Standards for Cloud Risk Assessments – What's Missing?

Timothy Weil
Principal (Cybersecurity)
SecurityFeeds LLC
Denver, CO. USA
trweil@ieee.org

Abstract— **Conducting a risk assessment (RA) for cloud computing platforms presents new challenges in the space of Information Security Management Systems (ISMS). ISO 27001 RA methods have been used for Alcohol Monitoring Systems (AMS) across a portfolio of products and services. Scaling these localized techniques to national and international cloud security standards shows that a 'one size fits all' Risk Assessment approach does not exist in the industry today. The context and methods for conducting cloud risk assessment are examined across representative national and international standards and guidelines.**

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

I. INTRODUCTION

This paper examines risk management and risk assessment (RA) methods for cloud security in the context of national and international guidelines. Fundamental to the implementation of an ISO 27001 ISMS a formal RA must be conducted to examine information risk. This process determines a representative scope of interest involving the stakeholders, security boundaries, management and technical controls and other facets of information risk governing the ISMS. Recently, ISO 27001 compliance projects developed for Alcohol Monitoring Systems (AMS) in Littleton, CO. have been assessed against a body of governance frameworks in the US, EU, and Asia. As might be expected, the requirements for cloud security vary from country to country. This summary review of cloud security methods suggests that the Risk Assessment discipline for cloud systems has challenges to be addressed in the marketplace of ideas.

II. CONTEXT OF THE CLOUD RISK ASSESSMENT

The RA process for securing cloud systems in the AMS ISMS has been discussed in previous work [1][2]. Some of the issues to be highlighted in previous work includes –

- Cloud deployment models (hybrid, private, community clouds)
- Cloud service models (Software as a Service/SaaS, Platform as a Service/PaaS, Infrastructure as a Service/IaaS)
- Regulatory and governmental cloud requirements
- Portability of cloud certifications across international boundaries

Over time, this work has scaled to include other established risk catalog and compliance models for cloud security [3][4]. Any conversation on cloud risk must be based on established cloud security taxonomies that highlight attack surfaces and threat vectors to be managed [5][6]. Research in this area has developed over the past few years to include unique approaches for conducting the risk assessment process specific to managing cloud security [7] [8].

Judicial Management Services are 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 backend (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.

III. STANDARDS FOR CLOUD SECURITY ASSESSMENT

In the areas of national and international cloud compliance standards, AMS has evaluated criteria for US (FedRAMP), UK (G-Cloud), NZ (PSPF-Cloud) and AU (IRAP) cloud security requirements. These 'high end' standards are governed by in-country agencies National Institute of Standards and Technology (NIST-US), National Cyber Security Centre (NCSC-UK), and Australia Signals Directorate (ASD-AU). Table I (National Cloud Security Standard) below highlights other comparable national cloud security standards in Singapore (MSCI) and Germany (C5). Three standards shown in Table I present a variety of cloud compliance options that cross-national borders and are often adopted for international use. Previous papers by DiGiulio et al. 'Cloud Standards in Comparison (2017) [11]' and 'IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Provider (2017),[12]' describe the strengths and weakness of Cloud Security frameworks using FedRAMP, ISO 27001 and C5 models. AMS has evaluated both the ISO 27017 and CSA CCM approach to cloud security.

Specific to the risk assessment for cloud services the ENISA Risk Assessment (2009) is a comprehensive document that has relevance 10 years on. That said, it is a 125-page document and not easily consumed by ISO 27001 implementers. Also, the US FedRAMP and Australia IRAP compliance models are costly, documentation heavy and time-consuming for adaptation by national agencies [4].

