IQ-CYBER, INC.

VOLUME 1, ISSUE 1

Secure Cloud Migration

Datasheet

Why iQ-Cyber?

Our staff has more than 18 years' experience delivering mature cybersecurity services to federal government and commercial customers in the Washington D.C. metro area and the nation. We bring a deep understanding of cyber prevention techniques and skillsets to address advanced and emerging cyber threats.

Service Overview

As cyber-attacks targeting cloud infrastructures increase, using a Cloud Security Assessment can help you determine how best to reduce your organization's risk. Cloud providers, like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and many others have worked to provide assurances that they could offer secure environments to replace the old network perimeter.

However, there is a point at which cloud provisioning and the responsibility for data security, become somewhat fuzzy. Which is why this has led to the concept of the "shared responsibility model". Shared responsibility is described as:

- Security of the cloud – the responsibility of the cloud provider
- Security in the cloud – the responsibility of the customer (organization client)

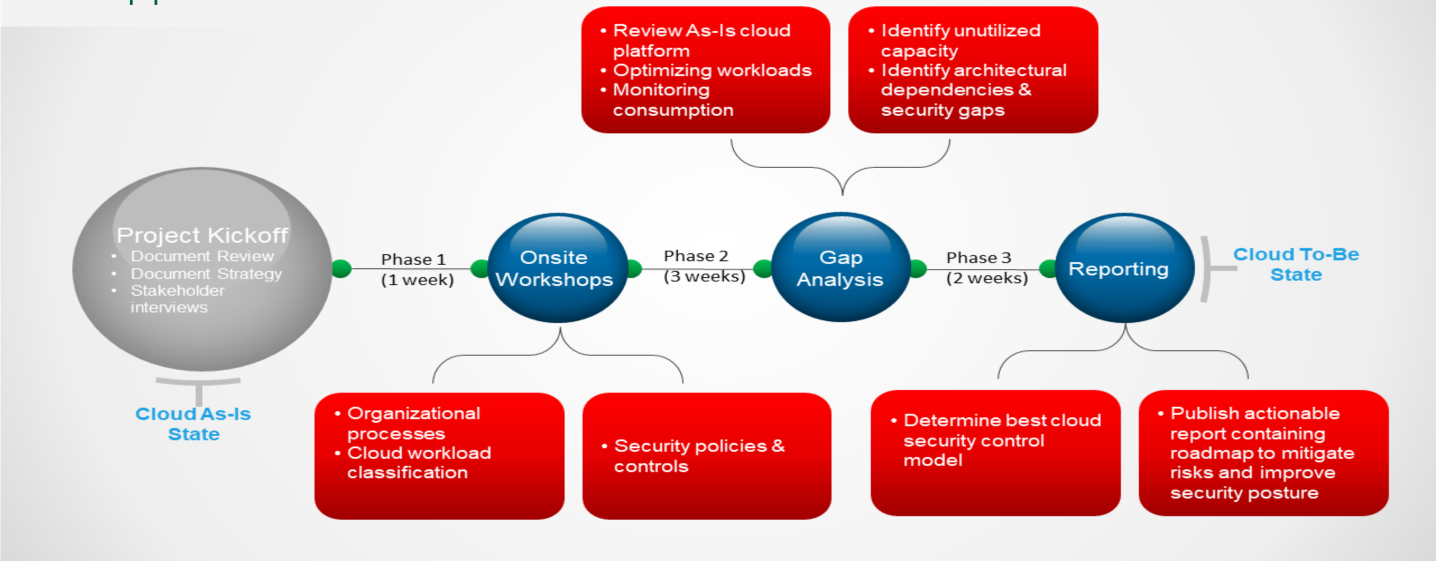
In other words, the cloud vendor must provide the security of the infrastructure pieces, such as the Operating System (OS), the virtualization layer, physical security, etc. And the customer (i.e. the organization using the cloud) is responsible for the security of cloud apps and data. This includes security controls such as: encryption for data-in-transit and at-rest, performing security scans of cloud containers and maintaining the structural and operational security controls of these containers. You are still responsible for your own data. Also, the responsibility to verify that security requirements are being met always lies with the customer. This is where a Cloud Security Assessment comes in.

Our Cloud Security Assessment is a process that allows you to test out the security of your cloud environment. The assessment provides a holistic view of your internal and external security posture of your cloud business environment and identifies any gaps in security that could amplify attackable surface areas.

