Tools and Techniques Using ISO Standards

Risk Assessment Methods for Cloud Computing Platforms

Tim Weil – CISSP/CCSP, CISA, PMP
Audit and Compliance Manager
Alcohol Monitoring Systems (AMS)

IEEE Communications Society (Denver Chapter)
http://comsoc.ieee-Denver.org

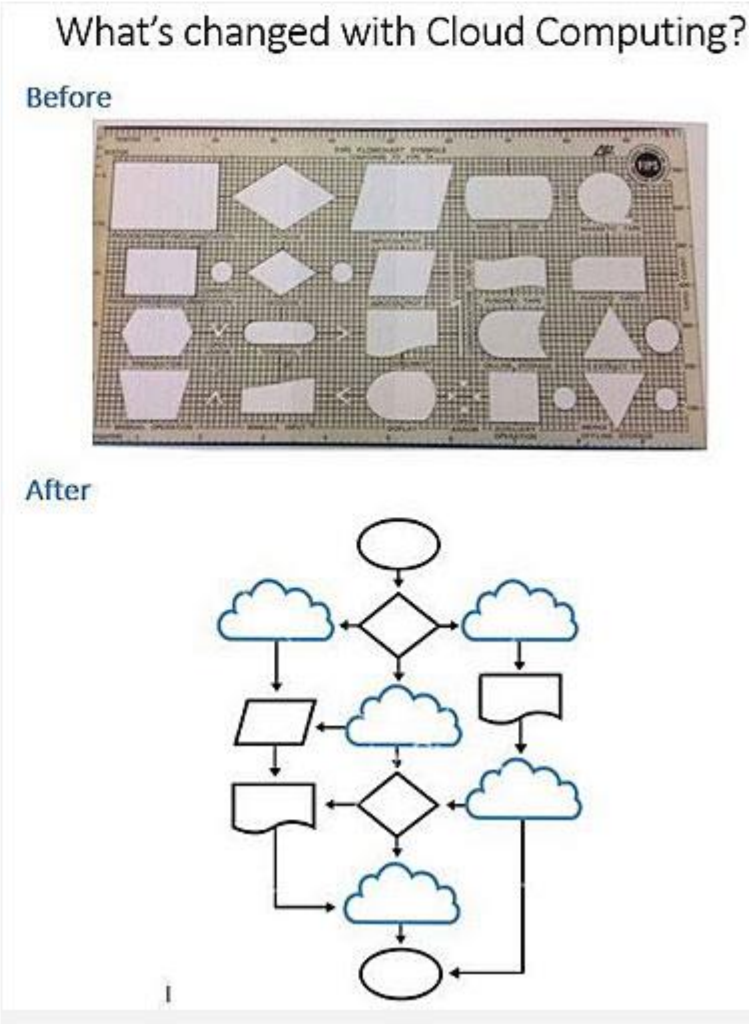
Dine and Learn
Westminser, CO 10Sept19

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
- ISO Standards for Cloud Security and Privacy
- 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

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

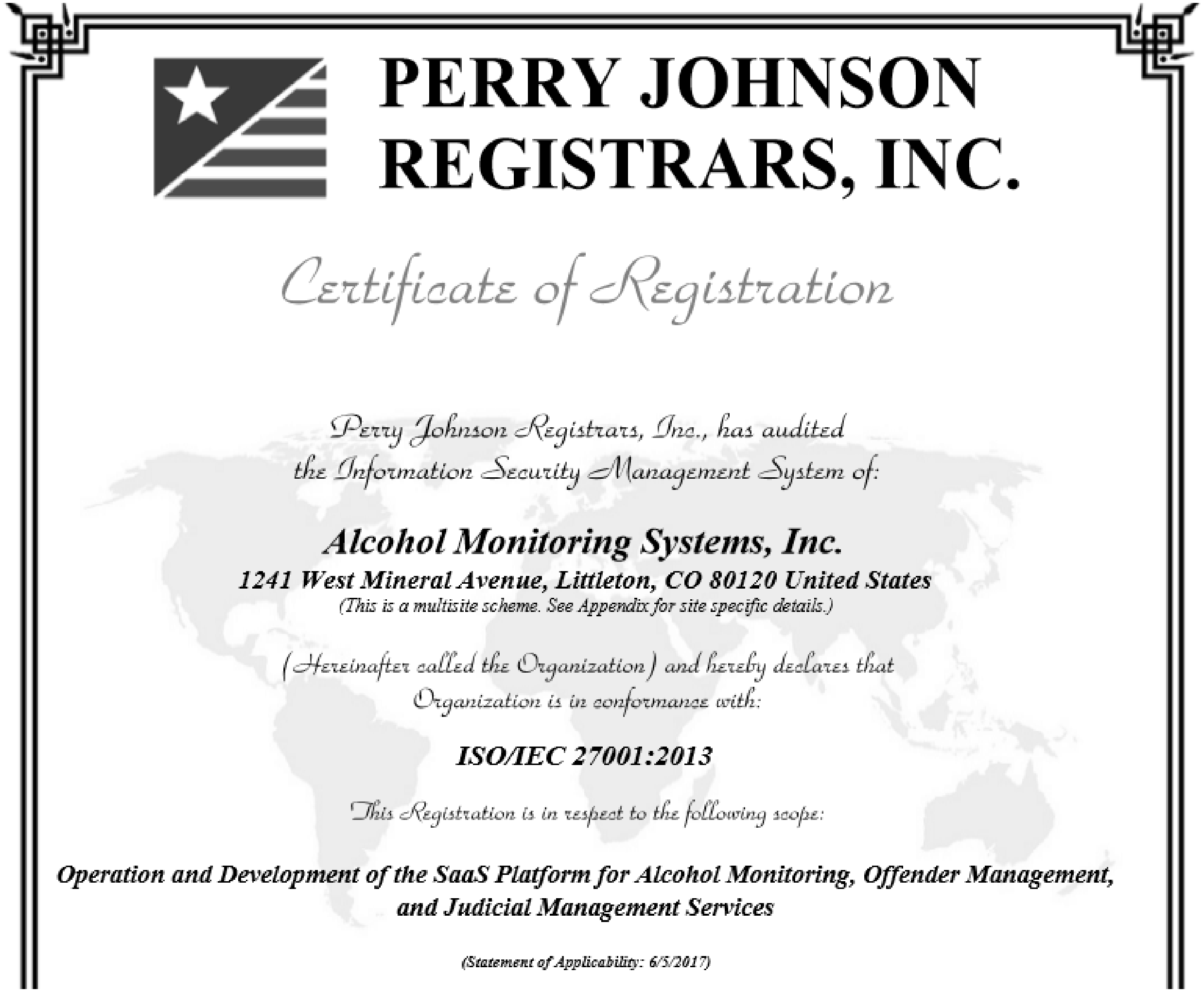
Supporting individuals and communities

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 private 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

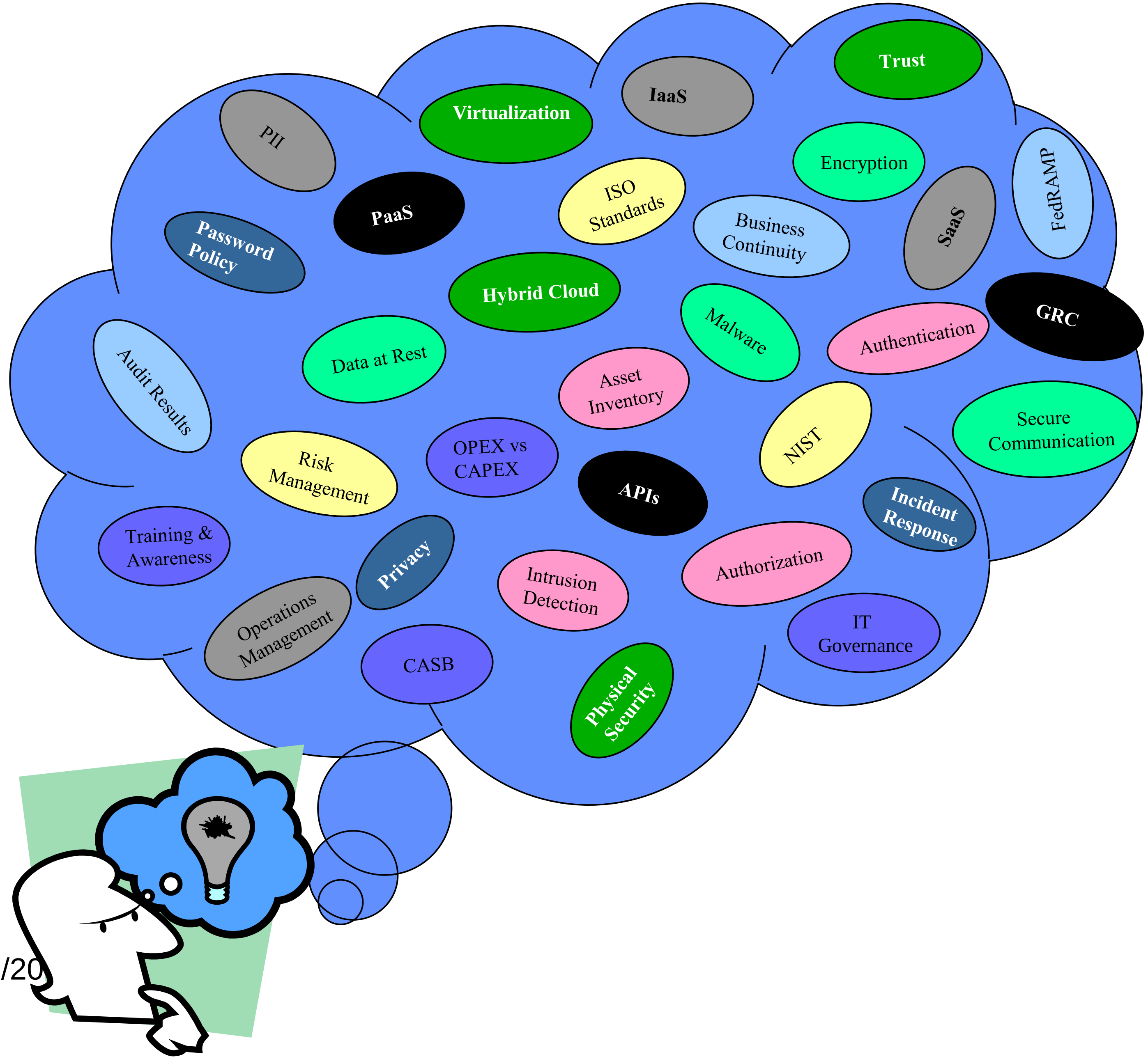
(Statement of Applicability: 6/5/2017)

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.

Now What?