TABLE I. - NATIONAL CLOUD SECURITY STANDARDS

National Cloud Security Standard	Organization
FedRAMP (US)	Federal Risk Assessment Management Program [8]
G-Cloud (UK)	UK National Cybersecurity Center [9]
IRAP (AU)	Australia Information Security Registered Assessors Program [10]
Cloud Computing Risk and Assuarance Framework (NZ)	Protective Security Policy Framework (Cloud Risk) [11]
MTSC (SS)	Singapore Multi-Tier Cloud Security [12]
C5 (GE)	Cloud Computing Compliance Controls Catalogue [13]
International Cloud Security Standard	**Organization**
ENISA Cloud Risk Assessment (2009) [14]	European Union Agency for Cybersecurity
CSA CCM 2019 [15]	Cloud Security Alliance Cloud Control Matrix
ISO 27017:2015 Cloud Security Controls [16]	International Standards Organization

CSA's Cloud Control Matrix and STAR certification is widely practiced in the industry. That said, this is more of a best practices attestation and risk management does not directly overlay this approach. The same can be said of the ISO 27017 Cloud Security Controls standard which covers about 10% of the CCM requirements. Further discussion of the risk assessment methods in these frameworks will be presented after a summary look at the RA methods in the AMS ISMS.

IV. METHODS FOR AMS CLOUD RISK ASSESSMENT

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 [2].

TABLE II. AMS RISK ASSESSMENT METHODS

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

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 were performed in the using the standard ISMS PDCA development cycle. Subsequent RAs have been developed as part of the yearly ISO 27001 program affecting the changing scope of the ISMS.

FIGURE 1. RISK ASSESSMENT IN THE ISO27001 MODEL

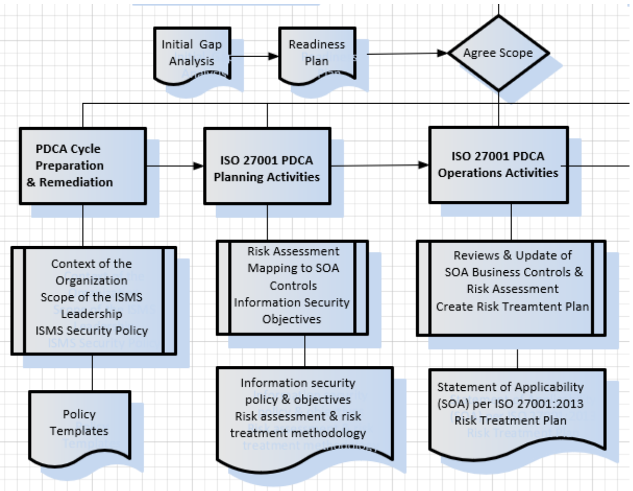

Initial Gap Analysis
Readiness Plan
Agree Scope
PDCA Cycle Preparation & Remediation
ISO 27001 PDCA Planning Activities
ISO 27001 PDCA Operations Activities
Context of the Organization Scope of the ISMS Leadership ISMS Security Policy
Risk Assessment Mapping to SOA Controls Information Security Objectives
Reviews & Update of SOA Business Controls & Risk Assessment Create Risk Treamtent Plan
Policy Templates
Information security policy & objectives Risk assessment & risk treatment methodology
Statement of Applicability (SOA) per ISO 27001:2013 Risk Treatment Plan

Figure 1 shows the risk assessment approach using the ISO 27001 risk model. An implementation of this 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.

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 effect such as

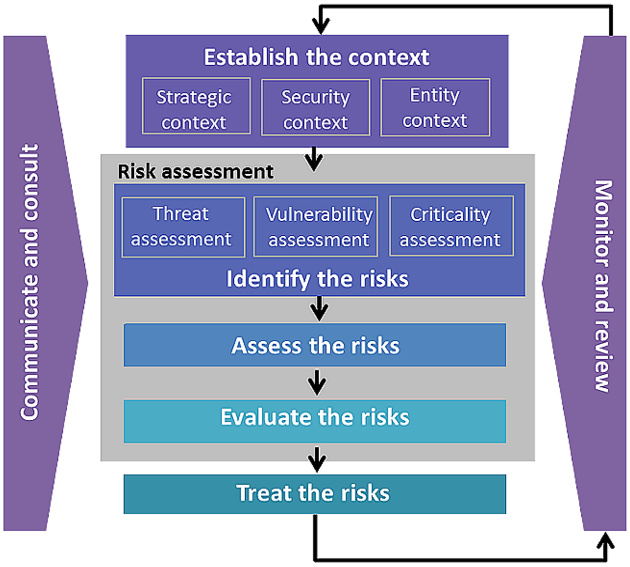
- A business has not realized stated corporate objectives
- Safeguarding assets of the company fails to protect from loss
- Policies and procedures are non-compliant with regulatory, legal and/or organization standards
- Inefficient and ineffective use of resources of the business
- Information confidentiality,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

