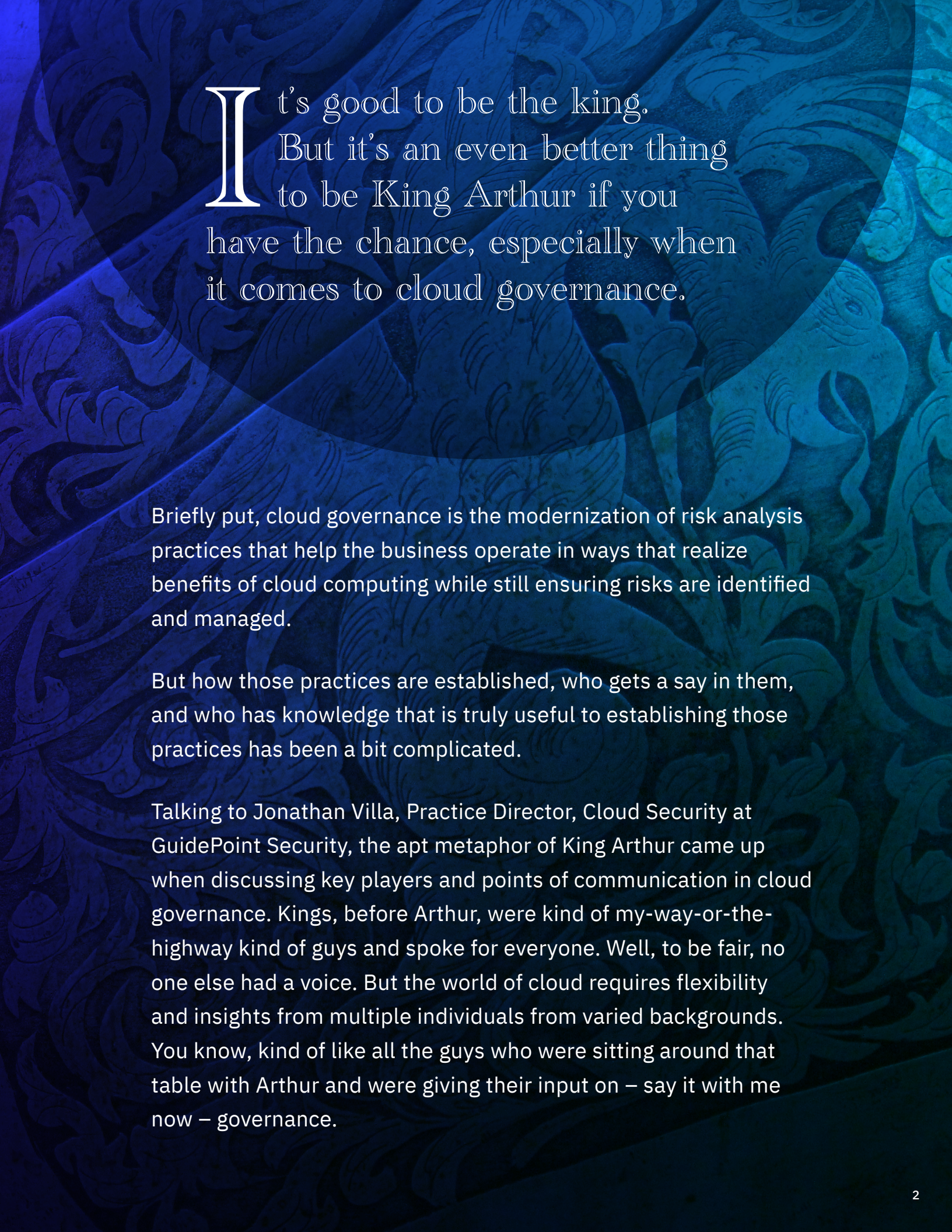


EBOOK

King Arthur and  
the Knights of the  
Cloud Table



**GUIDEPOINT**  
SECURITY



It's good to be the king.  
But it's an even better thing  
to be King Arthur if you  
have the chance, especially when  
it comes to cloud governance.