Trust

IaaS

Virtualization

PII

Encryption

FedRAMP

ISO Standards

PaaS

SaaS

Business Continuity

Password Policy

Hybrid Cloud

GRC

Malware

Authentication

Data at Rest

Audit Results

Asset Inventory

Secure Communication

NIST

OPEX vs CAPEX

Risk Management

APIs

Incident Response

Training & Awareness

Privacy

Authorization

Intrusion Detection

Operations Management

IT Governance

CASB

Physical Security

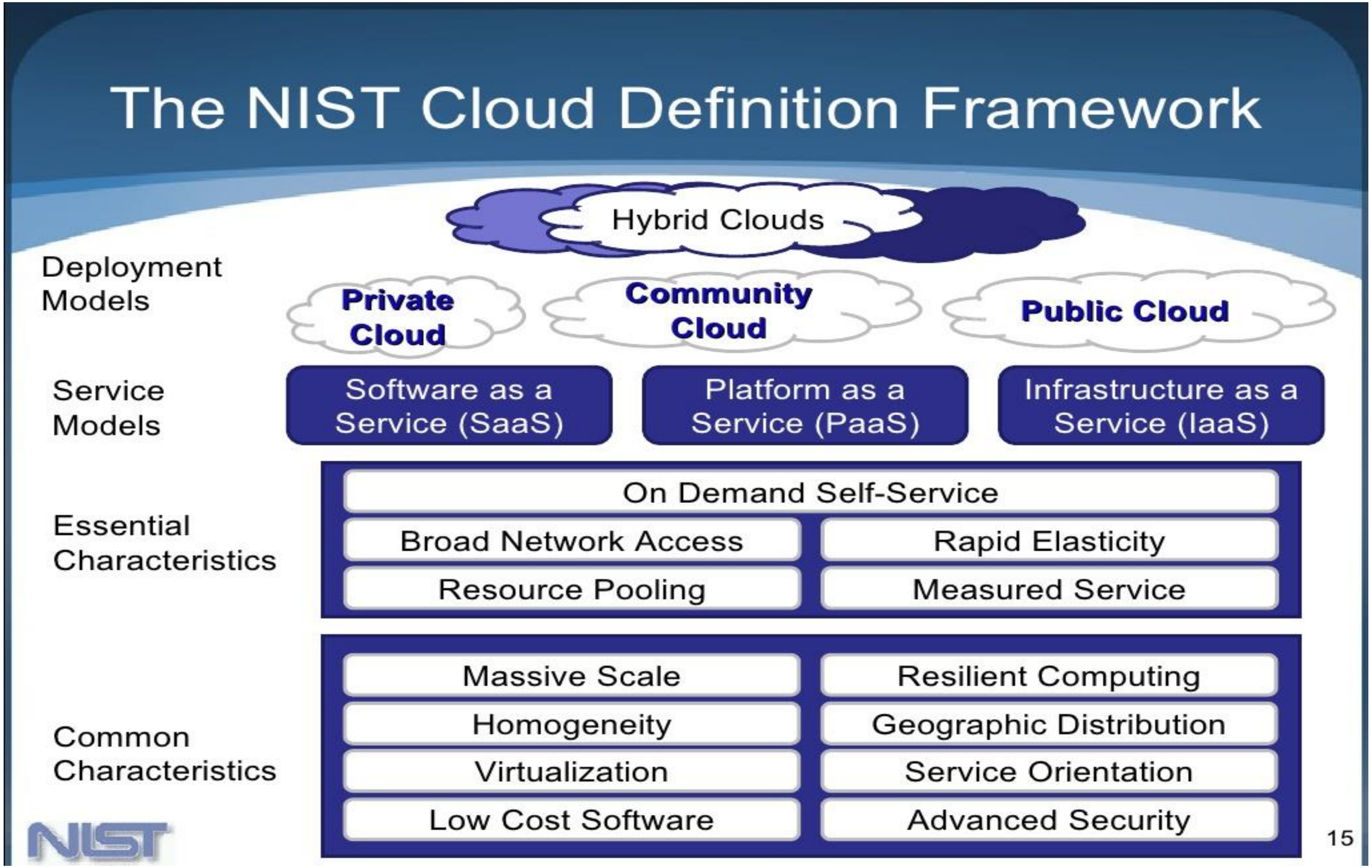
IT 101 – What Problems Are We Trying to Solve?

- 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

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
- ISO Standards for Cloud Security and Privacy
- 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

General Cloud Structure (SaaS PaaS, IaaS)

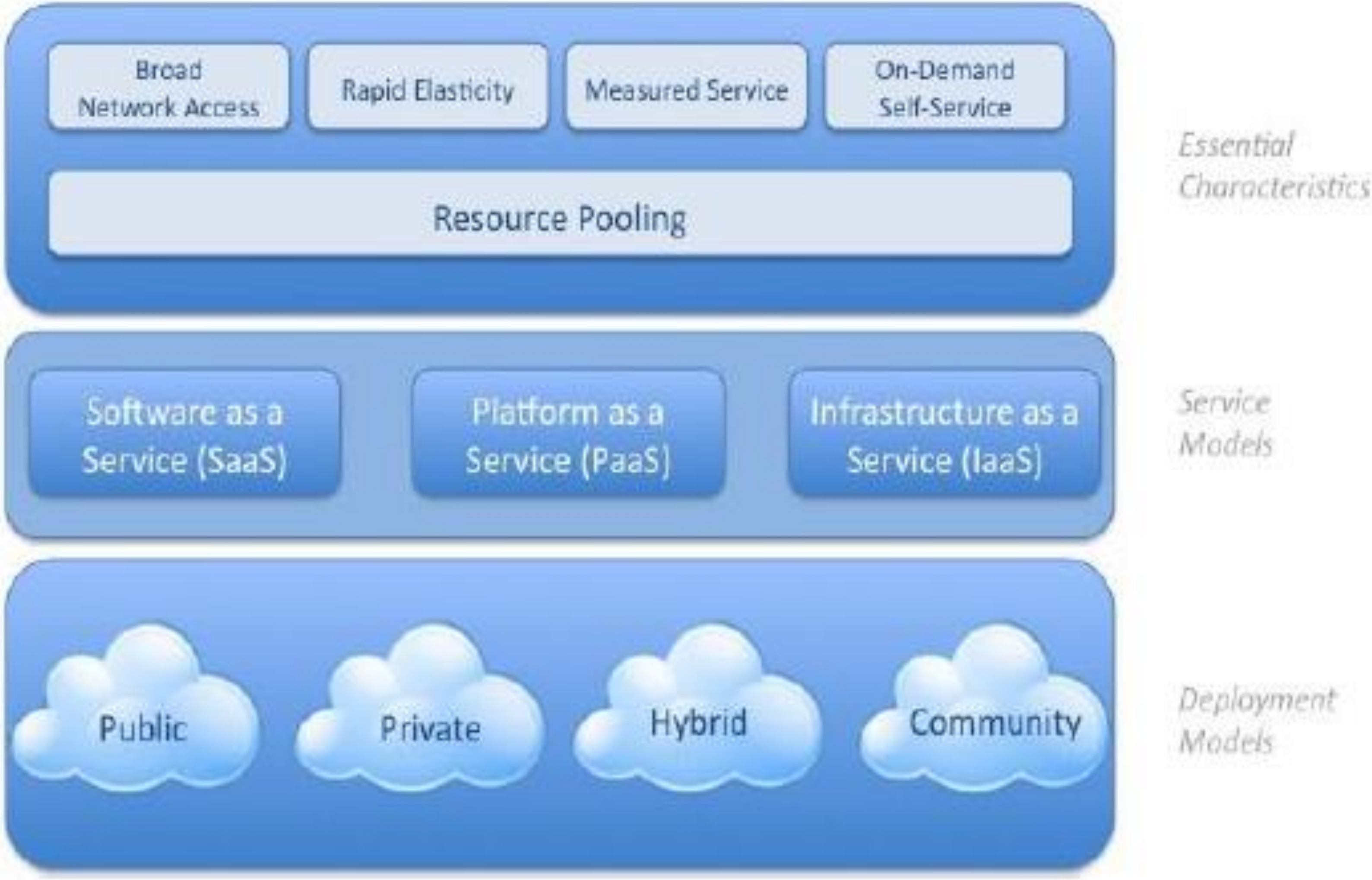
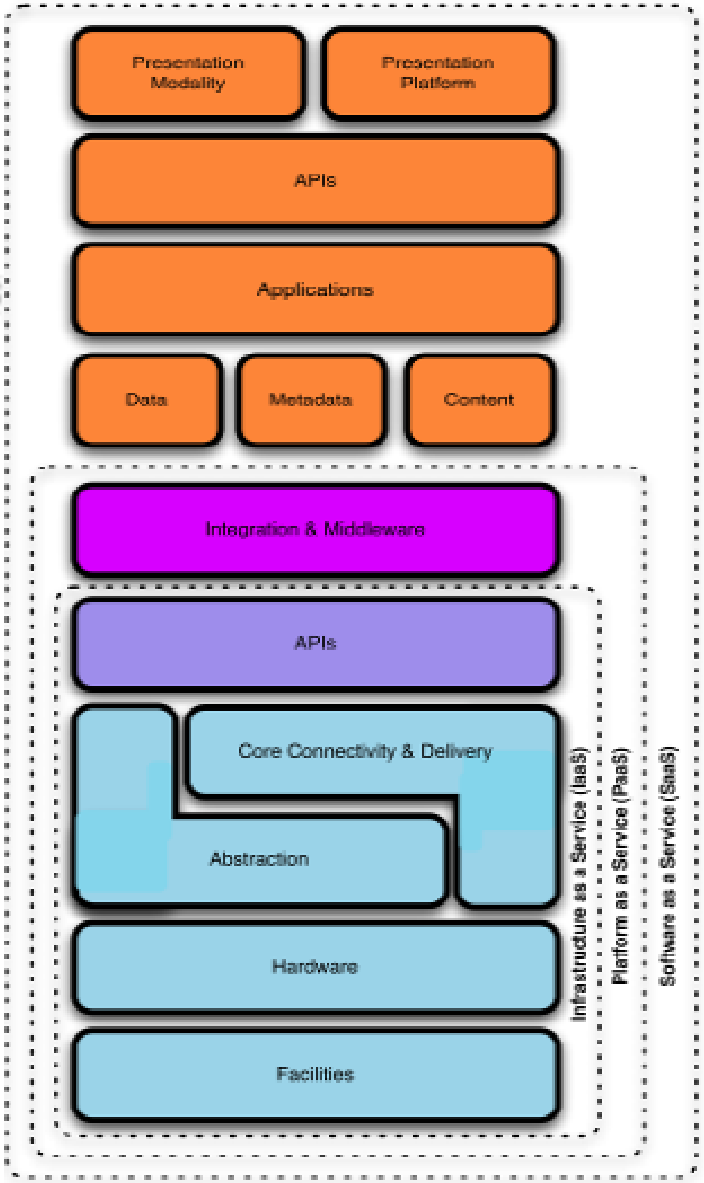


Figure 1—NIST Visual Model of Cloud Computing Definition[2]

