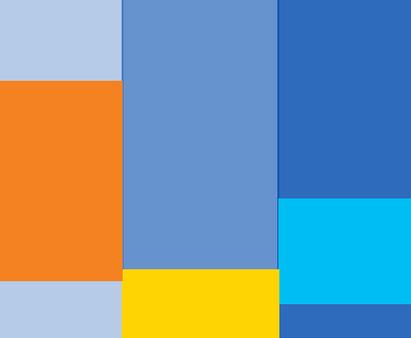
With enterprises moving their data and applications substantially on the cloud, security threats and breaches across all operations emerge as their biggest concern. Recent data from Risk Based Security revealed that the number of records exposed has increased to a staggering 36 billion in 2020 with Q3 alone depicting an additional 8.3 billion records to what was already the "worst year so far."

2020 has witnessed a sharp accelerated impact, demand and growth of cloud computing practices due to the onset of the unexpected Covid-19 pandemic with the current financial year's estimates rising to almost USD 165 billion as against the pre-Covid estimate of USD 158 billion.

To curb the adverse effects of such concerns and keep pace with the growing market, it is vital that organizations emphasize strongly on strategic planning and attain full visibility and foresight on security, governance and compliance on cloud more than ever.

"CIOs looking to prepare their organization to thrive in the upcoming turns must take a differentiated approach to cloud computing," says Gregor Petri, Vice President Analyst, Gartner.

A successful shift to the cloud needs complete alignment of businesses and resources, which is why a comprehensive cloud governance structure along with an additional focus on cloud operational excellence is crucial.



Cruising Towards a Promising Cloud Future

However, with the uncertainty of the pandemic and the constant pressure on organizations to continually provide business flexibility and acceleration, automating and managing cloud operations is not enough. There is an urgent need to implement intelligent automation on the governance of cloud itself. Cloud governance automation can be accomplished by establishing a dedicated centralized Cloud Centre of Excellence (CCoE).

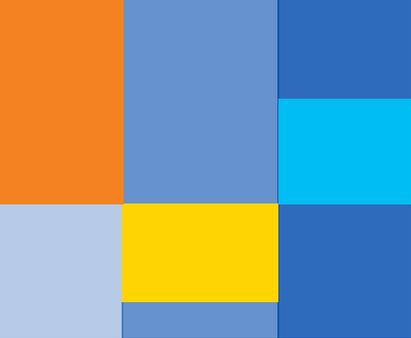
We saw in our preceding whitepapers how a CCoE is a cross-functional team comprising mainly of DevOps, CloudOps, Infrastructure, Security and FinOps that enables cloud operational excellence across all cloud service models of infrastructure, platform and software as a service (IaaS, PaaS, and SaaS) and are focused mainly on the people, process and technology framework.

CCoE bridges the gap between the available knowledge and skills vis-à-vis what is required to establish matured cloud-centric operations.

Additionally, the CCoE team of experts institute cloud governance practices by creating cloud policies and guidelines in collaboration with cross-functional teams, offer governance tools and strategies on IT and cloud systems, align itself to the organization's objectives and tracks performances on the cloud. For detailed insights on CCoE and governance tools please [click here](#). (Provide links of both the previous whitepapers here)

Moving forward, enterprises are looking at scaling and enhancing their cloud governance structure and expertise before which they need to acknowledge the difference between cloud automation and automating cloud governance.



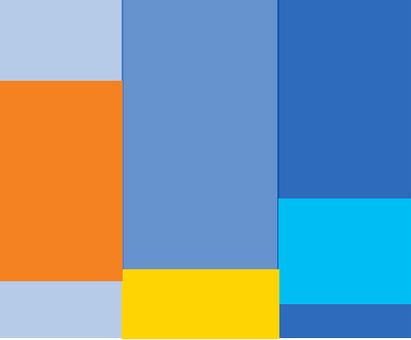


Cloud automation is the technique of integrating cloud management processes by using cloud-based tools that design, execute, modify and segregate assets on cloud whereas automating cloud governance is the process of automating an organization's policy management to standardize cloud operations and increase operational efficiency and innovative capabilities by implementing advanced technology on governance.

In the present time, with technological advancement on the rise, enterprises are making sincere attempts at building sophisticated workflows as well as getting approvals and signoffs from relevant stakeholders to implement and run automated cloud governance processes.