Briefly put, cloud governance is the modernization of risk analysis practices that help the business operate in ways that realize benefits of cloud computing while still ensuring risks are identified and managed.

But how those practices are established, who gets a say in them, and who has knowledge that is truly useful to establishing those practices has been a bit complicated.

Talking to Jonathan Villa, Practice Director, Cloud Security at GuidePoint Security, the apt metaphor of King Arthur came up when discussing key players and points of communication in cloud governance. Kings, before Arthur, were kind of my-way-or-the-highway kind of guys and spoke for everyone. Well, to be fair, no one else had a voice. But the world of cloud requires flexibility and insights from multiple individuals from varied backgrounds. You know, kind of like all the guys who were sitting around that table with Arthur and were giving their input on – say it with me now – governance.

# W

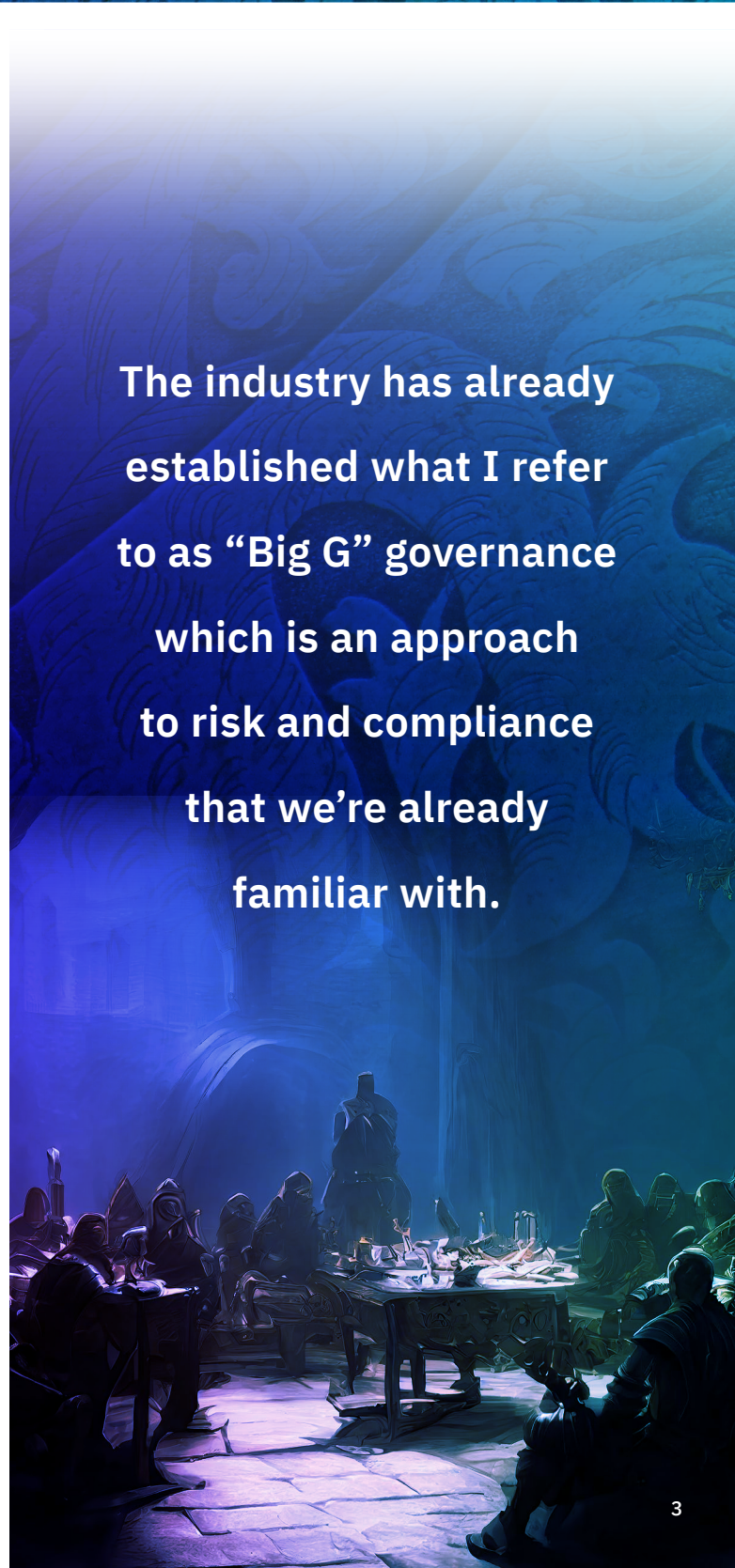
## hat does “cloud governance” mean? What are the key features?

