Managing cloud risks with a

CLOUD SECURITY ASSESSMENT

SECURITY PURSUIT

New Risks in Your Cloud

Whether you have a small portion of your systems, or your entire infrastructure in the Cloud, it is extremely easy for new security gaps to open.

There are several reasons for this:

1. Operations Over Security.

When moving to the cloud, you need to prioritize operational stability. There are literally thousands of configuration choices, and your first priority is to ensure a smooth transition with little or no downtime. It's common for IT teams and consultants to skip or simplify security configurations. One or two mistakes is understandable and easy to correct later. But they add up and several minor configuration mistakes can result in a very vulnerable cloud environment.

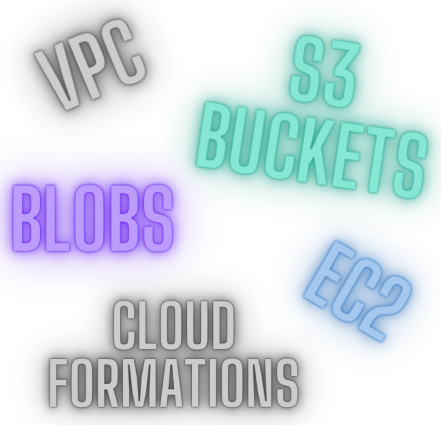
Is your cloud environment optimized for security now that you are operationally stable? Did you make short-term security compromises to ensure a smooth transition? Did you correct them all?

2. Shared Responsibilities

One primary benefit of the cloud is that you offload much of the traditional work of maintaining an operational IT architecture. This results in a shared security environment. Your Cloud vendor is responsible for securing their cloud, but you are responsible for security what's in your cloud. This sharing of responsibilities requires you to know where your responsibilities start and stop. While that sounds straight forward, in reality it is complicated.

Do you know where your security responsibilities start and stop? How do you know if you are making an assumption that you shouldn't be?

3. A New Language. A New Skillset.



New technology brings new risk. You are used to that. But moving to the cloud introduces a whole new language and significant new skills. Despite taking courses and reading about new best practices, learning the full extent of the cloud security skills required takes time. It is not reasonable to know everything by the time you finish deploying.

Has your team learned the language and required skills to maintain your cloud environment? Did you use a consultant, and did they setup your cloud to really protect you the way you needed them to?

4. Everyone Gets Access.

A benefit of the Cloud is that it allows for more access and openness. The openness facilitated work from home, vendor and customer access, and shared services. But, with this expanded capability comes an expanded attack surface. Permissions, logging, data management, and incident management all become more complicated in a perimeter-less environment. While MFA is practically required now, it is not absolute protection against the larger risks.

Do you have subnets not assigned to a group? Are access keys rotated sufficiently? Do you have Blob Containers with public access?

5. Constant Changes.

One of the biggest benefits of the cloud is the ability to spin up and tear down resources on demand. This is usually done with pre-set parameters. Expanded use often happens without IT knowing until the bill comes at the end of the month. In addition, to stay competitive, Cloud vendors are constantly changing services, adding new 'features' and updating the environment. These changes create continual new risks.

How are you staying current with changes to your cloud environment? Have any recent changes shifted your risk profile?

6. Hackers Love the Cloud, too.

Of course they do! Anything new gets examined by the criminal community to find new and innovative compromises. As always, criminals are learning the Cloud faster than the cybersecurity industry. New threats and vulnerabilities unique to the Cloud are are being found.

Are you keeping up with the latest vulnerabilities to your Cloud environment? Are your tools designed for your Cloud?

How is a Cloud Security Assessment Different?

AWS, Azure and Google Cloud Platform (GCP) have the same purposes, but they accomplish them in different ways. Their language is different, parameters are different, and each provide unique security services that you may or may not have subscribed to. Their operating agreements are also different, which can shift responsibilities to you.