Key Benefits

- **Identify and mitigate** the most common cloud security configuration errors and weaknesses that could be exploited by attackers
- **Perform gap analysis** of the organization's current (As-Is) cloud platform to determine if current controls are adequate and effective to address risk
- **Reduce** amplification of your attackable surface areas from common exploitation techniques
- **Gain better visibility** into your cloud environment through the use of security monitoring tools and logs
- **Prioritize** the correct security control enhancements to avoid attacks and survive incidents to your cloud environment

Our Approach



- Review As-Is cloud platform
- Optimizing workloads
- Monitoring consumption

- Identify unutilized capacity
- Identify architectural dependencies & security gaps

Project Kickoff
- Document Review
- Document Strategy
- Stakeholder interviews

Cloud As-Is State

Phase 1 (1 week)

Onsite Workshops

Phase 2 (3 weeks)

Gap Analysis

Phase 3 (2 weeks)

Reporting

Cloud To-Be State

- Organizational processes
- Cloud workload classification

- Security policies & controls

- Determine best cloud security control model

- Publish actionable report containing roadmap to mitigate risks and improve security posture

Week 1: Initial Document Review of cloud security and migration strategy. Conduct interviews with client stakeholders regarding existing or projected cloud delivery models (public, private, hybrid, multi..). Review documentation (i.e. architecture diagrams, access control & data protection policies, cloud logging standards, SOPs/playbooks, etc.).

Week 2: Onsite Results-Driven Workshops –This is a collaborative effort that takes a deep discovery through stakeholder meetings focusing on:

- organizational processes to identify affected technology infrastructures and applications
- workload classification - restructure and rehouse the enterprise workloads that deploy applications into the cloud
- assessing security policies and controls—everything that might encompass a cloud migration or implementation

Week 3 – 4: Review the as-is cloud platform to understand application architecture, dependencies and requirements. Ensure cloud security controls are implemented properly. Confirm learnings from the Results-Driven Workshops to identify the most common cloud security configuration errors and weaknesses that could be exploited by attackers.

Week 5: Actionable Report that details practical steps to harden the cloud environment using the Center for Internet Security (CIS), NIST, OWASP, Gartner and other industry recognized hardening guidelines. The Cloud Assessment Artifact documentation will also provide detailed observations and recommendations realized by our team during the discovery sessions.

Deliverables

The post assessment report includes:

❑ A snapshot of your current cloud (As-Is) environment detailing architecture and security controls

❑ Actionable report containing roadmap and practical recommendations to mitigate your risks and improve your security posture

❑ Steps to translate your on-premise security framework to the cloud

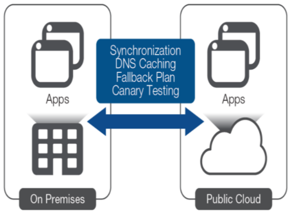
❑ Capabilities of security tools to manage security across the cloud

❑ Next steps to implement tools and processes to enable a security framework for your cloud

We can engage with you during any stage of your cloud migration effort.

Before Cloud Migration – Prior to going to the Cloud, we will assess your readiness to the Cloud aligned to your business risk and legal obligations.

For new cloud migrations we will deliver a cloud security tactical plan that provides security controls that should be considered depending on your desired journey to the cloud (i.e. cloud native, lift and shift, or refactoring).



During Cloud Migration – This activity will begin with understanding the scope, objectives and key assets of your cloud project.

As the Cloud environment is ever-evolving, it is important to prioritize security all while moving your data to the Cloud. This activity and subsequent deliverable will provide security guidance for a risk-based approach to secure Cloud adoption.

After Cloud Migration – Continuous monitoring processes must be established to ensure your applications run smoothly and cost-effectively in the cloud by optimizing workloads already on the cloud, monitoring consumption and identifying unutilized capacity that can be switched off.

Security doesn't stop after a cloud migration project is completed. Processes must be established to evaluate cloud security posture on a regular basis and to monitor the cloud environment to document any changes or potential cloud risks.

Offices: Dover, DE 19901;   Clarksville, TN 37042;   Burtonsville, MD 20866

Ph: 844.429.2371 301.825.8934   Email: info@iq-cyber.com

www.iq-cyber.com