Just like AI/ML, governance automation is an emerging trend, set to bring about a digital revolution into industries in the current decade to strengthen cloud infrastructure visibility while stimulating minimal or zero human interference in the ongoing business operations.





Attributes of a Cloud Governance Automated Tool

The primary objective of adopting pre-integrated cloud automation tools is to automate and manage repetitive day-to-day operations whereas automating the cloud governance processes helps IT and cloud professionals simplify application lifecycle management and effectively manage multi-cloud environments.

It minimizes manual operations by provisioning for code or patch auto-updating, capacity management, configuration management, continuous integration, disaster recovery and reporting.

Beyond the obvious benefit of reducing manual work, organizations must employ governance tools to:

- Define policy standards,
- Monitor security and compliance,
- Integrate as well as automate workflows,
- Remediate issues in real-time
- Forge best practices, thus accommodating more time for innovation and mission-critical tasks
- Provide a centralized automated governance structure that facilitates scalability, flexibility, agility and cost optimization holistically.

Modernizing Governance Through Technology

Why Shift from Manual to Automation?

To keep abreast with cut-throat competition, organizations using the cloud need to adhere to a speed of innovation at all times.

Gartner predicts that by 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020.

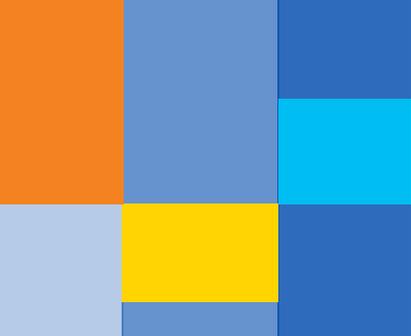
According to Sundar Pichai, CEO of Google, “Today, computing mainly automates things for you, but when we connect all these things, you can truly start assisting people in a more meaningful way. If I go and pick up my kids, it would be good for my car to be aware that my kids have entered the car and change the music to something that’s appropriate for them.”

With such a radical shift in the expectation from technology,

overseeing all the resources and applications across multi-functional and multi-cloud environments manually would surely get exhaustive and time-consuming.

If enterprises opt to function manually, it would be highly challenging to identify which resources will be compliant to what standards for efficiency, scale and speed or teams may fail to cater to fast-moving release frequencies, configuration changes, security and compliance regulations and ascertain expertise in every such individual domain resulting in ad-hoc operations as well as potential wastage of cloud spend.

Provisioning for the cloud in the planning phase itself helps businesses to respond or react to an event before it has actually occurred.