So why do they need to segment off cloud governance? Cloud governance is about going deeper into blending the risk perspective, i.e., identifying threats to the business, with an understanding of the technology and modern processes used to build and support modern technology patterns.

Traditionally governance folks have had a fair understanding of technology and well-known risks to traditional technology and have done a great job at communicating and articulating those risks. This was partly driven because the business owned the data center or if using a collocated service, it was also within a known architecture type and operations model of a data center. But with Cloud governance the variable is that what you’re being asked to govern, or to establish rules for, is a platform that you do not have full control over. It’s a Shared Responsibility Model. Additionally, the standard tech stack changes frequently with the availability of more cloud services as well a new capabilities from various vendors.

You shouldn’t be taking the historical, or the traditional approach to governance in the cloud. Meaning, you can’t come in with a static checklist and say, here’s everything we need to do. You have to first understand how the environment is utilizing cloud services. The approach to securing IaaS vs. PaaS vs. SaaS will be different. But more importantly is understanding what Cloud computing is. It’s no longer, “we had new software shipped to us on a CD and we’re going to install it on a server”. While those days were fun and an opportunity to sneak away into the cold data center, away from

**The industry has already established what I refer to as “Big G” governance which is an approach to risk and compliance that we’re already familiar with.**



everyone else, cloud has now brought the data center to you and fully accessible from the comfort of your office chair or living room sofa.

---

## Cloud has revolutionized how we deliver in the industry.

---

It's changed aspects of society as well. Everything in today's world seems to be driven by cloud in one way or another and business' understand this and want to leverage the benefits of cloud computing. As a person responsible for governance in Cloud, you have to learn how to apply the skills that you've built over time with respect to identifying and managing risk and come to the business with a plan

of enablement. You have to do your due diligence to understand the platforms and bring a risk perspective that understands what the true risks are. You cannot take a static approach to defining what are dos and don'ts. More importantly, you have to learn how to collaborate with the architects and engineers. You'll learn more over water cooler conversation and lunch and learns (perhaps sitting at a *round table*) with cloud practitioners than attending a week long training session on cloud security.

That's what makes cloud governance different from the traditional Big G governance. It requires a broader and deeper understanding of the tech stack and processes, knowledge that not many have on their own or can learn in a week through a book or virtual training. It requires more collaboration, i.e., something akin to a round table set for collaboration.



# W hat's the biggest issue in cloud governance? How is this issue being dealt with currently?

I don't know where I heard this, but it's been in my head for almost my whole life. It's a quote from somewhere:

---

“people perish because of a lack of knowledge.”

---

I think that the biggest issue right now in cloud governance is a lack of practical cloud knowledge. I've been in the industry for 23 years and a lot of times people would say about me, “jack of all trades, master of none”. I would respond with, “jack of all trades, master of none, is always better than a master of one”. I've worn many hats in my career. I started working with Cloud as a platform around '07 or '08 — very, very early, and since then I have shared what I've learned in my various roles to help people rethink about risk and security in cloud computing. I've sat at tables wearing different hats: developer, system admin, PCI advisor, risk analyst, penetration tester, and more. I've learned to collaborate as I've been part of teams adopting cloud in various industries.

Early on, one of the biggest issues I encountered was an unwillingness by some to become educated on what cloud computing is. Some saw it as a new form of virtualization instead of a new architecture

and delivery pattern. A lot of people were coming from the security side and were very stringent. They would have their checklists in hand. The cloud teams would swiftly respond with,



“that’s not how it’s done in the cloud” or “that’s not even supported in the cloud”. It was challenging getting folks to break away from their way of thinking and the biggest hindrance for security to be an early influencer in cloud computing.

