Cheatography

CSCC: 10 Steps Security for Cloud Computing Cheat Sheet

by [deleted] via cheatography.com/2754/cs/16689/

Introduction

The Cloud Standards Customer Council (CSCC) announced version 3 of its Security for Cloud Computing: 10 Steps to Ensure Success. The 10 steps are meant to be a reference guide for organizations to better analyze the security effects of cloud computing on the organization as a whole.
According to the CSCC, cloud security risks include loss of governance, isolation failure, management interface vulnerabilities, vendor lock-in, service unavailability, business failure of provider, malicious behavior of insiders, and insecure or incomplete data deletion.

Source: https://sdtimes.com/cloud-computing/cscc-10-steps-ensure--security-cloud-computing-success/

Step One

Ensure effective governance, risk and compliance by establishing chains of responsibility, understanding risk tolerance, understanding specific laws, notifying users if a breach occurs and ensuring app and data security

Step Two

Audit operational and business processes. Audits should leverage an established standard, be carried out by skilled staff, and be done as part of a formal certification process, according to the CSCC.

Step Three

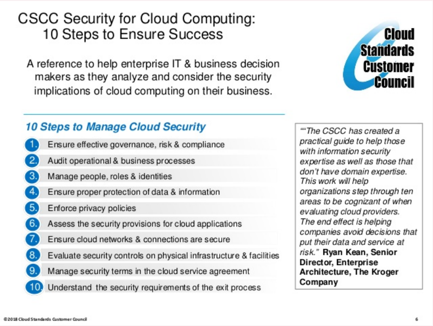
Manage people, roles and identities. “Customers must ensure that the cloud service provider has processes and functionality that govern who has access to the customer’s data and applications. Conversely, cloud service providers must allow the customer to assign and manage the roles and associated levels of authorization for each of their users in accordance with their security policies, and apply the principle of least privilege. These roles and authorization rights are applied on a per-resource, service or application basis,” the CSCC wrote..

Step Four

Ensure proper protection of data and information. According to the authors, “data protection is a component of enterprise risk management.” Protecting data is crucial in terms of risk management.

Step Five

Security for Cloud Computing



CSCC Security for Cloud Computing:
10 Steps to Ensure Success

A reference to help enterprise IT & business decision makers as they analyze and consider the security implications of cloud computing on their business.

Cloud Standards Customer Council

10 Steps to Manage Cloud Security

1. Ensure effective governance, risk & compliance
2. Audit operational & business processes
3. Manage people, roles & identities
4. Ensure proper protection of data & information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks & connections are secure
8. Evaluate security controls on physical infrastructure & facilities
9. Manage security terms in the cloud service agreement
10. Understand the security requirements of the exit process

““The CSCC has created a practical guide to help those with information security expertise as well as those that don’t have domain expertise. This work will help organizations step through ten areas to be cognizant of when evaluating cloud providers. The end effect is helping companies avoid decisions that put their data and service at risk.” **Ryan Kean, Senior Director, Enterprise Architecture, The Kroger Company**

©2018 Cloud Standards Customer Council 6

Step Six

Assess the security provisions for cloud applications.The authors say that “organizations must apply the same diligence to application security in the cloud as in a traditional IT environment.” The responsibilities differ depending on the deployment model.

For example, in IaaS, the customer is responsible for most security components. In Platform-as-a-Service the provider is responsible for securing the operating system while the customer is responsible for application security. For Software-as-a-Service, the provider provides application security, while the customer is responsible for understanding things such as data encryption standards, audit capabilities, and SLAs.

Step Seven

Ensure cloud networks and connections are secure. The authors suggest that customers should have assurance on a provider’s internal and external network security.

Step Eight

Evaluate security controls on physical infrastructure and facilities. Security controls include: holding physical infrastructure in secure areas, protecting against external and environmental threats, putting controls in place to prevent loss of assets, proper equipment maintenance, and backup, redundancy and continuity plans

Step Nine

Manage security terms in the cloud service agreement. “Since cloud computing typically involves at least two organizations – customer and provider, the respective security responsibilities of each party must be made clear. This is typically done by means of a cloud service agreement (CSA), which specifies the services provided and the terms of the contract between the customer and the provider,” according to the council.

Step Ten

Enforce privacy policies. “Enterprises are responsible for defining policies to address privacy concerns and raise awareness of data protection within their organization. They are also responsible for ensuring that their cloud service providers adhere to the defined privacy policies. Thus, customers have an ongoing obligation to monitor their provider’s compliance with customer policies. This includes an audit program covering all aspects of the privacy policies, including methods of ensuring that corrective actions will take place,” the council wrote..

Understand the security requirements of the exit process. Customer data should not remain with the provider after the exit process. The provider should be forced to cleanse log and audit data, though in some jurisdictions this isn’t possible because retention of records might be required by law.