Cloud Cybersecurity Advisory Assessment

A large percentage of today's enterprise infrastructure(s) and application deployments are now requiring multiple cloud technology models (SaaS, IaaS and PaaS). Each model and approach require varying levels of compliance, security subject matter expertise, and Cybersecurity considerations.

By performing a Cloud Cybersecurity Advisory Assessment (CCAA), you can know precisely where your Cybersecurity risk lies when moving infrastructure and applications to cloud native services either from Microsoft Azure, Google Cloud, or AWS. With the CCAA, customers know where their risk lies, where they need to be, and how to get to where they need to be as part of their Cloud first strategy. Below are the main deliverables provided by our senior IAM, Cloud, and Cybersecurity consultants to help customers along this journey.

Main Assessment Deliverables

- Cloud Cybersecurity Capability Framework.
- Microsoft Word document describing the current and desired state analysis covering major Cloud Cybersecurity Capability areas.
- Microsoft PowerPoint document describing all major gaps and application and infrastructure workload security requirements based on transitional steps below.
- Microsoft Visio and Microsoft Word documents describing current, transitional, and future state Cloud Cybersecurity architectures based on transitional steps below.
- Microsoft PowerPoint executive summary containing major aspects of deliverables and overall Cloud Cybersecurity assessment.

Pricing and Duration

- Fixed fee, excluding travel and entertainment costs.
- Six to eight-week duration.

Microsoft Azure | amazon web services | Google Cloud

Key Tasks & Areas of Coverage

- Introduce customer to the Cloud Cybersecurity Capability Framework. This framework covers all main technical areas in assessment. See page 2 for details.
- Perform current state discovery against the capability framework by conducting a series of up to four workshops.
- Document current state analysis as viewed from the lens of the Cloud Cybersecurity Capability Framework.
- Perform future state discovery by conducting a series of up to two workshops. Future state will be documented desired cybersecurity capabilities and controls for transitioning to the cloud.
- Perform and document a detailed gap analysis between the current and desired states. A current Cloud Cybersecurity maturity level will be assigned and compared against required future state maturity.
- Document current state architectures based on Cloud model (SaaS, PaaS, IaaS).
- Develop and document "future state" Cloud Cybersecurity architecture.
- Develop and document an executable and agile Cloud Cybersecurity Capability roadmap for getting you from current state architecture through transitional state architectures, and finally realizing the "end state" architecture based on chosen Cloud model (IaaS, PaaS, SaaS).
- Provide executive summary and final deliverable package for execution.

Transitional Steps for Applications and Infrastructure Workloads

Steps for Transitioning Workloads into a Secure Cloud Environment

- Identify class and type of Asset (UCMD, ITSM)
- Review compliance and regulatory requirements for the asset (i.e. GDPR, HIPPA, SOX, NERC/FERC)
- Identify application, infrastructure, and service security controls aligned to requirements
- Measure risk, identify thresholds, and implement mandatory mitigation strategy and controls
- Design or reuse security controls for asset based on compliance and risk mitigation strategy
- Implement security controls for the asset (i.e. CIS Benchmark, NIST guidance, Cloud Cybersecurity Best Practices)
- Monitor, operate, and provide effective and efficient incident response workflows

Founded in 2014, Good Dog Labs, a Spyglass company, disrupted the Identity ecosystem by building a microservices driven approach to Identity access management and governance security products. They focus on helping their customers address the challenges of cybersecurity, DevOps and cloud security implementations head on. Their product, Perseus IAM, is the world's first IAM microservices driven platform that reduces complexity, leverages existing investments, reduces implementation costs, promotes agility, and helps meet current and future Identity and Access Governance (IGA) needs. Good Dog Labs closely partners with HashiCorp, Sailpoint, IBM and Okta.

Main Technical Areas That Comprise the Assessment

Virtual Networking & Security

- Cloud network connectivity model (Private Circuit vs. VPN)
- Gateways
- Firewalls
- Routers
- Load balancers

Application, Service, and Data Security

- IaaS Storage, PaaS services, Containerization (Microservices)
- Media and Data Encryption / Key Management / Secrets Management (Vault / HSM)
- Data Classification

Business Logic, Patching, Change Management and Configuration

- Service quality, security, patching, and vulnerability assessment
- Service to service communication, encryption, and non-repudiation
- Business continuity and availability

Identity and Access Management

- Cloud IAM Services (Just in time access and access certification)
- On-Premise identity bridges and Services Layers (Perseus IAM)
- Cloud resource (i.e. PaaS, Infrastructure Items) role-based access control
- Password Management (Lifecycle, Rotation)
- Single Sign On / Identity Federation
- Multi-Factor Authentication (Infrastructure and Application Access)

Security Monitoring

- Security Operations (SIEM)
- Privileged Account Management
- Threat vulnerability and management for Application, Infrastructure, and Services
- Infrastructure and Business Logic (Network, Data, Applications)

Incident Response

- Emergency response planning
- Incident response workflow
- Incident Investigation
- Risk mitigation and protective control implementation (Feedback Loop)

GoodDogLabs.
A SPYGLASS COMPANY.