Again, I’ve said “people perish because of a lack of knowledge”, but it’s not just on the security side, it’s also been on the cloud engineering side, too. I believe that cloud engineers weren’t as educated themselves. There was a lot of misinformation, a lot of misunderstanding. They would say things like, “well, you know, Microsoft, or Amazon, they’re secure so we’re secure, right?” On the flip side, you would have security people that have said, “well, we don’t trust Amazon, and we don’t trust Microsoft” without understanding how cloud services worked.

Today, in 2023, fortunately it’s a different world. The security folks have now been at this for four, five, or six years. They’ve even said, “if you do it right, you can actually be more secure in the cloud so we want you to move to the cloud because there are improvements in how things are done.” The industry is pushing automation and standardization. Standardization is a friend to security. Automation can also be a friend to security. There’s comfort in knowing that you can approve a process and rinse, lather, and repeat. It’s all done the same each time. Not to get too technical, but the focus can now be on reviewing pipelines, image creation processes for immutable architecture, and deployment policies with smaller sample sets to

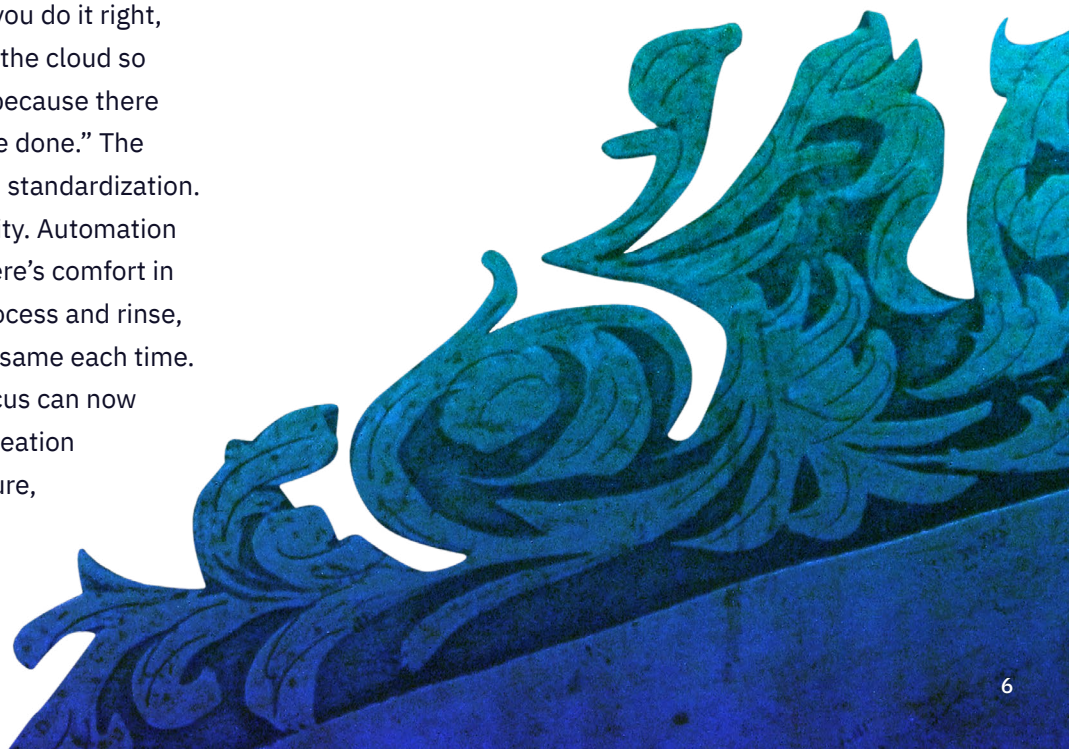
validate. Back to the other flip side, the cloud engineers. They have gotten more educated and more informed on security. I would say that cloud engineers have moved closer to the middle than most security people have.

