Risk Assessment Methods for Cloud Computing Platforms

Timothy Weil
Audit and Compliance
Alcohol Monitoring Systems
Littleton, USA
trweil@ieee.org

***Abstract*—Risk assessment (RA) use cases for cloud computing platforms are presented in the context of an ISO 27001 Information Security Management System (ISMS) developed for Alcohol Monitoring Systems (AMS) across a portfolio of products and services.**

Keywords-ISO Standard; cloud computing;information security;risk management; risk assessment

I. INTRODUCTION

This paper presents risk management and risk assessment (RA) use cases for implementing an ISO 27001 Information Security Management System (ISMS) governing cloud computing in multiple deployment models (public cloud, hybrid cloud, government cloud, international cloud) and deploying common cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS). The models presented here have been derived from ISO 27001 compliance projects at Alcohol Monitoring Systems (AMS) headquartered in Littleton, CO. In the Electronic Monitoring (EM), Rehabilitation and Corrections/Law Enforcement industries, our products and services are branded as SCRAM Systems ™ (http://www.scramsystems.com). Over several years, a governing SCRAM ISMS has been developed from a set of commercial risk management policies described here

II. CONTEXT OF THE CLOUD RISK ASSESSMENT

The simple question of "What are the risks of deploying my software (SaaS), tools (PaaS), and/or infrastructure (IaaS) in the cloud?" presents a classic scoping and scalability problem in information systems [2][3][4]. To analyze different approaches to the cloud RA methods, combinatorial factors may include the context of the risk assessment (IT operations, information and data management, compliance), standards of the target domains (international, government, regional, industry sector), capabilities of the management organization and specifically defining the 'right tools for the job' to perform the risk assessment process [5][6].

Judicial Management Services are new cloud-hosted applications developed by SCRAM Systems. Components include NEXUS™ (Parole Evidence-Based Decision Support), 24x7 Sobriety Service plus user interface and mobility services provided by Optix™, and TouchPoint™ applications. These SaaS products have been developed in the Microsoft Azure cloud and complement existing back-end (on premises, data center) electronic monitoring systems for alcohol monitoring and offender management (SCRAMnet™ and SCRAM GPS™). Since 2016, SCRAM Systems has received ISO/IEC 27001:2013 certification for Alcohol Monitoring, Offender Management, and Judicial Management services in SCRAMnet for these SaaS programs. Recently, a private cloud IaaS data center has been integrated into the ISO 27001 ISMS and will be certified later this year.

III. RISK ASSESSMENT INTEGRATION IN THE ISMS

The development of the AMS ISMS has required periodic risk assessment as new features and products have been implemented in the ISO 27001 cycle of documentation, risk assessment and treatment, management review, control selection, internal audit, monitoring and certification (the classic Plan-Do-Check-Act PDCA cycle). The risk assessment use cases developed over the course of these certifications have optimized industry practices which can be too expensive, provide insufficient data, and slow down the management and business delivery process. The following table summarizes the criteria associated with the different product lines and the challenges posed by RA methods.

TABLE I. RISK ASSESSMENT CRITERIA

Applications	Cloud Deployment	Target Domain	Risk Assessment Approach
Alcohol Monitoring	Hybrid Cloud - SaaS	Corrections /Rehabilitation	ISO 27005 – RA Scenario-based
Offender Management	Hybrid Cloud - SaaS	Corrections Industry	ISO 27005 – RA Scenario-based National Self-Assessment
Judicial Management Services	Hybrid Cloud - SaaS	Government Corrections Industry	ISO 27005 – RA Scenario-Based
International Data Center	Private Cloud - IaaS	International Government Corrections Industry	ISO 27005 – RA Asset-based National Self-Assessment

The four applications in Table 1 present a variety of RA options that will be described after a brief discussion of the risk management methods generically developed for the SCRAM Systems ISMS program. A previous paper, 'Taking Compliance to the Cloud' [1} described these RA methods applied with ISO 27001 for Hybrid Cloud, SaaS services, Government market (UK National Centre for Cyber Security Cloud Security Principles) and a scenario-based RA approach aligned with these ISO standards –