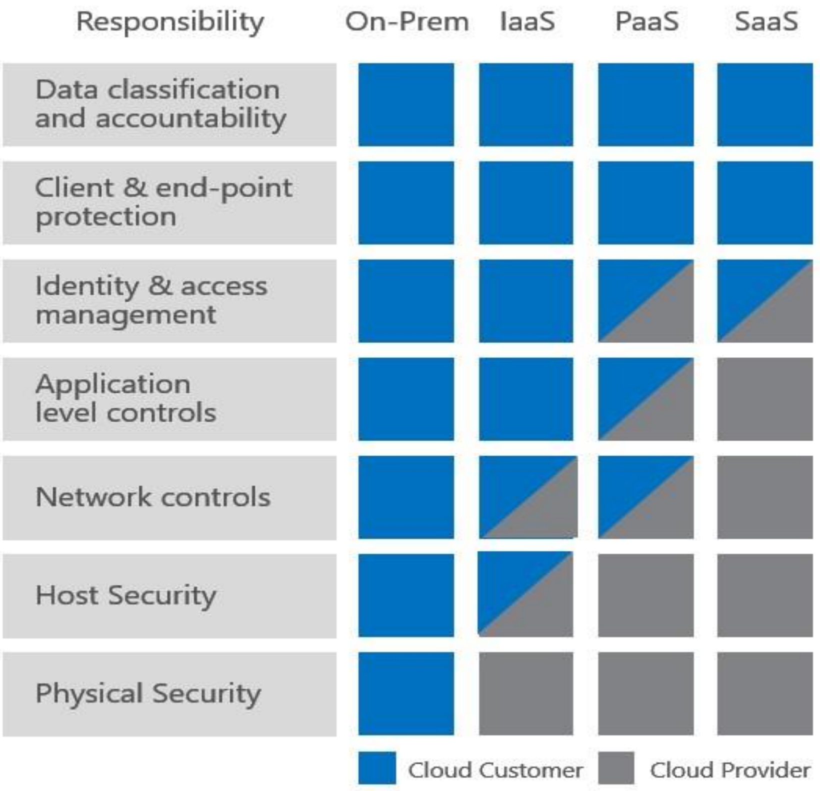


13 Effective Security Controls for ISO 27001 Compliance
When using Microsoft Azure

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

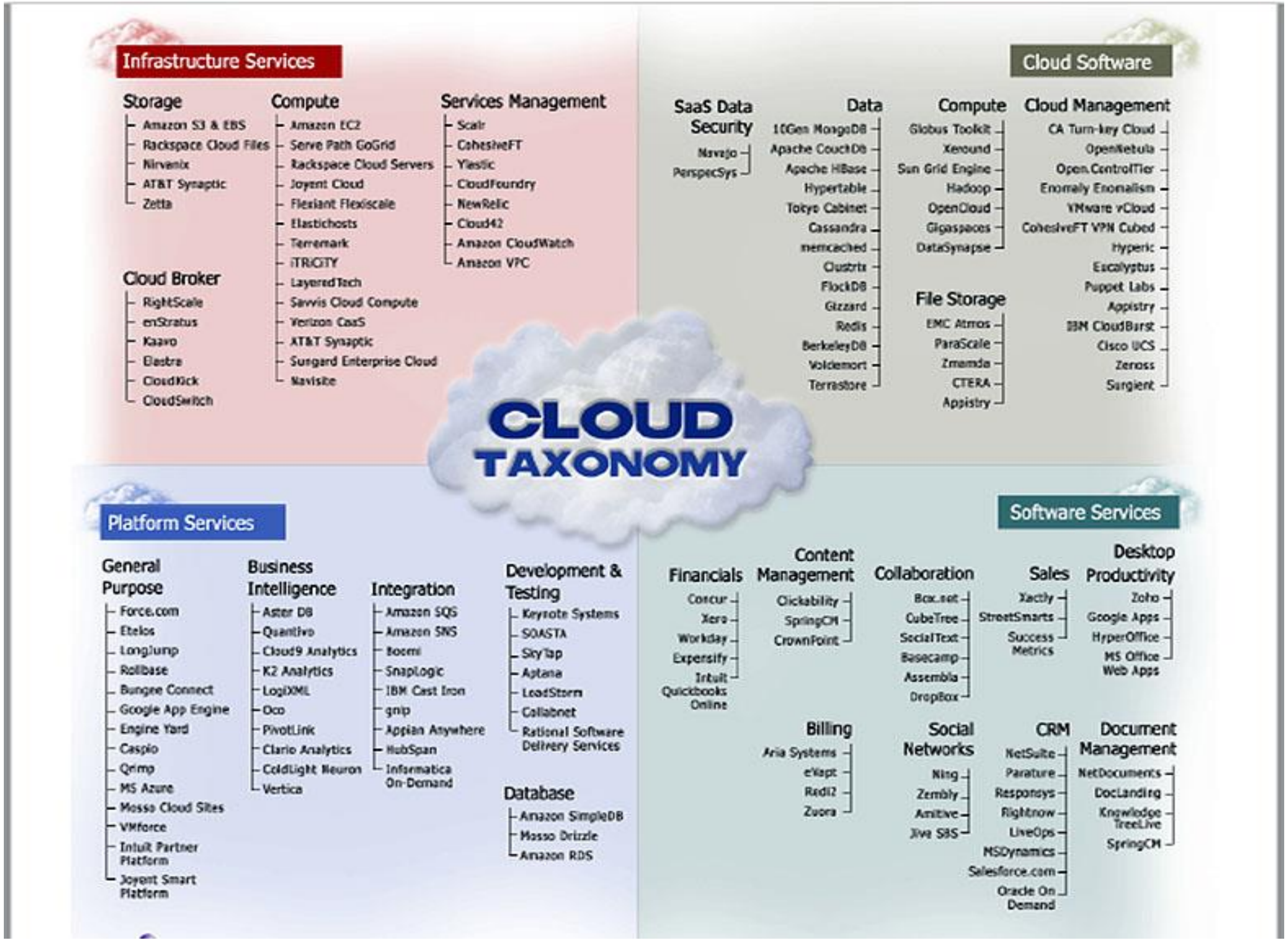


Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	◼
Network controls	🟦	◩	◩	◼
Host Security	🟦	◩	◼	◼
Physical Security	🟦	◼	◼	◼

🟦 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).

Cloud Resources and Services (examples)



CLOUD TAXONOMY

Infrastructure Services

Storage
- Amazon S3 & EBS
- Rackspace Cloud Files
- Nirvanix
- AT&T Synaptic
- Zetta

Cloud Broker
- RightScale
- enStratus
- Kaavo
- Elastra
- CloudKick
- CloudSwitch

Compute
- Amazon EC2
- Serve Path GoGrid
- Rackspace Cloud Servers
- Joyent Cloud
- Flexiant Flexiscale
- Elastichosts
- Terremark
- iTRiCiTY
- LayeredTech
- Savvis Cloud Compute
- Verizon CaaS
- AT&T Synaptic
- Sungard Enterprise Cloud
- Navisite

Services Management
- Scalr
- CohesiveFT
- Ylastic
- CloudFoundry
- NewRelic
- Cloud42
- Amazon CloudWatch
- Amazon VPC

Cloud Software

SaaS Data Security
- Navajo
- PerspecSys

Data
- 10Gen MongoDB
- Apache CouchDB
- Apache HBase
- Hypertable
- Tokyo Cabinet
- Cassandra
- memcached
- Clustrix
- FlockDB
- Gizzard
- Redis
- BerkeleyDB
- Voldemort
- Terrastore

Compute
- Globus Toolkit
- Xeround
- Sun Grid Engine
- Hadoop
- OpenCloud
- Gigaspaces
- DataSynapse

File Storage
- EMC Atmos
- ParaScale
- Zmanda
- CTERA
- Appistry

Cloud Management
- CA Turn-key Cloud
- OpenNebula
- Open.ControlTier
- Enomaly Enomalism
- VMware vCloud
- CohesiveFT VPN Cubed
- Hyperic
- Eucalyptus
- Puppet Labs
- Appistry
- IBM CloudBurst
- Cisco UCS
- Zenoss
- Surgient

Platform Services

General Purpose
- Force.com
- Etelos
- LongJump
- Rollbase
- Bungee Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure
- Mosso Cloud Sites
- VMforce
- Intuit Partner Platform
- Joyent Smart Platform

Business Intelligence
- Aster DB
- Quantivo
- Cloud9 Analytics
- K2 Analytics
- LogiXML
- Oco
- PivotLink
- Clario Analytics
- Coldlight Neuron
- Vertica

Integration
- Amazon SQS
- Amazon SNS
- Boomi
- SnapLogic
- IBM Cast Iron
- gnip
- Appian Anywhere
- HubSpan
- Informatica On-Demand

Development & Testing
- Keynote Systems
- SOASTA
- SkyTap
- Aptana
- LoadStorm
- Collabnet
- Rational Software Delivery Services

Database
- Amazon SimpleDB
- Mosso Drizzle
- Amazon RDS

Software Services

Financials
- Concur
- Xero
- Workday
- Expensify
- Intuit Quickbooks Online

Content Management
- Clickability
- SpringCM
- CrownPoint

Billing
- Aria Systems
- eVapt
- Redi2
- Zuora

Collaboration
- Box.net
- CubeTree
- SocialText
- Basecamp
- Assembla
- DropBox

Social Networks
- Ning
- Zembly
- Amitive
- Jive SBS

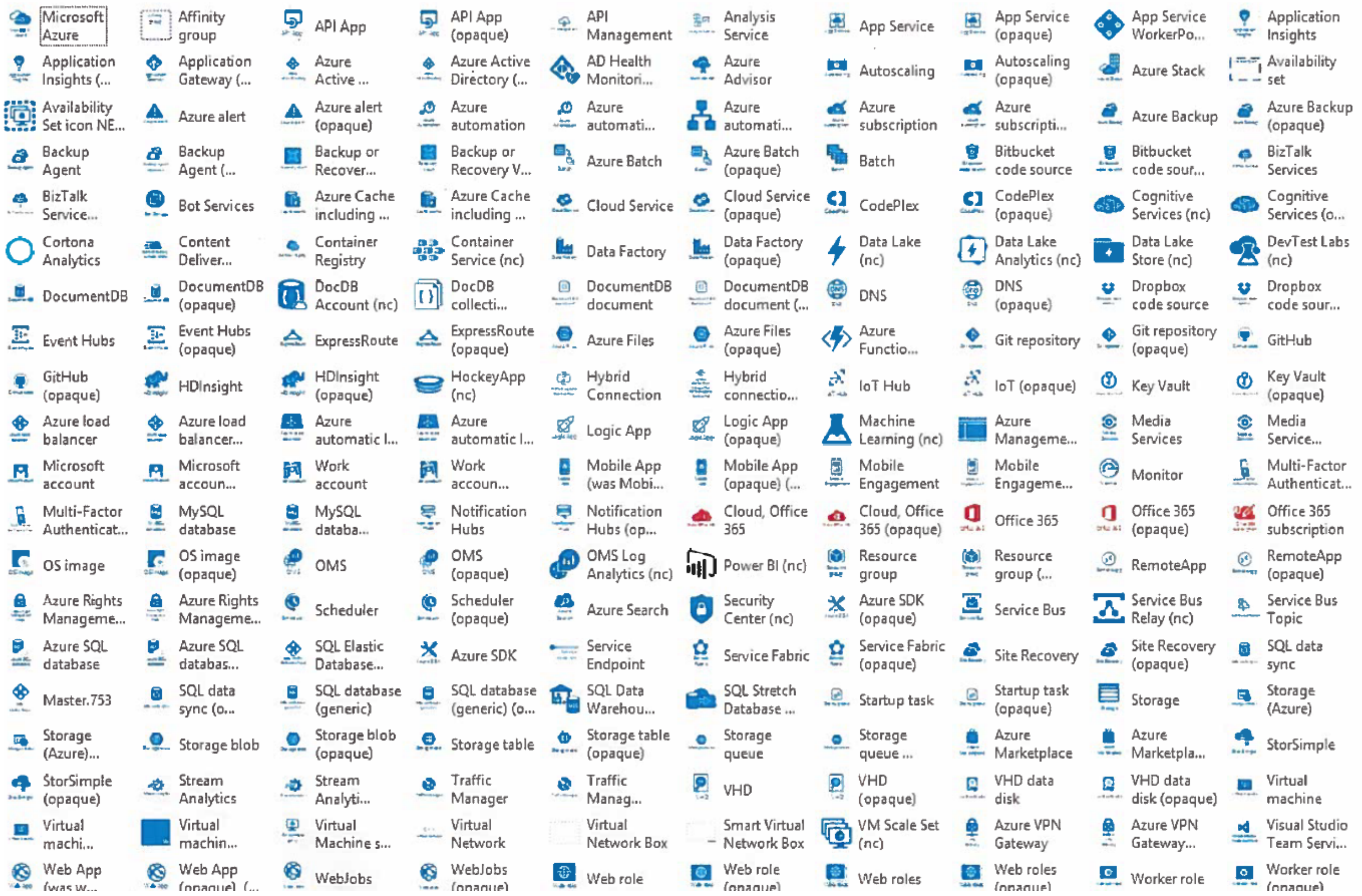
Sales
- Xactly
- StreetSmarts
- Success Metrics

CRM
- NetSuite
- Parature
- Responsys
- Rightnow
- LiveOps
- MSDynamics
- Salesforce.com
- Oracle On Demand

Desktop Productivity
- Zoho
- Google Apps
- HyperOffice
- MS Office Web Apps

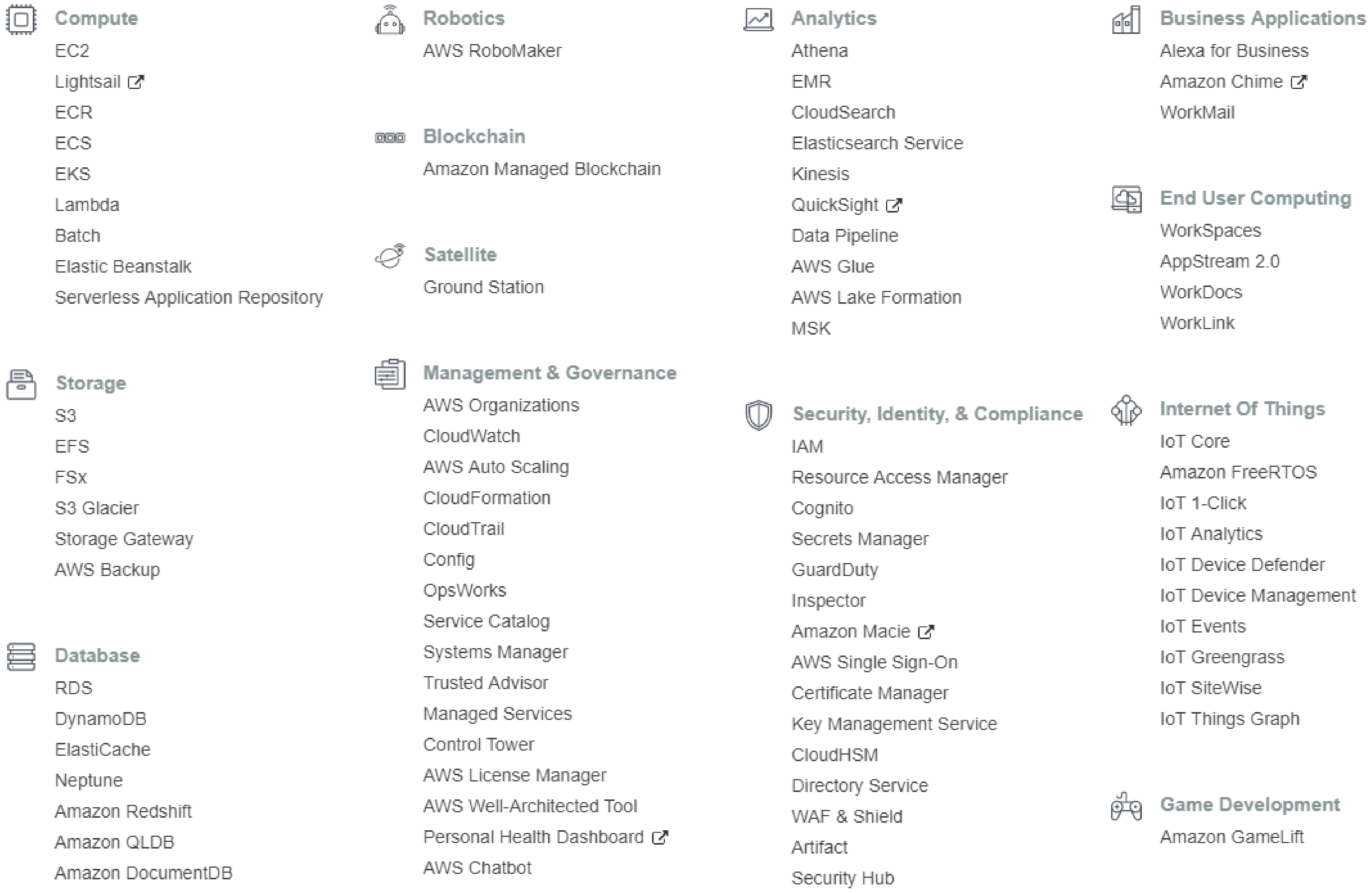
Document Management
- NetDocuments
- DocLanding
- Knowledge TreeLive
- SpringCM

