Chapter 4
Trusted Cloud Initiative Reference Architecture

Yushi Shen
Microsoft Corporation, USA

Ling Wu
EMC² Corporation, USA

Yale Li
Microsoft Corporation, USA

Shaofeng Liu
Microsoft Corporation, USA

Qian Wen
Endronic Corp, USA

ABSTRACT

The Trusted Cloud Initiative helps cloud providers develop industry-recommended, secure, and interoperable identity, access, and compliance management configurations and practices. The Trusted Cloud Initiative is to develop reference models and provide education in a vendor-neutral manner, inclusive of all CSA members and affiliates who wish to participate. The Trusted Cloud Initiative Reference Architecture is both a methodology and a set of tools, enabling security architects, enterprise architects, and risk management professionals to leverage a common set of solutions to fulfill their common needs. It enables them to assess their internal IT service and that of their cloud providers in terms of security capabilities, and to plan a roadmap to meet the security needs of their business. The purpose of this quick guide is to take a user through the Trusted Cloud architecture much like an owner's manual walks a consumer through a product.

OVERVIEW OF THE REFERENCE ARCHITECTURE

Out of the common needs, there come the common solutions. The Trusted Cloud Initiative Reference Architecture is both a methodology and a set of tools that enable security architects, enterprise architects and risk management professionals to leverage a common set of solutions. These solutions fulfill a set of common requirements, which risk managers must assess regarding the operational status of internal IT security and cloud provider controls. These controls are expressed in terms of security capabilities, and

designed to create a common roadmap to meet the security needs of their business.

Architecture must be guided by business requirements. In the case of the Trusted Cloud Initiative, these requirements come from a controls matrix guided by regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley, standard frameworks such as ISO-27002, the Payment Card Industry Data Security Standards, and the IT Audit Frameworks, such as COBIT, all in the context of cloud delivery models, such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Services (IaaS).

From these requirements, a set of security capabilities have been defined and organized according to best practice architecture frameworks. The Sherwood Business Security Architecture (SABSA) defines security capabilities from a business perspective. The Information Technology Infrastructure Library (ITIL) defines the capabilities needed to manage the IT services of the company, which includes the security capabilities necessary to securely manage those services. The Jericho Forum defines technical security capabilities, which arises from the reality of the traditional in-the-datacenter technology environments shifting to one where solutions span the internet across multiple datacenters, some owned by the business and some purely used as outsourced services. Lastly, The Open Group Architecture Framework (TOGAF) provides an enterprise architecture framework and methodology for planning, designing and governing information architectures, and thus a common framework to integrate the work of the security architect with the enterprise architecture of an organization.

You can interact with and learn more about the TCI Reference Architecture online at https://research.cloudsecurityalliance.org/tci/.

HOW TO USE THE TCI REFERENCE ARCHITECTURE

The TCI Reference Architecture can be used in multiple enterprise security design phases, from assessing opportunities for improvement and creating road maps for technology adoption, to defining reusable security patterns and assessing various cloud providers and security technology vendors against a common set of capabilities.

Figure 1. TCI reference architecture
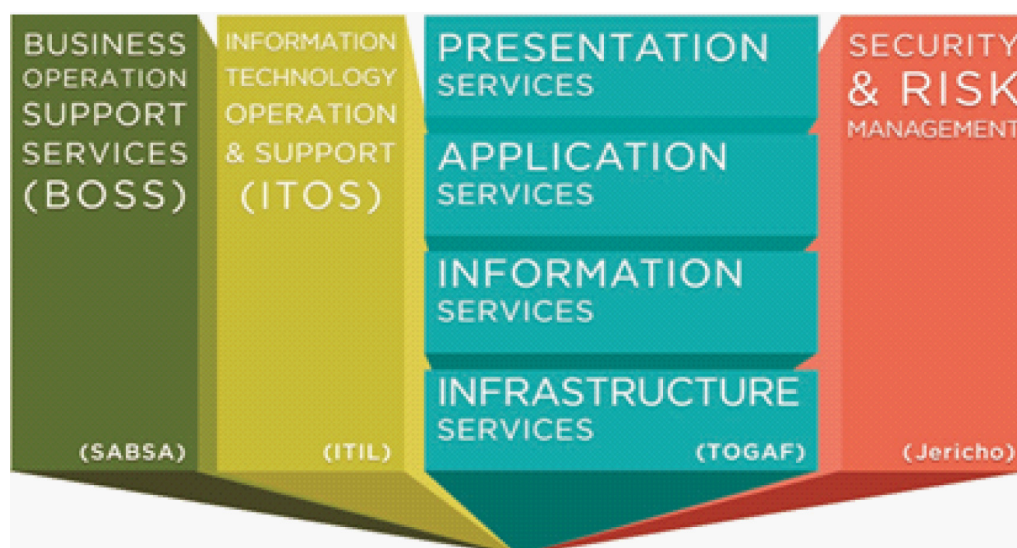
14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/trusted-cloud-initiative-reference-architecture/88003

Related Content

From Cloud Computing to Fog Computing: Platforms for the Internet of Things (IoT)
Sanjay P. Ahujaand Niharika Deval (2018). *International Journal of Fog Computing (pp. 1-14).*
www.irma-international.org/article/from-cloud-computing-to-fog-computing/198409

Security Challenges for Cloud Computing Development Framework in Saudi Arabia
Lawan A. Mohammedand Kashif Munir (2015). *Handbook of Research on Security Considerations in Cloud Computing (pp. 285-300).*
www.irma-international.org/chapter/security-challenges-for-cloud-computing-development-framework-in-saudi-arabia/134296

Managing the Cloud for Information Systems Agility
Haibo Yang, Sid Huffand Mary Tate (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 1877-1899).*
www.irma-international.org/chapter/managing-the-cloud-for-information-systems-agility/119937

An IoT-Based Framework for Health Monitoring Systems: A Case Study Approach
N. Sudhakar Yadav, K. G. Srinivasaand B. Eswara Reddy (2019). *International Journal of Fog Computing (pp. 43-60).*
www.irma-international.org/article/an-iot-based-framework-for-health-monitoring-systems/219360

Advanced Data Storage Security System for Public Cloud
Jitendra Kumar, Mohammed Ammar, Shah Abhay Kantilaland Vaishali R. Thakare (2020). *International Journal of Fog Computing (pp. 21-30).*
www.irma-international.org/article/advanced-data-storage-security-system-for-public-cloud/266474