- ISO27002 Security techniques – Code of practice for information security controls
- ISO27005--Information Security Risk Management
- IS 27017—Information security controls based on ISO27002 for cloud services
- ISO27018—Protection of Personally Identifiable Information (PII) in public clouds

A. *Methods for the Cloud Risk Assessment*

For the on-premises, data center applications (Alcohol Monitoring, Offender Management) an ISO 27001 implementation project was performed in 2016-17. The initial ISMS risk assessments was performed in the using the tandard ISMS PDCA development cycle. Subsequent RAs have been developed as part of the yearly ISO 27001 program affecting the changing scope of the ISMS.

A risk assessment approach using the NIST SP 800-30 risk model is well-described in the 'Scenario-Based Methodology for Cloud Computing Security Risk Assessment' paper [7}. An ISO 27005 risk management method for cloud systems is presented in the previous 'Taking Compliance to the Cloud' work [1]. The basic steps of these methods have been integrated into our ISMS program.

TABLE II. RISK ASSESSMENT AND RISK MANAGEMENT TECHNIQUES

NIST SP 800-30 Risk Assessment	ISO 27005 Information Security Risk Management
System Characterization	Context Establishment
Threat Identification	Risk Assessment
Vulnerability Identification	Risk Analysis – Risk Identification
Control Analysis	Risk Analysis – Risk Estimation
Likelihood Determination	Risk Evaluation
Impact Analysis	Risk Treatment
Risk Determination	Risk Acceptance or
Control Recommendation	Risk Monitoring and Review, Communication and Redo

Per the assessment and management policies and methodologies being implemented, the primary objective of an ISMS is the management of risk. The goal is to protect the business from events which have a negative effective such as

- A business has not realized stated corporate objectives
- Safeguarding assets of the company fails to protect from loss
- Policies and procedures are non-compliant with regulatory, legal and/or organization standards
- Inefficient and ineffective use of resources of the business
- Information confidentiality, integrity and availability is not maintained

B. *Scenario-based vs Asset-based Risk Assessments*

The RA models for AMS utilize both approaches in evaluating cloud systems for the ISMS. The distinction between asset-based and scenario-based RA methods has been described as "A risk is usually defined as a threat combined with a vulnerability, but with ISO27001:2013 you need not go through the whole process of identifying threats and vulnerabilities separately – you can simply define and identify the risk. This is commonly referred to as a scenario-based risk assessment approach." (https://www.vigilantsoftware.co.uk/)

IV. USE CASES FOR THE CLOUD RISK ASSESSMENT

The examples presented here are derived from the integration of multiple AMS products and the RA cycles to scope and expand the boundaries of the ISMS.

A. *Hybrid Cloud*

From ISO 27017, a new cloud control, CLD.13.1.4 alignment of security management for virtual and physical networks, presents the risk that virtual networks are configured differently from physical ones and as a consequence do not provide the same required level of security.

B. *Application Program Interface (API)*

Multiple controls from the Cloud Security Alliance (CSA) cloud control matrix examine the APIs which may transit cloud applications and on-premises data resources

- AIS-01 - Application & Interface Security Application Security
- CCC-05 - Change Control & Configuration Management Production Changes
- IAM-02 - Identity & Access Management Credential Lifecycle / Provision Management
- IPY-03 - Interoperability & Portability Policy & Legal

C. *Asset Inventory*

The initial risk assessment for Alcohol Monitoring and Offender Management ISMS systems includes asset management for servers, workstations, storage and backup, network equipment, network segments, applications, data repositories, virtual technologies, and service providers. Although an asset-based risk assessment has not performed, data center systems configurations have been maintained and updated annually.

D. Asset-based Risk Assessment

An asset-based inventory for cloud systems is not widely adopted in the industry. ISO 27001 asset definition might deal with components like 'an IaaS system' rather than examining the detailed components of a cloud deployment comparable to data center inventories. This topic was highlighted in 'Taking Compliance to the Cloud' [1] only to suggest that protection of data assets may have more scope in a cloud RA.