Microsoft Azure Resources and Services (examples)



Microsoft Azure	Affinity group	API App	API App (opaque)	API Management	Analysis Service	App Service	App Service (opaque)	App Service WorkerPo...	Application Insights
Application Insights (...	Application Gateway (...	Azure Active ...	Azure Active Directory (...	AD Health Monitori...	Azure Advisor	Autoscaling	Autoscaling (opaque)	Azure Stack	Availability set
Availability Set icon NE...	Azure alert	Azure alert (opaque)	Azure automation	Azure automati...	Azure automati...	Azure subscription	Azure subscripti...	Azure Backup	Azure Backup (opaque)
Backup Agent	Backup Agent (...	Backup or Recover...	Backup or Recovery V...	Azure Batch	Azure Batch (opaque)	Batch	Bitbucket code source	Bitbucket code sour...	BizTalk Services
BizTalk Service...	Bot Services	Azure Cache including ...	Azure Cache including ...	Cloud Service	Cloud Service (opaque)	CodePlex	CodePlex (opaque)	Cognitive Services (nc)	Cognitive Services (o...
Cortona Analytics	Content Deliver...	Container Registry	Container Service (nc)	Data Factory	Data Factory (opaque)	Data Lake (nc)	Data Lake Analytics (nc)	Data Lake Store (nc)	DevTest Labs (nc)
DocumentDB	DocumentDB (opaque)	DocDB Account (nc)	DocDB collecti...	DocumentDB document	DocumentDB document (...	DNS	DNS (opaque)	Dropbox code source	Dropbox code sour...
Event Hubs	Event Hubs (opaque)	ExpressRoute	ExpressRoute (opaque)	Azure Files	Azure Files (opaque)	Azure Functio...	Git repository	Git repository (opaque)	GitHub
GitHub (opaque)	HDInsight	HDInsight (opaque)	HockeyApp (nc)	Hybrid Connection	Hybrid connectio...	IoT Hub	IoT (opaque)	Key Vault	Key Vault (opaque)
Azure load balancer	Azure load balancer...	Azure automatic l...	Azure automatic l...	Logic App	Logic App (opaque)	Machine Learning (nc)	Azure Manageme...	Media Services	Media Service...
Microsoft account	Microsoft accoun...	Work account	Work accoun...	Mobile App (was Mobi...	Mobile App (opaque) (...	Mobile Engagement	Mobile Engageme...	Monitor	Multi-Factor Authenticat...
Multi-Factor Authenticat...	MySQL database	MySQL databa...	Notification Hubs	Notification Hubs (op...	Cloud, Office 365	Cloud, Office 365 (opaque)	Office 365	Office 365 (opaque)	Office 365 subscription
OS image	OS image (opaque)	OMS	OMS (opaque)	OMS Log Analytics (nc)	Power BI (nc)	Resource group	Resource group (...	RemoteApp	RemoteApp (opaque)
Azure Rights Manageme...	Azure Rights Manageme...	Scheduler	Scheduler (opaque)	Azure Search	Security Center (nc)	Azure SDK (opaque)	Service Bus	Service Bus Relay (nc)	Service Bus Topic
Azure SQL database	Azure SQL databas...	SQL Elastic Database...	Azure SDK	Service Endpoint	Service Fabric	Service Fabric (opaque)	Site Recovery	Site Recovery (opaque)	SQL data sync
Master.753	SQL data sync (o...	SQL database (generic)	SQL database (generic) (o...	SQL Data Warehou...	SQL Stretch Database ...	Startup task	Startup task (opaque)	Storage	Storage (Azure)
Storage (Azure)...	Storage blob	Storage blob (opaque)	Storage table	Storage table (opaque)	Storage queue	Storage queue ...	Azure Marketplace	Azure Marketpla...	StorSimple
StorSimple (opaque)	Stream Analytics	Stream Analyti...	Traffic Manager	Traffic Manag...	VHD	VHD (opaque)	VHD data disk	VHD data disk (opaque)	Virtual machine
Virtual machi...	Virtual machin...	Virtual Machine s...	Virtual Network	Virtual Network Box	Smart Virtual Network Box	VM Scale Set (nc)	Azure VPN Gateway	Azure VPN Gateway...	Visual Studio Team Servi...
Web App (was w...	Web App (opaque) (...	WebJobs	WebJobs (opaque)	Web role	Web role (opaque)	Web roles	Web roles (opaque)	Worker role	Worker role (opaque)

Amazon Cloud Resources and Services (examples)



Compute
- EC2
- Lightsail
- ECR
- ECS
- EKS
- Lambda
- Batch
- Elastic Beanstalk
- Serverless Application Repository

Storage
- S3
- EFS
- FSx
- S3 Glacier
- Storage Gateway
- AWS Backup

Database
- RDS
- DynamoDB
- ElastiCache
- Neptune
- Amazon Redshift
- Amazon QLDB
- Amazon DocumentDB

Robotics
- AWS RoboMaker

Blockchain
- Amazon Managed Blockchain

Satellite
- Ground Station

Management & Governance
- AWS Organizations
- CloudWatch
- AWS Auto Scaling
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Systems Manager
- Trusted Advisor
- Managed Services
- Control Tower
- AWS License Manager
- AWS Well-Architected Tool
- Personal Health Dashboard
- AWS Chatbot

Analytics
- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- QuickSight
- Data Pipeline
- AWS Glue
- AWS Lake Formation
- MSK

Security, Identity, & Compliance
- IAM
- Resource Access Manager
- Cognito
- Secrets Manager
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- Key Management Service
- CloudHSM
- Directory Service
- WAF & Shield
- Artifact
- Security Hub

Business Applications
- Alexa for Business
- Amazon Chime
- WorkMail

End User Computing
- WorkSpaces
- AppStream 2.0
- WorkDocs
- WorkLink

Internet Of Things
- IoT Core
- Amazon FreeRTOS
- IoT 1-Click
- IoT Analytics
- IoT Device Defender
- IoT Device Management
- IoT Events
- IoT Greengrass
- IoT SiteWise
- IoT Things Graph

Game Development
- Amazon GameLift

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)

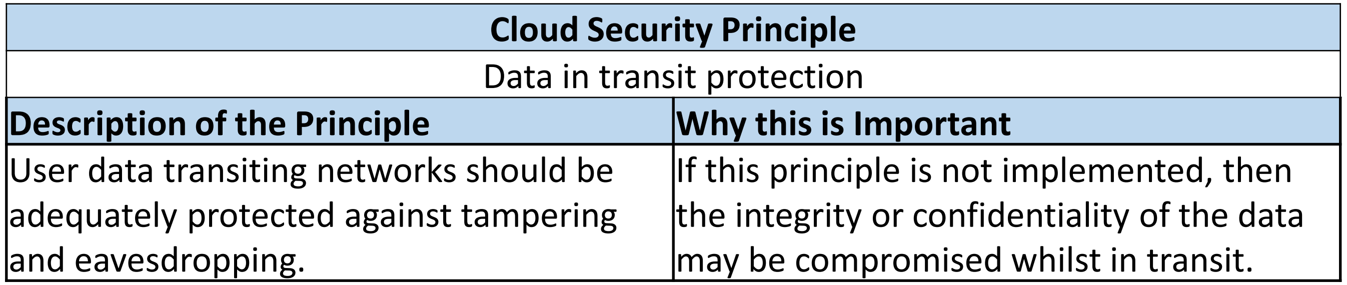
National Cyber Security Centre
a part of GCHQ

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

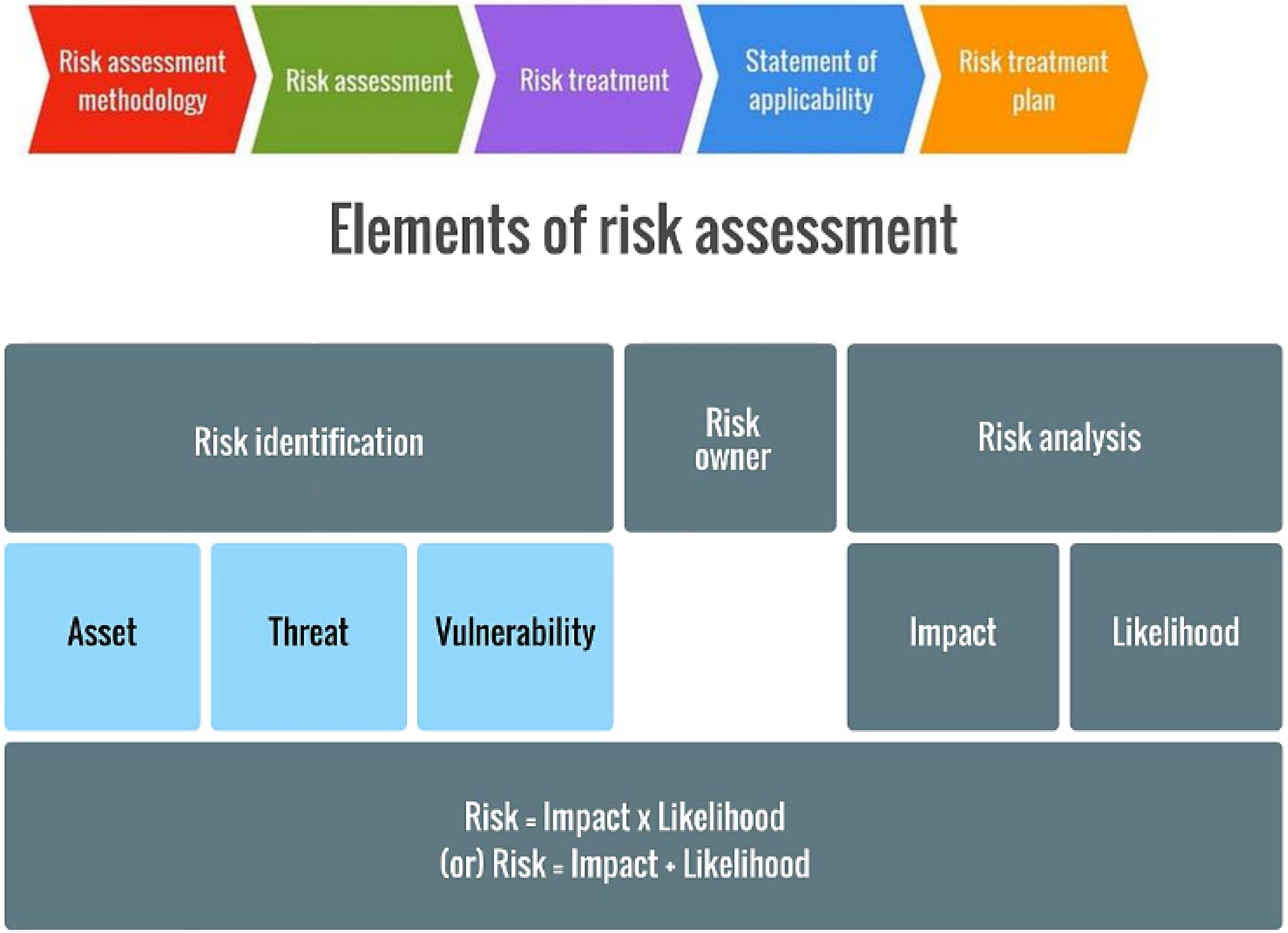


Cloud Security Principle	
Data in transit protection	
Description of the Principle	**Why this is Important**
User data transiting networks should be adequately protected against tampering and eavesdropping.	If this principle is not implemented, then the integrity or confidentiality of the data may be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

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Top 10 Security & Privacy Threats in the Cloud
- Risk Assessment Methods for Cloud Applications
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

Risk Management Principles (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