V. Risk Assessment Models in Cloud Security Standards

What has been challenging in the AMS RA cycles are the context and control issues [2] including –

- Scenario vs Asset-based RA methods
- Maintaining cloud asset inventory
- Software security in Application Program Interface
- Data categorization and data sharing with 3rd parties

FIGURE 2. ISO 27005 Risk Assessment and Risk Treatment Method

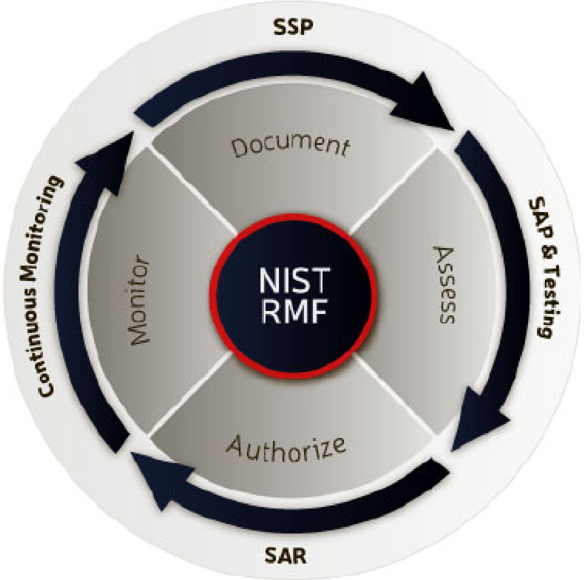


These topics were addressed in 'Risk Assessment Methods for Cloud Computing Platforms' work [2]. Typically, the national requirements will include a large documentation set, control compliance catalogs, operational security inspection and a governance framework that aligns with national IT programs. The specific use of the Risk Assessment process will vary from border to border. We will now discuss these topics in the context of national and international standards.

A. FedRAMP Risk Assessment Report

Federal Risk and Authorization Management Program (FedRAMP) is a mandatory US government program that provides a standardized approach to security assessment, authorization, and monitoring for cloud services used by federal agencies. NIST SP 800-145 [20] establishes FedRAMP's definitions for cloud services that are IaaS, PaaS, or SaaS for Cloud Service Providers (CSPs) needing to define their offerings as one or multiple of the service models.

FIGURE 3. FedRAMP Authorization cycle with agency sponsorship



- System Security Plan and Appendices
- Information Security Policies and Procedures
- User Guide
- Digital Identity Worksheet
- Privacy Impact Assessment (PIA) Template
- Rules of Behavior (RoB) Template
- Information System Contingency Plan (ISCP) Template
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Control Implementation Summary (CIS)
- Federal Information Processing Standard (FIPS) 199 Categorization Template
- Separation of Duties Matrix
- FedRAMP Laws and Regulations
- FedRAMP Integrated Inventory Workbook Template

The findings from review of the documentation package, application and vulnerability testing results are presented in the FedRAMP Security Assessment Report (SAR) and the Risk Exposure Table which provides Risk Descriptions and Exposure from the vulnerability scanning results.

B. IRAP Cloud Certification (Australia)

The Australian Signals Directorate (ASD) maintains the ASD Certified Cloud Services List (CCSL) for the storage and processing of unclassified data. The Certification recognizes the successful completion, review and acceptance of a comprehensive assessment undertaken by an independent security registered assessor.

