前瞻科技與管理　5卷2期，41-94頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 41-94 (November, 2015)
DOI: 10.3966/222014242015110502003

雲端運算資訊安全管理標準化初探：根基於國際標準組織之標準化的進程

樊國楨[1,*]　韓宜蓁[2]

[1]臺灣網路安全防護協會秘書長
[2]中國文化大學推廣教育部遠距教學中心數位教學規劃師

摘要

國際標準組織（International Organization for Standardization, ISO）自2009年11月起分別由新成立的ISO JTC（Joint Technical Committee）I/SC（Subcommittee）38WG（Working Group）主責其詞彙及參考架構、ISO/JTCI/SC7主責其服務管理，以及ISO/IEC JTCI/SC27（以下SC27）主責其安全與隱私之標準系列的制定工作項目；2012年10月，ISO已正式將雲端運算之資訊安全管理納入資訊安全管理系統（Information Security Management System, ISMS）新擴增的服務（Services）類別之標準系列的類別（Classification），分由SC27之WG1、WG4及WG5負責其標準化的工作項目。

根基於ISO已有之成果、美國聯邦政府自2012年2月7日正式開展的雲端運算之聯邦風險與管理授權計畫（Federal Risk and Management Program, Fed RAMP），以及在2014年2月定案的關鍵基礎建設（Critical Infrastructure）之網路安全框架（Cybersecurity Framework）的識別（Identity）、防護（Protect）、偵測

* 通訊作者：樊國楨
電子郵件：kjf.nctu@gmail.com

（Detect）、反應（Respond）及回復（Recovery）之IPDR2的資訊安全管理模型，本文探討我國雲端運算資訊安全管理之應然與實然。

關鍵詞：脆弱性資料庫、測試與評估、雲端運算、資訊安全管理系統、標準化

前瞻科技與管理　5卷2期，41-94頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 41-94 (November, 2015)

Primary Study on the Standardization of Information Security Management of Cloud Computing: Standardization Progress Based on International Organizations for Standardization

Kwo-Jean Farn[1,*], I-Chen Han[2]
[1]Secretary General, Taiwan Internet Protection Association
[2]e-Instructional Planner, School of Continuing Education, Chinese Culture University

Abstract

In April, 2010, the Ministry of Economic Affairs proposed the Cloud Computing (CC for short) Industry Solutions, which was approved by the Executive Yuan and has officially become the foundation of the CC industry policies. In November, 2012, the solution was renamed as Cloud Computing Application and Industry Development Plan, which depicts the objectives that the public sectors have utilized the cloud computing to establish relevant information and communication systems, so as to promote the participation and investment of private sectors and lead the industry development to mature stage, as well as establish the output representative sector possessing international competiveness.

Standards can accumulate knowledge and experiences, while standardization is to strengthen the knowledge about standard practices for inheritance via systematic, common and harmonious methods. Considering the popularization of cloud computing, its standard series shall be regulated; so in November, 2009, the International Organization for Standardization (ISO for short) established the ISO JTC (Joint Technical Committee)

* Corresponding Author: Kwo-Jean Farn
E-mail: kjf.nctu@gmail.com

I/SC (Subcommittee) 38WG (Working Group) to take charge of the words and reference framework, ISO/JTCI/SC7 to be responsible for its service management and ISO/IEC JTCI/SC27 (hereinafter referred to as SC27) to undertake the formulation of security and privacy standards. In October, 2012, ISO officially brought the information security management for cloud computing into Information Security Management System (ISMS), falling into the Classification of the newly added Services categories, and the WG1, WG4 and WG5 in SC27 take charge of the process items of standardization.

Based on the achieved results by ISO and the Federal Risk and management Program (Fed RAMP for short) for cloud computing officially issued by American federal government on February 7th, 2012, as well as the IPDR2 information security management model in the Cybersecurity Framework of Critical Infrastructure published on February 14th, 2014, covering Identity, Protect, Detect, Respond and Recovery, this study explores the ought-to-be and its actual situation of the cloud computing information security management in Taiwan.

Keywords: vulnerability database, testing and evaluation, cloud computing, information security management, standardization