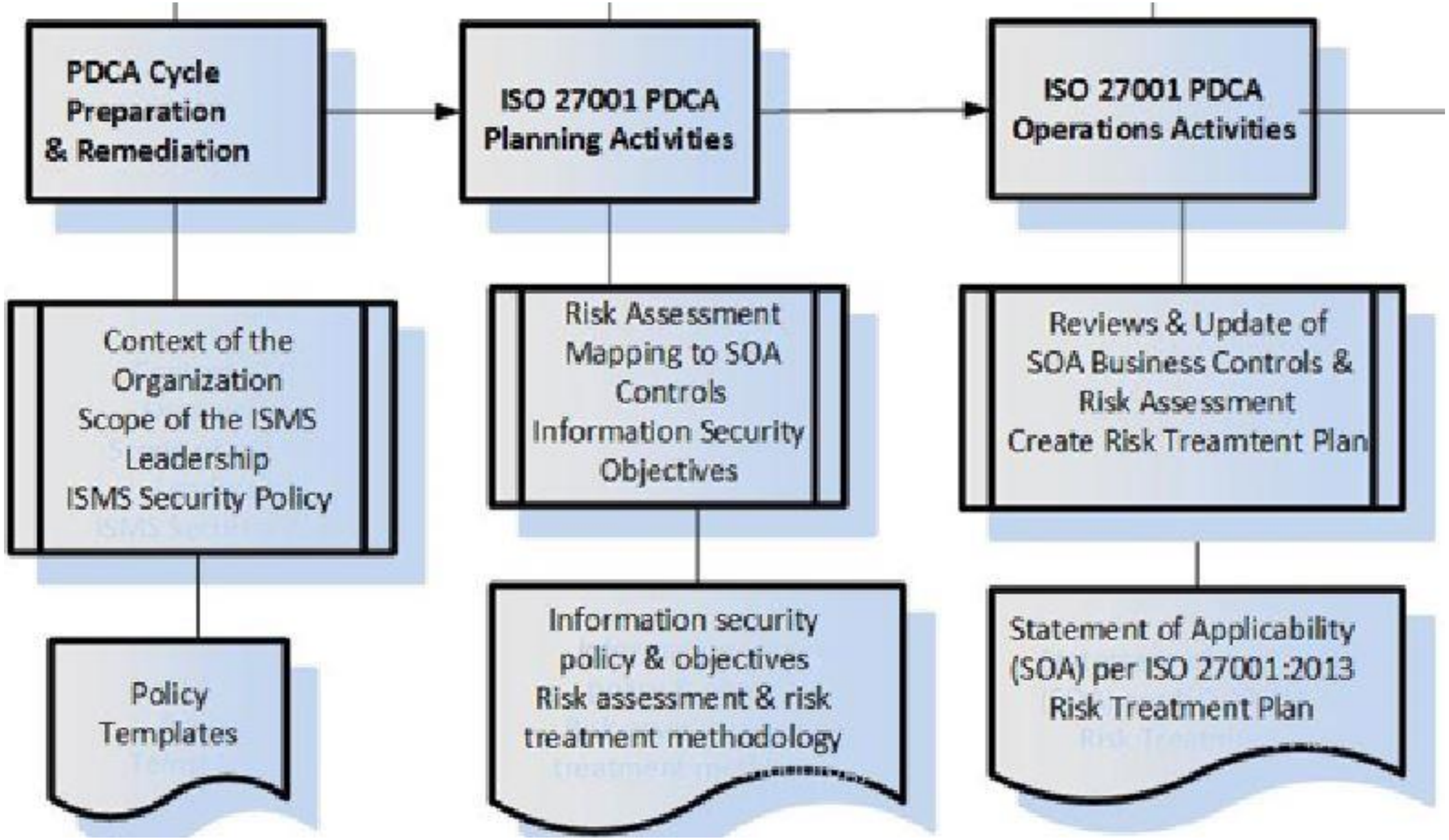
Impact

Likelihood

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

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

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

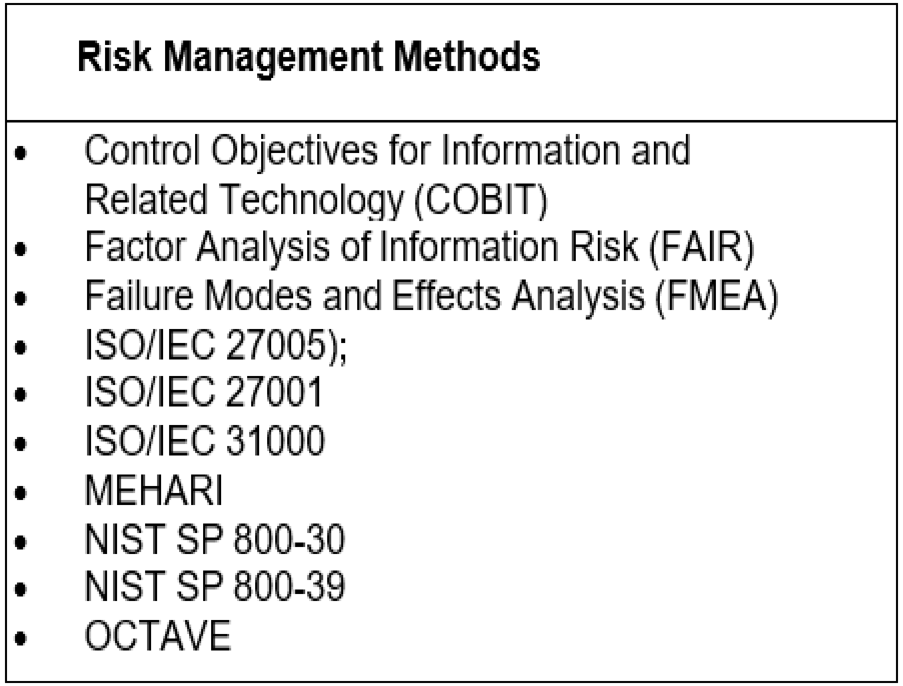
Information security policy & objectives
Risk assessment & risk treatment methodology

Statement of Applicability (SOA) per ISO 27001:2013
Risk Treatment Plan

9/10/2019

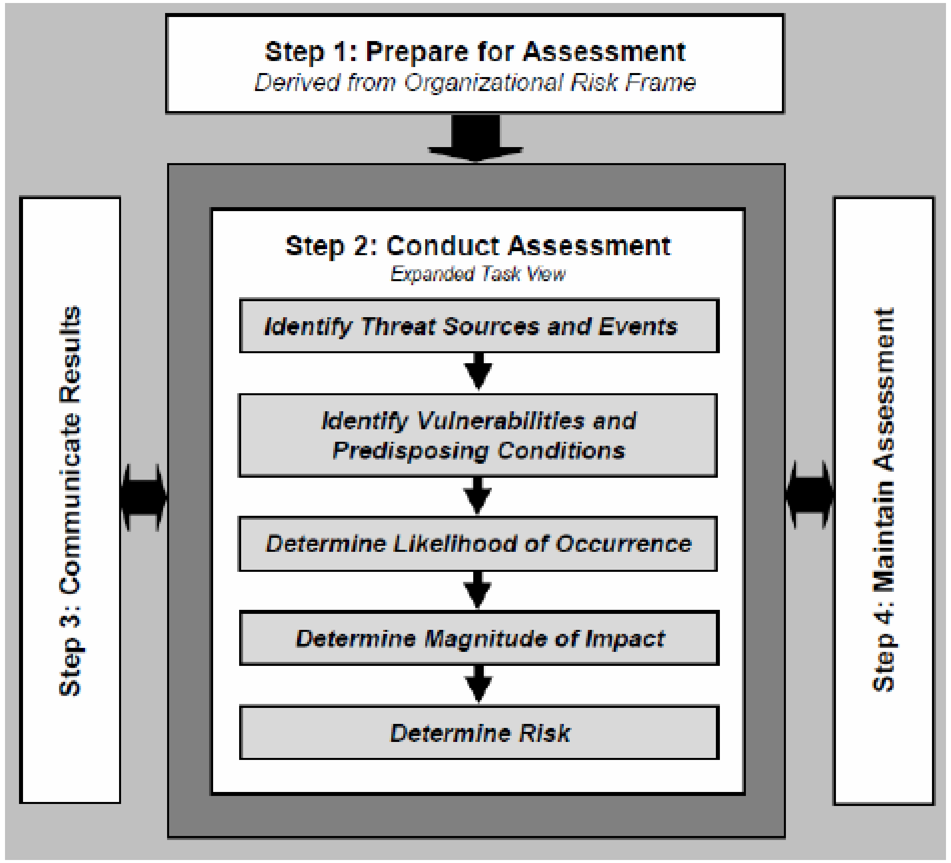
Risk Assessments for Cloud Applications – where to get started?

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



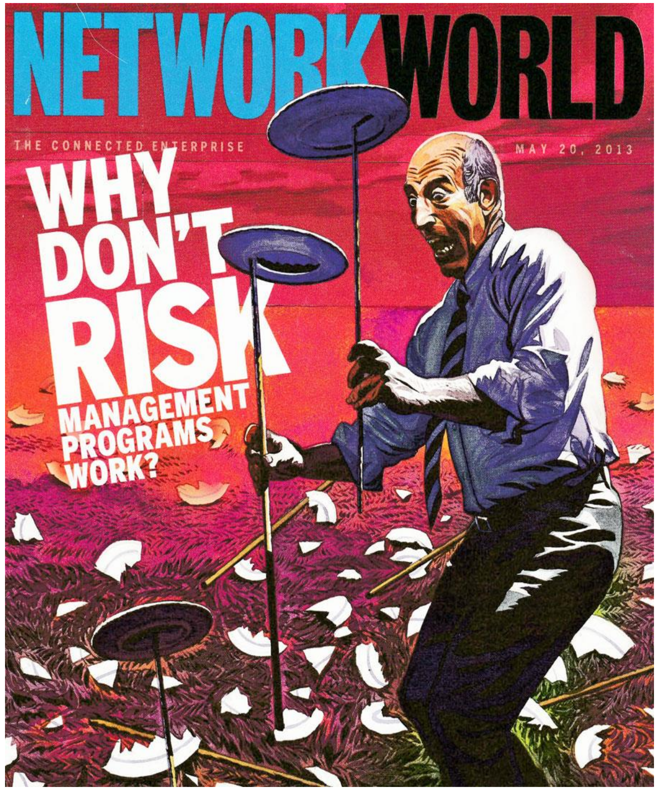
Risk Management Methods

- 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


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

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 – definition of terms (per ISO Standards)

IISO/IEC 27000:2017 defines risk in vague and not-very helpful terms for defining Risk:

effect of uncertainty on objectives (3.49)
Note 1 to entry: An effect is a deviation from the expected — positive or negative.
Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

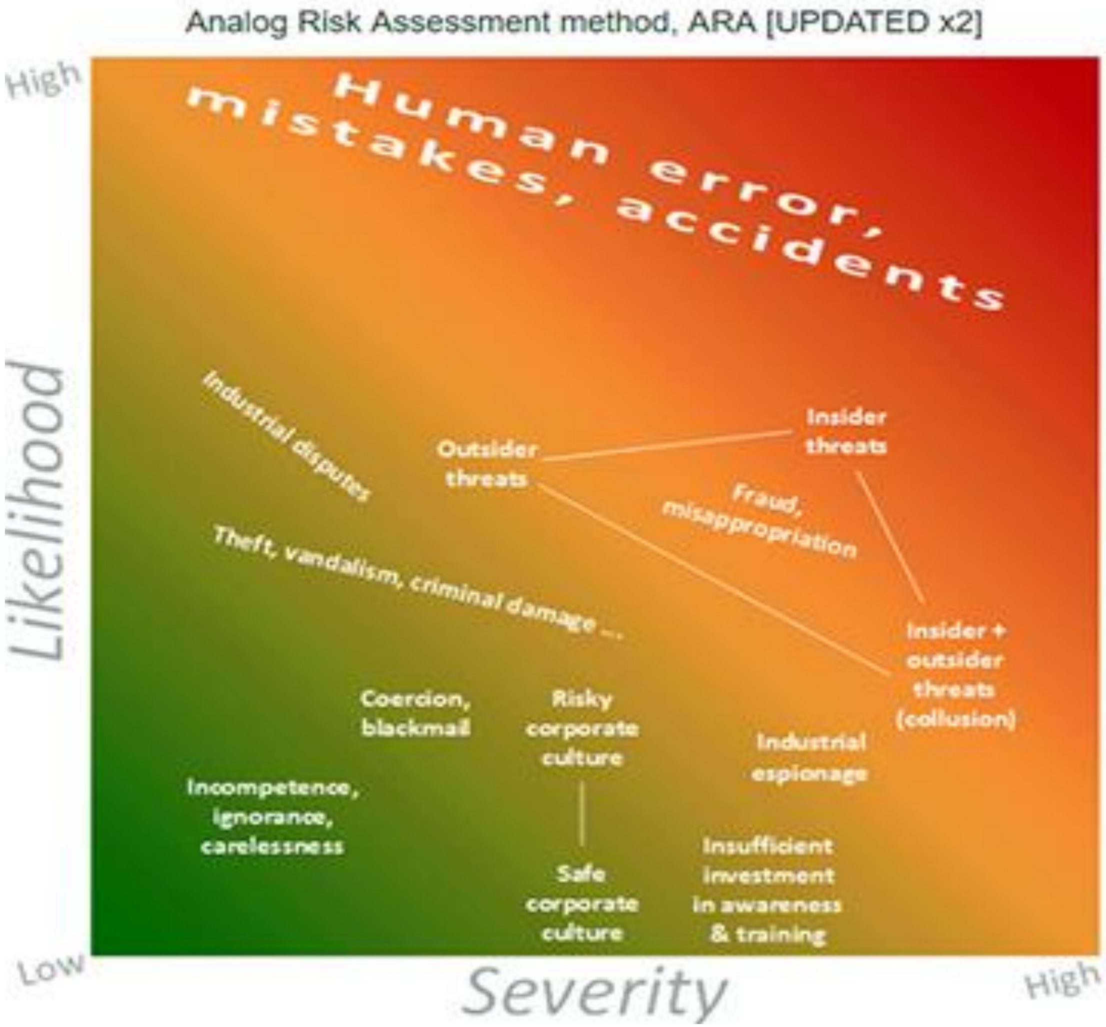
Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of ***information security management systems (ISMS), information security risks can be expressed as effect of uncertainty on information security objectives.***