The IRAP cloud certification process is conducted by the Australian Signals Directorate (ASD), based on government principles and policies as defined in the government's Protective Security Policy Framework (PSPF) and the Australian Government Information Security Manual (ISM). The Cloud Services models in the ISM use terminology consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, the NIST Definition of Cloud Computing [20]. When a cloud service provider (CSP) successfully meets the expected Australian Government security requirements ASD Certification is granted and the CSP cloud service is published on the ASD Certified Cloud Services List (CCSL) at http://www.asd.gov.au/irap/certified_clouds.htm.

IRAP certification sits within a risk management accreditation framework as described in the ISM. Risk management best practice suggests all systems be accredited before they are deployed. Accreditation using the ISM methods follows a similar pattern to FedRAMP using an independent security assessment, certification and identification of residual risk and final accreditation formally accepting mitigations and residual security risk. Detailed ASD cloud security guidelines are published at https://www.cyber.gov.au/publications/cloud-computing-security-considerations

C. New Zealand Cloud Computing Risk and Assurance Framework

The New Zealand (NZ) Government Chief Information Officer (GCIO) has published a framework of 105 questions focused on the security and privacy aspects of cloud services that are fundamentally related to data sovereignty. Categorization of cloud risk listed below are available at https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/

1) Security Privacy Risk and Issue Model [19]

a) Environment Related Issues

- Conflicts in Jurisdiction
- Misuse of Authority
- Inefficient Judicial Cooperation
- Complicated Adaptation to Globalization
- Limited Offshore Service Usage
- Ambiguous Definition in Regulations
- Outdated Policies and Strategies
- Lack of Enforcement Technique
- Lack of Service Continuity Protection

b) People Related Issues

- Lopsided Contractual Balance
- Ambiguous Data Residual Policy
- Lack of SLA Alteration Notification
- Lack of Risk Prediction from User Side
- ICT Supply Chain Visibility
- Disaster Recovery Plan Notification
- Diverse Understanding of Contract
- Ambiguous ICT Supply Chain Responsibility
- Diverse Understanding of Terms
- Ambiguous Definitions in Contract

c) Technology Related Issues

- Lack of Activity Detection
- Unforeseeable Data Location
- Lack of Evidence Preservation
- Lack of Data Flow Monitoring
- Inappropriate Multi-tenancy Management
- Inappropriate API Usages

D. NCSC 14 Cloud Security Principles

The UK NCSC office, established in 2016, publishes a set of 14 design principles for building confidence and transparency in cloud-computing systems [3]. These guidelines must be attested to in accrediting CSP applications to the UK government's G-Cloud marketplace.

- Data in Transit Protection
- Asset Protection and Resilience
- Separation Between Users (Multi-tenancy)
- Governance Framework
- Operational Security
- Personnel Security
- Secure Development
- Supply Chain Security
- Secure User Management
- Identity and Authentication
- External Interface Protection
- Secure Service Administration
- Audit Information for Users
- Secure Use of the Service

The structure of the NCSC cloud portal lends itself to a methodical review of these best practices by providing questions to be addressed for each subject. An example is given here –

Cloud Security Principle	
Data in transit protection	
Description of the Principle	**Why this is important**
User data transiting networks should be adequately protected against tampering and eavesdropping.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.

E. *ENISA Cloud Security Risk Assessment*

A 2011 ITGI study of Japan's use of cloud computing and risk posture [18] as compared to the ENISA report (2009) [16] highlighted categories and sub-categories of risk shown below -

- Organization Risk
  - Vendor Lock-In
  - Loss of Governance
  - Compliance Challenges
  - Loss of Business Reputation Due to Multi-Tenancy
- Technical Risk
  - Resource Exhaustion
  - Isolation Failure
  - Malicious Insider
  - Management Interface Compromise
- Legal Risk
  - Subpoena and E-Discovery
  - Changes of Jurisdiction
  - Licensing Risks
- Common Risk
  - Network Attacks
  - Social Engineering
  - Operations Security
  - Physical Security

