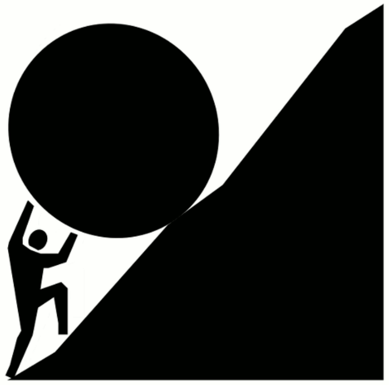
IEEE Cloud Computing Summit 2020

Standards for Cloud Risk Assessment – What’s Missing?

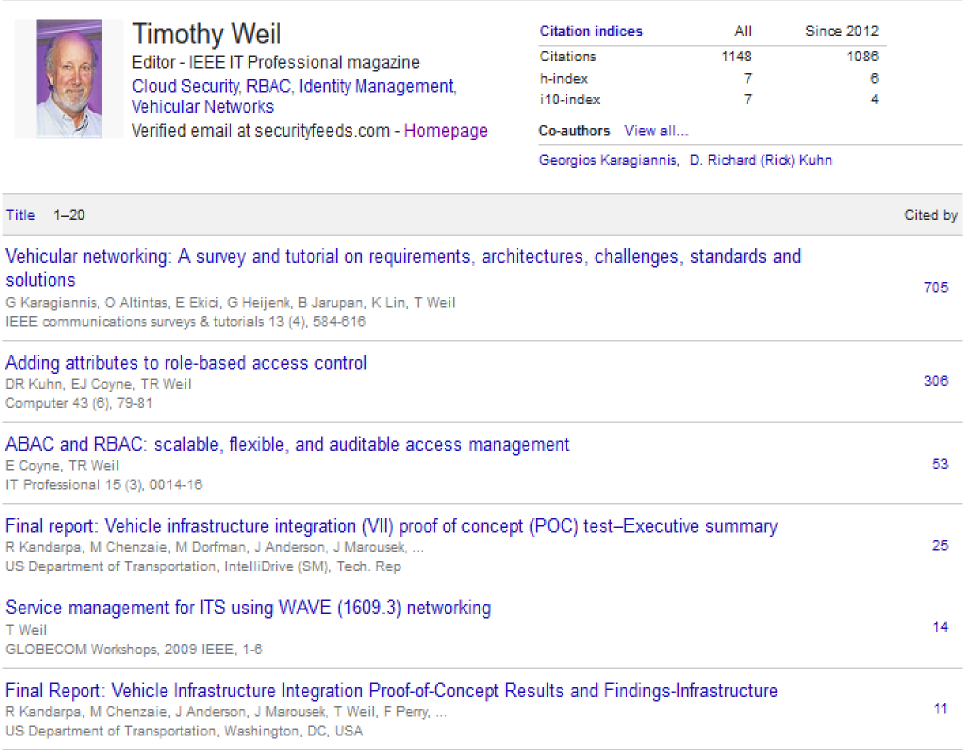


Tim Weil – IEEE Senior Member
Chair – IEEE Denver COMSOC Chapter
http://comsoc.ieee-denver.org

Cybersecurity Professional / Executive Advisor
SecurityFeeds – http://www.securityfeeds.com
Denver, CO

Oct 20th, 2020

A Writer's Life –

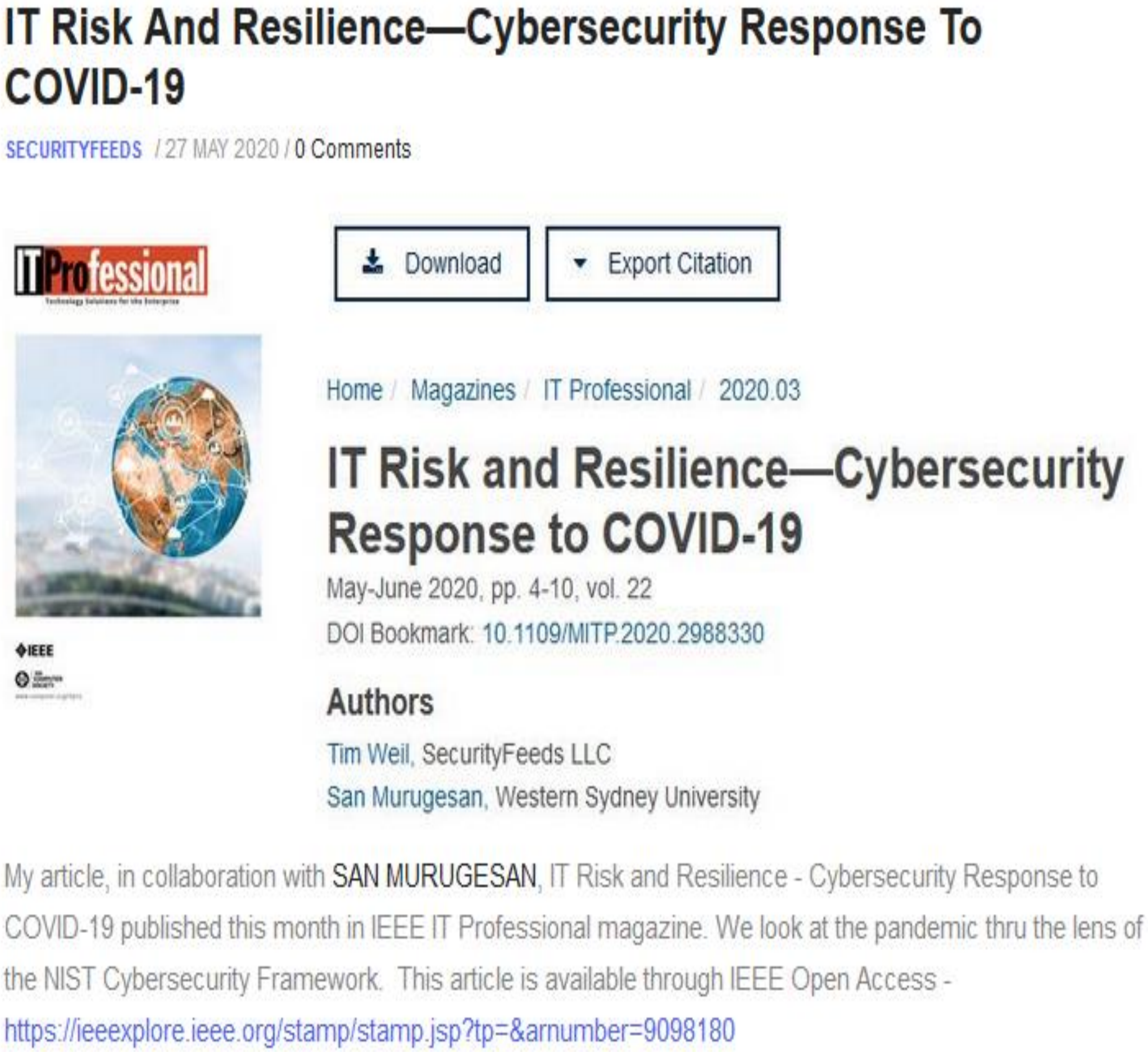


Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ... US Department of Transportation, Washington, DC, USA	11



IT Risk And Resilience—Cybersecurity Response To COVID-19

SECURITYFEEDS / 27 MAY 2020 / 0 Comments

Home / Magazines / IT Professional / 2020.03

IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22

DOI Bookmark: 10.1109/MITP.2020.2988330

Authors

Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

My article, in collaboration with SAN MURUGESAN, IT Risk and Resilience - Cybersecurity Response to COVID-19 published this month in IEEE IT Professional magazine. We look at the pandemic thru the lens of the NIST Cybersecurity Framework. This article is available through IEEE Open Access - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9098180

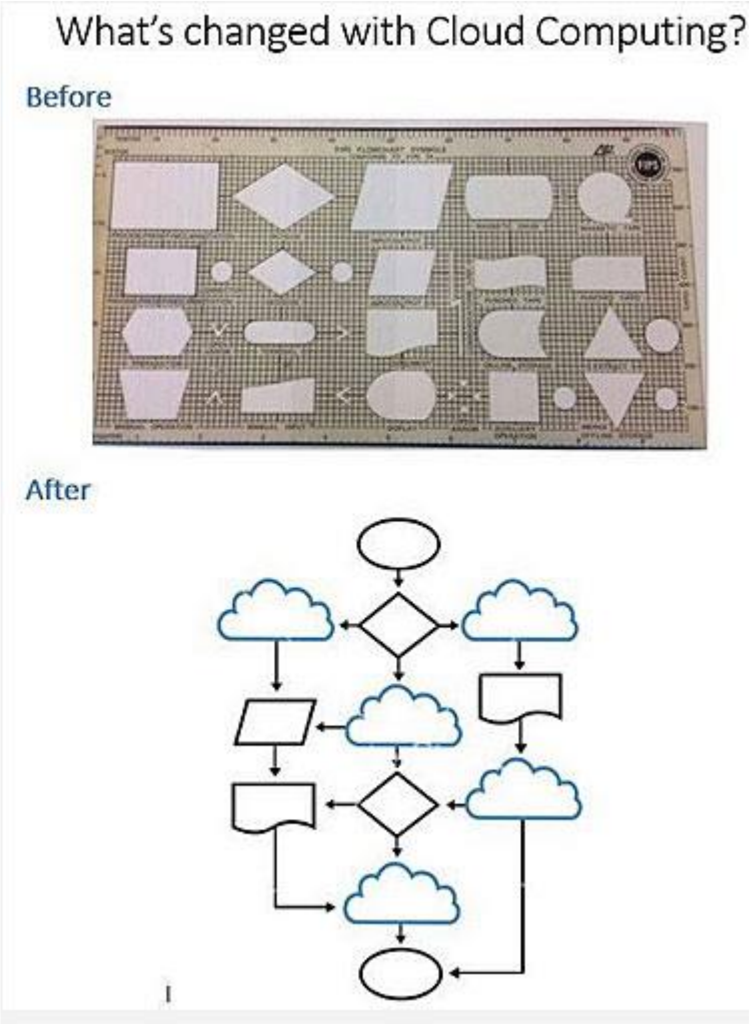
Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment – What’s Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

How we got to the cloud

The evolution of federal IT

A look at the people, policies and technologies that have transformed federal IT in the past 25 years



What's changed with Cloud Computing?

Before

After

European Union Agency for Network & Information Security (ENISA) Cloud Security Guidelines – Top 8 Cloud Security Risks

Cloud Computing

November

Benefits, risks and recommendations for information security

ENISA Cloud Computing Risk Assessment (2009)

- Loss of Governance
- Vendor Lock-In
- Isolation Failure (multi-tenancy)
- Compliance Risk
  - ○ Cloud Provider Compliance Evidence
  - ○ Cloud Provider Audit by Cloud Customer
- Management Interface Compromise
- Data Protection
- Insecure or Incomplete Data Deletion
- Malicious Insider

Produced by ENISA with contributions from a group of subject matter expert comprising representatives from Industry, Academia and Governmental Organizations, a risk assessment of cloud computing business model and technologies The report provide also a set of practical recommendations. **125 Pages**

enisa European Union Agency for Network and Information Security

Cloud Security Alliance – The Dirty Dozen: 12 top cloud security threats (2018)

2018 Top 12 Cloud Security Threats

- Data Breaches
- Insufficient Identity, Credential and Access Management
- Insecurity Interfaces and APIs
- System Vulnerabilities
- Account Hijacking
- Malicious Insider
- Advanced Persistent Threats
- Data Loss
- Insufficient Due Diligence
- Abuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Vulnerabilities

CSA Report on the Treacherous 12 – Top Threats

National Cyber Security Centre (UK)

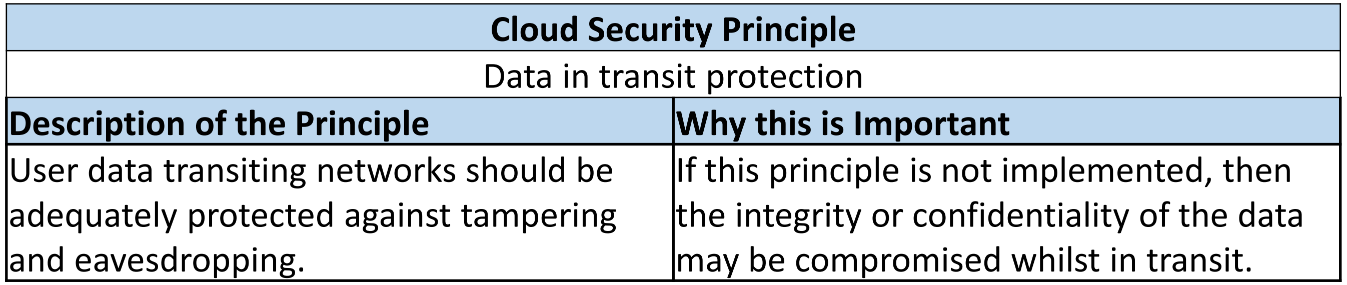
National Cyber Security Centre
a part of GCHQ

Implementing the Cloud Security Principles

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

For each of the 14 principles, we answer three questions:

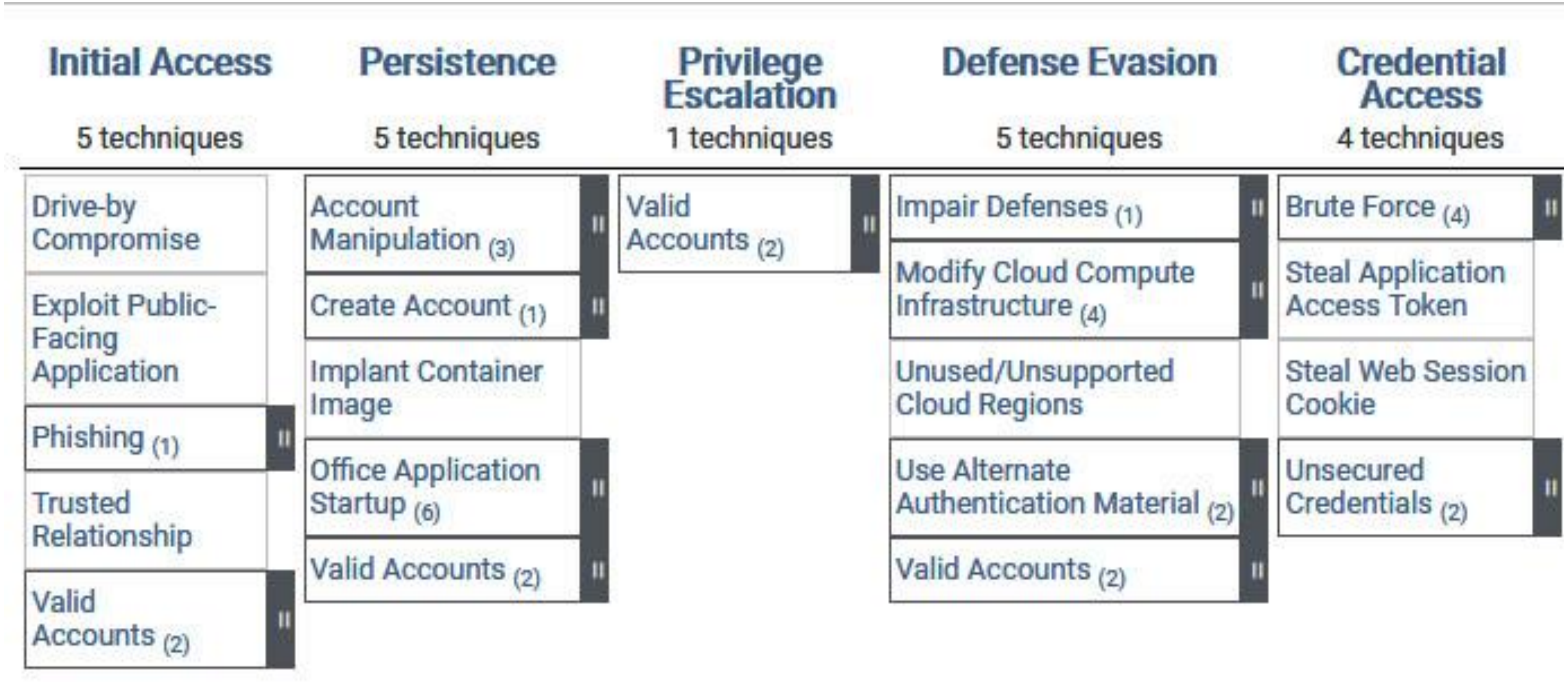
1. **What is the principle?** A description giving the principle some context
2. **What are the goals of the principle?** Concrete objectives for the implementation to achieve
3. **How is the principle implemented?** Details for a set of possible implementations



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.

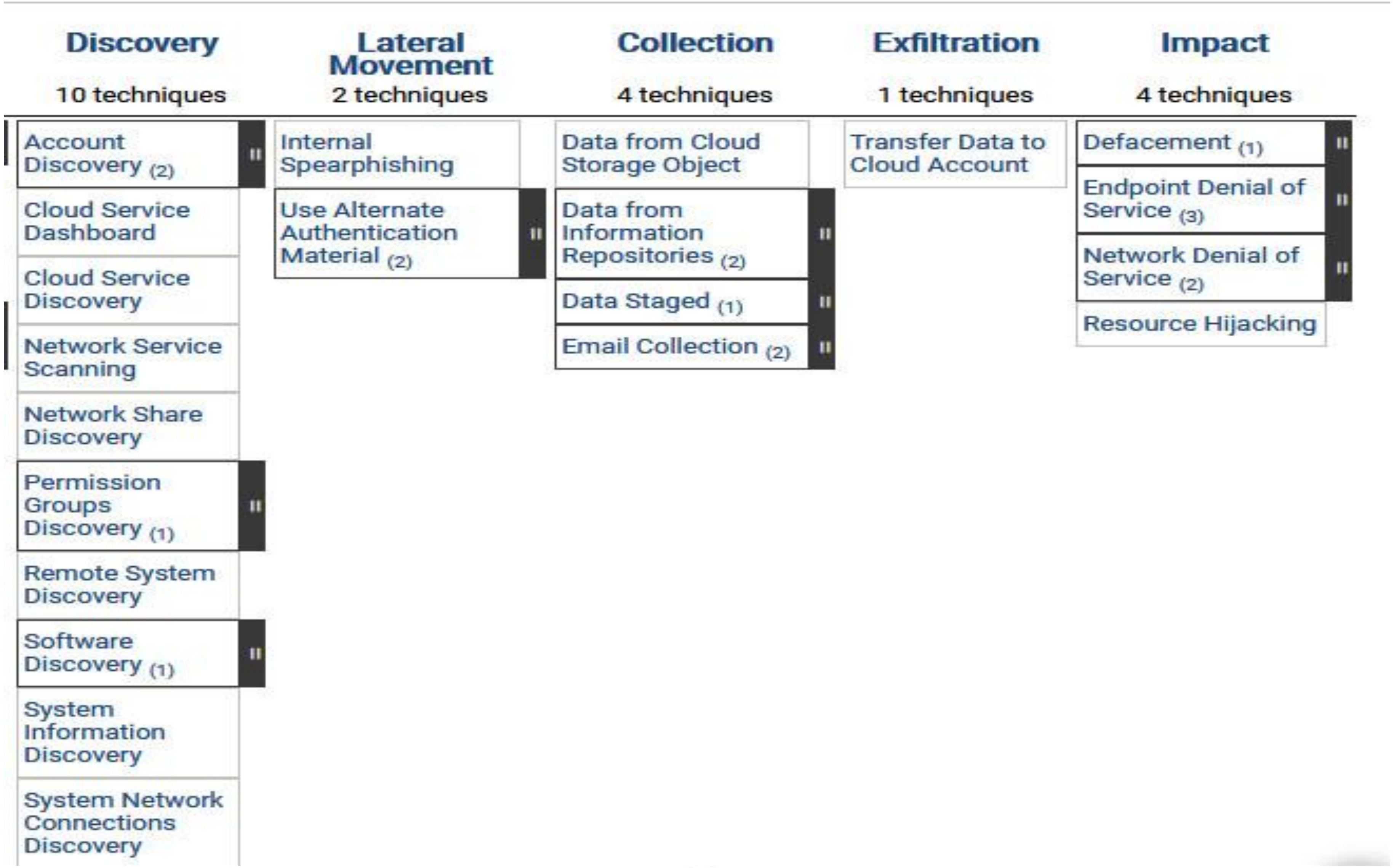
IEEE CLOUD COMPUTING

MITRE ATT&CK Cloud Matrix - https://attack.mitre.org/matrices/enterprise/cloud/



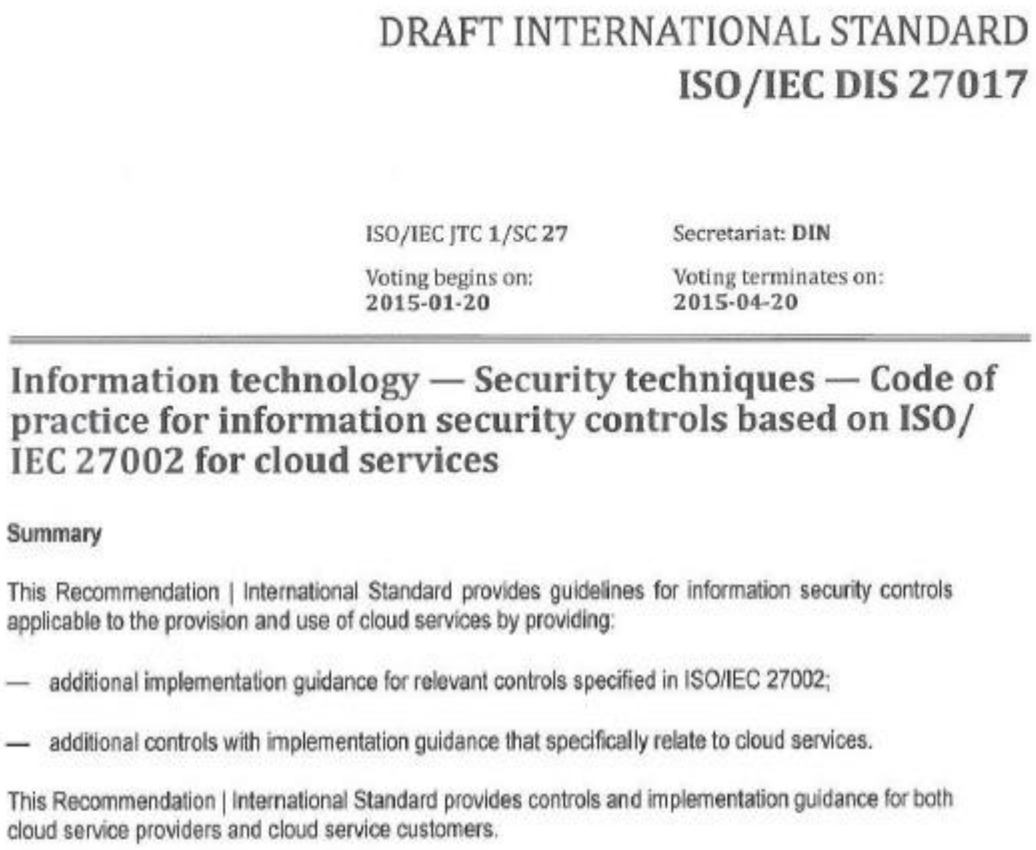
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
5 techniques	5 techniques	1 techniques	5 techniques	4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)	

MITRE ATT&CK Cloud Matrix (2 of 2) - https://attack.mitre.org/matrices/enterprise/cloud/



Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Network Service Scanning		Email Collection (2)		Resource Hijacking
Network Share Discovery				
Permission Groups Discovery (1)				
Remote System Discovery				
Software Discovery (1)				
System Information Discovery				
System Network Connections Discovery				

ISO/IEC 27017 standard – Information Security Controls based on ISO 27002 for Cloud Services



DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 27017

ISO/IEC JTC 1/SC 27	Secretariat: DIN
Voting begins on: 2015-01-20	Voting terminates on: 2015-04-20

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

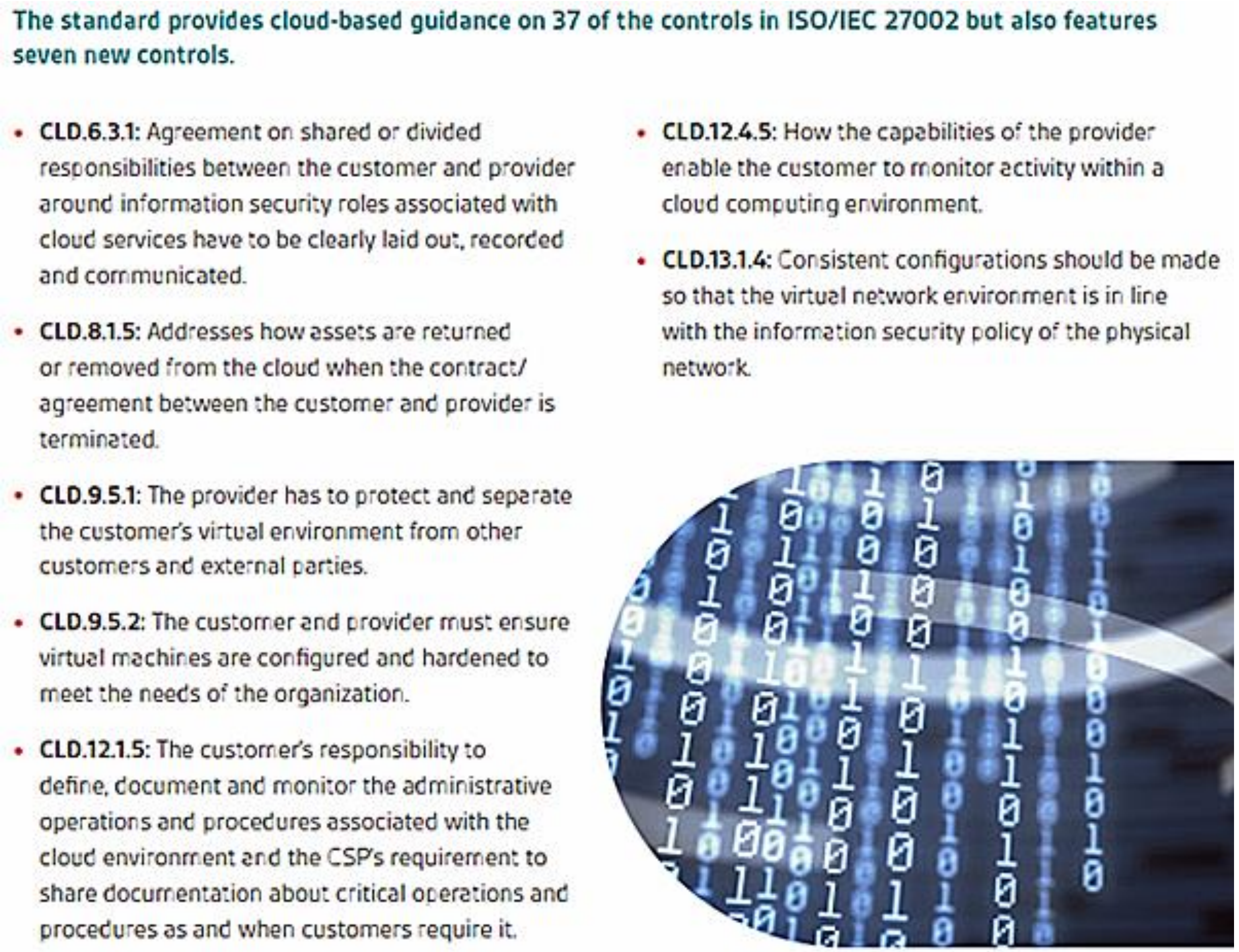
Summary

This Recommendation | International Standard provides guidelines for information security controls applicable to the provision and use of cloud services by providing:

— additional implementation guidance for relevant controls specified in ISO/IEC 27002;

— additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

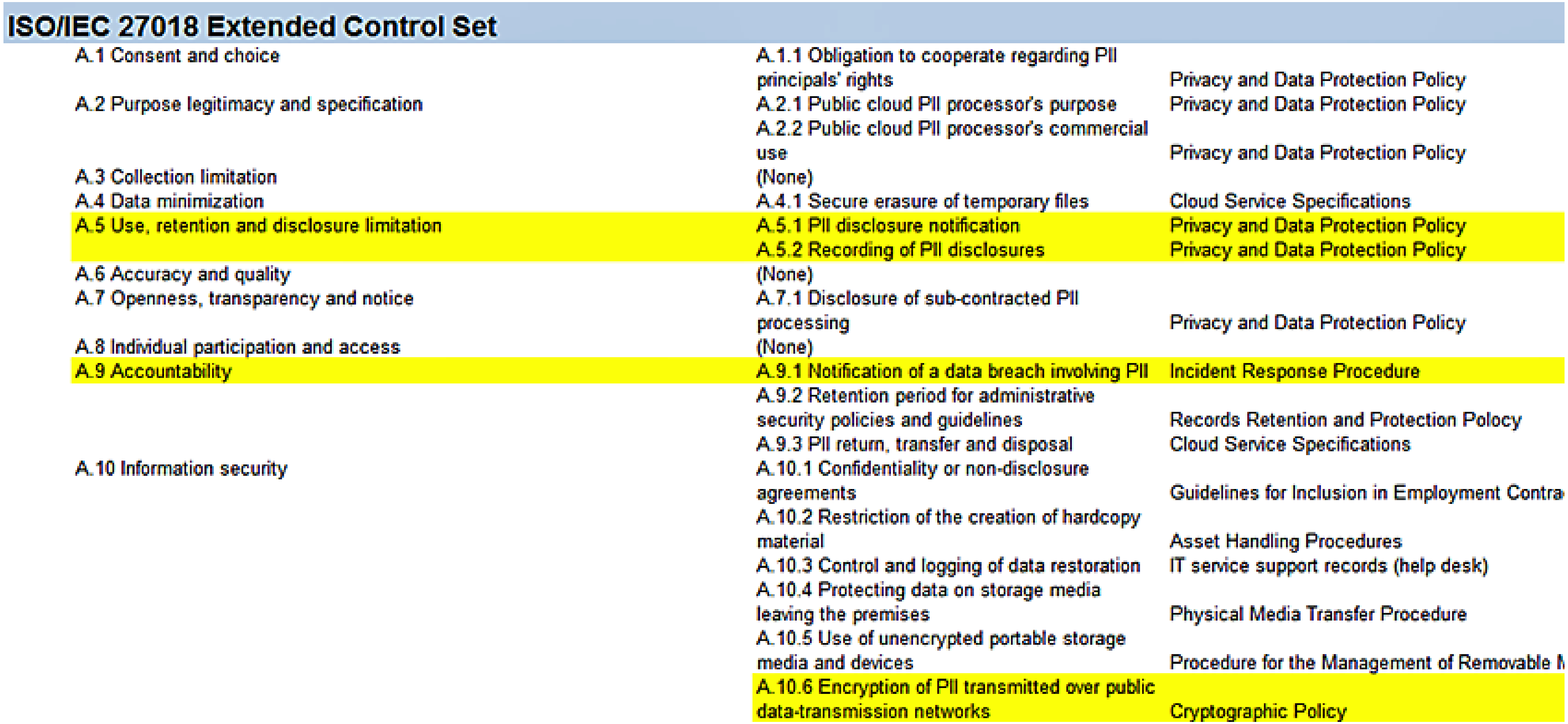


The standard provides cloud-based guidance on 37 of the controls in ISO/IEC 27002 but also features seven new controls.

- **CLD.6.3.1:** Agreement on shared or divided responsibilities between the customer and provider around information security roles associated with cloud services have to be clearly laid out, recorded and communicated.
- **CLD.8.1.5:** Addresses how assets are returned or removed from the cloud when the contract/ agreement between the customer and provider is terminated.
- **CLD.9.5.1:** The provider has to protect and separate the customer's virtual environment from other customers and external parties.
- **CLD.9.5.2:** The customer and provider must ensure virtual machines are configured and hardened to meet the needs of the organization.
- **CLD.12.1.5:** The customer's responsibility to define, document and monitor the administrative operations and procedures associated with the cloud environment and the CSP's requirement to share documentation about critical operations and procedures as and when customers require it.
- **CLD.12.4.5:** How the capabilities of the provider enable the customer to monitor activity within a cloud computing environment.
- **CLD.13.1.4:** Consistent configurations should be made so that the virtual network environment is in line with the information security policy of the physical network.

BSI White Paper - https://www.bsigroup.com/Documents/iso-27017/resources/ISO-27017-overview.pdf

Protection of personally identifiable information (PII) in *public clouds* acting as PII processors



ISO/IEC 27018 Extended Control Set

A.1 Consent and choice	A.1.1 Obligation to cooperate regarding PII principals' rights	Privacy and Data Protection Policy
A.2 Purpose legitimacy and specification	A.2.1 Public cloud PII processor's purpose	Privacy and Data Protection Policy
	A.2.2 Public cloud PII processor's commercial use	Privacy and Data Protection Policy
A.3 Collection limitation	(None)	
A.4 Data minimization	A.4.1 Secure erasure of temporary files	Cloud Service Specifications
A.5 Use, retention and disclosure limitation	A.5.1 PII disclosure notification	Privacy and Data Protection Policy
	A.5.2 Recording of PII disclosures	Privacy and Data Protection Policy
A.6 Accuracy and quality	(None)	
A.7 Openness, transparency and notice	A.7.1 Disclosure of sub-contracted PII processing	Privacy and Data Protection Policy
A.8 Individual participation and access	(None)	
A.9 Accountability	A.9.1 Notification of a data breach involving PII	Incident Response Procedure
	A.9.2 Retention period for administrative security policies and guidelines	Records Retention and Protection Polocy
	A.9.3 PII return, transfer and disposal	Cloud Service Specifications
A.10 Information security	A.10.1 Confidentiality or non-disclosure agreements	Guidelines for Inclusion in Employment Contra
	A.10.2 Restriction of the creation of hardcopy material	Asset Handling Procedures
	A.10.3 Control and logging of data restoration	IT service support records (help desk)
	A.10.4 Protecting data on storage media leaving the premises	Physical Media Transfer Procedure
	A.10.5 Use of unencrypted portable storage media and devices	Procedure for the Management of Removable M
	A.10.6 Encryption of PII transmitted over public data-transmission networks	Cryptographic Policy

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment – What’s Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

Context of the Risk Assessment – AMS Products and Services – http://www.scramsystems.com

BETTER MATTERS

ELECTRONIC MONITORING SOLUTIONS

Better products. Better data. Better outcomes. That's the driving force behind our integrated suite of electronic monitoring technologies, mobile apps, and software.

Introducing SCRAM Nexus™
Better data. Better decisions. Better outcomes.

Drunk & Impaired Driving
1 Million DUI Arrests Each Year and Counting

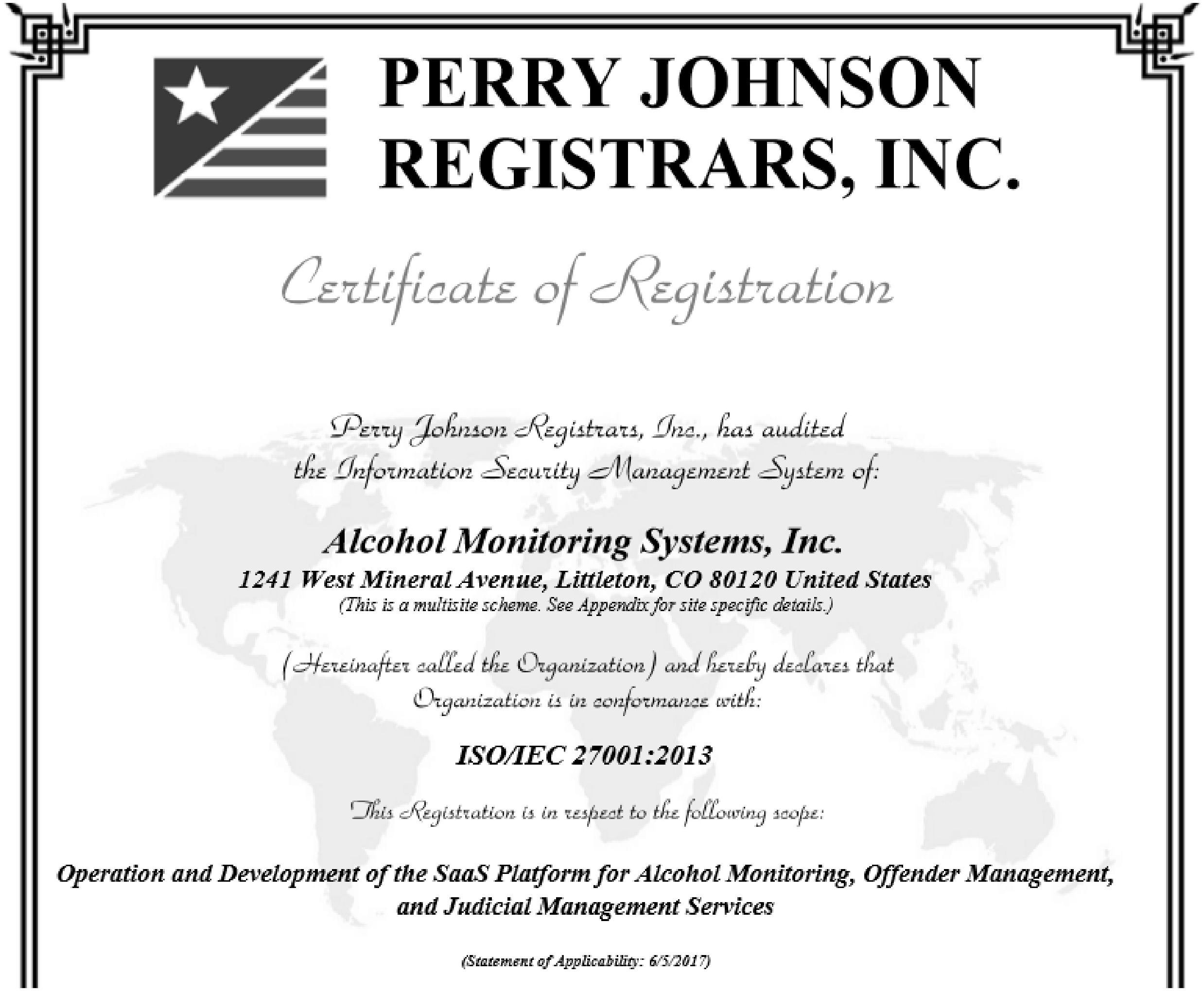
Make a Difference
Supporting individuals and communities

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 community cloud IaaS data center has been integrated into the ISO 27001 ISMS and will be certified later this year.

Context of the Risk Assessment – AMS Products and Services – http://www.scramsystems.com



PERRY JOHNSON
REGISTRARS, INC.

Certificate of Registration

Perry Johnson Registrars, Inc., has audited
the Information Security Management System of:

Alcohol Monitoring Systems, Inc.
1241 West Mineral Avenue, Littleton, CO 80120 United States
(This is a multisite scheme. See Appendix for site specific details.)

(Hereinafter called the Organization) and hereby declares that
Organization is in conformance with:

ISO/IEC 27001:2013

This Registration is in respect to the following scope:

Operation and Development of the SaaS Platform for Alcohol Monitoring, Offender Management, and Judicial Management Services

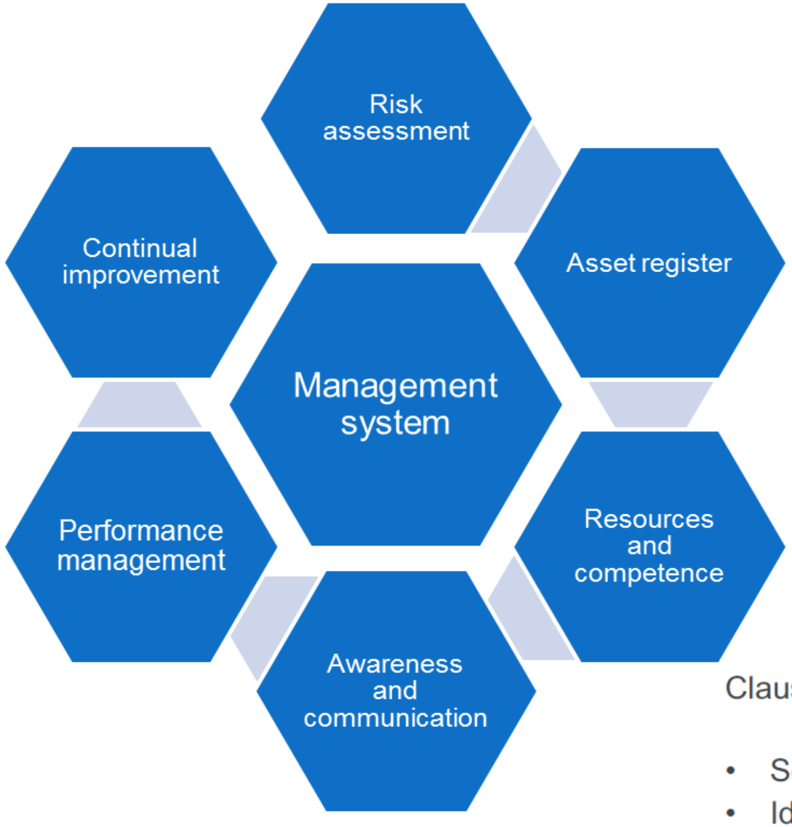
(Statement of Applicability: 6/5/2017)

After a thorough independent audit, SCRAM Systems has received ISO/IEC 27001:2013 ***certification for alcohol monitoring, offender management, and judicial management services in SCRAMnet, our Software as a Service (SaaS) program***. This confirms that SCRAM Systems has implemented internationally-recognized best practices and standards for its Information Security Management System (ISMS).

The certification complements the ISO 9001 certification for quality management systems (QMS) acquired previously.

ISO is an independent, international organization that develops standards to help businesses create and deliver quality products, services, and systems. The International Electrotechnical Commission (IEC) develops standards for information technology (IT) and information and communications technology (ICT).nt.