Note 6 to entry: ***Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.***

ISO 31010:2009 says "Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk." So consequences and probabilities (determine who-knows-how) are "combined" (in some unspecified manner), "taking into account" the controls (somehow). ***It could hardly be any more vague!***

Risk Methodologies Continued (Gary Hinson)



A definition of information risk (specifically) as “risk pertaining to information” which can be assessed and compared visually using the Analog Risk Assessment method implying Risk = Likelihood x Severity.

ARA method is simply a visual device to get people ‘on the same page’, considering and discussing information risks on a comparable basis to reach a consensus … which then forms a rational basis for prioritizing their treatment.

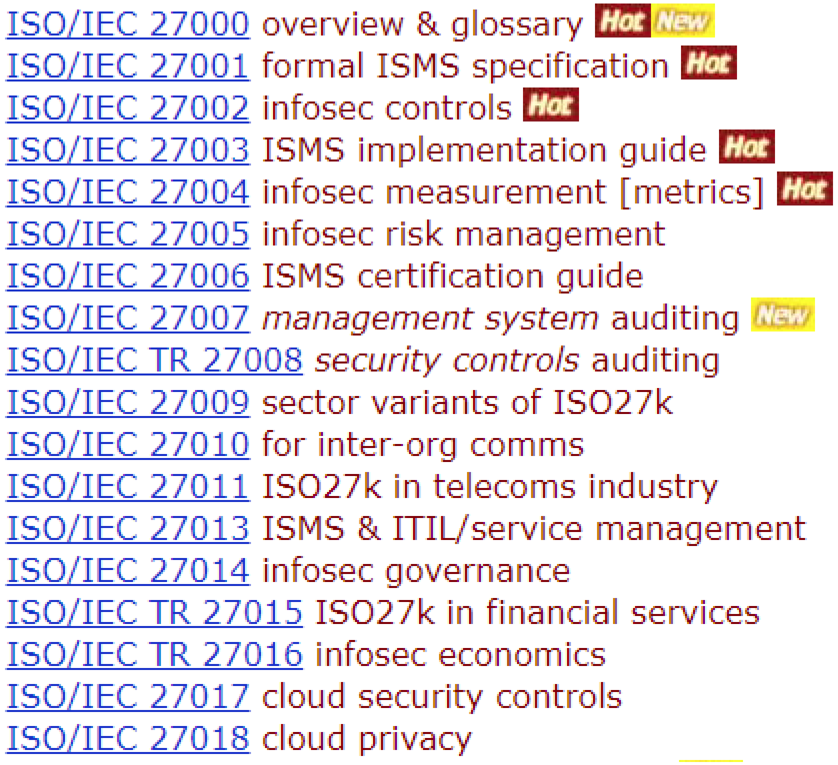
Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Top 10 Security & Privacy Threats in the Cloud
- Risk Assessment Methods for Cloud Applications
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

ISO Codes of Practice

- ISO27001 is part of a family of information security guidance which provides enhanced and additional controls.

- Examples:
  - ISO27002 – More detail on all of the ISO27001 controls
  - ISO27005 – Risk assessment
  - ISO27017 – Application to cloud services
  - ISO27018 – Protection of Personally Identifiable Information (PII) in the cloud
  - ISO31000 – Risk Management – Principles and Guidelines
  - ISO31010 – Risk Management – Risk Assessment Techniques
  - ISO22031 – Business Continuity Management



ISO/IEC 27000 overview & glossary Hot New
ISO/IEC 27001 formal ISMS specification Hot
ISO/IEC 27002 infosec controls Hot
ISO/IEC 27003 ISMS implementation guide Hot
ISO/IEC 27004 infosec measurement [metrics] Hot
ISO/IEC 27005 infosec risk management
ISO/IEC 27006 ISMS certification guide
ISO/IEC 27007 *management system* auditing New
ISO/IEC TR 27008 *security controls* auditing
ISO/IEC 27009 sector variants of ISO27k
ISO/IEC 27010 for inter-org comms
ISO/IEC 27011 ISO27k in telecoms industry
ISO/IEC 27013 ISMS & ITIL/service management
ISO/IEC 27014 infosec governance
ISO/IEC TR 27015 ISO27k in financial services
ISO/IEC TR 27016 infosec economics
ISO/IEC 27017 cloud security controls
ISO/IEC 27018 cloud privacy

The ISO 27001 Forum - http://iso27001security.com/index.html

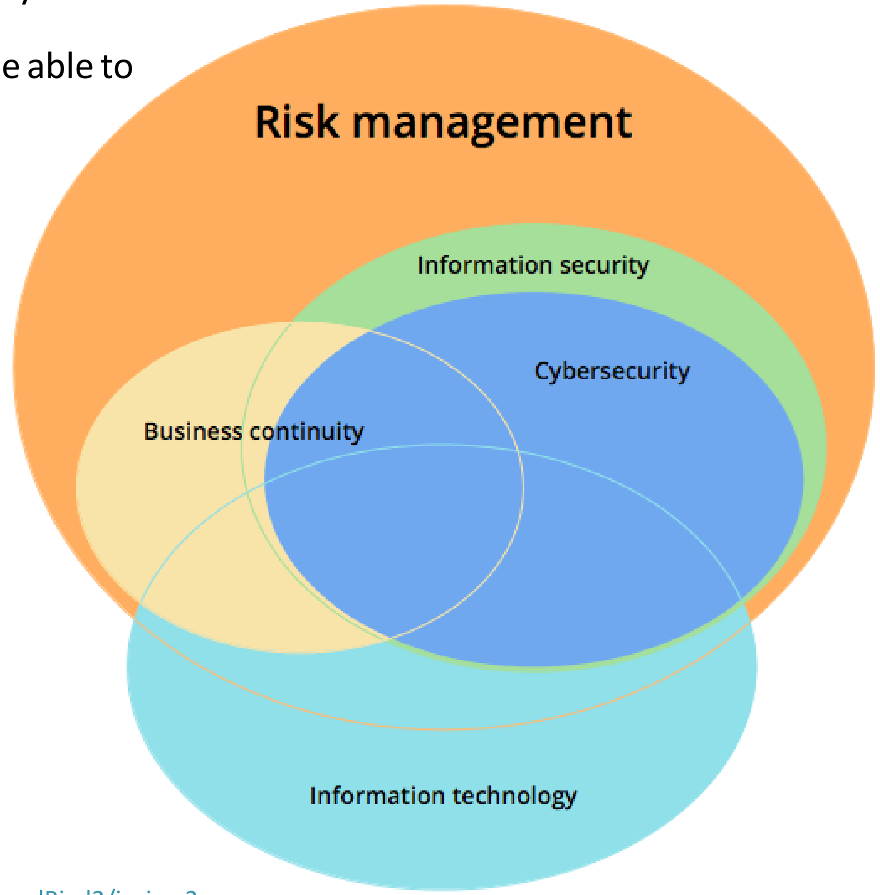
The primary purpose of this website is to describe, promote and share the information risk and security practices described in the ISO/IEC 27000-series information security management systems standards.

Benefits of ISO 27001 - ISO /IEC 27001:2013 Structure and Content

ISO/IEC 27001:2013 Implementation, Certification from a certification body demonstrates that the security of organization information has been addressed, valuable data and information assets properly controlled.

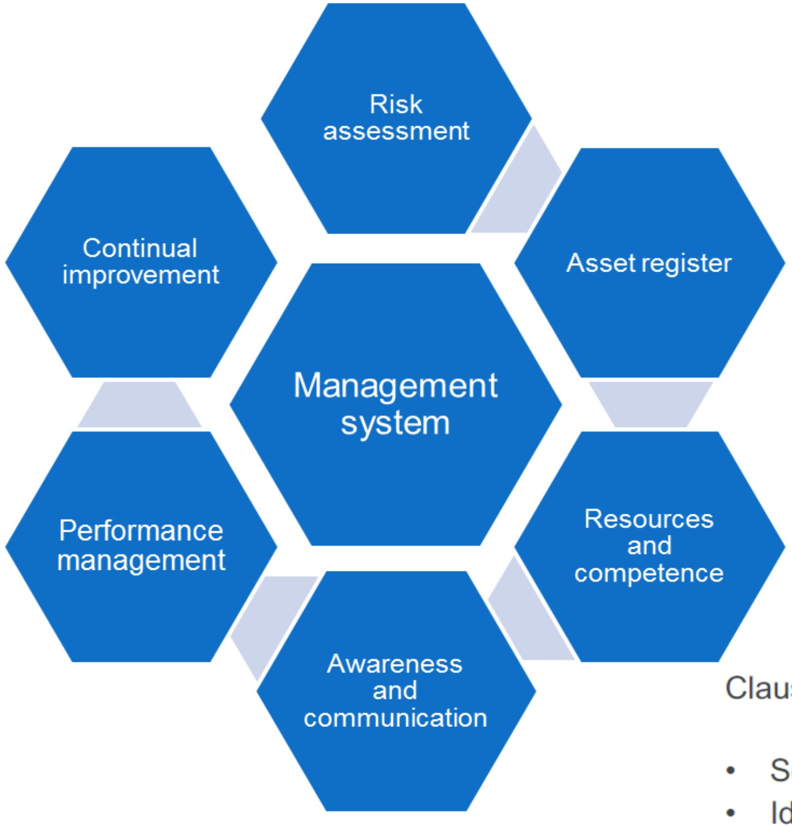
Also there is List of benefits By achieving certification to ISO/IEC 27001:2013 organization will be able to acquire numerous benefits including:

- Keeps confidential information secure
- Provides customers and stakeholders with confidence in how you manage risk
- Secure exchange of information
- Provide Organization with a competitive advantage
- Enhanced customer satisfaction
- Consistency in the delivery of your service or product
- Manages and minimises risk exposure
- Builds a culture of security
- Protects the Organization assets, shareholders and Customers
- Protects the company, assets, shareholders and directors



Ahmed Riad, BlueKaizen Magazine, Benefits of ISO 27001- https://www.slideshare.net/AhmedRiad2/isoiec-https://www.slideshare.net/AhmedRiad2/isoiec-2

The ISO/IEC 27001 standard



ISO/IEC 27001 Controls

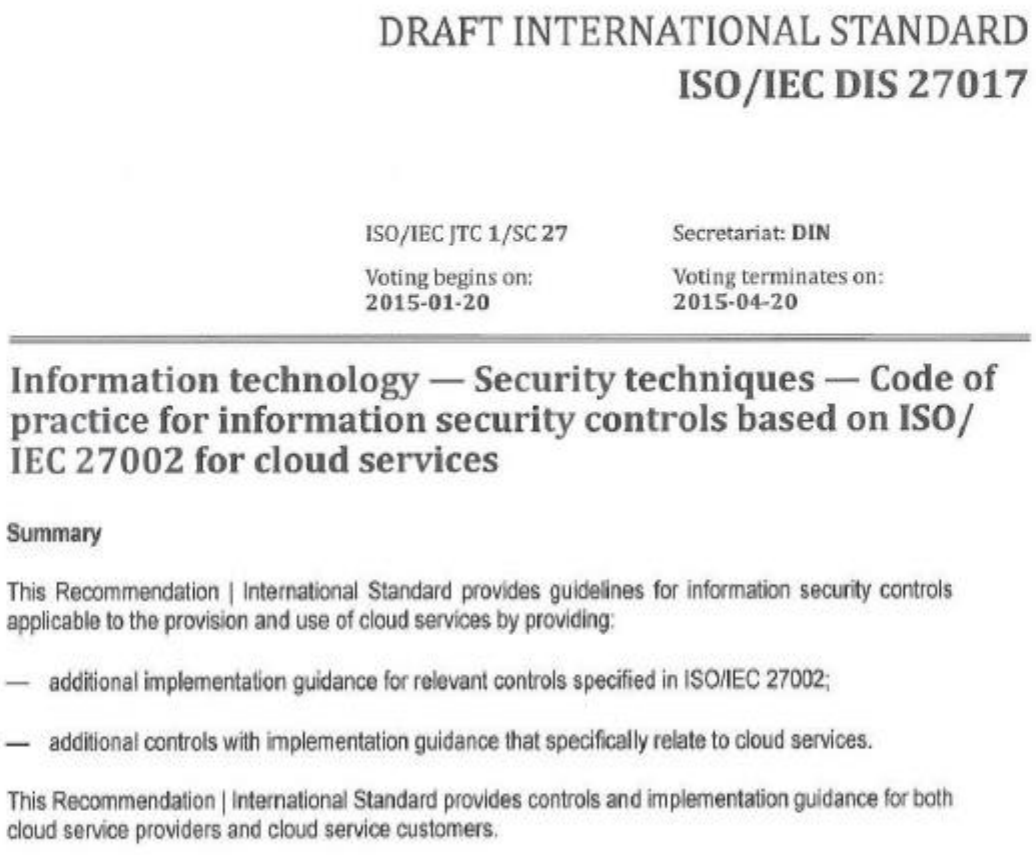
Information security policies	Organisation of information security	Human resources security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development and maintenance	Supplier relationships	Incident management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

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 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

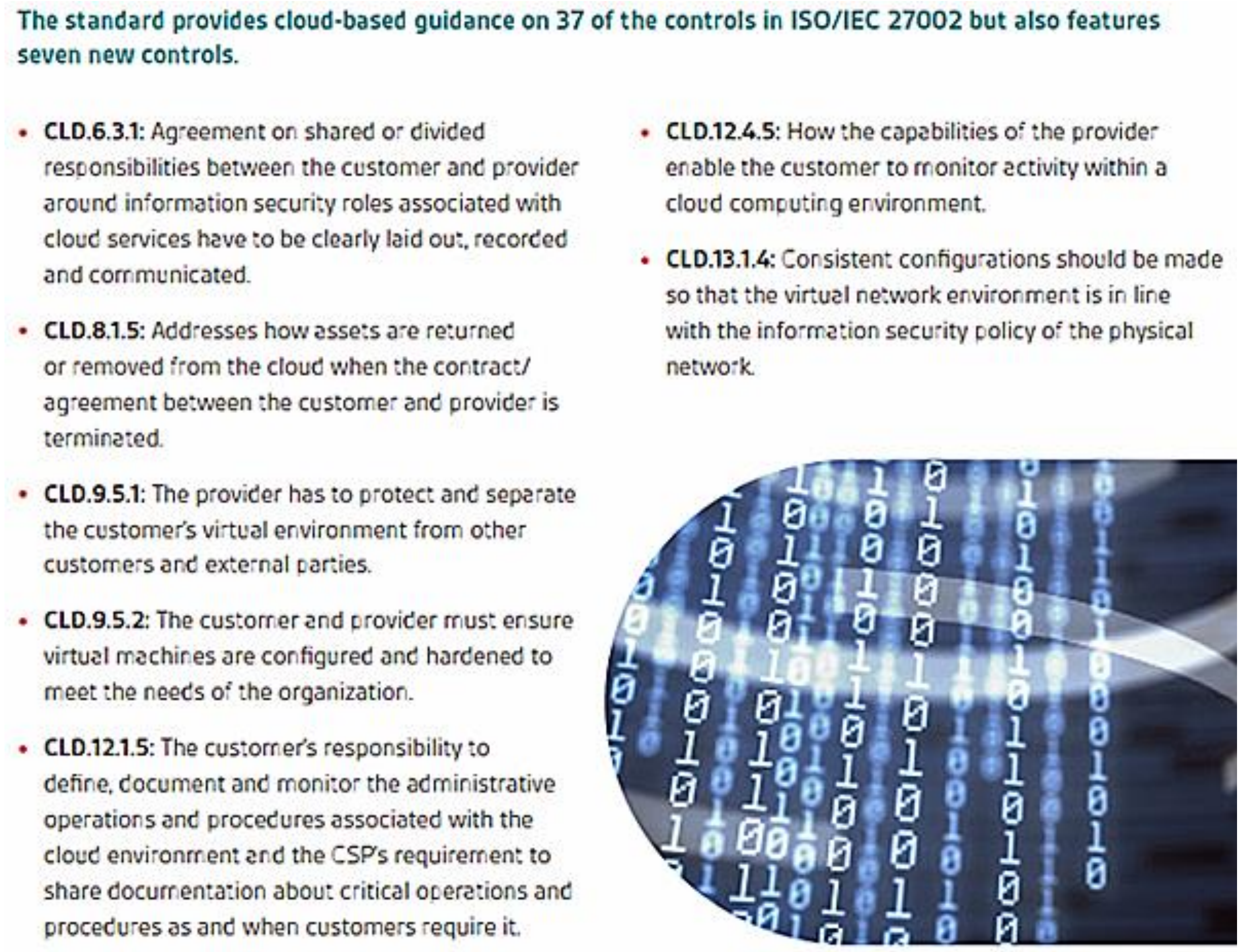
Summary

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.

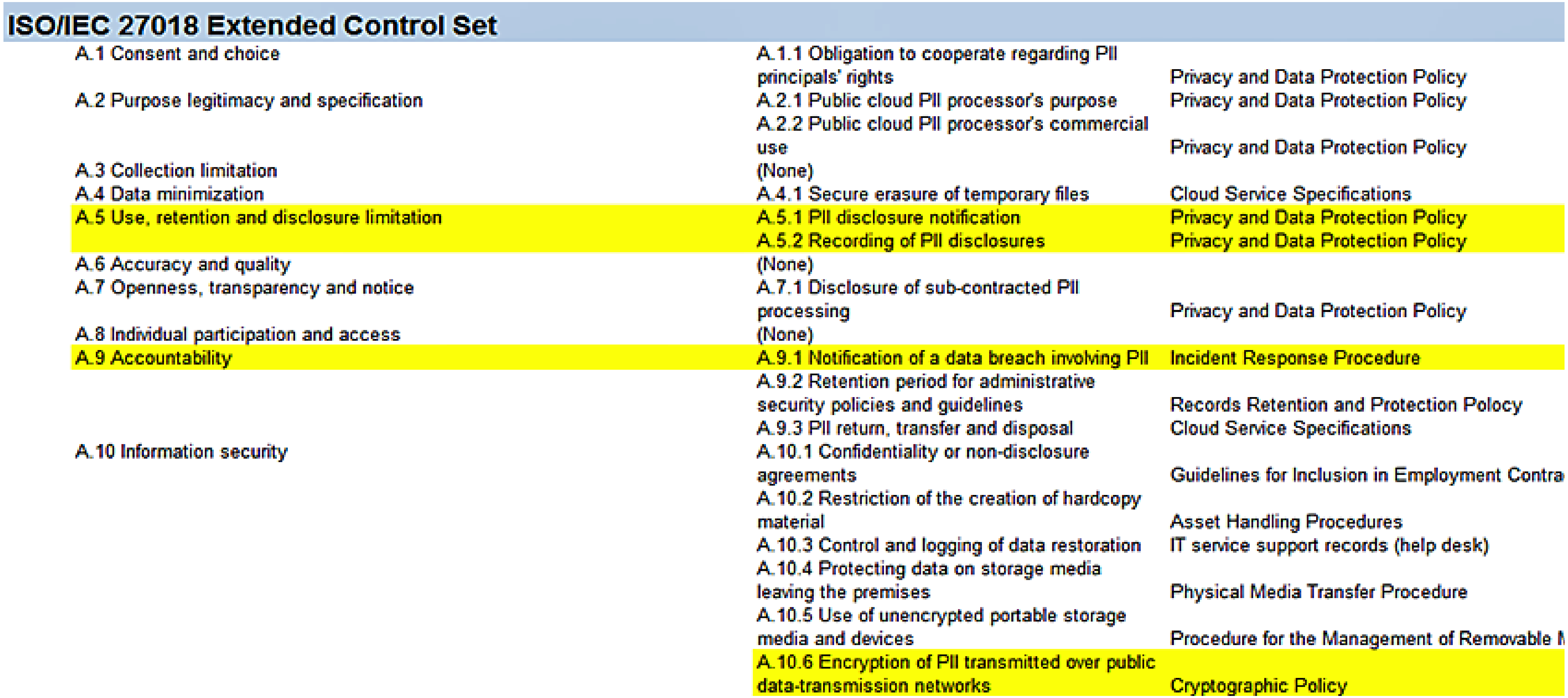


The standard provides cloud-based guidance on 37 of the controls in ISO/IEC 27002 but also features seven new controls.

- **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
	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?
- Top 10 Security & Privacy Threats in the Cloud
- Risk Assessment Methods for Cloud Applications
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

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

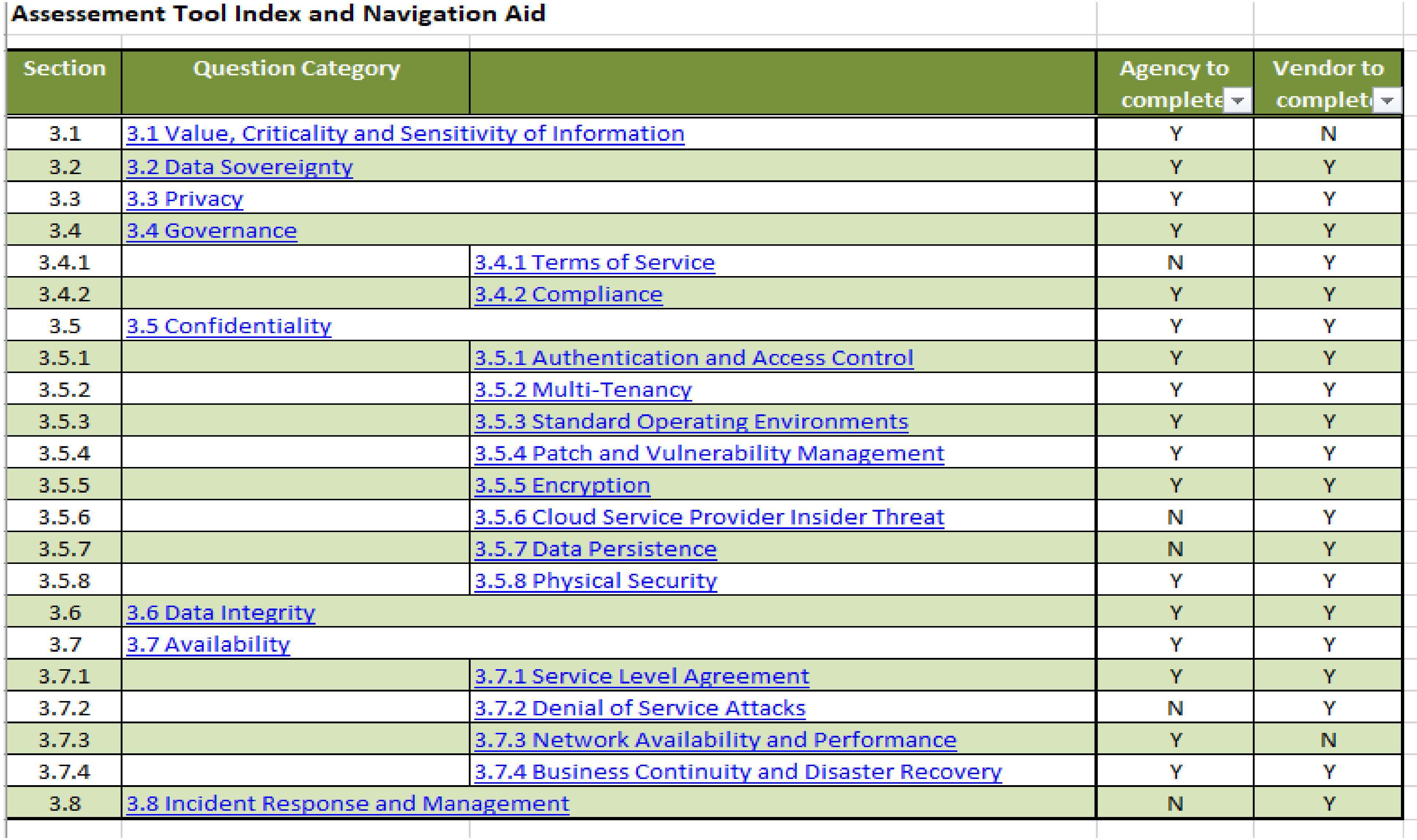
Summary Cloud Risk Findings and Mitigations