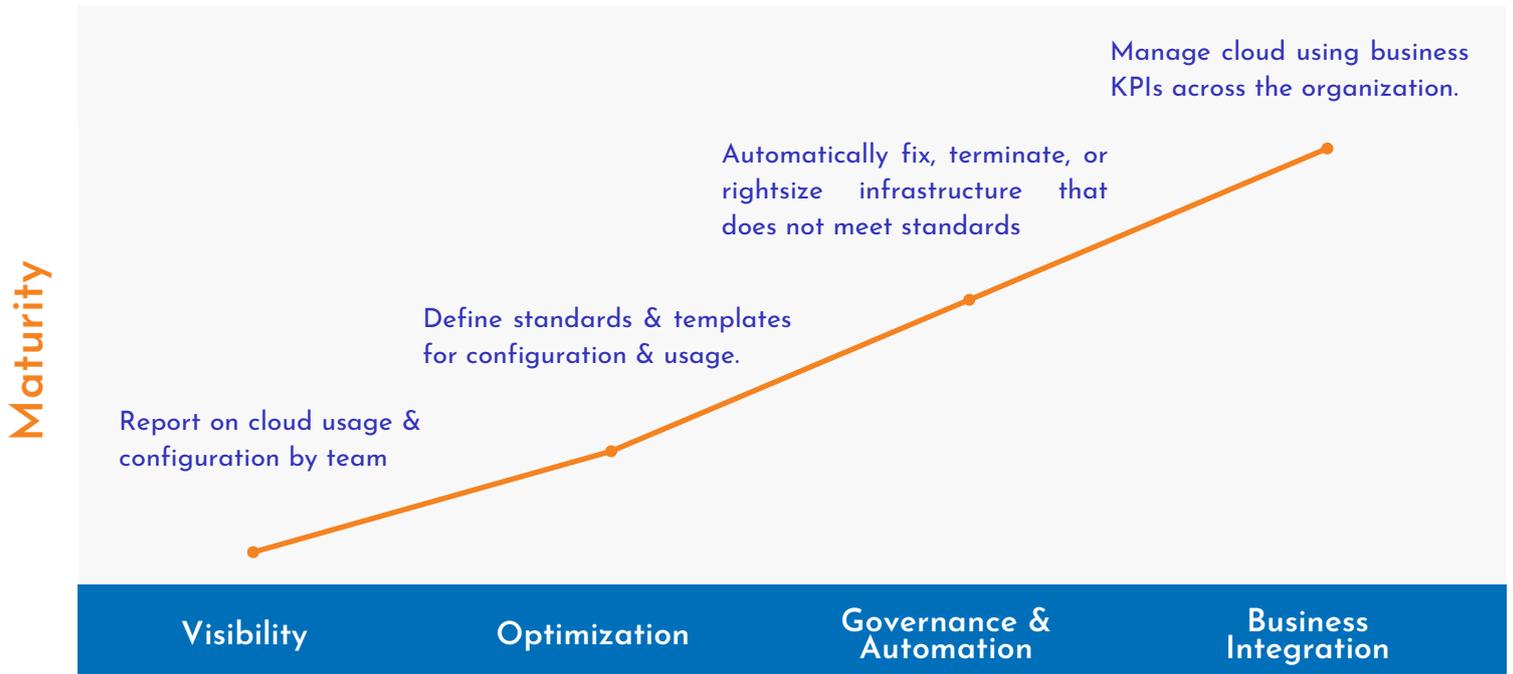
Also known as proactive governance, cloud solutions can be simplified by configuring and defining policies to recognize and remediate the root cause of risks and events beforehand whereas in reactive solutions, an event or an issue that triggers the event has already occurred.

For instance, the system will trigger an alert to a user sign-in if that particular user has not been assigned to a group. Proactive monitoring, on the other hand, will revoke the IAM user access until the user is assigned to a group.

Other examples of proactive governance can be automated tools enabling the ops team to identify and highlight a memory leak before it causes the application to crash or facilitating well-architected workloads to be built at a faster rate and with increased performance efficiency.

Organizations are moving from manual to automated governance mainly because automation unravels built-in tools and standardized security policies to streamline and implement controls and mechanisms for regulatory compliance and audits, address access, security, configuration and test management, provide a well-architected framework along with backup and recovery, continuous integration and multiple reporting tools. The automated framework may also include validation of code, artifact documents and on-going maintenance and support depending on the defined capabilities.

The Right Way to Good Governance



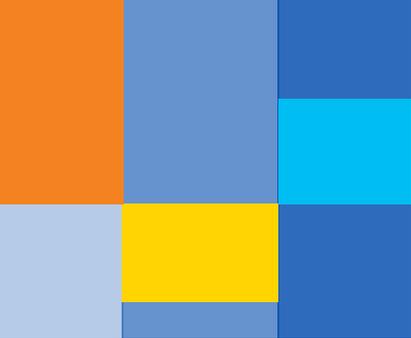
Collaboration

Define Business Policies:

Business policies must be defined in the business plan based on the organization's requirements. Organizations should have the expertise to understand and interpret the rules, conduct tests to validate policies, establish expected outputs, set the frequency of the policies to be run, the risks involved, stakeholders and vendors that need to be roped in and the plan to map the necessary teams, processes, tools and controls.

As the business progresses, processes and policies should be reviewed and accounted for at regular intervals with the intent of altering the set rules as and when required.

Organizations can even custom build their policies and workflows to run, manage and control their cloud environments. For example, if banking automation is not configured and monitored properly, it could become vulnerable to a cyberattack or make a biased decision on a loan application, which could cause heavy reputational and financial damage.



Prioritize and Integrate Controls:

Enterprises need to prioritize and accommodate only those governance checks that are of utmost importance and scope out what is not. Also, compliance policies must adhere to and be managed across regulatory controls like HIPPA, SOX, PCI, etc in which case it is ideal for enterprises to consolidate policies into one integrated framework instead of running each regulatory control independently. This enables policies to run cross-functionally as well as perform multiple repetitive tasks like audits, validation checks and tests while saving on time and costs significantly.

