
GlobalDots
Your 2022 Guide to a Successful Cloud Strategy
#3: Cloud Governance Best Practices
Author: Steven Puddephatt, Senior Cloud Architect at GlobalDots
#1 How to Choose Your Cloud Provider(s)
#2 Cloud Security Tooling
#3 Cloud Governance Best Practices
#4 Budget Allocations & Procurement
#5 Building Your Company's Cloud Centre of Excellence(CCE)
Download Full Guide

Table of contents

GlobalDots

Executive Summary

This whitepaper is part of a 5-whitepaper series suggesting guiding principles for moving towards a successful cloud environment. It applies to both newly migrated and already cloud-based organisations.

A successful cloud environment is one that provides maximum benefit to business processes, with minimal spend and complexity, and with the utmost security.

GlobalDots has been helping organisations successfully migrate to the cloud for years, and in that time we have seen businesses fall foul of the same mistakes over and over.

It's much easier, cheaper, and more efficient for your business to plan how you will use a cloud estate before you migrate there. In other words, spend more time planning your cloud estate before you let everyone loose in it, thereby turning it into what I like to call a 'double W' estate, or a Wild West estate!

If you have already migrated to a cloud provider, don't worry – the principles laid out here still apply. However, tidying up is a slightly more laborious task than starting from scratch.

Why is a cloud strategy necessary?

Shift problems left:

By spending time now to determine a set of rules (that are enforced by software tools), problems later can be severely reduced. By setting up rules and governance policies you can ensure your cloud journey runs smoothly right from the start.

The most common mistake we see is rushing into the cloud. It's easier to set up a safe landing zone for your cloud resources than it is to try and clean it up once production workloads are already running. Spend the time setting up in advance and make sure your cloud estate is clearly organised from the outset. That way, clean-up operations won't be necessary.

Spend money to save money:

Most organisations are reluctant to spend large sums of money on governance software before they build out their cloud infrastructure. This is actually a harmful mindset and will cost more in the long run.

SREs, DevOps and senior sys admins are some of the most expensive human resources on the planet, and it is exactly these people that you'll be asking to monitor and investigate goings on in your platform. They'll end up writing a complex set of admin scripts in order to ensure IAM roles are used correctly, API access keys are rotated, resources are spun down when they are not needed, and so on.

As your cloud estate grows your IT engineers will be swamped with requests. It's not realistic to expect them to be able to keep eyes on the whole estate. That's why it's so valuable to spend money on governance and security tools at the outset. Adding tools too late in a cloud journey will lead to a bumpy integration and security dashboards will be flooded with unremediated alerts.

Long-term thinking is a must:

Simple cloud platforms quickly become complicated, single VPCs become many and the connections between platforms can become vast and complex. When deciding on a cloud strategy the long-term effects of early decisions must be thought through, as these decisions will determine all the legacy systems, not just the new ones.

A well-governed cloud environment takes careful planning, budgeting and execution. Be prepared to fight the budget holders for money which won't reap benefits for 12 - 24 months. Be brave with proposals and use examples of horrific cloud sprawl (a quick google search will turn up results) to scare money from the company coffers.

Cloud Governance Best Practices

What is cloud governance?

Cloud governance is essentially a set of rules to maintain your estate and ensure compliance in a consistent way. One example of this would be not allowing engineers to make a storage bucket that is open to the public. Without cloud governance we may state “no storage buckets open to the public”, but there is no system to actually back up the rule, and so it happens anyway (this kind of thing is in the news every day).

With cloud governance in place an ‘all seeing eye’ will sweep your cloud environment, constantly looking for misconfigurations (infrastructure that doesn’t meet your governance policies). If it finds any such misconfigurations, it will then either send an alert or remediate the misconfiguration. In the example I gave, a storage bucket made open to the public would automatically be closed to public access (unless an explicit exception has been made).

Why do you need it?