The ISO/IEC 27001 standard



Risk assessment

Asset register

Resources and competence

Awareness and communication

Performance management

Continual improvement

Management system

Clauses 4 through 10 deal with:

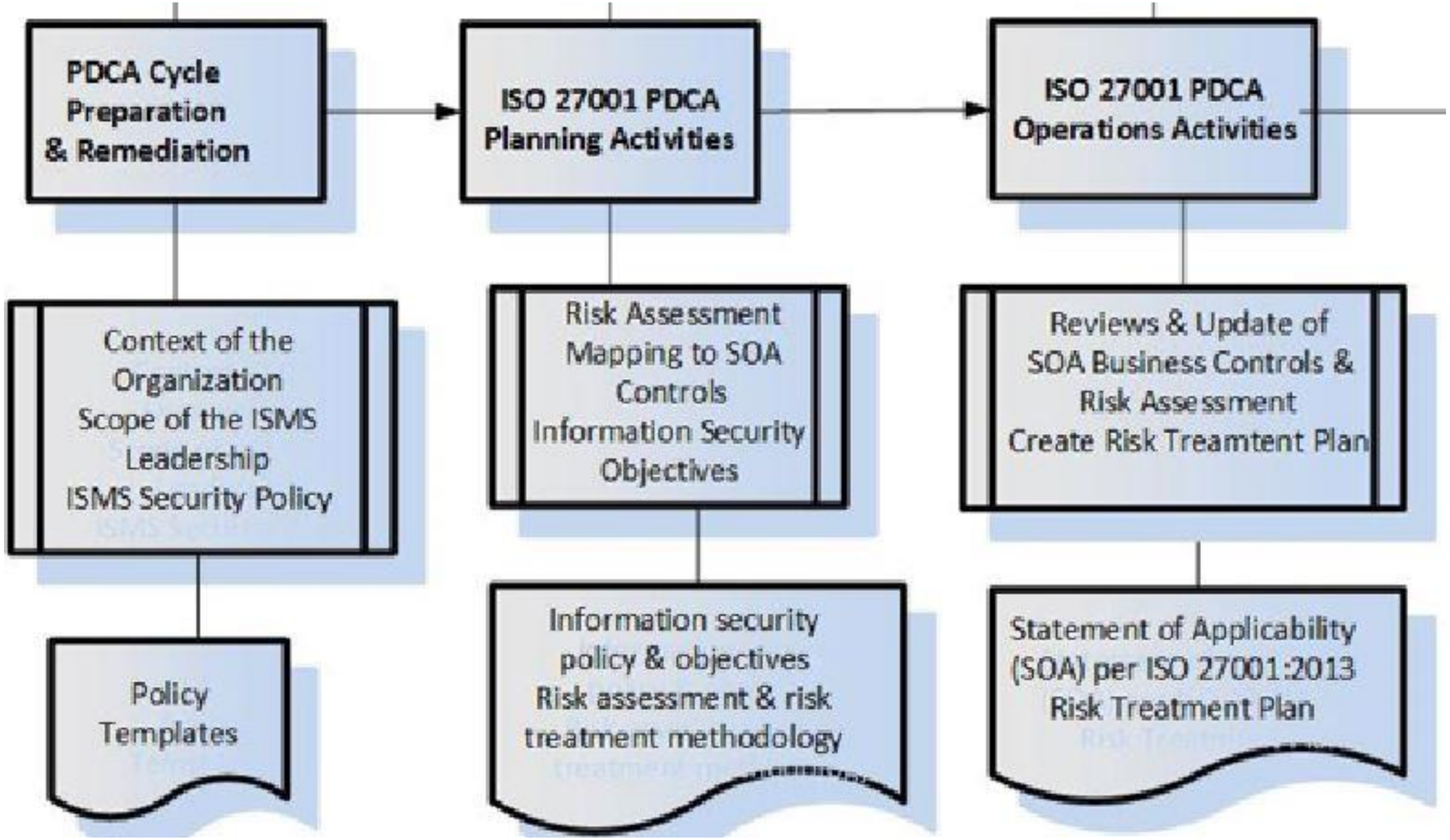
- Scoping of the ISMS
- Identifying and evaluating Risks
- Risk Treatment and mitigation
- Managing and measuring performance of the ISMS
- Tracking non-conformities and resolution
- Continuous improvement

Annex A deals with:
114 Optional controls for risk mitigation

ISO/IEC 27001 Controls

Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management
	Business continuity management	Compliance	

Risk Assessment Methods in the ISO 27001 Implementation (PDCA)



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

IEEE CLOUD COMPUTING

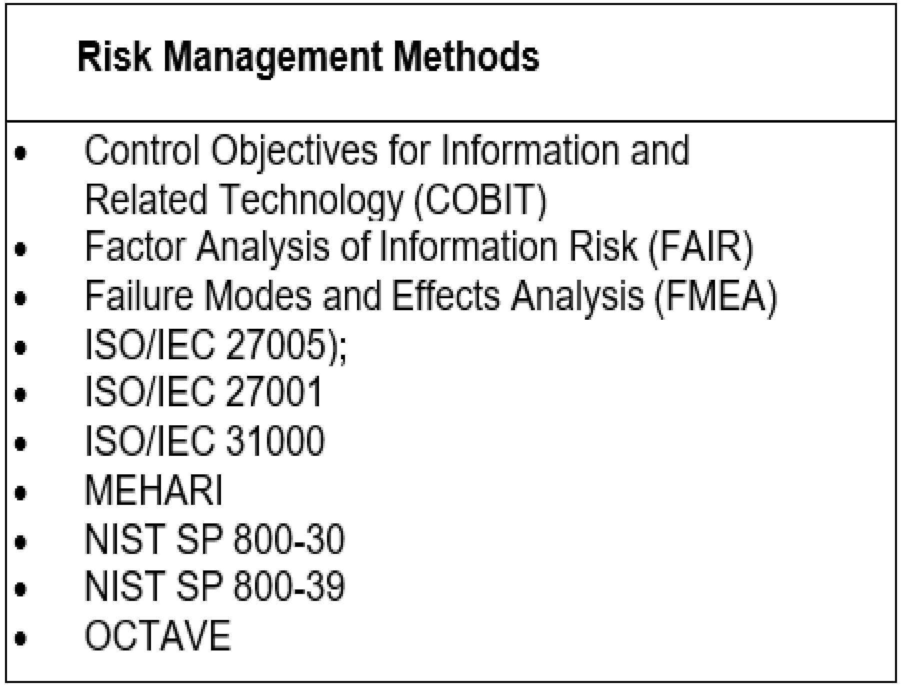
Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment – What's Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

A

Risk Assessments for Cloud Applications – where to get started?

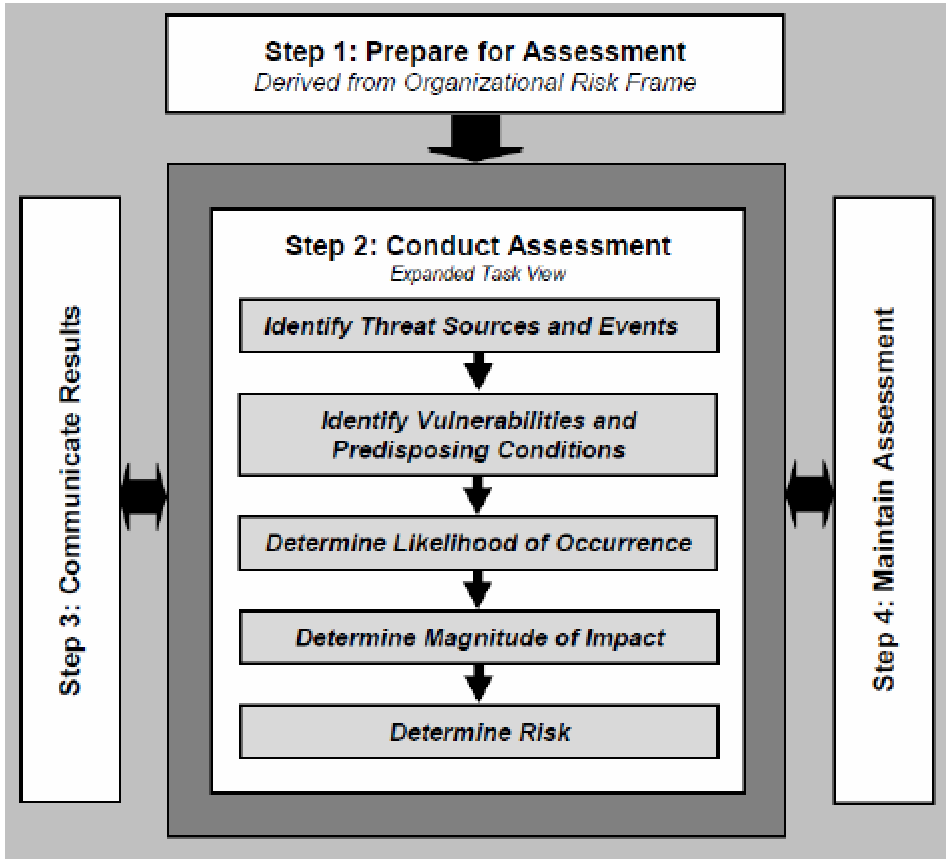
Compliance Specific Context – Commercial Control Frameworks (ISO 27001/27002,, PCI, NIST, NERC CIP). Governmental Compliance Standards (FISMA, FedRAMP, NIST, DFARS, CJIS, HIPAA)



Risk Management Methods

- Control Objectives for Information and Related Technology (COBIT)
- Factor Analysis of Information Risk (FAIR)
- Failure Modes and Effects Analysis (FMEA)
- ISO/IEC 27005);
- ISO/IEC 27001
- ISO/IEC 31000
- MEHARI
- NIST SP 800-30
- NIST SP 800-39
- OCTAVE

Ghazouani, Mohamed et. al. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. International Journal of Computer Applications. 103. 10.5120/18097-9155.



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

Determine Likelihood of Occurrence

Determine Magnitude of Impact

Determine Risk

Step 3: Communicate Results

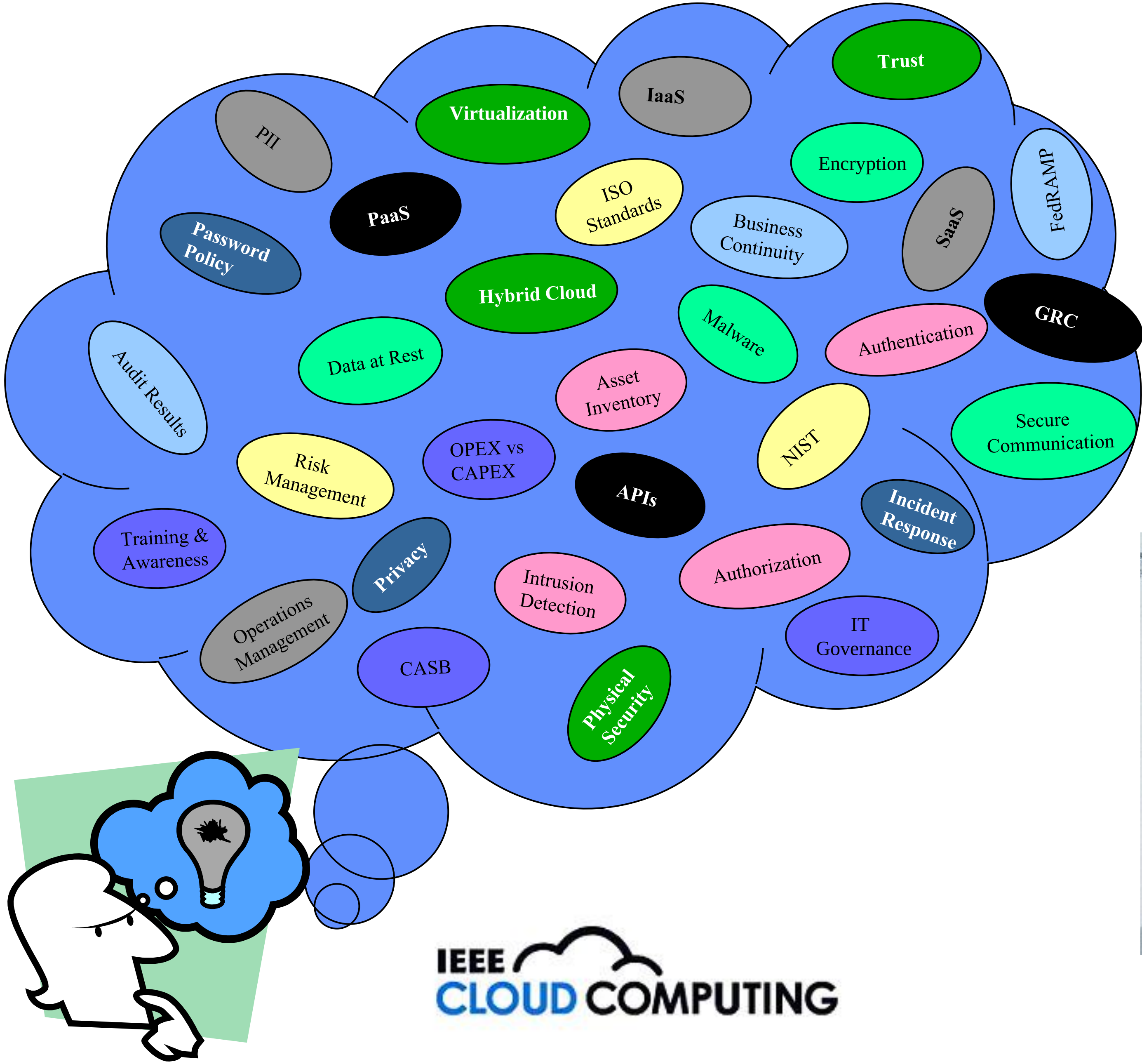
Step 4: Maintain Assessment

NIST SP 800-30 Risk Model

10/14/2020

IEEE CLOUD COMPUTING

Now What? (Lessons learn from Enterprise Risk Assessment of the National Science Foundation’s US Antarctic Program)