Forecast Risks and Impact:

Determine the risks encountered as well as the probability of it occurring again vis-à-vis its impact on business operations to ensure appropriate measures are taken to minimize the impact or loss from it.

It will also help organizations realize where controls might be failing or not adhering to their full potential, based on which, they can focus on the precise governance tools and techniques to refine testing and remediation activities.

Gradually Implement Continuous Monitoring:

Implement governance and verification checks on an incremental basis instead of applying checks across the entire setup at one go. Identify loopholes and shortfalls with continuous monitoring and tracking methodologies on a step-by-step basis to begin remediation, if any, with immediate effect.

Salient Features of Governance Automation

Automate:

Strategize the governance framework to design intelligent automation. It is vital to apply the right type of automation to the right type of task along with ensuring that the right automation tool is utilized as well. Automate processes based on current audit reports, test findings and policy shortcomings. Enterprises must cater to automate business areas that come with high managerial costs to curb risks and expenses substantially.

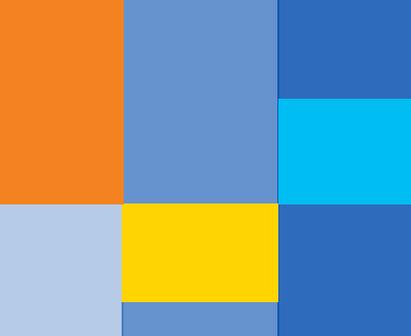
The key to automation implementation is to design exclusive initiatives and strategies to accelerate business from a governance point of view.

Some noteworthy features of automation in cloud governance are:

Cloud Governance

Bringing Everything Together





Regulatory Compliance:

Organizations are most concerned about their cloud operations being compliant with industry standards as well as geography-based compliance regulations while assuring their clients that the data is well secured. It must specifically be built for multi-level use with role-based functionalities to provide a comprehensive analysis of the cloud environment through continuous monitoring and audits.

Compliance tools are a substitute to the manual verification process where automated methods to check controls are written as a code that can be run on cloud events.

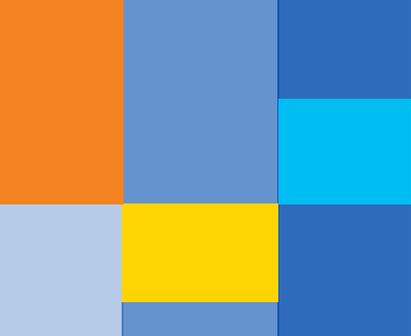
Automating governance policies help generate multiple reports to highlight gaps, if any, list out improvement areas that can match up to industry compliance benchmarks and help mitigate risks. The tools provision for compliance scores to get an approximate idea about how much is a business complying with standards and how much more it needs to accelerate.

Thus, depending on the location and industry the enterprise belongs to, the most suitable compliance standards can be opted for.

Stakeholders can be involved early in the process to configure and navigate customized policy-driven automation. Policies can be applied as a whole or business unit-wise based on organizational requirements, with pre-defined automated alerts and notifications when potential threats or violations occur. Global tagging policy further helps security teams prioritize notifications. The automated governance platform is also capable of enforcing data access policies where in case of unauthorized access or misconfiguration of data, the tools can remediate the vulnerability automatically.

Automated regulatory compliance thus validates cloud security from the beginning ensuring increased safety and scalability along with reduced costs and technical debts.



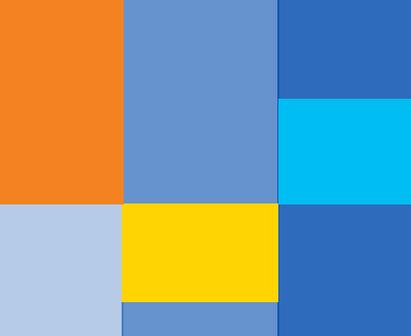


Well-Architected Framework

The well-architected governance tool helps understand, evaluate and design the architecture with ease as well as analyze and deliver business operations to meet expectations. The tool aggregates general design principles with specific best practices, presenting a point-to-point evaluation and measurement system on the cloud set-up. It continuously monitors and governs the cloud architecture with proactive recommendations to shape the infrastructure into a secure, optimized, cost-efficient, reliable and operational efficient system.