E. Private Cloud

The ascendancy of 'infrastructure as code' has been adopted for emerging systems at AMS. This includes modeling complete data center services in an IaaS system. An assessment of this type of delivery network has emerged in companies like Soft Layer for which the ISMS scope statement reads – "SoftLayer's operational functions are integrated into its proprietary management system, known as IMS. IMS automates all critical aspects of the business, such as dedicated servers, power strips, firewalls, load balancers, updates, accounting, compliance controls, inventory, contracts, etc.".

F. Government Cloud (SaaS Deployment)

Worth mentioning in the Government Cloud (Azure GovCloud) are the more restrictive controls of advanced data protection, security identity, data at rest protection using data at rest encryption, managed secrets and dedicated cloud infrastructure resources for hosting PaaS objects and providing SaaS service to government agencies. In providing services to government communities, GovCloud uses physically isolated datacenters and networks (located in U.S. only). Azure Government customers (US federal, state, and local government or their partners) are subject to validation of eligibility.

G. International Cloud Deployments

In scaling cloud solutions to national and international deployments companies will be complying to global, government, industry and regional regulatory requirements. This attestation can be typically found on compliance portals maintained by major Cloud Service Providers (CSP) such as Azure, Google and AWS . A good example of a National Cloud Security Risk Self-Assessment is available on the New Zealand governments ICT portal [8]

V. Summary Findings and Future Research

This article has introduced different approaches for an ISO 27001 program to address the questions – "What are the risks of deploying my software (SaaS), tools (PaaS), and/or infrastructure (IaaS) in the cloud?" Many Chief Business Officers (CxOs) adopting a 'cloud first strategy' face the challenge of methods and process to operate securely in commercial, government, and regulatory markets. The adoption of the ISO 27017 standard for controls for cloud services is a good first step. However, this standard represents only about 10% of the industry's Cloud Security Alliance Cloud Control Matrix (CSA CCM) which has been widely implemented by leading Cloud Security Providers.

At the end of the day Risk.net's 2018 survey of financial industry executives provides risk taxonomies with real-world insight into what keeps CxOs awake at night [9]. The top 3 risks should come as no surprise – IT disruption, protecting customer data and meeting regulatory compliance. The use cases presented here are a first step for implementing risk assessment context for the cloud computing platforms (Anything as a Service/XaaS, Cloud Security Provider, Cloud Security Customer, etc.). Work will continue to define 'standard, practical, non-theoretical' RA techniques for the cloud out here in the ISO 27001 field of practice.

Acknowledgment

Thanks to Rick Kuhn (NIST) and Roger Hughes (AMS) for their comments and encouragement on this paper.

References

[1] T. Weil, "Taking Compliance to the Cloud—Using ISO Standards (Tools and Techniques)," in IT Professional, vol. 20, no. 6, pp. 20-30, 1 Nov.-Dec. 2018.

[2] M. Iorga and A. Karmel, "Managing Risk in a Cloud Ecosystem," in IEEE Cloud Computing, vol. 2, no. 6, pp. 51-57, Nov.-Dec. 2015.

[3] S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange a Nina Viktoria Juliadotter; Kim-Kwang Raymond Choo, "Cloud Attack and Risk Assessment Taxonomy", in IEEE Cloud Computing, vol. 2, no. 1, pp. 14-20, Jan-Feb. 2015.

[4] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011.

[5] G. Wangen, "Information Security Risk Assessment: A Method Comparison," in Computer, vol. 50, no. 4, pp. 52-61, April 2017.

[6] Khogali, I. M. A., & Ammar, P. H. (2017). A Scenario-Based Methodology for Cloud Computing Security Risk Assessment. International Journal of Innovation Education and Research, 5(12), 127-155.

[7] SoftLayer ISO 27001 certifcation, online available- https://www.softlayer.com/SoftLayer4/pdfs/SoftLayer_ISO_Certificate.pdf

[8] New Zealand National Cloud Security Risk Assessment, online available-NZ ICT Portal - https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/

[9] Risk.net 2018 IT Risk Survey of Financial Business Executives online available- https://www.risk.net/risk-management/5426111/top-10-op-risks-it-disruption-tops-2018-poll