PII

Virtualization

IaaS

Trust

PaaS

ISO Standards

Encryption

Password Policy

Business Continuity

SaaS

FedRAMP

Hybrid Cloud

Malware

Audit Results

Data at Rest

Authentication

GRC

Asset Inventory

NIST

Secure Communication

Risk Management

OPEX vs CAPEX

APIs

Incident Response

Training & Awareness

Privacy

Intrusion Detection

Authorization

Operations Management

CASB

Physical Security

IT Governance

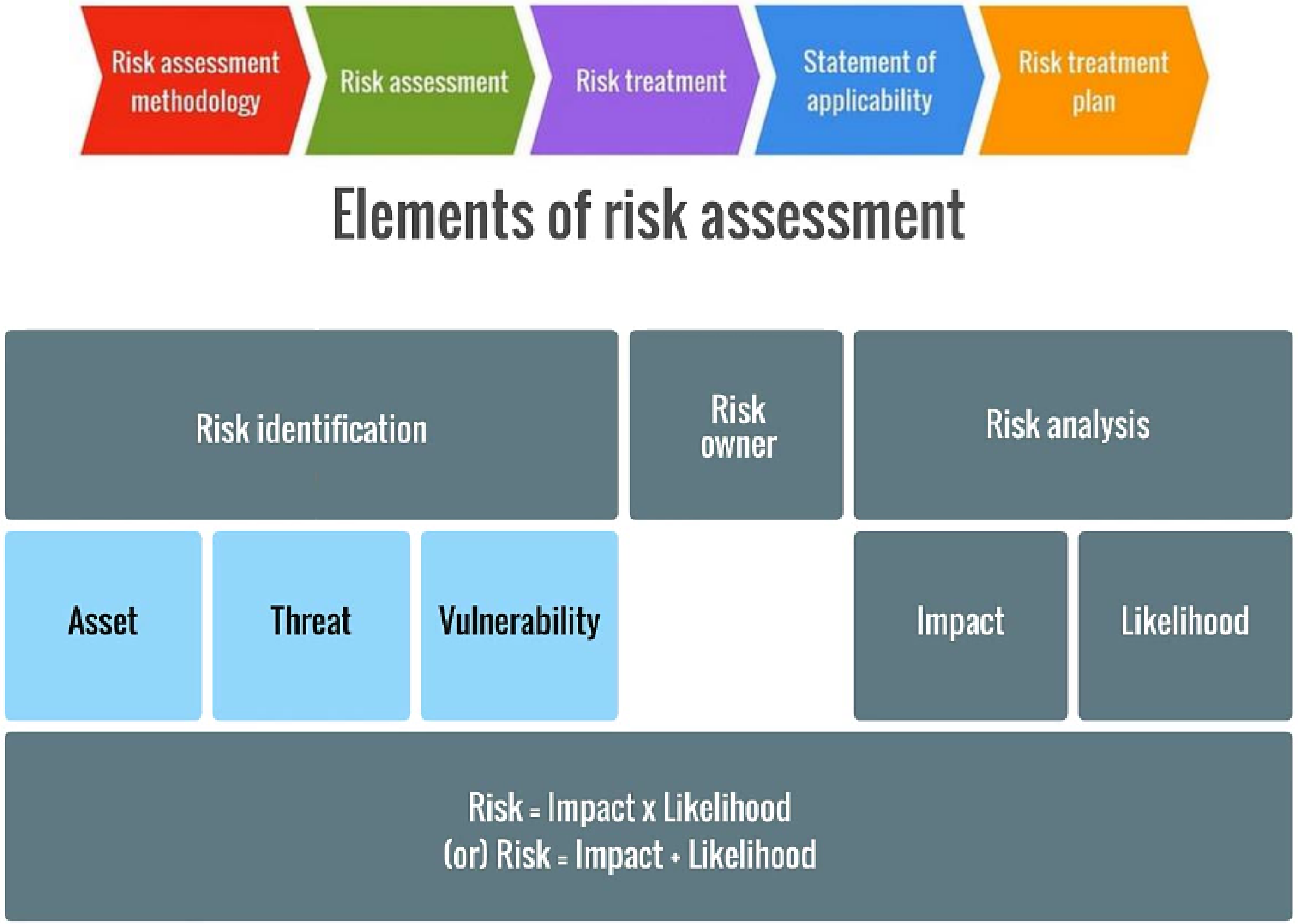
IT 101 – What Problems Are We Trying to Solve?

- Identify ‘Fix-It’ areas in the program
- Understand Current State (Remediation)
- Improve ‘ad hoc’, ‘not my problem’ state
- **Manage Information Security Risk**
- Improve Continuous Monitoring Process

IEEE CLOUD COMPUTING

10/14/2020

Risk Management Principles for ISO 27001 (IT Risk Foundation)



Risk assessment methodology → Risk assessment → Risk treatment → Statement of applicability → Risk treatment plan

Elements of risk assessment

Risk identification

- Asset
- Threat
- Vulnerability

Risk owner

Risk analysis

- Impact
- Likelihood

Risk = Impact x Likelihood
(or) Risk = Impact + Likelihood

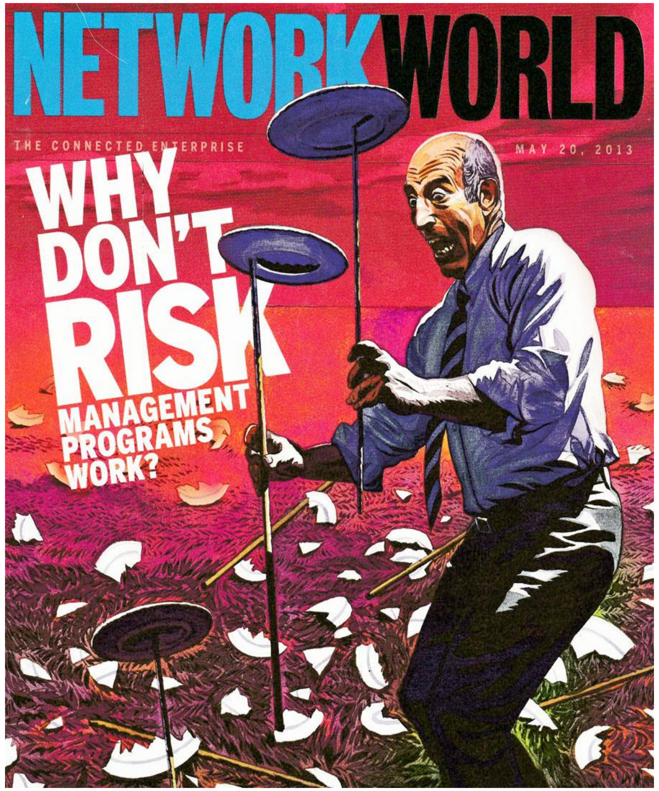
The Failure of Asset-Based Risk Assessments (Walt Williams) https://infosecuritymetrics.wordpress.com/

Most people don’t understand that asset management risk management models have been failing us for years, and we’re seeing the consequences of that failure in various laws and regulations. ***Assets are owned by an organization and have value. It makes sense to protect your assets, regardless of how you define what an asset is*****.**

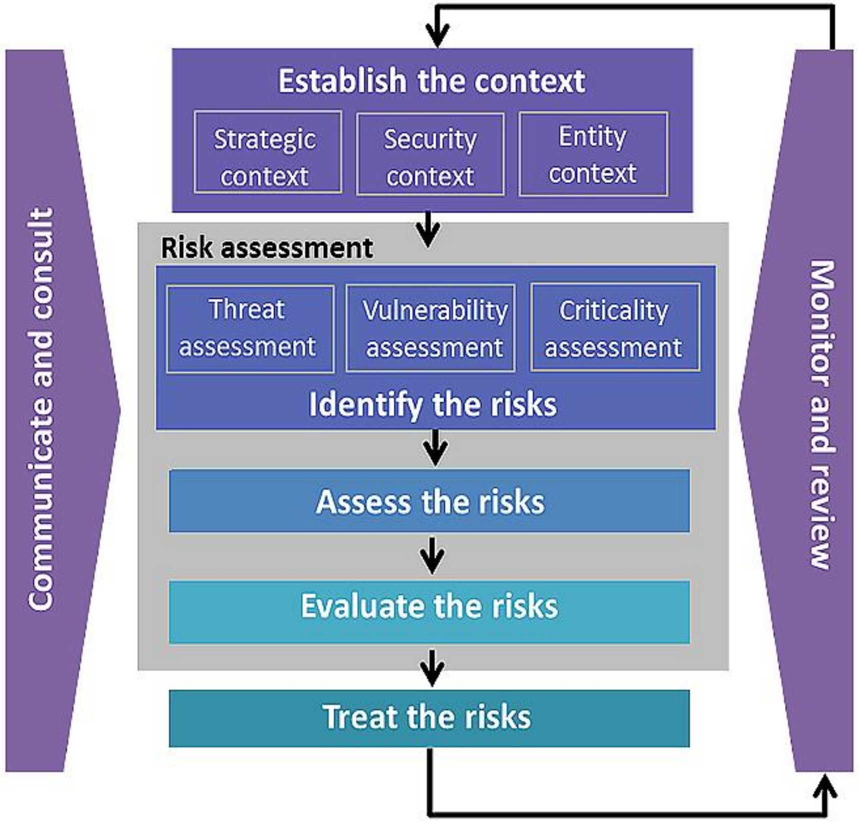
The GDPR, and other data privacy laws have been introduced over the last decade precisely because the ***data that is in scope for the data privacy laws is not an asset for any organization. It is an asset for various individuals. This information doesn’t bring the organization any value, and because of that, it is often not protected***.

Until the GDPR is enforced there is no incentive to protect name & email address. Organizations consider these data items to have no value. Individuals, on the other hand, expect that the value of the information is understood and properly protected by organizations that the data is entrusted to.

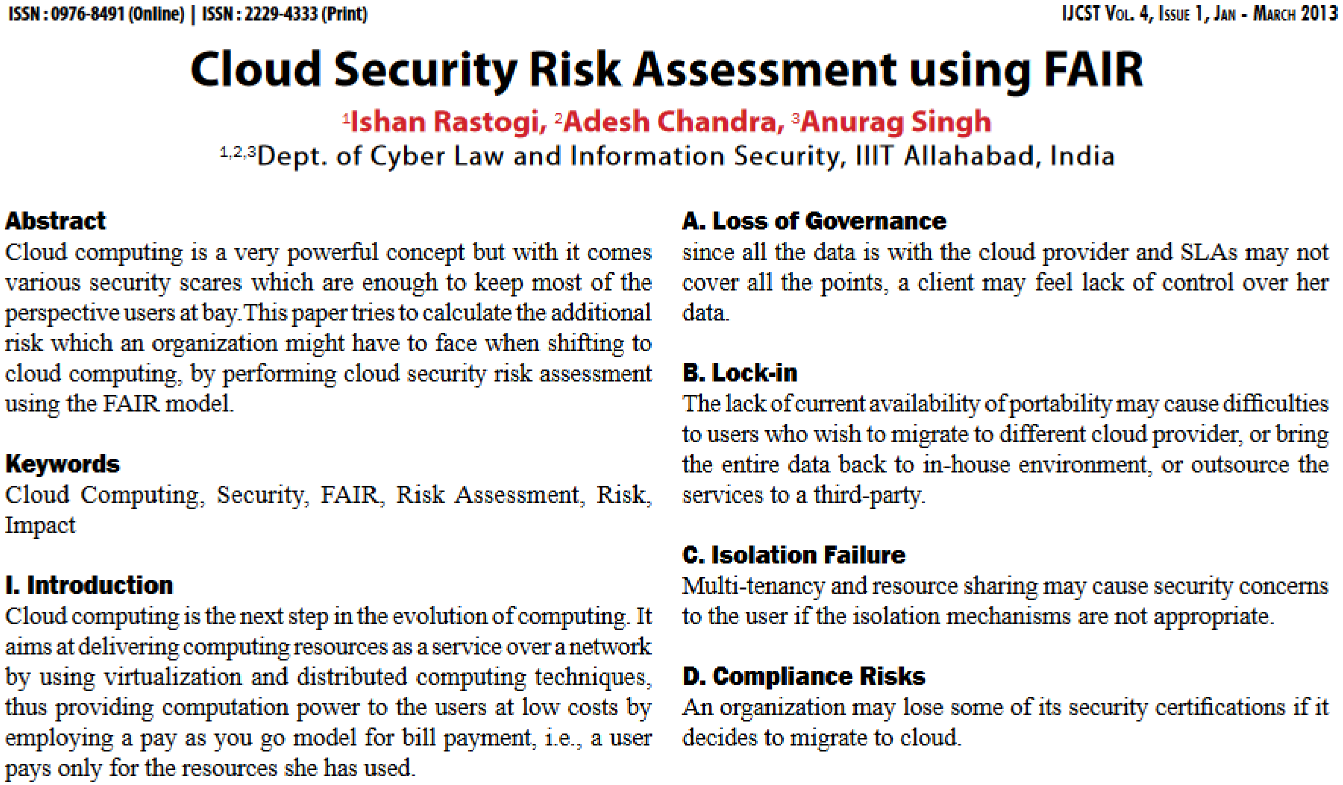
The data simply hasn’t been an asset to the organization, not worth protecting. Until organizations cease using an asset based approach to risk management, you will see governments stepping with impactful regulations because ***asset based risk management frameworks don’t lead to organizations protecting all the data. Just the data that drives business value. And this is why we fail***.



Risk Assessments for Cloud Applications – where to get started?



ISO 27005 Information Security Risk Management Process


ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) IJCST Vol. 4, Issue 1, Jan - March 2013

Cloud Security Risk Assessment using FAIR

[1]Ishan Rastogi, [2]Adesh Chandra, [3]Anurag Singh
[1,2,3]Dept. of Cyber Law and Information Security, IIIT Allahabad, India

Abstract

Cloud computing is a very powerful concept but with it comes various security scares which are enough to keep most of the perspective users at bay. This paper tries to calculate the additional risk which an organization might have to face when shifting to cloud computing, by performing cloud security risk assessment using the FAIR model.

Keywords

Cloud Computing, Security, FAIR, Risk Assessment, Risk, Impact

I. Introduction

Cloud computing is the next step in the evolution of computing. It aims at delivering computing resources as a service over a network by using virtualization and distributed computing techniques, thus providing computation power to the users at low costs by employing a pay as you go model for bill payment, i.e., a user pays only for the resources she has used.

A. Loss of Governance

since all the data is with the cloud provider and SLAs may not cover all the points, a client may feel lack of control over her data.

B. Lock-in

The lack of current availability of portability may cause difficulties to users who wish to migrate to different cloud provider, or bring the entire data back to in-house environment, or outsource the services to a third-party.

C. Isolation Failure

Multi-tenancy and resource sharing may cause security concerns to the user if the isolation mechanisms are not appropriate.

D. Compliance Risks

An organization may lose some of its security certifications if it decides to migrate to cloud.

FAIR – Factor Analysis of Information Risk. The **Open FAIR Cookbook** uses ISO/IEC 27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results.

Online available - https://publications.opengroup.org/c103

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment - What's Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

Risk Assessment Methodologies for Cloud Computing - Examples

With regards to cloud risk assessments, these papers

addressed five key questions relating to cloud security risk management ***whilst reiterating eight distinguishing characteristics of cloud computing***,

presented ***some ISO 27001 information security management system (ISMS) based risk assessment use cases for various cloud computing deployment models and the three common cloud computing service models***,

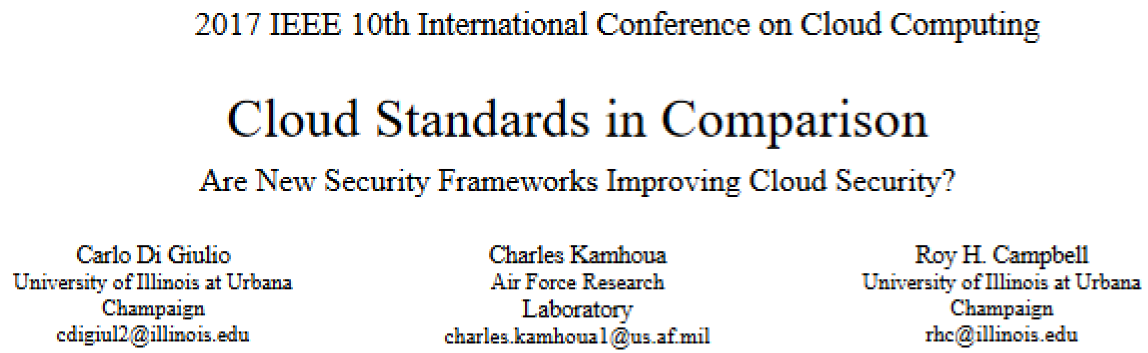
presented a ***conceptual cloud attack and risk assessment taxonomy for assessing security risks and threats for cloud computing deployment models and cloud computing service models***,

presented a ***new asset based quantitative cloud risk assessment methodology***, which assesses for each asset, their vulnerabilities and threats and calculates the specific risks associated with each asset

presented a ***Bayesian network based security risk assessment methodology*** for assessing and prioritizing cloud computing security risks and used an existing scenario to illustrate their methodology.

Cybersecurity Threat Modelling: A Case Study of An Ecommerce Platform Migration to the Public Cloud -
EJECE, European Journal of Electrical Engineering and Computer Science Vol. 4, No. 4, August 2020

Risk Assessment Methodologies for Cloud Computing



2017 IEEE 10th International Conference on Cloud Computing

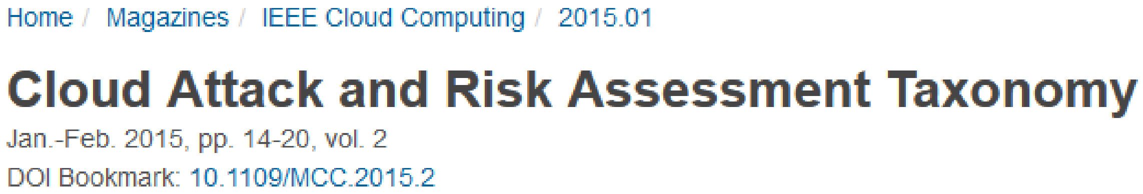
Cloud Standards in Comparison

Are New Security Frameworks Improving Cloud Security?

Carlo Di Giulio
University of Illinois at Urbana Champaign
cdigiul2@illinois.edu

Charles Kamhoua
Air Force Research Laboratory
charles.kamhoua1@us.af.mil

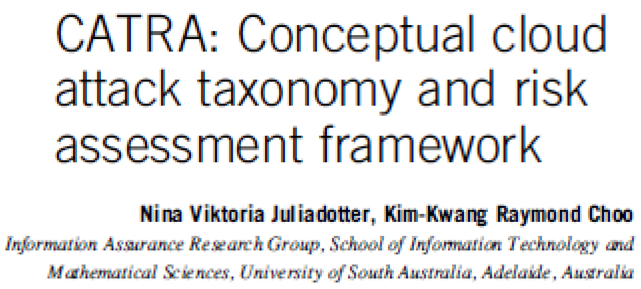
Roy H. Campbell
University of Illinois at Urbana Champaign
rhc@illinois.edu



Home / Magazines / IEEE Cloud Computing / 2015.01

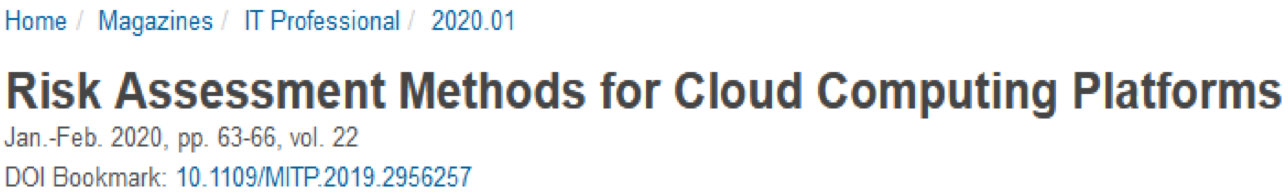
Cloud Attack and Risk Assessment Taxonomy

Jan.-Feb. 2015, pp. 14-20, vol. 2
DOI Bookmark: 10.1109/MCC.2015.2



CATRA: Conceptual cloud attack taxonomy and risk assessment framework

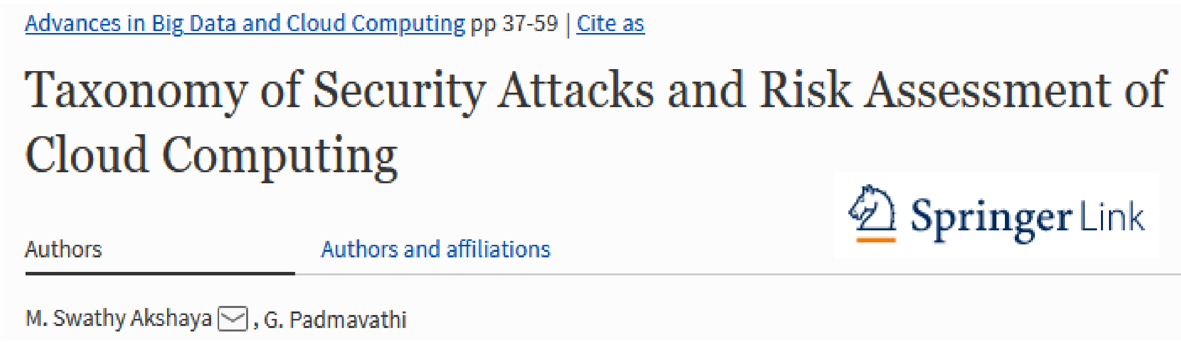
Nina Viktoria Juliadotter, Kim-Kwang Raymond Choo
Information Assurance Research Group, School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia



Home / Magazines / IT Professional / 2020.01

Risk Assessment Methods for Cloud Computing Platforms

Jan.-Feb. 2020, pp. 63-66, vol. 22
DOI Bookmark: 10.1109/MITP.2019.2956257



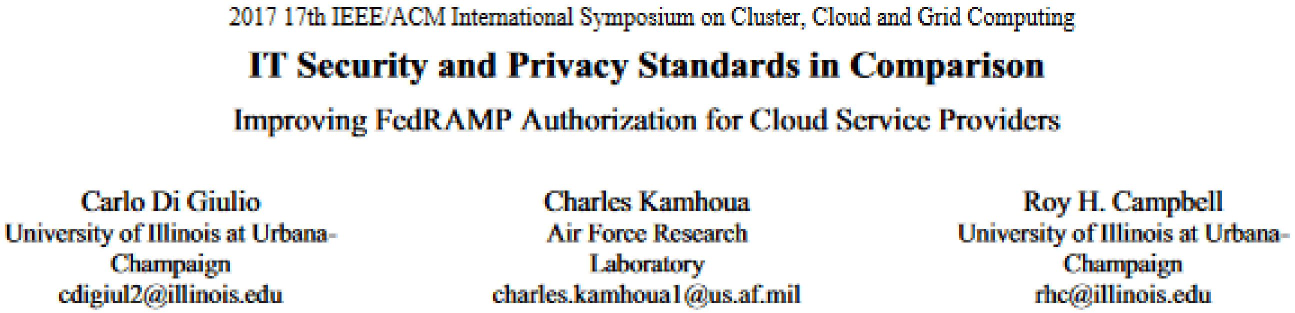
Advances in Big Data and Cloud Computing pp 37-59 | Cite as

Taxonomy of Security Attacks and Risk Assessment of Cloud Computing

Springer Link

Authors Authors and affiliations

M. Swathy Akshaya ✉, G. Padmavathi



2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

IT Security and Privacy Standards in Comparison

Improving FedRAMP Authorization for Cloud Service Providers

Carlo Di Giulio
University of Illinois at Urbana-Champaign
cdigiul2@illinois.edu

Charles Kamhoua
Air Force Research Laboratory
charles.kamhoua1@us.af.mil

Roy H. Campbell
University of Illinois at Urbana-Champaign
rhc@illinois.edu

IEEE CLOUD COMPUTING

Context for Cloud Risk Assessments (1 or 2)

Standards based Risk Assessment methods
Asset-based vs Process-based vs Hybrid RA approach
Data-based Privacy Protection (Consumer Protection)
Quantitative vs qualitative RA methodology

Risk Management and Cybersecurity Maturity Model
Both the NIST Cybersecurity Framework (CSF) and the Carnegie Mellon University Cybersecurity Maturity Model are examples of scaling the cloud risk assessment.

NIST Risk Management Framework for Cloud (RMF4CE) –

"In general, risk management activities can be grouped as:
- Organization level (tier 1)
- Mission and business process level (tier 2)
- Information systems level (tier 3)

Business Driver
Legislative, Regulatory and Compliance
International Markets
Competitive differentiator

Stakeholder Identification (Interested Parties)
Customers, Employees
Information Security Forum (ISO 27001 ISMS)
Third party auditor and client requests

Similar to traditional risk management methods, cloud-based ecosystem risk management must also concentrate on ***quantifying the acceptable residual risk after applying the minimum viable security controls***

Context for Cloud Risk Assessments (2 or 2)

Decision Support Communication

Information Security and Privacy budgets
Training and awareness of Cloud Risk Practices
Contract fulfillment
Board level information security briefing

Context of the Cloud (multi-cloud) Risk Assessment

Scoping the ISMS (ISO 27001)
Scoping the cloud - Anything as a Service (XaaS)
Data localization (in-country privacy protection)
Cloud Prosumer versus Provider responsibilities

Multi-use Compliance Requirements

Cloud Risk Assessment and Treatment Reports
Applicable control frameworks (industry, best practices)
Applicable international control frameworks

Cloud Risk Assessment Taxonomy – Control Models

Commonly used cloud security control frameworks include – Center for Internet Security (CIS), Cloud Security Alliance (Cloud Control Matrix), ISO 27017, Risk Management Framework for Cloud Environments (NIST RMF4CE), FedRAMP

Metrics and performance criteria

Boardroom Key Performance Indicators (KPI)
ISMS monitoring (confidentiality, integrity, availability)

National and International Cloud Security Standards

National Cloud Security Standard	Organization
FedRAMP (US)	Federal Risk Assessment Management Program
G-Cloud (UK)	UK National Cybersecurity Center
Cyber Security Centre (AU)	Australia Cybersecurity Cloud Security Guidance
Cloud Computing Risk and Assurance Framework (NZ)	Protective Security Policy Framework (Cloud Risk)
MTSC (SS)	Singapore Multi-Tier Cloud Security
C5 (GE)	Cloud Computing Compliance Controls Catalogue
International Cloud Security Standard	**Organization**
CSA CCM 2019	Cloud Security Alliance Cloud Control Matrix
ENISA Cloud Risk Assessment (2009)	European Union Agency for Cybersecurity
ISO 27017:2015 Cloud Security Controls	International Standards Organization

NIST Risk Management Framework for Cloud

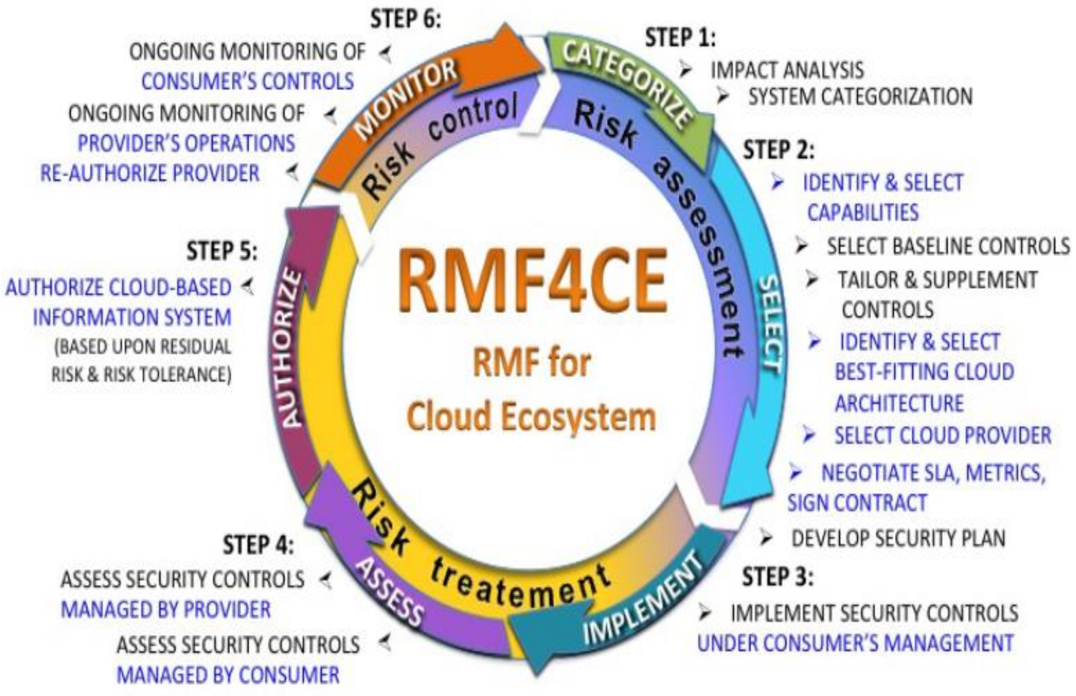
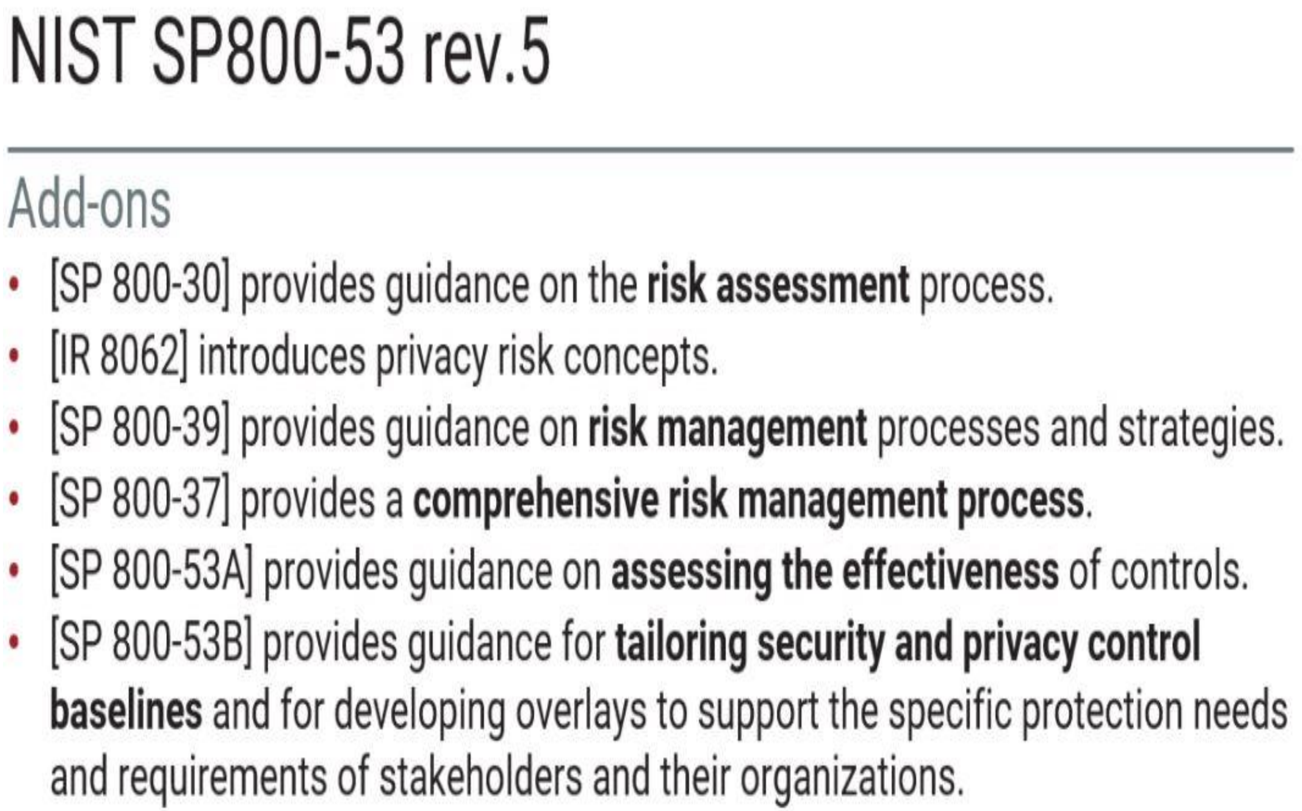