F. *CSA Egregious Eleven Cloud Security Threats*

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) provides detailed information about how cloud service providers fulfill the security, privacy, compliance, and risk management requirements defined in the CCM version 3.0.1 [15]/ The 2019 CSA 'Egregious Eleven' cloud security threats list the following attack vectors -

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control Plane
9. Metastructure and Application-structure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

G. *ISO 27017 Risk Assessment*

Previous work described in 'Taking Compliance to the Cloud' [1] illustrates a risk-assessment approach for cloud computing Software as a Service applications derived from the ISO 27001 Information Security Management System (ISMS) standard and complemented by ISO 27017 practices for Cloud Security and Protecting Personal Information in the Cloud. A simple model used in this exercise conforms to a definition of risk (per ISO standards) as 'the combination of the probability of an event and its consequences'.

The 27017 Annex A standard extends the control sets from ISO 27001 with an additional 37 control enhancements. Clarity is required between both Cloud Service provider and customer, on who is responsible for what. Recognition that some security responsibilities lie with the provider, some with customer, some shared. A summary of unique cloud security risks in ISO 27017 include the following -

- CLD.6.3.1: Requires agreement on cloud service information security roles that are shared between cloud service provider and customer
- CLD.8.1.5: Provide clarity around what happens to assets in the cloud at contract termination
- CLD.9.5.1: Provider must protect and separate the customer's virtual environment
- CLD.9.5.2: Both provider and customer ensure virtual machines are configured and hardened.
- CLD.12.1.5: Lay out the details on customer's responsibility to define, document and monitor administrative
- CLD.12.4.5: Lay out how the provider should facilitate the customer's ability to monitor their cloud computing environment.
- CLD.13.1.4: Address build standards and configurations that will be in place between the virtual network and physical environments

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.

VI. What's Missing in Cloud Risk Assessment Methods

Previous papers by Akshaya et al. 'Taxonomy of Security Attacks and Risk Assessment of Cloud Computing [7]' and Choo et al. 'Cloud Attack and Risk Assessment Taxonomy [11]' describe Cloud Security attack strengths and weaknesses and provide different risk assessment methods. The observations can be compared with these extracts from the AMS ISMS RA projects.

TABLE III. Cloud Risk using ISO 270177 Standard

ISO 27017 Control	Example Risk
CLD.6.3 Relationship between cloud service customer and cloud service provider	It is not clear who does what with respect to cloud security and so data is compromised because one party was under the impression that the other was monitoring cloud security

CLD.9.5.1 Segregation in virtual computing environments	Another cloud customer can access the organization's information stored in a cloud application.
CLD.9.5.2 Virtual machine hardening	A virtual machine is used as an entry point for an attack.
CLD.13.1.4 Alignment of security management for virtual and physical networks	Virtual networks are configured differently to physical ones and therefore don't provide the same required level of security.

TABLE IV. CLOUD RISK USING NCSC (UK) CLOUD SECURITY PRINCIPLES

NCSC Cloud Security Principle and CIA	**Example Risk**
Data in transit protection (confidentiality)	The integrity or confidentiality of the data may be compromised while in transit.
Asset protection and resilience (integrity)	Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.
Governance framework (integrity)	Any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.
Supply chain security (availability)	It is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

What has yet to be seen in the literature and industry practice is a generalized, systematized approach to conducting Risk Assessment for Cloud Computing across the national and international standards illustrated in this paper.

