



Understanding the Costs and Benefits of Cloud Risk



Introduction: Understanding the Costs and Benefits of Cloud Risk	3
<hr/>	
Part 1: Defining Cloud Risk	6
<hr/>	
A. The Foundations and Economics of Cloud Risk	7
<hr/>	
B. Total Cost of Cloud Governance	8
<hr/>	
C. MTTD, MTTR, and the Realities of a Maturing Cloud Lifecycle	10
<hr/>	
D. Total Cost of Cloud Governance: Factors	11
<hr/>	
E. Managing Complexity is Key	13
<hr/>	
Part 2: Assessing Cloud Risk	14
<hr/>	
Part 3: Governing Cloud Risk	18
<hr/>	
Achieving Cloud Maturity	20
<hr/>	
Terminology	21



The cloud operating model offers companies unprecedented benefits — and changes the risk equation.

The cloud expands your potential for innovation, drives competitive advantage, and can significantly enhance your security and compliance capabilities. Unfortunately, as thousands of companies learn each year, it also extends the landscape of risk, adds complexity to your infrastructure and processes, and challenges traditional roles and responsibilities.

As technology workers ourselves, we understand the pressure on organizations to ensure resilience while also convincing senior decision-makers about the value and economics of governance. The key to meeting this challenge is to elevate your cloud maturity through improved strategy, better context, and increased automation so that you can more effectively assess and govern cloud risk.

The technology that embodies these capabilities is Policy-as-Code. But how you apply and scale this technology—and how you integrate it with your people and processes—depends on the unique goals of your business.

Which combination of people, processes and technology will help your organization best assess, manage and govern risk, with the lowest investment for the highest returns? That question is the subject of this paper. While the specific answer will be different for every organization, the overall approach is the same, as are the factors that companies must weigh when deciding how to elevate their cloud governance strategy.



What you will get from this paper:



Deeper understanding of how cloud governance addresses risk.



Insight into the economics and business considerations of governing cloud risk.



Expanded knowledge of the role of Policy-as-Code, automation, and scalability in cloud governance.



Insight into how the cloud affects security and compliance best practices, teams, and culture.



TERMINOLOGY

“As-Code”

Whether it’s policy, governance, security, or any other business activity, anything “as-Code” encodes human capabilities and activities in programming language. Doing so is powerful, because it transforms these activities into technological capabilities that are editable and scalable beyond human capacities.

“As-Code” is what makes the cloud (and cloud security) so game-changing, because it:

- Enables you to embrace exponential data growth.
- Enables consistency.
- Enables automation.
- Empowers you to build replicable libraries of code around key activities like configuration and policy-enforcement.
- Creates potential for “immutable infrastructure” that is deployed and maintained in code without manual intervention, which means less scope for error and therefore less chance of risk.

Examples

- **Policy-as-Code (PaC)**
Using code to define and manage the rules and conditions that make up the policy.
- **Governance-as-Code (GaC)**
Using Policy-as-Code to automate the governance of a system and share the information across teams.
- **Security-as-Code (SaC)**
Leveraging Policy-as-Code to define and manage the security rules and definitions that make up the intended policy.
- **Regulatory-Compliance-as-Code (RCaC)**
Leveraging Policy-as-Code to map compliance regulations to compliance policies.



Part One

Defining Cloud Risk



The Foundations and Economics of Cloud Risk

To do business is to engage in risk. After all, business is about defining goals, baselines, and tolerances, and (since to err is human) deviating from them from time to time. The cloud compounds risk by exponentially expanding the chance that an error or misconfiguration will make you deviate from your goals and baselines.

But the cloud also drives unprecedented opportunity for growth and innovation—and for greater resilience.

Google Cloud CISO Phil Venables recently made this last point when he described how the cloud, rather than forcing new notions of security, empowers security professionals to actually achieve first principles of security like least privilege, segmentation, and default denial.

Established in the Stone Ages of the 1970s and 80s, these security ideas emerged at the dawn of business computing, but weren't always feasible in the context of enterprise software. As it turns out, they work exceptionally well in the context of cloud security.

As Venables summarizes, *"it's not a case of shifting on-premises mindsets to the cloud, but of going back to first principles and realizing that what you struggled with in on-premise, you can now do in the cloud."*¹

As for the economics of risk? The cloud can be a help and a hindrance there too. As the cost of governing risk goes down, it stands to reason that companies can continually increase their risk baseline as what was once 'risky' becomes easier to secure. Add to that the business advantages of cloud or hybrid environments, and there's a lot of growth potential.

On the other hand, as we will see below, the calculus of cloud risk and reward is far from simple, and we're only in the early days of understanding the economic implications of the full cloud lifecycle. But one thing we at Secberus know for sure: the economics of cloud risk is probably the most important consideration for CISOs as our collective understanding of the cloud's impact matures.





Total Cost of Cloud Governance

According to IBM Security's 2021 *Cost of a Data Breach Report*, the average total cost of a data breach in 2020-2021 was USD \$4.24 million – that's an increase of 10% over the previous year. The average per record² cost of a data breach also increased about 10%, from \$146 in 2020 to \$161 in 2021. The most common initial attack vectors were compromised credentials (20%), phishing (17%), and cloud misconfiguration (15%).

Security breaches almost always begin internally as a failure of governance – generally some kind of misconfiguration, whether it's neglecting to encrypt applications, failing to restrict data access sufficiently, misconfiguring security groups, or insecure software development that creates unintended functionality that threat actors can leverage.

These errors then create vulnerability to internal and external threats. An internal threat might be a disgruntled or dishonest employee who wants to target the company or personally benefit from its assets (such as by selling intellectual property, customer and employee PII, etc.). External threats include exposing the company to bad actors who either happen upon an "open door" and exploit it, or advanced persistent threats with broad geopolitical and economic implications.



The risks posed by the cloud:

- **Internal vulnerabilities** – Employees, partners, or others acting from within.
- **Misconfiguration risk** – Neglecting to configure the proper requirements to uphold the level of security the business needs.
- **External cyber-threats** – Bad actors outside the company taking advantage of vulnerabilities.
- **Stalled growth** – The risk that addressing the issues above slows the pace of innovation and growth, and lowers returns on your business investments in people, processes and technology.

These risks raise important questions for the business:

No. 1

Are we secure? Compliant? Under attack?

No. 2

What is the total cost of addressing these risks over the long term?

No. 3

Do the potential returns of our cloud strategy outweigh these costs?

No. 4

If not, how do we right-size our costs to drive the most value from our cloud investments?

Your team might successfully protect the company from configuration risk, vulnerability risk and activity risk (attacks), but if the costs to do so are too high, you're still operating at a loss. You're also missing out on the full promise of the cloud: competitive advantage, growth, efficiency, and streamlining. If you're not seeing this promise realized, that failure to optimize can represent an additional significant economic risk if your competitors and partners *are* seeing growth.

In other words, if security is costing too much, requiring too many resources, and exacting too high a toll on your organization's agility – then that is not only an erosion of value but also a significant business risk in itself.



MTTD, MTTR, and the Realities of a Maturing Cloud Lifecycle

The security industry measures the effectiveness of cloud governance through metrics like Median Time to Detect (MTTD) and Median Time to Remediate (MTTR). These metrics offer important insight into how effectively your security approach is working compared to global benchmarks and when measured against your own goals. Generally speaking, the lower the MTTD and MTTR, the lower the impact of breaches across multiple categories of cost, from reputational impact to fines.

But these metrics don't necessarily help the business understand the overall effectiveness, costliness, or value of its cloud governance strategy. For that, you must evaluate total costs, from initial acquisition costs, maintenance, and operating costs to remaining costs as assets lose value over time.

But when we're talking about the value of your cloud governance strategy, we're not just dealing with infrastructure. There is also compliance, workflow efficiency, culture and risk to consider. Risk is an especially important input, since governance revolves around assessing and mitigating risk in addition to pursuing business objectives.

The good news is that we're arriving at that stage of the technological lifecycle where analysts can understand more clearly the longer-term impact of the cloud on business.

In their analysis of the cloud's longer-term economic impact on business growth, "*The Cost of Cloud, a Trillion Dollar Paradox*," analysts Sarah Wang and Martin Casado observe a distinct pattern once companies hit scale. As companies achieve scale, they hit a wall of diminishing returns: "*when evaluated relative to the scale of potentially lost market capitalization [...] the calculus changes.*"³

As we better understand the general economic impact of the cloud across the entire cloud lifecycle, from creation/migration to scale, we're becoming more adept at weighing the full impact of taking on, assessing, addressing, and accepting cloud risk – the costs and the potential returns. Businesses that understand this are better positioned to choose the right path.





Total Cost of Cloud Governance: Factors



We are not proposing a specific Total Cost of Cloud Governance calculation; rather, we're exploring the economic factors that businesses should account for when they are building or migrating some or all of their applications to the cloud, designing security strategy, and making decisions about their tech stack, workflows, and goals.

Risk isn't an absolute; it's a spectrum. Some parts of a company can take on more, and others should take on less. The "secret" of successful security is knowing which parts of your company fall into which category. Simply put, the "secret" isn't really a secret at all – it's good governance.

Building a governance strategy begins with understanding the cost and value of the various factors that impact that strategy. Like any analysis of cost, value, and returns, these factors fall into the broad categories of potential costs/risks and benefits/returns.



Costs/Risks

Some of the key costs and risks associated with experiencing breaches, mitigating against attacks and vulnerabilities, misconfigurations, missed opportunities/slowdowns, etc.

Type Of Risk/Cost

Examples

Costs and risks associated with experiencing attacks/vulnerabilities.

Forensics, hotline support, free services/accommodations/discounts in lieu, internal investigations and communications, reputation loss, lower customer acquisition/additional marketing costs, fines and remuneration, etc.

Costs and risks associated with addressing vulnerability.

The resource and tool cost to investigate and address the vulnerability.

The full costs of your governance assets (people, processes, technology):

- Pre-acquisition costs
- Acquisition costs
- Operating costs
- Maintenance costs
- Downtime costs
- End of lifecycle costs
- Talent (attracting, retaining, retraining) costs and risks

Benefits/Returns

Some of the key returns and benefits of the cloud despite the associated risk, with the right governance strategy in place.

Type Of Benefit/Return

Examples

The value of your cloud governance assets (the returns you are getting from them in terms of growth, opportunity, security/peace-of-mind, culture).

Improvements in productivity and efficiencies for SOC, governance team, compliance team, CSA/CSEs, developers, CISO/CTO/management of moving to encoded, automated, scalable digital solutions.

Reduced hardware and connectivity costs associated with cloud solutions.

Built-in resiliency of cloud services:

- Security capabilities integrated at the scales required of cloud services providers.
- Capabilities that must operate reliably across providers' client base.
- Bonus capacity that enables you to enjoy a level of security specialization you might not be able to build yourself.



Managing Complexity is Key

Being able to manage the complexity of cloud security drives significant economic value for any business, according to IBM Security's 2021 *Cost of a Data Breach Report*. As the report summarizes, organizations with "high system complexity (tools, systems, devices, data, users)"⁷ experienced average data breach costs that were more than 50% higher (USD \$5.18m) than those paid by organizations with less complexity in their systems (USD \$3.03m).

The researchers also found that while identifying and containing a breach took 287 days (212 to identify, 75 to contain) on average,⁸ having capabilities in place that addressed complexity significantly reduced this time. For example, companies with security AI and automation fully deployed reduced their resultant costs by a whopping 80%.⁹

From these findings, we can extrapolate a few truths about cloud risk. The first is that technology is key—but in a very specific way. Technology that reduces complexity, that helps companies streamline their "tools, systems, devices, data, users," is of massive benefit. The second is that this technology is more useful when it

is further along its maturity lifecycle. Note that businesses only realized the reduced costs associated with security AI and automation once those technologies were "fully deployed." The third is something we know by virtue of our business: that neither of these first two truths is possible if you attempt to manage risk 'the old fashioned way,' through point solutions, trendy tools, or by throwing more engineers at the problem.

In short, the solution is to simplify complexity through a governance strategy that takes a business-first approach centered on innovative technology, centrally managed security, and automation.

7 – IBM Security, *Cost of a Data Breach Report 2021*, IBM: Armonk, NY, July 2021, p. 42.

8 – *Ibid.*, p. 22.

9 – *Ibid.*, p. 38.



Part Two

Assessing Cloud Risk



As we saw above, managing complexity is key to managing cloud risk. The only way to close gaps and break down the silos that drive complexity is by using technology that can automate key aspects of cloud security implementation and maintenance, and gather context data so that the right people can make appropriate decisions in real time with high accuracy. This technology is Policy-as-Code.









Policy-as-Code is simply business policy written in a programming language like Python, YAML, or Rego. By encoding policies, you benefit from all of the capacities of digital technology – like automation and scalability.

Whereas traditional tooling for policies is generic and applies policies in bulk, Policy-as-Code allows you to be specific about how you will apply and verify policies.

The extensibility of Policy-as-Code also allows event-based triggering to work extremely efficiently. For instance, you can call only the APIs of the resources relevant to the policy that you need to verify. This capability lowers your MTTD, makes inventory more accurate, reduces the cost of your API calls, and doesn't miss any introduced risk.



Policy-as-Code allows you to:

-  **Organize and govern your cloud infrastructure** – Organize applications, cloud accounts, resources and teams based on specific business criteria (regulatory compliance, business units, integrations, etc.) within your governance solution (including cloud security posture management, or CSPM functionality). Ensure that the specified organizational criteria comes from pre-existing tags in the cloud environments that you have already created. Policy-as-Code lets you do this without needing additional engineers to manually and continuously search for cloud resource tags and assign tagged resources to specific OUs in your CSPM, or create custom scripts to add cloud environments and resources to appropriate account groups in the CSPM.
-  **Map your regulatory compliance requirements to your policies** – Map regulatory compliance requirements to custom policies and specific scopes of applications, OUs, divisions, clouds, and cloud accounts.
-  **Manage your cloud posture with fewer third-party tools** – Apply a cloud security posture management (CSPM) approach with minimal costs and without as many tools.
-  **Reduce/eliminate false positives** – Fully customize policies for your specific needs, from business intent to resource ownership. This approach allows you to eliminate virtually all false positives and allows resource owners to move faster, receive only true violations, and accelerate remediation.
-  **Clearly define, globally manage** – Build highly specific policy that accurately reflects the unique needs of your business.
-  **Use as many policies as you need** – Build a global cloud security strategy that contains all the policies you need, no matter how many, and apply this strategy to specific OUs, applications, and environments in order to monitor and manage drift from intended baseline security configurations. Ideally, your Policy-as-Code platform lets you do this without limitations on policy customization. These limitations can contribute to a high false-positive alert rate and longer median time to remediate (MTTR).
-  **Eliminate alert fatigue** – Some industry benchmarks estimate that the average enterprise spends one full business day on triage for every 32 alerts—and enterprises can easily surpass 500 alerts per day. Policy-as-Code helps minimize alert fatigue and get the most from advanced workflow capabilities without the need to hire more people to do triage and investigation.
-  **Scale your governance policies** – Auto-scale global governance policies (security, compliance, operations) as your cloud footprint and tools evolve from a single platform—ideally without needing to build internal applications to determine your global governance posture and having teams manually apply and investigate generic policies.



How the cloud affects security and compliance teams, best practices, and culture

The technology that enables and automates the symbiosis of business strategy and security strategy is Policy-as-Code, but it's also important to understand the human part of the equation.

This table summarizes the roles of the various teams in assessing risk and what it means to take a top-down/business-first approach to cloud risk:

○ Board & C-Level

We typically view the security role of the Board and senior management to be primarily staying up-to-date on cloud governance strategy, security strategy, cloud journey strategy, and auditing. But it is becoming increasingly clear that these senior decision-makers should also take an active role in supporting risk governance by considering the potential security implications of every business decision. Security is not just an IT issue or a compliance check box; it's integral to growth and competitive advantage.

○ Compliance

Compliance plans the compliance policies and risk framework, and implements compliance policies.

○ CSAs & CSEs

Cloud Security Architects and Cloud Security Engineers plan security policies and the overall risk framework, and implement security policies.

○ CTO

The CTO's role is to define the cloud journey strategy and implement and refine the cloud journey. They also provide important input into cloud governance and overall security strategy.