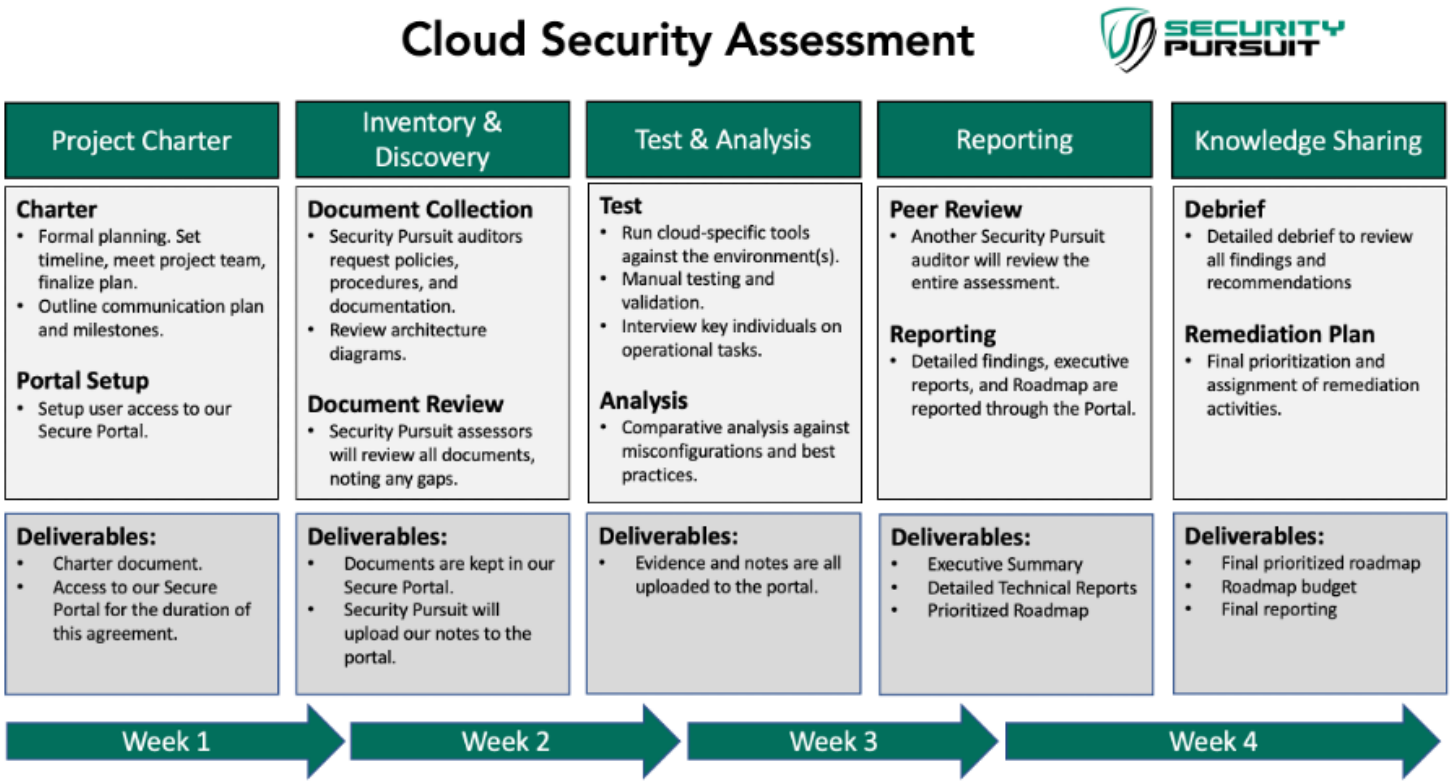
Because of this, tools and techniques are also different for each Cloud service provider.

Security Pursuit has invested heavily in the latest assessment tools and techniques. We adapt our process depending on what Cloud you are using, the services you subscribe to, and your overall risk posture.

Industry Standard Benchmarks

• **Unknown exposed servers** • **Unencrypted data** • **Misconfigured least privilege** • **Lateral movement risk** • **Azure Security errors (when used)**	• **Misconfigured backup** • **Active Directory misconfigurations** • **Permissive IAM** • **Unsecured data** • **and much more!**

How do you do perform a Cloud Security Assessment?



- **Project Charter** – every Security Pursuit project starts with a formal Charter Meeting. This ensures all parties know the schedule, how to contact people, how to safely share information, and agree on the schedule. It is the key to project success.
- **Inventory & Discover**y – we begin by understanding your past, present and future in regard to cybersecurity. In addition, we collect architecture diagrams, policies and procedures to begin the benchmarking process.
- **Test and Analysis** – Security Pursuit has made significant investments in tools that streamline the Cloud Security Assessment regardless of what platform you are on. As with all assessments, we use these tools to quickly gather significant amounts of data against industry standard benchmarks, which we then evaluate and validate manually. Our assessor's skills, along with alignment to your deployment, make our Cloud Security Assessment unique to you.
- **Reporting** – you need a variety of reports to understand and share our findings and recommendations. We provide an Executive Summary that you can share with your Board of Directors, executives and stakeholders. Most important, we provide a detailed listing of all parameters tested, good and bad findings, and prioritized recommendations for remediation.
- **Knowledge Sharing** – of course, we are never really finished with a project until you are. We provide a formal debrief to discuss everything. Questions month down the line are no problem. Security Pursuit is always available to clarify our findings.

Business Outcomes

Security Pursuit's Cloud Security Assessment provides a comprehensive review of all configuration parameters and deployment best practices of your cloud environment.

This assessment provides clients the assurance that their environment is configured and secured correctly. Any gaps found are thoroughly reviewed with your team, and remediation is prioritized.

Specific outcomes include:

- Lower risk due to configuration errors.
- Benchmarking to industry standards.
- Assurance that your cloud environment balances security with operational efficiency.
- Clear direction and budget on where to invest next.
- More confidence as you move more systems to the Cloud.

Part of CAP

Many of our clients subscribe to our Cyber Alliance Program (CAP). CAP provides critical cybersecurity services on a quarterly basis, giving clients ongoing assurance that they are keeping up with the latest vulnerabilities, while also they are ready to respond to any cybersecurity event.

We now include ongoing Cloud Security Assessments in our CAP as an option. We conduct a full annual Cloud Security Assessment, then run update scans every quarter. Like all CAP services, this is provided at a substantial discount.

With CAP, you no longer have to worry about a change to your Cloud services, new vulnerabilities in your Cloud, or where to invest next.

Next Steps

Security Pursuit has been a leading cybersecurity service provider for over 10 years. Our goal is to provide our clients unbiased, independent testing and advisory services.

Security Pursuit is unique in the cybersecurity world. We answer emails. We answer the phone! When you need us...we are there. We also don't bother our clients with endless sales calls.

If you want the best cybersecurity service partner, you need not look any further.

Contact us today to scope out your Cloud Security Assessment

SECURITY PURSUIT

720-675-ROOT (7668)
www.securitypursuit.com