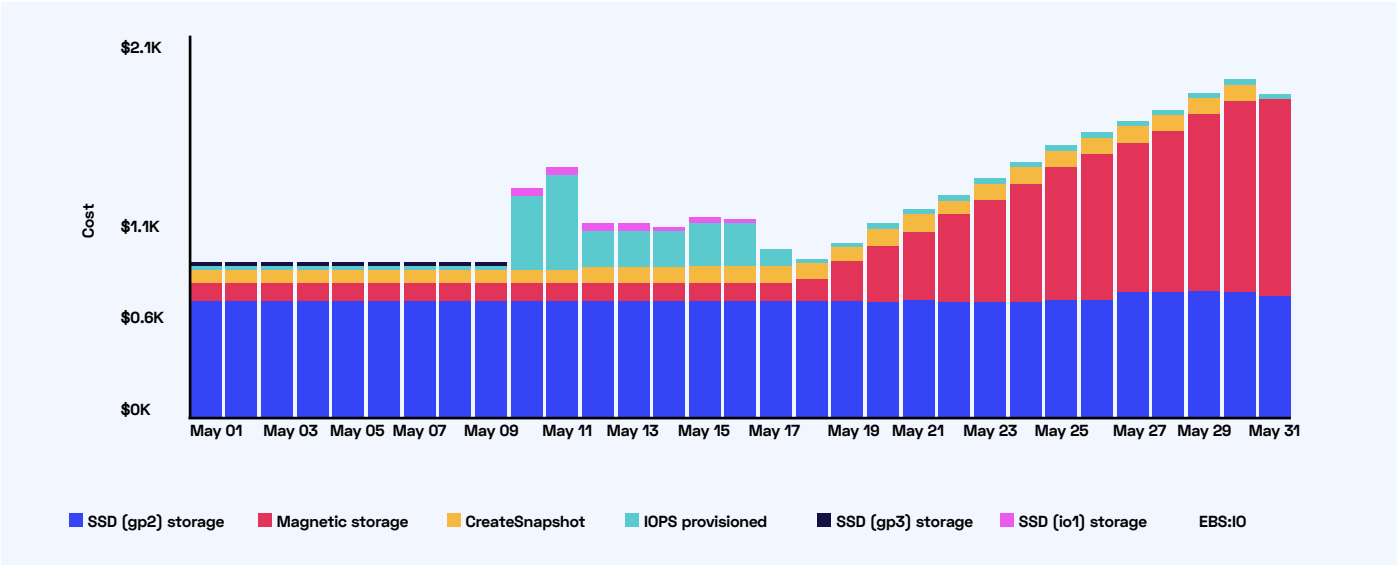
Good governance is one of the most important things currently missing from most estates. Without it, simple mistakes is made that either causes costs to spiral or leaves infrastructure in an inconsistent state. The below slide shows one example where a small configuration left behind 5000 EC2 zombie volumes. It was captured as part of an anomaly-spotting project, but with good cloud governance this problem might appear once, then we set a rule and then it never appears again.

EBS anomaly detected

Saving $1,000 / day = $470k / year

Anomaly found - costing **$1,000 / day**

5000 unnattached volumes cleaned up - launch template modified to fix this moving



Resource identification

In order to achieve good resource identification we really need to know 3 things:
What services are you are consuming - cloud features
What applications are using these services - company apps
Who owns these services/applications - unit or tech team responsible?

The first two of these require an organisation to have a configuration management database **(CMDB)**. This is essentially a list of all resources you're consuming (configuration items, CIs), ordered into logical layers, as appropriate for your company. Once all CIs have been discovered, it would likely make sense to group them into applications and then assign them to business units (BUs):

Tagging

In order to achieve effective governance of your estate, tagging is absolutely crucial. Each organisation will need to decide what tags are useful for them, but as a bare minimum we would suggest the following top-level tags:

- APP (i.e. Catalog search)
- BU (i.e. Retail)
- ENV (i.e. Dev)

Other tags that would likely be very useful for you include:

- OWNER (specific person or team that owns the resource)
- CREATED_DATE (automatic time/date stamp when something is built)
- CREATED_BY (i.e. Joe Bloggs, if created by specific team members)
- CREATED_PURPOSE (open text field to explain why a service was created)
- JIRA_TICKET (link to Jira ticket explaining why something was made – in theory all of your infrastructure should have a Jira ticket, so it makes sense to link it)
- CONFLUENCE_LINK (link to any corresponding internal wiki information)

By tagging the environments in this way we will far more easily be able to apply rules and budgets to:

- Services
- Environments
- Applications
- BUs

On top of that, engineers will more easily be able to identify what a particular piece of infrastructure is doing and who's responsible for it. As new members join your team this convention will help them understand which infrastructure the apps are being supported by, and who owns them.

It is also possible to have infrastructure auto-tagged where downstream services can be linked to a common resource. An example of this would be tagging an AWS server instance, then using metadata to discover which volumes were associated with that instance, and also tag those. This is a simple example, but much more sophisticated auto-tagging rules could be put in place, e.g. pulling details from git repositories or Jira tickets and applying those to infrastructure, adding much needed context.

CMDB

Creating a CMDB is not a manual task. Using a governance tool, you can easily discover all the resources in your estate and enforce certain rules on the infrastructure it discovers.
Examples of this might be:

- Do certain tags exist, e.g.:
  - APP, BU, ENV, etc.
- Are certain settings enabled, talking specifically about S3 buckets:
  - Encryption at rest enabled?
  - Encryption in transit enabled?
  - Lifecycle policy exists?

With these governance rules in place we can then decide if you want to:

- Skip - Take no action with CI that has been found to be out of policy
- Alert - Take no action but alert the necessary team that there is a rogue CI
- Act - Remediate the CI, for example enforcing s3 encryption settings automatically or removing s3 public access, etc.

As an example, if we see the 'Dev' environment tag, you may want to just alert and not remediate, as things are frequently changing in your dev environment. However, if we see the 'Prod' environment tag you may want to enforce your policy rules.

The key thing here is that all circumstances are captured because all of your cloud estate is being monitored. So if we insist that a certain tag MUST be present on resources, then you'll know when teams do not adhere to this. We no longer need to ask, we will know.

We can also use these governance rules to enforce auto-tagging of resources (discussed earlier), so for example setting an auto-tag of CREATED_BY would ensure every resource created by an operator has their name on it. Again, this is a simple example; much more sophisticated measures can be taken including calling APIs for data, etc.

The key thing here is that all circumstances are captured because all of your cloud estate is being monitored. So if we insist that a certain tag MUST be present on resources, then you'll know when teams do not adhere to this. We no longer need to ask, we will know.

Summary

The cloud can enable businesses to grow rapidly but without a good strategy you'll end up in a mess.

Technical staff are required to build a competence centre or a 'Cloud Centre of Excellence' (CCE). With this team in place better engineering and technical decisions can be made on behalf of the whole business. The CCE should oversee enterprise-wide technology decisions and responsible for introducing good governance of those tools.

By bridging the gap between business units, technical teams, and management, a CCE would make sure the right decisions are made, reducing technical debt and standardising the tools and technologies used in cloud environments.

Only through good governance, good tooling and good teamwork will an organisation achieve an optimised cloud environment. Time, money and effort needs to be expended up front in order that the future cloud environment is flexible, tidy and well governed.

Additionally, most tech stacks remain unprotected at some level. Therefore, there is a specific importance to cloud workload protection and open source vulnerability detection. We highly recommend organisations look at tooling to address these common blind spots.

There is an ever-growing variety of cloud solutions for performance and security. The right ones for each business are a needle in a haystack. Therefore, consulting an impartial cloud technology partner can save much of the investment in research, evaluation, and proper implementation.

Download Full Guide

Appendix: Example toolset

Below is a summary of example technologies needed to ensure good governance and effective security in cloud environments.

To learn more about them, make sure to read all 5 parts in this Cloud Strategy series! Download Full Guide

A

API Security

Application monitoring

C

Cloud cost reduction

Cloud Governance (SDO)

Cloud migration

Cloud Workload Protection

I

Identity Management

K

Kubernetes Security

L

Log management

O

Open Source Security

P

Passwordless Authentication

S

SD-WAN & SASE

Z

Zero Trust Access

GlobalDots Your Tech Innovation Partner

GlobalDots is a world leader in discovering and implementing cloud & web innovation. Over the last **17** years, GlobalDots enabled streamlining and smart growth in over **500** business customers, providing enterprise-grade web performance & CDN; Web Security & anti-fraud solutions; DevOps & Cloud services; Cloud Security; Corporate IT; Cloud-native networking and infrastructure.

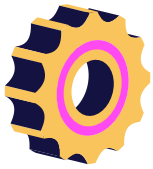
Our vendors range from world leaders to innovative, cutting-edge startups.

Our seasoned engineers test & master each solution's capabilities, pros, cons, and best practices. This allows them to quickly spot your perfect fit of technology and enable fast, smooth adoption.

The GlobalDots Innovation Edge

Innovation Hunters

Constantly tracking the industry to provide spot-on solution s for your ecosystem.

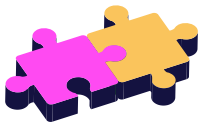


Vendor-Agnostic

Our ever-evolving portfolio and customizable solutions cater for each unique use case.

Streamlining Technology Adoption

Breezing you through from selection to deployment, exhausting every feature to your business benefit.



Holistic, Business-Oriented Approach

We align your IT architecture with your business profile, use case and goals focusing on what matters in terms of complexity and financial impact.

Do you want to know more? Contact Us