VII. SUMMARY FINDINGS AND FUTURE RESEARCH

This article has different contexts in which risk assessment methods are applied in both national and international guidelines and standards. In keeping with the ISO 27001 Planning Clause 6.1.2 the organization risk assessment process will –

- Establish and maintain information security risk criteria
- Produce repeatable and verifiable information security risk assessment results
- Identify, analyze and evaluate information risk

At the end of the day KPMG's white paper on 'Five Key Cloud Computing Risks' [21] provides risk taxonomies with real-world insight. These top risk categories should come as no surprise – technology, operational, vendor, financial, protection of customer data and regulatory compliance. The national and international standards models for cloud risk assessment present a variety of solutions that are 'all over the map.' Implementing a risk assessment context for the cloud computing platforms (Anything as a Service/XaaS, Cloud Security Provider, Cloud Security Customer, etc.) is an important first step worth further research and study. 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 Fred Beck (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. DOI - https://doi.ieeecomputersociety.org/10.1109/MITP.2018.2877312

[2] T. Weil, "Risk Assessment Methods for Cloud Computing Platforms," *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Milwaukee, WI, USA, 2019, pp. 545-547. doi: 10.1109/COMPSAC.2019.00083

[3] C. D. Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell and M. N. Bashir, "Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, CA, 2017, pp. 50-57.

[4] Carlo Di Giulio, Charles Kamhoua, Roy H. Campbell, Read Sprabery, Kevin Kwiat, and Masooda N. Bashir. 2017. IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (CCGrid '17). IEEE Press, Piscataway, NJ, USA, 1090-1099. DOI: https://doi.org/10.1109/CCGRID.2017.137

[5] N. V., & Choo, K.-K. R. (2015). CATRA. The Cloud Security Ecosystem, 37–81. doi:10.1016/b978-0-12-801595-7.00003-3

[6] Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman Khan, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. 2016. On cloud security attacks. *J. Netw. Comput. Appl.* 74, C (October 2016), 98-120. DOI: https://doi.org/10.1016/j.jnca.2016.08.016

[7] Akshaya, M., Padmavathi, G., 2019/01/01, Taxonomy of Security Attacks and Risk Assessment of Cloud Computing: Proceedings of ICBDCC18, DO - 10.1007/978-981-13-1882-5_4

[8] Nina Viktoria Juliadotter, Kim-Kwang Raymond Choo, Cloud Attack and Risk Assessment Taxonomy, IEEE Cloud Computing, 2015}, vol 2, pgs 14-20}

[9] Federal Risk Assessment Management Program (US) - https://www.fedramp.gov/

[10] UK National Cyber Security Center (NCSC) Cloud Security Requirements - https://www.ncsc.gov.uk/

[11] Australia Information Security Registered Assessors Program (IRAP)- [1]https://www.cyber.gov.au/irap/what-irap

[12] New Zealand Cloud Computing Risk and Assurance Framework - https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/

[13] MTSC Multi-Tiered Cloud Security Standard (Singapore) - https://www.imda.gov.sg/-/media/imda/files/industry-development/infrastructure/ida_mtcs-x-cert---implementation-guideline-report_csa-star-to-mtcs_release.pdf?la=en

[14] C5 Compliance Controls Catalogue (Germany) https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

[15] CSA (2019) Cloud Security Alliance Cloud Control Matrix 3.0.1, Cloud Security Alliance - https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/

[16] ENISA (2009) Cloud Computing: Benefits, risks and recommendations for information security, ENISA https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[17] ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services - https://www.iso.org/standard/43757.html

[18] Professor Yonosuke Harada, The Study on Cloud security in Japan 2011/February, Institute of Information Security Management (ITGI), https://m.isaca.org/Knowledge-Center/Research/Documents/Study-on-Cloud-Security-in-Japan_res_Eng_0211.pdf

[19] Janczewski, Lech J. and Miao, Morris Ruoyu, "Regulatory Environment of Cloud Computing in New Zealand" (2017). CONF-IRM 2017 Proceedings. 27. https://aisel.aisnet.org/confirm2017/27

[20] NIST SP 800-145, The NIST Definition of Cloud Computing,
at https://csrc.nist.gov/publications/detail/sp/800-145/final

[21] Sai Gadia, KPMG, ‘How to Manage Five Key Cloud Computing Risks, 2018 at https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf