https://cloudsecurityalliance.org/guidance/

SECURITY GUIDANCE v.4
Info Sheet

The Cloud Security Alliance is proud to announce the release of the Security Guidance for Critical Areas of Focus in Cloud Computing v.4.

Introduction

This version, the first major update since 2011, is the culmination of over a year of dedicated research and public participation from the CSA community, working groups, and the public at large. The Cloud Security Alliance's *Security Guidance for Critical Areas of Focus in Cloud Computing* acts as a practical, actionable roadmap for individuals and organizations looking to safely and securely adopt the cloud paradigm. Version 4 has been updated significantly to:

- Incorporate advances in cloud, security, and supporting technologies.
- Better reflect real-world cloud security practices.
- Integrate the latest in CSA research projects, such as the Cloud Controls Matrix and the Consensus Assessments Initiative Questionnaire.
- Provide guidance for related technologies, such as DevOps, IoT, mobile, and Big Data.

Extensive Content Updates

Aside from the structural changes, version 4 of the *Guidance* includes extensive content updates to address leading-edge cloud security practices. Some of these topics include:

- DevOps, continuous delivery, and secure software development.
- Software Defined Networks, the Software Defined Perimeter, and cloud network security.
- Microservices and containers.
- New regulatory guidance and evolving roles of audits and compliance inheritance.
- Using CSA tools like the CCM, CAIQ, and STAR Registry to inform cloud risk decisions.
- Securing the cloud management plane.
- More practical guidance for hybrid cloud.
- Compute security guidance for containers and serverless, plus updates to managing virtual machine security.
- The use of immutable, serverless, and "new" cloud architectures.
- Updated data protection guidance that includes cross-border data transfers, GDPR, NIS Directive and other country specific examples (i.e. APAC, Americas, and EMEA regions).

Process and Methodology

To enhance consistency and readability, version 4 of the *Guidance* was assembled by the professional research analysts at Securosis based on an open research model relying on community contributions and feedback during all phases of the project. The entire history of contributions and research development is available online for complete transparency. Approximately 80% of version 4 was rewritten from the ground up and the domains were restructured to better represent the current state and future of cloud computing security.

Structural Changes to the Guidance

Major structural changes to the *Guidance* include the following:

- Removal of "*An editorial note on risk*." Risk management is instead addressed more deeply in the appropriate domains and through other CSA GRC projects.
- A new "Regional Examples" section was added to **DOMAIN 3** to provided a global perspective on legal frameworks governing data protection and privacy.
- Data security and information governance are better structured. **DOMAIN 5**, *Information Governance*, covers governance issues, while all operational data security issues are moved into **DOMAIN 11**.
- **DOMAIN 6** now addresses *Management Plane Security and Business Continuity* in the cloud. It was previously *Portability and Interoperability*. Appropriate content from version 3 is integrated in other areas and the rest is depreciated.
- **DOMAIN 7** is now dedicated to *Infrastructure Security*. In version 3 of the *Guidance*, **DOMAIN 7** was *Traditional Security, Business Continuity, and Disaster Recovery*. Relevant content is incorporated in the other appropriate domains, and non-cloud security guidance is depreciated in version 4.
- **DOMAIN 8** is now *Virtualization and Containers. Data Center Operations* from version 3 is fully depreciated to focus the *Guidance* on cloud computing specific issues. CSA determined that the community is better served by existing data center security standards.
- **DOMAIN 11** has expanded from *Encryption and Key Management* to *Data Security and Encryption* to incorporate non-governance material from **DOMAIN 5** and expand additional data security options.
- **DOMAINS 10 AND 12** were extensively rewritten and restructured to remove overlapping IAM recommendations and reflect real-world practices over unused standards.
- The content of **DOMAIN 13** is now integrated into **DOMAIN 8**, *Virtualization*, and the previous **DOMAIN 14**, *Security as a Service*, is now **DOMAIN 13**.
- **DOMAIN 14** is a new domain for *Related Technologies*, including Big Data, IoT, mobile devices, and serverless. Moving forward, this domain will enable the CSA to update the *Guidance* to include emerging technologies and practices related to cloud computing that may later be incorporated into other domains.