Assessing Your Agency's Cloud Security

Cloud computing is crucial for digitally transforming agencies. With benefits including flexibility and scalability, cloud can modernize IT and help agencies at every level serve citizens better.

Today, many agencies use public clouds, which vendors provide to multiple organizations simultaneously. But as public cloud use grows more common, the number of security concerns about the technology are also rising.

GovLoop and Oracle developed this worksheet to assess your agency's progress in five cloud security categories.

Rate your agency on a scale of one to five, with one representing "completely disagree" and five representing "completely agree," in response to each of the prompts below.

Category #1: Cybersecurity

My agency practices least-privilege access – meaning processes, programs and users can only access the information and resources they need.

1 *completely disagree* 2 3 *neutral* 4 5 *completely agree*

Multiple factors – in addition to passwords – are used to authenticate users accessing my agency's data.

1 2 3 4 5

Category #2: Data Security

All my agency's data is always encrypted everywhere, regardless of whether this information is in transit or at rest.

1 2 3 4 5

My agency's cloud provider does not have insights into the contents of our data, no matter the format this information exists in.

1 2 3 4 5

My agency's cloud provider helps us find and protect confidential or privileged data.

1 2 3 4 5

My agency's cloud provider offers fully redundant storage to protect my data from corruption.

1 2 3 4 5

Category #3: Compliance

My agency's cloud vendor complies with federal, state, local and international cybersecurity standards such as the Federal Risk and Authorization Management Program (FedRAMP).

1 2 3 4 5

Our cloud vendor routinely audits its compliance with all applicable cybersecurity standards for recurring reports to our leadership.

1 2 3 4 5

Category #4: System Security

Our cloud vendor considers factors such as generator and power availability before building new data centers.

1 2 3 4 5

My agency's cloud vendor uses data centers with physical defenses such as cameras.

1 2 3 4 5

My agency's cloud vendor provides automated security patching without taking down systems.

1 2 3 4 5

My agency's cloud vendor regularly provides penetration testing, vulnerability testing and security assessments.

1 2 3 4 5

Category #5: Infrastructure Security

My agency's hypervisor was built with cloud security in mind and designed to prevent attacks.

1 2 3 4 5

My agency's cloud vendor practices isolated network virtualization, putting control of our cloud on a network separate from my agency's host and hypervisor networks.

1 2 3 4 5

My agency's cloud vendor supports hardware-based wiping and reinstalling of firmware.

1 2 3 4 5

Results

If you answered mostly ones or twos...

Your agency has low cloud security.

Your agency's cloud may not be compatible with its legacy technology and has a wide attack surface.

Your agency also rarely complies with cloud cybersecurity standards.

Additionally, much of your agency's data is exposed as encryption is used infrequently. Cyberattackers can roam freely if they breach your agency's perimeter.

Overall, your agency's security culture could use more resources.

If you answered mostly threes...

Your agency's cloud security is adequate.

The data centers your agency uses are resilient, boasting tools such as fire suppression systems.

Your agency has a reliable cloud vendor that complies with basic cybersecurity standards.

Finally, your agency has dedicated cybersecurity personnel.

If you answered mostly fours or fives...

Your agency has good cloud security.

What can other agencies learn from yours? First, your agency's network is segmented to prevent preaches from spreading. And there are multiple authentication layers for users accessing data. And your agency's cybersecurity personnel? They use automation to assist with tasks such as patching software. The icing on the cake is the isolated network virtualization to fortify its cloud.

Your agency's cloud vendor, however, also chips in. It complies with the highest cybersecurity standards, deploys IT built for security and provides quality support with compliance and security.

Working together, your agency and its cloud vendor enable you and your co-workers to focus on mission success.

Regardless of your answers, Oracle is helping agencies with multi-layered cloud security for defense in-depth.

Oracle Cloud security aligns people, processes and technology—augmented with robust physical controls—to provide integrated defense-in-depth protection and consistent security across complex hybrid and multi-cloud environments. When it comes to technology, Oracle's second-generation cloud reduces risks from constant cyberthreats with security-first design principles such as least privilege access.

Agencies can also easily implement security controls such as data encryption and network segmentation. Additionally, automation can reduce human error and quickly deploy cybersecurity best practices agencywide. The icing on the cake is isolated network virtualization and pristine physical host deployment. Collectively, these features make Oracle's cloud more isolated for agencies than earlier public clouds and reduces the risk from cyberthreats.

To learn more, visit www.oracle.com/federal

ORACLE

govloop