STEP 6:
ONGOING MONITORING OF CONSUMER'S CONTROLS
ONGOING MONITORING OF PROVIDER'S OPERATIONS
RE-AUTHORIZE PROVIDER
STEP 1:
IMPACT ANALYSIS
SYSTEM CATEGORIZATION
STEP 2:
IDENTIFY & SELECT CAPABILITIES
SELECT BASELINE CONTROLS
TAILOR & SUPPLEMENT CONTROLS
IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
SELECT CLOUD PROVIDER
NEGOTIATE SLA, METRICS, SIGN CONTRACT
DEVELOP SECURITY PLAN
STEP 3:
IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT
STEP 4:
ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
ASSESS SECURITY CONTROLS MANAGED BY CONSUMER
STEP 5:
AUTHORIZE CLOUD-BASED INFORMATION SYSTEM
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)
MONITOR
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
Risk control
Risk assessment
Risk treatement
RMF4CE
RMF for Cloud Ecosystem

Figure 3: Cloud Consumers' View of the Risk Management Framework Applied to a Cloud Ecosystem

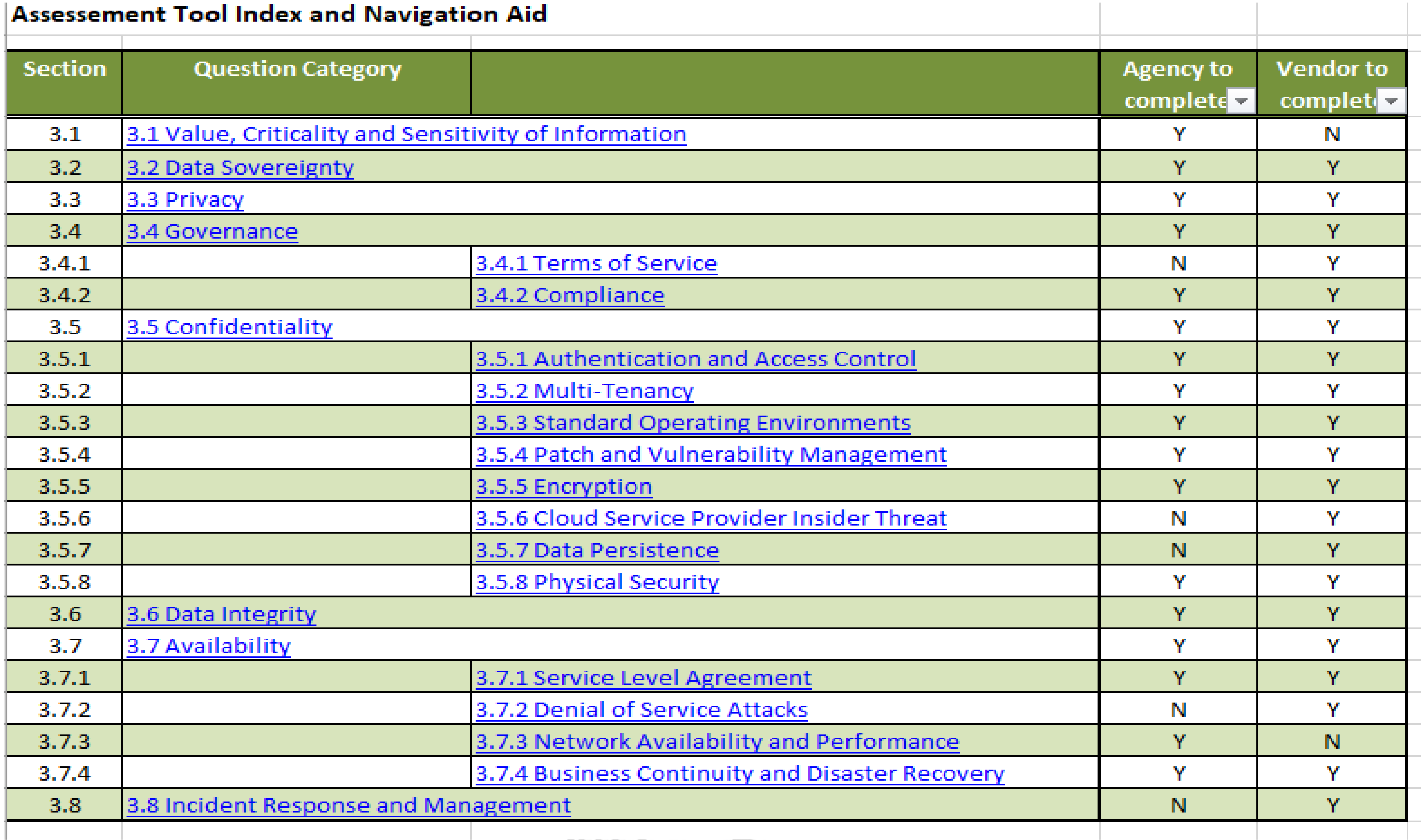


NIST SP800-53 rev.5

Add-ons

- [SP 800-30] provides guidance on the **risk assessment** process.
- [IR 8062] introduces privacy risk concepts.
- [SP 800-39] provides guidance on **risk management** processes and strategies.
- [SP 800-37] provides a **comprehensive risk management process**.
- [SP 800-53A] provides guidance on **assessing the effectiveness** of controls.
- [SP 800-53B] provides guidance for **tailoring security and privacy control baselines** and for developing overlays to support the specific protection needs and requirements of stakeholders and their organizations.

New Zealand National Cloud Security Risk Assessment – Example



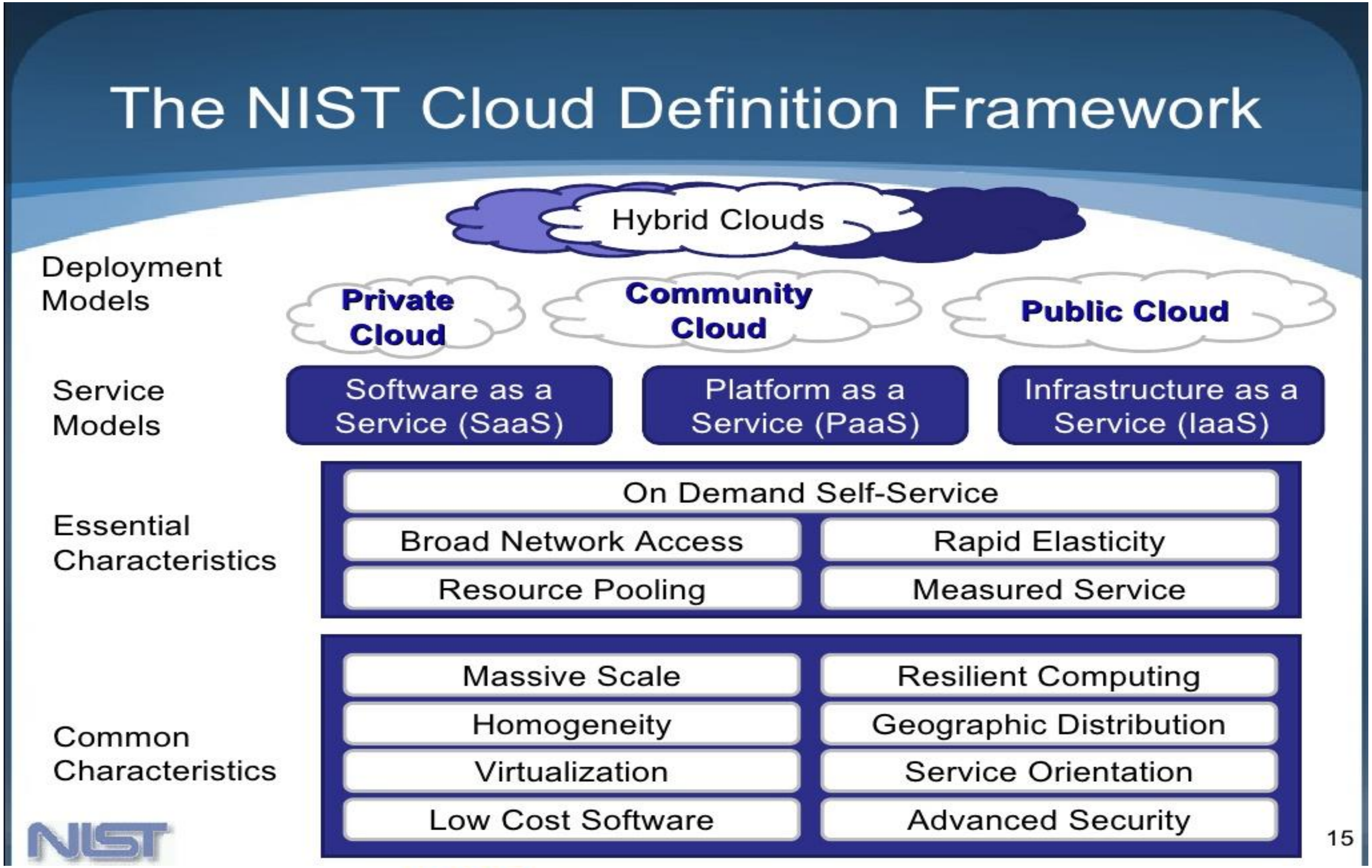
Assessement Tool Index and Navigation Aid

Section	Question Category		Agency to complete	Vendor to complet
3.1	3.1 Value, Criticality and Sensitivity of Information		Y	N
3.2	3.2 Data Sovereignty		Y	Y
3.3	3.3 Privacy		Y	Y
3.4	3.4 Governance		Y	Y
3.4.1		3.4.1 Terms of Service	N	Y
3.4.2		3.4.2 Compliance	Y	Y
3.5	3.5 Confidentiality		Y	Y
3.5.1		3.5.1 Authentication and Access Control	Y	Y
3.5.2		3.5.2 Multi-Tenancy	Y	Y
3.5.3		3.5.3 Standard Operating Environments	Y	Y
3.5.4		3.5.4 Patch and Vulnerability Management	Y	Y
3.5.5		3.5.5 Encryption	Y	Y
3.5.6		3.5.6 Cloud Service Provider Insider Threat	N	Y
3.5.7		3.5.7 Data Persistence	N	Y
3.5.8		3.5.8 Physical Security	Y	Y
3.6	3.6 Data Integrity		Y	Y
3.7	3.7 Availability		Y	Y
3.7.1		3.7.1 Service Level Agreement	Y	Y
3.7.2		3.7.2 Denial of Service Attacks	N	Y
3.7.3		3.7.3 Network Availability and Performance	Y	N
3.7.4		3.7.4 Business Continuity and Disaster Recovery	Y	Y
3.8	3.8 Incident Response and Management		N	Y

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment - What's Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

NIST Cloud Computing Reference Model



The NIST Cloud Definition Framework

Hybrid Clouds

Deployment Models: Private Cloud; Community Cloud; Public Cloud

Service Models: Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS)

Essential Characteristics:

- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

Common Characteristics:

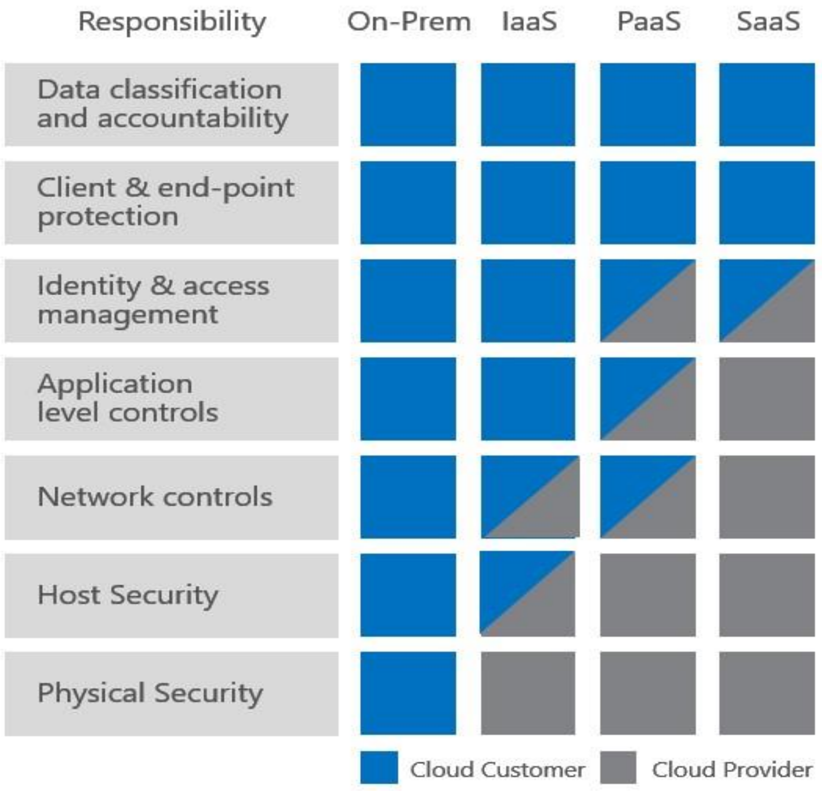
- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