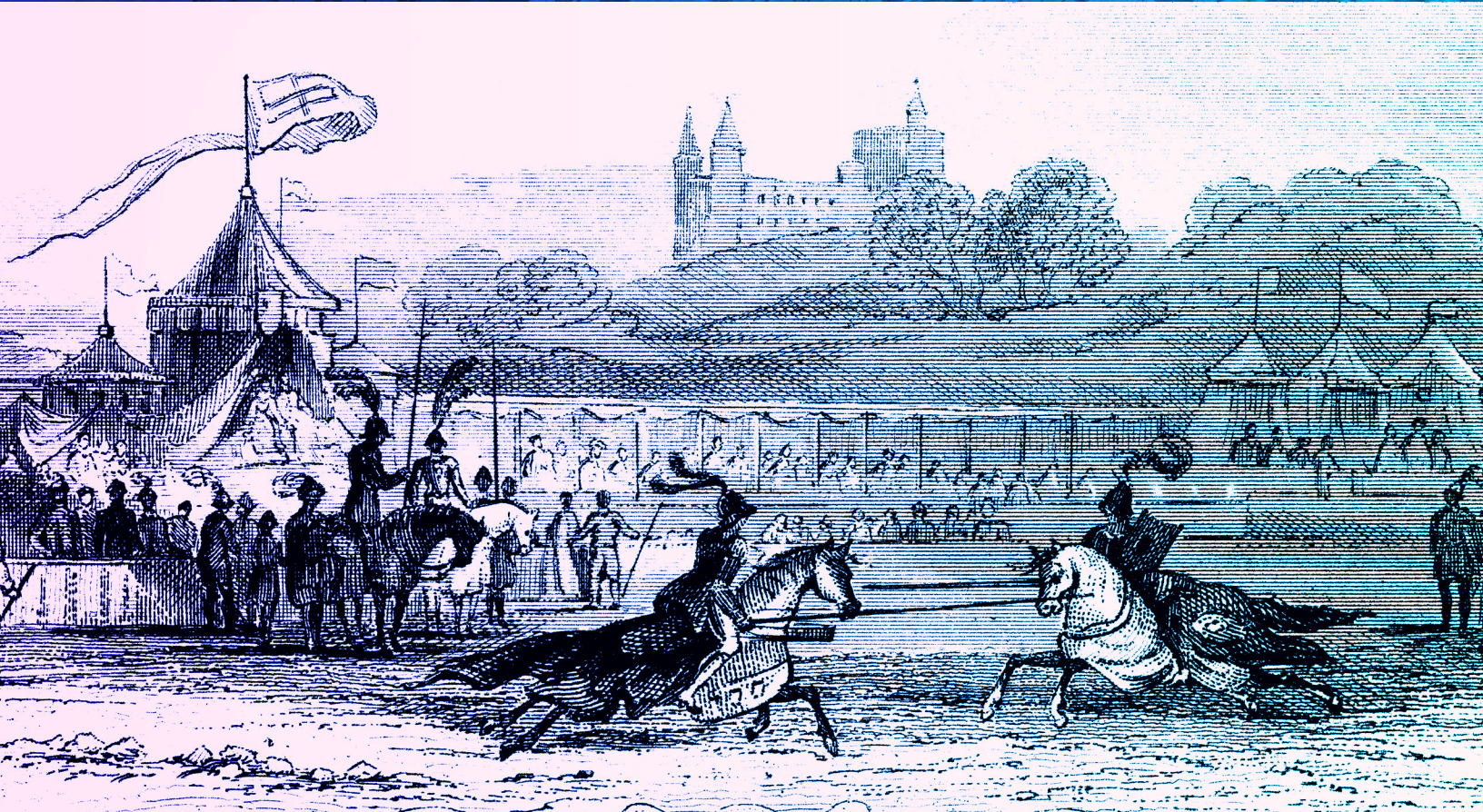
So what is currently the biggest challenge? The biggest challenge right now is finding the right individuals who can speak to the business, speak to the technology, and understand risk. We need more people to really understand all sides. In my observation, a lot of people have gone a certain distance and get comfortable. The issue that’s facing cloud security is that we really need people to keep making steps forward and maintain pace with the technology side.