○ Developer

In many organizations, Development is where the bulk of security strategy creation and maintenance happens. Policy-as-Code changes the equation by letting development teams easily inform, maintain, and implement business-defined cloud strategy. Development can focus on exception management and remediating violations, and stay up-to-date on risk and compliance posture, notifications, and reporting.

○ Governance Team

The Governance team plans and implements the key activities of cloud governance: defining security policies, defining compliance policies, and planning the risk framework. They're also responsible for reporting and auditing.

○ SOC

SOC is responsible for assessing logs and activity within the environments. They also look at information about vulnerabilities and then search for those in their environments.



Part Three

Governing Cloud Risk

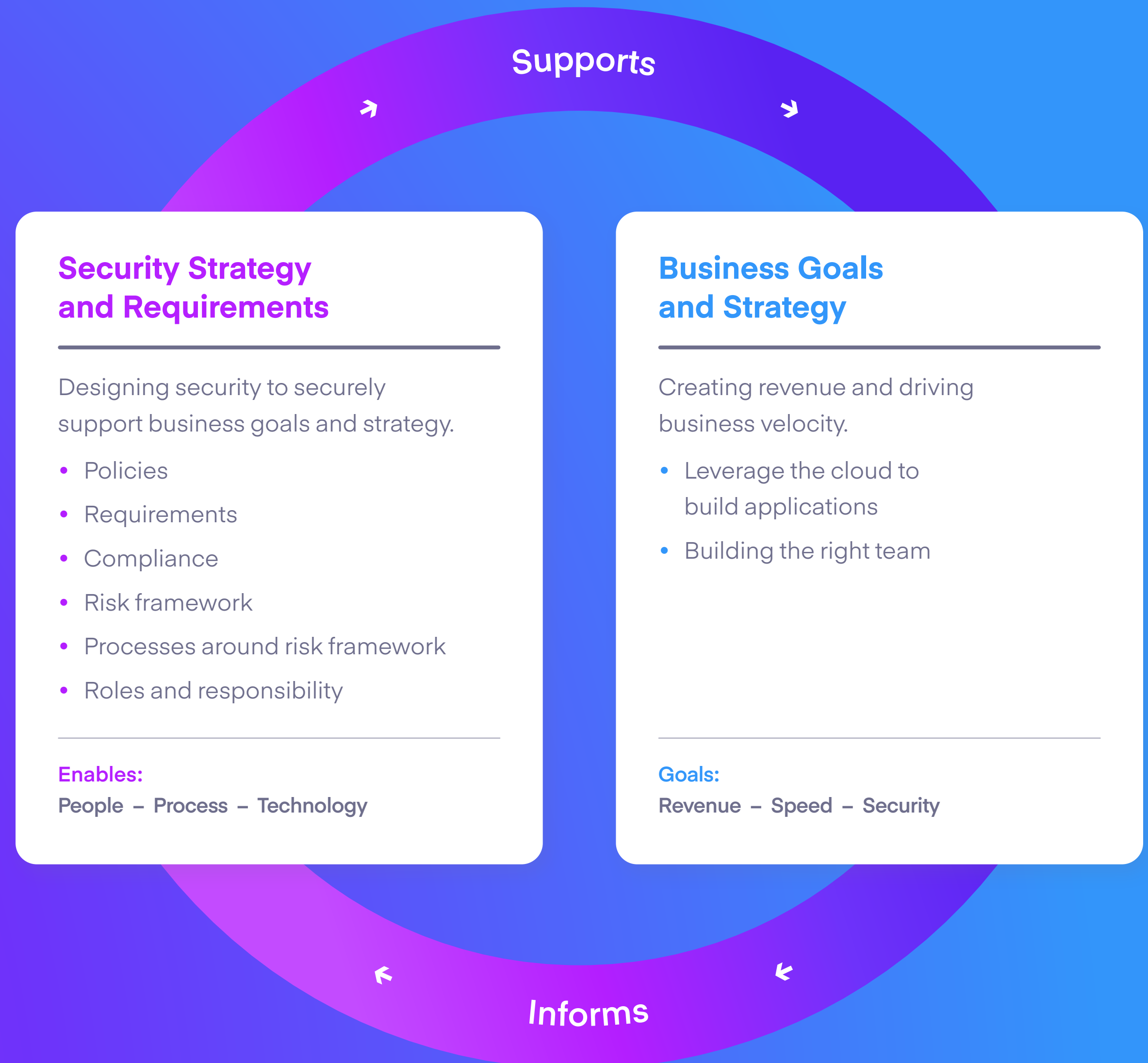


Cloud Governance: The relationship between business strategy and security requirements

For mature cloud governance, the main task of your security strategy and requirements should be to support the business' goals and its strategy for meeting those goals.