13 Effective Security Controls for ISO 27001 Compliance
When using Microsoft Azure

Key principles and recommendations for secure development & operations

1. Enable identity and authentication solutions
2. Use appropriate access controls
3. Use an industry-recommended, enterprise-wide antimalware solution
4. Effective certificate acquisition and management
5. Encrypt all customer data
6. Penetration testing
7. Threat modeling services and applications
8. Log security events, implement monitoring and visualization capabilities
9. Determine the root cause of incidents
10. Train all staff in cyber security
11. Patch all systems and ensure security updates are deployed
12. Keep service and server inventory current and up-to-date
13. Maintain clear server configuration with security in mind

Cloud Security Shared Responsibilities



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	◩	⬛
Host Security	🟦	◩	⬛	⬛
Physical Security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

The three primary cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Azure Assessment Checklist

- Database Services
- SQL Server Database
- MongoDB (NoSQL Database)
- Personal Identifiable Information (PII)
- Access Control and Identity Management
- Privileged User Accounts
- Azure Services
- App Services
- WebApp
- WebApi
- Content Delivery Network (CDN)
- Azure Infrastructure Services
- Storage
- Service Bus Messaging
- Traffic Manager
- Application Insights
- Visual Studio Team Services (Deploy Software to Azure)
- Azure Deployment Groups (Compliance Platform)
- Kudu (Git Deployments to Azure Services)

- Azure App Service Deployment
- VSTS to Azure Deployment (Compliance Platform)
- Risk Assessment and Treatment Process
- Appendix – Network Diagrams
- Appendix – Functional Services
- Appendix - High Level Asset Description (by Departments)
- High Level Asset Description – Network Development (NetDev)
- High Level Asset Description – Network Operations (NetOps)
- High Level Asset Description – Customer Service
- Probation Decision Services Application Subsystems
- Appendix –Core Services Functional Services
- Middleware Functional Services and component subsystems
- Middleware URLs and Software Components
- Core Services Inventory (Data Center Assets)
- Appendix – Privacy Policy (Cloud Apps)

Expanding ISO 27001 With a Cloud Risk Assessment

Applications	Cloud Deployment	Target Domain	Risk Assessment Approach
Alcohol Monitoring	Hybrid Cloud - SaaS	Corrections Industry	ISO 27005 - Scenario Based RA
Offender Management	Hybrid Cloud - SaaS	Corrections Industry	ISO 27005 - Scenario Based RA National Self-Assessment
Judicial Management Services	Hybrid Cloud - SaaS	State Government	ISO 27005 - Scenario Based RA
Interface Services	Public Cloud - SaaS	All Sectors	ISO 27005 - Scenario Based RA
International Data Center	Community Cloud - IaaS	International Corrections Industry	ISO 27005 - Asset Based RA
Offender Management	Public Cloud - SaaS	International Government Corrections Industry	ISO 27005 - Asset Based RA National Self-Assessment

Use Cases For Cloud Risk Assessment (1 if 2)

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.

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

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.

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.

Use Cases For Cloud Risk Assessment (2 of 2)

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.”

.

Community 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

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

Summary Cloud Risk Findings and Mitigations

Risk Summary	Risk Description	Proposed control	Annex A / ISO 27017-18 Reference
Data in transit protection	The integrity of the data may be compromised while in transit.	User data transiting networks is adequately protected against tampering and eavesdropping by (SSL, TLS, VPN)	A.10.1 Cryptographic controls
Asset protection and resilience	Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.	User data, and the assets storing or processing it, shall be protected against physical tampering, loss, damage or seizure. ISO 27018 (PII Protection in the Cloud)	A.8.1.1 Inventory of Assets (PII) A.8.2.1 Classification of Information (PII) A.8.2.2 Labelling of Information (PII)
Separation between users	Service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	A malicious or compromised user of the service shall not be able to affect the service or data of another.	CLD.9.5.1 Segregation in Virtual Environments - Multi-tenancy protection
Governance framework	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.	ISO 27017 (Cloud Security) and ISO 27018 (PII Protection in the Cloud) are recommended for adoption. The service provider shall have a security governance framework which coordinates and directs its management of the service and information within it.	A.5 Information security policies
Operational security	The service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security shall not require complex, bureaucratic, time consuming or expensive processes.	CLD.12.1.5 Administrator's Operational Security CLD.12.4.5 Monitoring of Cloud Services
Supply chain security	It is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	The service provider shall ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.	A.15 Supplier relationships
Secure user management	Unauthorised people may be able to access and alter consumers' resources, applications and data.	Your provider shall make the tools available for you to securely manage your use of their service.	A.9 Access control
Identity and authentication	Unauthorized changes to a consumer's service, theft or modification of data, or denial of service may occur.	All access to service interfaces shall be constrained to authenticated and authorized individuals.	CLD.12.1.5 Administrator's Operational Security

Summary Cloud Risk Scoring (Pre-Treatment)

Risk Summary	Risk Description	Risk Type	Risk Owner	Existing Controls	Likelihood	Impact	Risk Score	Risk Level
Data in transit protection	The integrity or confidentiality of the data may be compromised while in transit.	Confidentiality	NetOps, NetDev	User data transiting networks is adequately protected against tampering and eavesdropping by (SSL, TLS, VPN)	2	3	6	**MEDIUM**
Asset protection and resilience	Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.	Integrity	NetOps, NetDev	Access controls for MongoDB and SQL Server PII data in Azure	4	4	16	**HIGH**
Separation between users	Service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	Confidentiality	NetOps, NetDev	Microsoft Azure Risk Assessment Diagnostic tool	2	3	6	**MEDIUM**
Governance framework	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.	Integrity	NetOps, NetDev	ISO 27001 ISMS for Cloud Applications	4	3	12	**HIGH**
Operational security	The service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	Integrity	NetOps, NetDev	Application Insights (Azure) is used for cloud monitoring in development	4	4	16	**HIGH**
Supply chain security	It is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	Availability	NetOps, NetDev	Contract with Microsoft Azure services Microsoft Azure Risk Assessment Diagnostic tool	3	2	6	**MEDIUM**
Secure user management	Unauthorised people may be able to access and alter consumers' resources, applications and data.	Confidentiality	NetOps, NetDev	Microsoft Azure Risk Assessment Diagnostic tool	3	2	6	**MEDIUM**

Assessing Security and Privacy in the Cloud – Blue Sky or Rain?

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Taking Compliance to the Cloud
- Risk Assessment Methods for Cloud Applications
- Standards for Cloud Risk Assessment - What's Missing?
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

References – Standards for Cloud Risk Assessment – What’s Missing?

- 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.
- 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
- 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.
- Raymond Choo, "Cloud Attack and Risk Assessment Taxonomy”, in IEEE Cloud Computing, vol. 2, no. 1, pp. 14-20, Jan-Feb. 2015.
- G. Wangen, "Information Security Risk Assessment: A Method Comparison," in Computer, vol. 50, no. 4, pp. 52-61, April 2017.
- 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.
- Soft Layer ISO 27001 certifcation, online available https:///www.softlayer.com/SoftLayer4/pdfs/SoftLayer_ISO_Certificate.pdf
- New Zealand National Cloud Security Risk Assessment, online available-NZ ICT Portal - https://www.ict.govt.nz/guidance-andresources/ using-cloud-services/assess-the-risks-of-cloud-services/
- 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

References Used in This Presentation

- European Union Agency for Network & Information Security (ENISA) Cloud Security Guidelines - https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

- Cloud Security Alliance – The Dirty Dozen: 12 top cloud security threats (2018)
  https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html
  https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

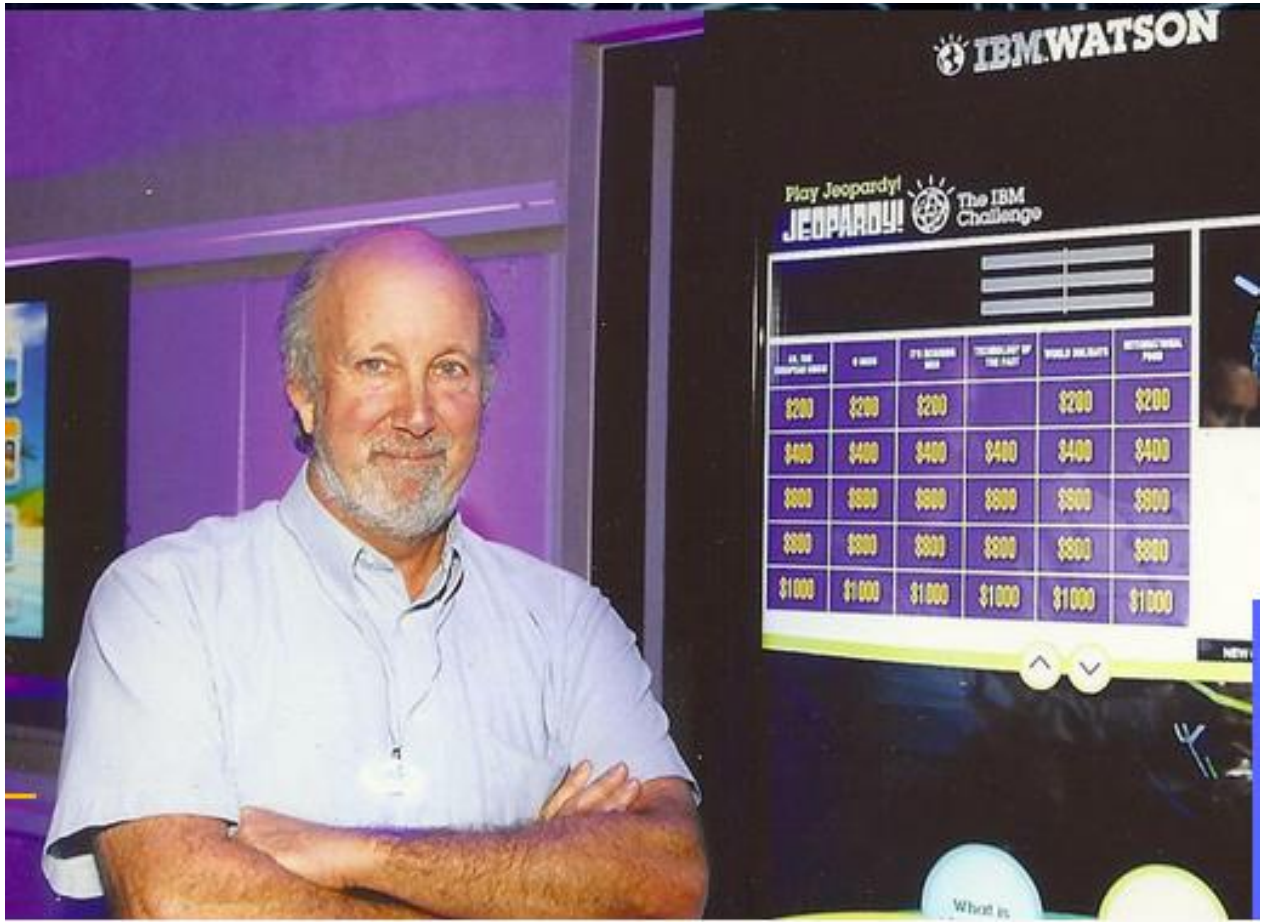
- Why Don’t Risk Management Programs Work (Network World 5/20/13) – RSA Panel Discussion – https://www.networkworld.com/article/2165934/software/why-don-t-risk-management-programs-work---.html

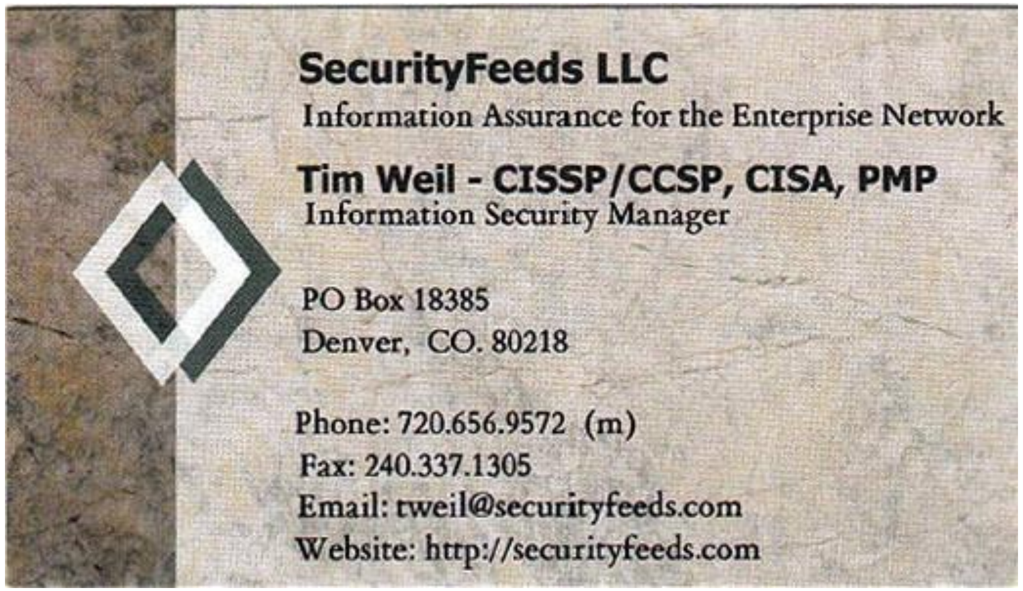
- 13 Effective Security Controls for ISO 27001 Compliance (Microsoft Azure White Paper)
  https://www.microsoft.com/en-us/download/details.aspx?id=50742

- Implementing the Cloud Security Principles (NCSC)
  https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

- Cloud Risk Assessment Using FAIR (Rastogi, Chandra, Singh) - Online available - http://ijcst.com/vol41/1/adesh.pdf

Thank you for joining us!





SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Information Security Manager

PO Box 18385
Denver, CO. 80218

Phone: 720.656.9572 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com
trweil@ieee.org