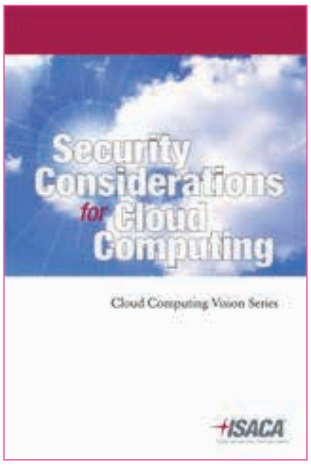
Security Considerations for Cloud Computing

Security Considerations for Cloud Computing provides a brief overview of cloud computing, its associated security risk and information for decision makers in an organization. The book is a useful resource for managers in all parts of an organization that is considering transitioning some, or all, of its current IT services onto cloud-based services and who want to understand the security implications of doing so.

This book describes the three different cloud service models (Infrastructure as a Service [IaaS], Platform as a Service [PaaS] and Software as a Service [SaaS]) and different deployment models (public, community, private and hybrid cloud).

The book explains that trust is a major component of mitigating security risk in cloud computing. It also outlines several facets to be considered before deciding on a cloud service provider (CSP), which include:

- The financial position of the CSP
- CSP certification or recognition by one or more security standards authorities (e.g., Australian Signals Directorate Certified Cloud Services)
- The existence of effective disaster recovery plans, business continuity plans and robust backup procedures, especially when the CSP is operating in many countries
- The quality of the organization's data; data classification (e.g., policies, principles and frameworks); and organizational structures, culture, skills and people
- General negotiations and the relationship with the CSP (contracts, service level agreements, communication processes, and roles and responsibilities)



The main section of the book discusses security risk and threats related to operating in the cloud. This section effectively covers the key risk factors and threats, with sufficient information to assist organizations that are deliberating on whether they should move to cloud services.

Security Considerations for Cloud Computing provides guidance to decision makers on the risk in relation to different cloud service models, e.g., SaaS and IaaS, and the various deployment models, e.g., community cloud and private cloud.

An entire chapter is dedicated to helping decision makers by providing the necessary aspects to consider when deciding to move to a cloud solution. This section has a very useful checklist that addresses key considerations prior to moving to the cloud, such as what should be requested from the cloud provider, e.g., security policy, list of infrastructure locations and technical specifications for access management. The decision-making process is made even easier with a decision tree that can help enterprises determine which deployment model to select.

The book sets out four straightforward steps, based on the seven COBIT® 5 enablers (Principles, Policies and Frameworks; Processes; Organizational Structures; Culture, Ethics and

Reviewed by Diana Hamono, CISA, CGEIT, COBIT 5 Foundation
Executive director in the governance, risk and assurance team at Synergy Group in Canberra, Australia, and a past president of the ISACA Canberra Chapter

Behavior; Information; Services, Infrastructure and Applications; and People, Skills and Competencies), that organizations must do to prepare for a move to cloud services. These steps are:

- Prepare the internal environment
- Select the cloud service model
- Select the cloud deployment model
- Select the cloud provider

However, the book makes it clear that the work does not stop once the provider is selected. There are further considerations and questions that need to be addressed relating primarily to the threats associated with the chosen service and deployment models.

Security Considerations for Cloud Computing is a concise and well-organized book that will be of great benefit to IT managers considering moving to a cloud-based solution or IT auditors who want to assess the risk involved in a move to cloud services.

Editor's Note

Security Considerations for Cloud Computing is available from the ISACA Bookstore. For information, visit *www.isaca.org/bookstore*, contact support at https://support.isaca.org/ or telephone +1.847.660.5650.