What does it look like when a company is 'doing cloud right'? It looks like symbiosis between business strategy and security strategy. You are taking advantage of Policy-as-Code to define and manage the security rules and conditions that express your intended policy. (That's Security-as-Code.) You're doing the same when it comes to regulatory compliance: using Policy-as-Code to map compliance policies to security policies and ensure that compliance is continuously and automatically monitored (Regulatory-Compliance-as-Code).

And when you use Policy-as-Code to automate governance of your security strategy and share information across teams, that's Governance-as-Code. Governance-as-Code also encodes workflows (call it 'Workflows-as-Code') to manage and share security and compliance at the speed of business. In this way, security and compliance help accelerate the business and make it more agile, rather than slowing it down.





Achieving Cloud Maturity

The capabilities described on the previous page enable the kind of robust streamlined and simplified governance expressed by the top tier of the IANS/Securosis/Cloud Security Alliance *Cloud Security Maturity Model (CSMM)*.

According to the CSMM, companies achieve cloud maturity when security:

- Is centrally managed.
- Covers all domains.
- Is integrated into infrastructure as code.
- Is built into the stack with provisioning automation.
- Has federation and MFA working consistently across tool chains.

This model offers the industry benchmark for understanding where your organization sits relative to others and relative to an ideal. It also gives you a roadmap for the overall approach you should take to 'level up' your cloud governance practices. But all of these goals and objectives also encompass activities that right-size your total cost of cloud governance, lower the costs associated with breaches, streamline your processes, simplify complexity, and ensure that the right resources are doing the right things at the right time.





○ Cloud Governance

An oversight practice where business goals drive security decision-making. It blends real-world experience, best practices, and technology to support and scale security decision-making, automate things that should be automated, focus people's attention where they can be most effective, and use the superior computing capabilities of technology to manage compliance and risk.

○ Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation exploitable by a threat source.⁴

○ Misconfiguration

An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.⁵

○ Risk

The Cloud Security Alliance defines risk as *"A subset of 'business risks' and, as such, should be talked about in business terms. Instead of defining risk in technical terms, cybersecurity professionals [...] can adopt the definition of risk used by almost every business manager and board of directors: the potential for monetary loss. In this context, 'risk' is the possibility that an event will lead to reduced profitability."*⁶ We concur, adding that risk is really any possibility that an activity will deviate from your business's defined baselines, goals, and tolerances. Risk is not inherently good or bad, and different parts of the business can often take on different types and levels of risk.

4 – National Institute of Standards and Technology. [Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments](#), National Institute of Standards and Technology, 2012. Gaithersburg, MD.

5 – [NIST Information Technology Laboratory Computer Security Resource Center Glossary](#).

6 – Angle, Dr. James. [Information Technology Governance, Risk, and Compliance in Healthcare](#). Cloud Security Alliance, 2021. Seattle, Washington: United States.



If cloud maturity is your goal (and it probably should be, whether that goal is realized through complete migration to the cloud or a hybrid model), the clearest path to that goal is cloud governance. Cloud governance simplifies complexity, and it is complexity that drives up risk and costs. This is also why point solutions or ‘tools-du-jour’ sometimes create more issues than they resolve—because they add to, rather than mitigate, complexity.

Finally, as a solution provider, we believe it’s crucial to choose cloud partners and providers who share your cloud governance vision. At the end of the day, while Policy-as-Code is key, it needs to be designed and deployed in ways that are flexible and that meet the unique needs of your organization.

**To learn more about
our approach to cloud
governance, or to speak
to us directly, visit us at:**

 secberus.com