---

Creativity is key in cloud security. My team works creatively to identify controls that enable business innovation. That is one thing that sets us apart.

---





Imagine walking into Home Depot. They seem to have everything. For example, they have four or five different types of plywood, they have countless tools, they have many options for various projects. When the average lay person that walks in, they don't know what to do with all those tools and materials. However, if someone like my brother-in-law, who's a master carpenter and is also creative, walks into a project his questions are, "what do you need and what do you want?" He has foundational knowledge and skills that allows him build almost anything.

I guarantee the word creativity is said by me to my team many times. Somebody asked me, "what do you think your biggest skill set is?" I said, "creativity". I can figure stuff out, basically. I've been in a lot of different situations throughout my career. When it comes to cloud, I've worked in PCI compliance, HIPAA, as a system administrator, a web developer, a pen tester. I've done all kinds of stuff. I've even been the court jester at work sometimes. Those diverse skills have enabled me to be creative when I'm solving problems in the cloud.

**It's seldom you find somebody that can really talk about cloud and risk at the same time. But when they do, they're very creative at identifying risks in the cloud or explaining why risk is mitigated.**

# W

# hich positions are key in cloud governance responsibility within an organization?

I don't think that it's a particular position, like a person. There's a term: the Cloud Center of Excellence. There's a lot of Centers of Excellence, a collective of representatives from different parts of the company. Within these groups, there are definitely Knights of the Round Table and there's still likely a King Arthur,. But that's just because any group like that should have a single voice.

Those organizations that have a well-formed Cloud Center of Excellence (CCoE) are, in my opinion, the most mature when it comes to cloud security because they have representation from various groups. The best organizations have representation from GRC that understand modern architecture and patterns as well as engineers, all being stakeholders in the CCoE. So again, not necessarily a key position, but a key group: The Cloud Center of Excellence.







# How is cloud governance evolving? What can we expect next?



The future is dependent on education and the pace of learning. Governance has typically been a clipboard with a checklist asking, “Are you doing this? Are you doing that? Thou shalt do this, thou shalt do that”. But now, because cloud is an API driven infrastructure, environments and tools are automating and broadening their reach over cloud services.

Even if you’re pointing and clicking in a web console, you’re making API calls to the underlying cloud platform. That API is also available for decision making on the governance side. I’m seeing more tools consume cloud IaaS and PaaS information and presenting it within the lens’ that GRC understands.

However, and perhaps as a warning, I’ll say it again, there’s a difference between little g governance and big G governance.

Technology is starting to allow for those individuals who think about how to protect the business to see cloud environments with a quantifiable risk. They’re able to now start using some of these platforms to operationalize some of their decision making, and to get immediate feedback and metrics.


So if I can put it all together, step One was, “we don’t trust the cloud”, or “you got to do it the way we know how to do it”. And then step two was, “hey, we understand a little bit more of the cloud. We’re totally open to you moving to the cloud and here’s some of the things that we think you should be doing”. Step three is going to be “we know cloud, and guess what? We’re going to automate our governance.”

---

Cloud governance requires proactive and constant collaboration with the architects and engineers leading the way.

---

**There are a lot of technology platforms that throw the governance label atop their capabilities. It’s little g governance. Big G governance is more risk-based decision making versus boolean values representing configuration state.**



## All told – why is a “round table” culture in cloud governance important?

Because a round table encourages equity and a plurality of inputs from diverse voices to derive the most creative solutions in an ever evolving landscape and transmit them with a single voice. A round table culture can become the vehicle by which these ideas are passed from one generation of analysts, engineers, and cybersecurity specialists to the next. Culture imparts meaning so that every generation can properly respond to it and fulfill its ideals. And what better culture to emulate than one as storied and as aspirational as the legend of King Arthur and the Knights of the Round Table.



# GUIDEPOINT

SECURITY



2201 Cooperative Way, Suite 225, Herndon, VA 20171  
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132  
03.2023