Thus, the well-architected framework provides a systematic way of comparing an organization's systems with best practices to furnish guidance and improvise with time. Workloads that follow a well-architected framework can build and deploy easily and at a faster rate, as well as mitigate risks and make system performance more efficient.

For instance, if manual audit checks took 30 days to complete only after which remediation actions would be undertaken, automated governance tools would facilitate the same task in 3 days before directly moving to auto-remediate the vulnerabilities thus reducing the processing time by almost 90%. Companies can cut down costs on reserved instances and unused resources by optimizing cloud operations.



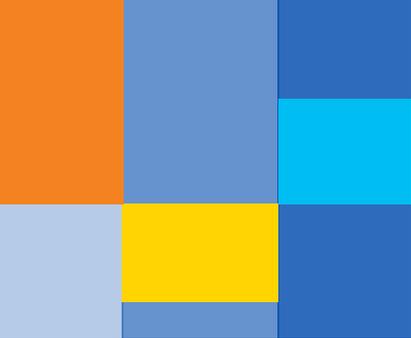
Reporting

A business intelligent governance tool has exhaustive reporting modules featuring multiple pre-defined policies and functions. Alerts get flashed whenever an occurrence matching existing policy surfaces. Policy violations if any, can be grouped and displayed on a dashboard. For example, if an organization's password policy sets the expiry of password in 60 days, then all the checks pertaining to that organization will be clubbed and notifications regarding password expiry will be sent out.

Alerts and centralized reports related to organization policies, log management, cost spends and security can be viewed, scheduled, sent via email, SMS, or even integrated with business communication platforms.

Reports can then be accessed, viewed and analyzed by users and cross-functional, multi-location-based teams at any given point in time. They can compare the number of recurring issues and monitor change management correspondingly.

Easy collaboration, as well as instant data sharing with auditors, pertinent stakeholders and teams that do not have direct access to reports on the tool, is also ensured. Reporting tools provide reports in summary as well as detailed form and can be scheduled on daily, weekly, monthly, or customized timelines to allow smooth conduct of recurring meetings and everyday business operations.

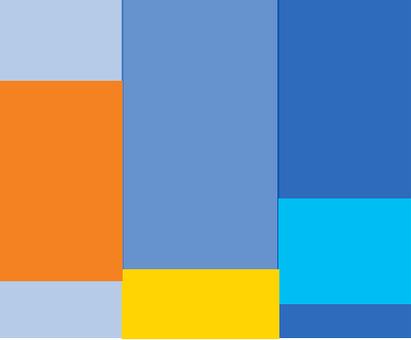


Cost Analytics

Cost analytics provides a comprehensive study of actual cloud spends vs budgets, in the form of graphs and metrics, providing complete visibility on the unused and orphaned cloud resources and their instances. Advanced cost analytics, additionally leveraging on AI, when incorporated with the cloud governance platform provide a series of cost recommendations that result in significant cost savings and guarantee cost consistency.

Users can easily monitor their daily and monthly spends on a single dashboard. With the help of cost trend analytics, users can examine their cost trends, identify their regular cost spend patterns and easily determine when they are spending more. Users can also compare their per day budgeted cost with actual cost spend on any particular day.

Such tools also furnish cost by service analysis as well as cost by region analysis allowing users to compare the cost spend on different services, region-wise. Apart from cost insights, the cost governance tools provide proactive recommendations to their customers regarding their cost spend on reserved instances, right-sizing, and unused resources. It provides an approximate cost saving in the cloud environment and helps customers restrict unnecessary spends.



Conclusion

It is laborious for organizations to bring together all the above mentioned features as the biggest challenge is to find the right platform. Often, enterprises are seen seeking open source solutions from various open source cloud platforms or testing tools and cost management tools from respective vendors individually and so on. The biggest need is for cloud service providers to offer a comprehensive package under one roof.

Gartner Inc forecasts that by 2023, 40% of product and platform teams will use AIOps for automated change risk analysis in DevOps pipelines and through 2024, enhancements in analytics and automatic remediation capabilities will refocus 30% of IT operations efforts, from support to continuous engineering.

Successful autonomous governance platforms like Cloud Ensure are available in the market that offer all of the above guaranteeing operational efficiency, enhanced data accessibility, cost optimization, real-time cognizance and scalability as a whole.

In the approaching decade, as the industries adapt to technology trends and are progressively moving towards modernization, the combination of automation and the cloud look to be the next big thing.