Risk Summary	Risk Description	Proposed control	Annex A / ISO 27017-18 Reference
Data in transit protection	Tthe integrity or confidentiality 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	Tthe 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

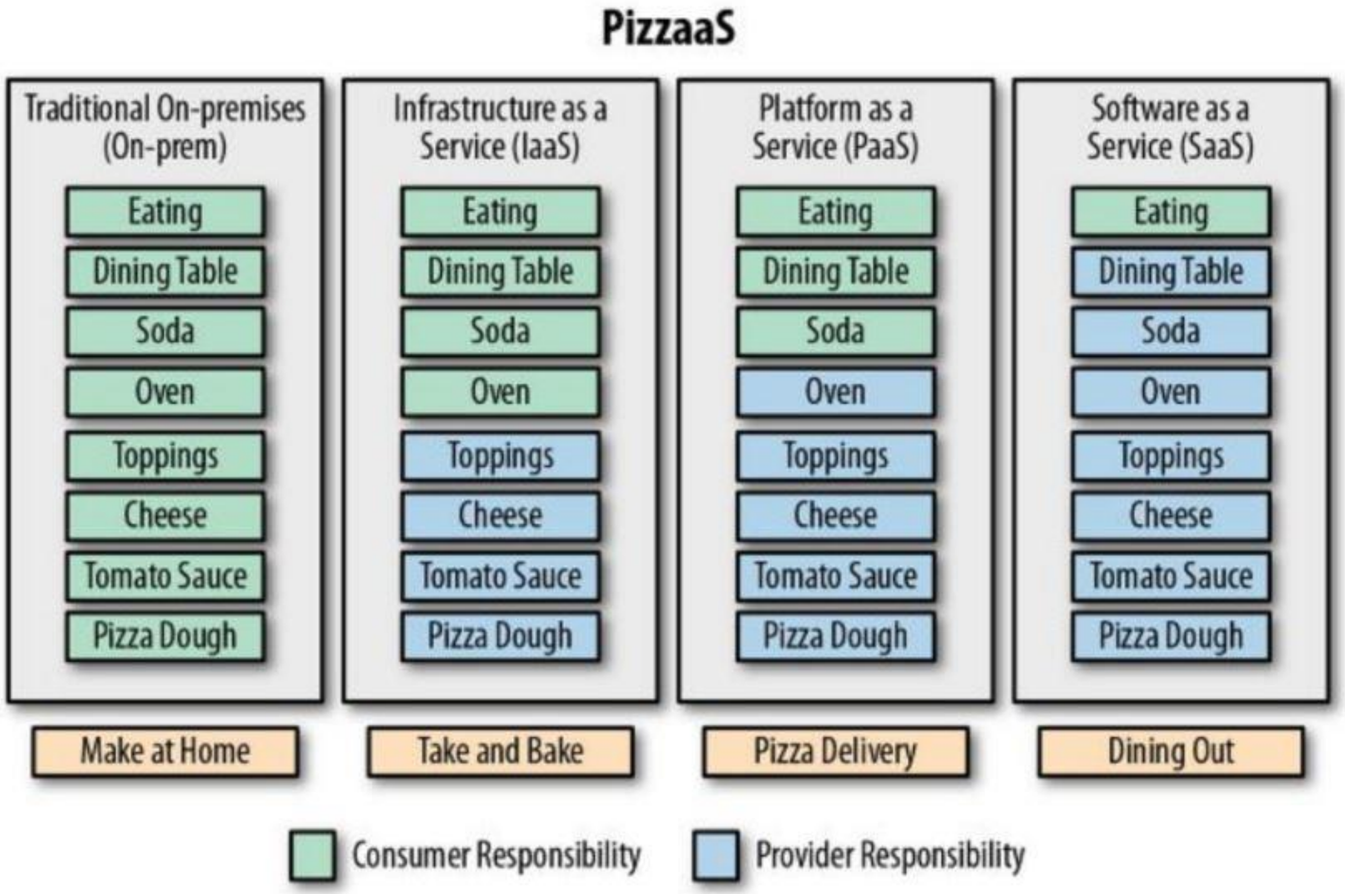
New Zealand National Cloud Security Risk Assessment – Example



Assessement Tool Index and Navigation Aid

Section	Question Category		Agency to complete	Vendor to complete
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

Pizza as a Service (PIZZaaS) – Simplified View of Cloud Security



PizzaaS

Traditional On-premises (On-prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟩 Eating	🟩 Eating	🟩 Eating	🟩 Eating
🟩 Dining Table	🟩 Dining Table	🟩 Dining Table	🟦 Dining Table
🟩 Soda	🟩 Soda	🟩 Soda	🟦 Soda
🟩 Oven	🟩 Oven	🟦 Oven	🟦 Oven
🟩 Toppings	🟦 Toppings	🟦 Toppings	🟦 Toppings
🟩 Cheese	🟦 Cheese	🟦 Cheese	🟦 Cheese
🟩 Tomato Sauce	🟦 Tomato Sauce	🟦 Tomato Sauce	🟦 Tomato Sauce
🟩 Pizza Dough	🟦 Pizza Dough	🟦 Pizza Dough	🟦 Pizza Dough
Make at Home	Take and Bake	Pizza Delivery	Dining Out

🟩 Consumer Responsibility 🟦 Provider Responsibility

Figure 1-7. Pizza as a Service

Practical Cloud Security (Chris Dotson), O'Reilly - http://shop.oreilly.com/product/0636920157199.do

Table of Contents

- Introduction – What are the Risks in the Age of Cloud Computing?
- Top 10 Security & Privacy Threats in the Cloud
- Risk Assessment Methods for Cloud Applications
- ISO Standards for Cloud Security and Privacy
- Tools and Techniques for Cloud Security Risk Assessments
- References + Q&A

References - Risk Assessment Methods for Cloud

- 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://snapshot.ict.govt.nz/guidance-and-resources/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

- Managing Privacy Risk in the Cloud (Deloitte)
  https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.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

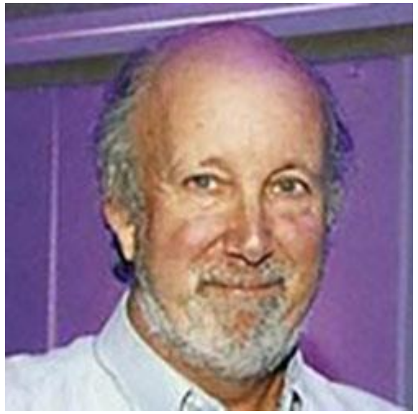
Tim Weil – Network Program Manager

Tim is a Security Architect/IT Security Manager with over twenty five years of IT management, consulting and engineering experience in the U.S. Government and Communications Industry. His technical areas of expertise includes FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security, enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.

He is a Senior Member of the IEEE and has served in several IEEE positions -

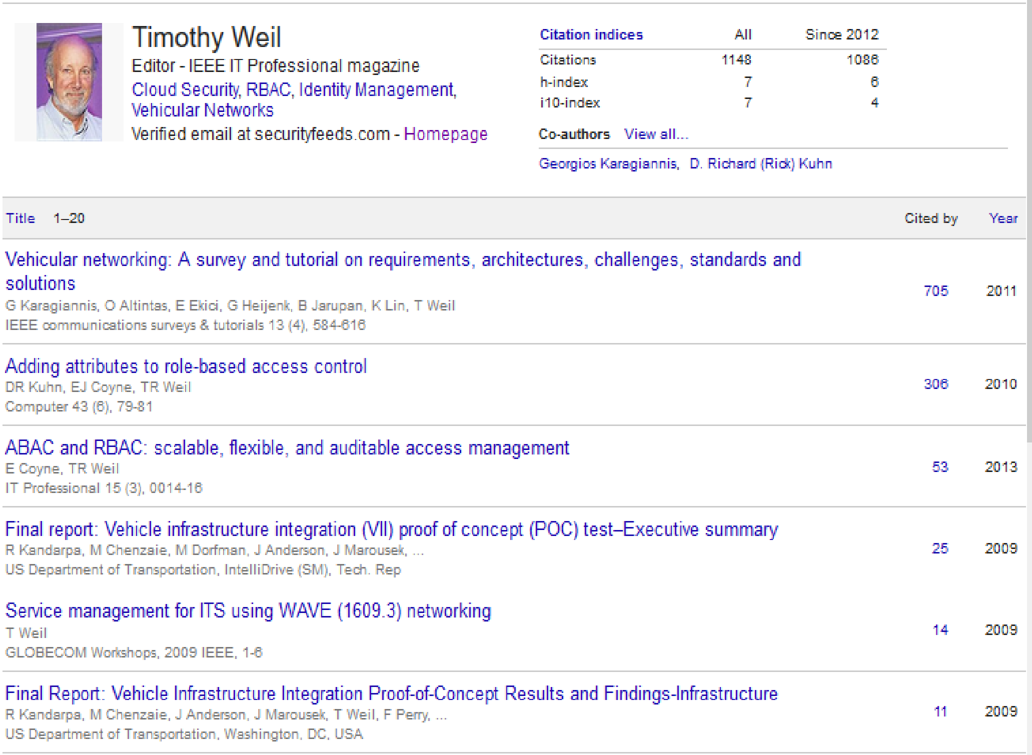
Chair of the Denver Section (2013); Chair of the Washington Section (2009); Cybersecurity Editor for IEEE IT Professional magazine. General Chair - IEEE GREENTECH Conference (2013)

His publications, blogs and speaking engagements are available from the website - http://securityfeeds.com



SCRAM SYSTEMS

A Writer's Life –



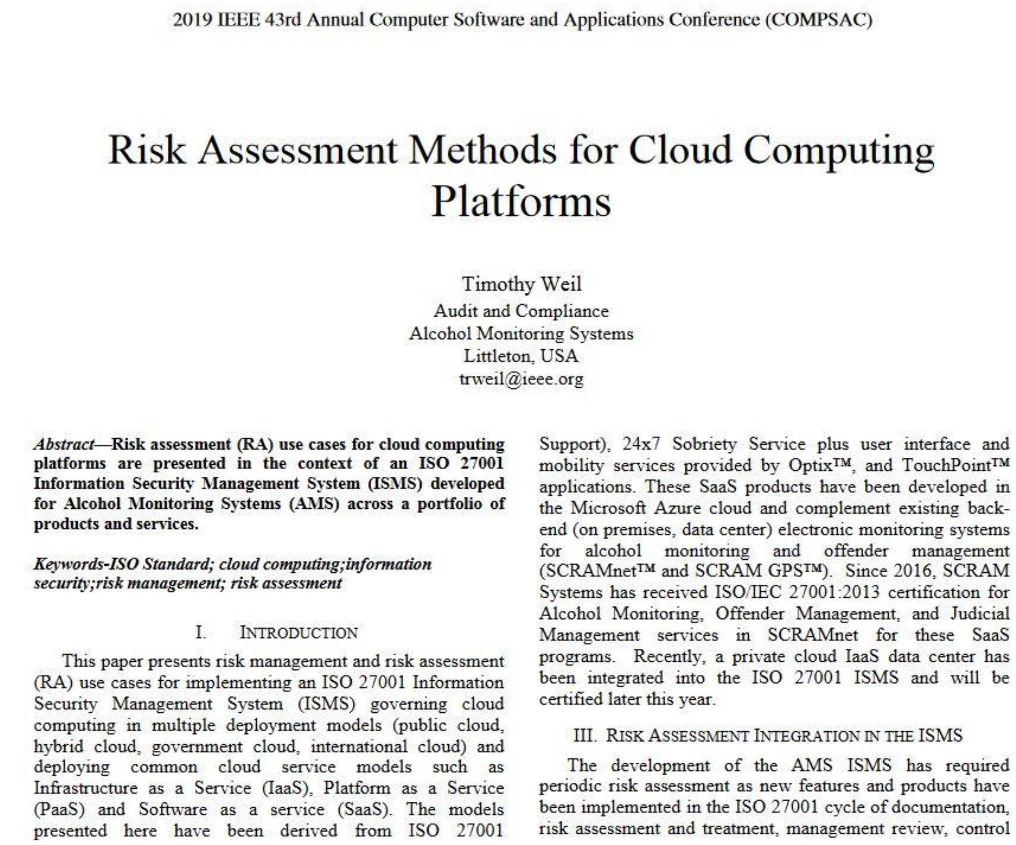
Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

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	Year
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	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
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	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
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	2009



2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)

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

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

SECURING IT

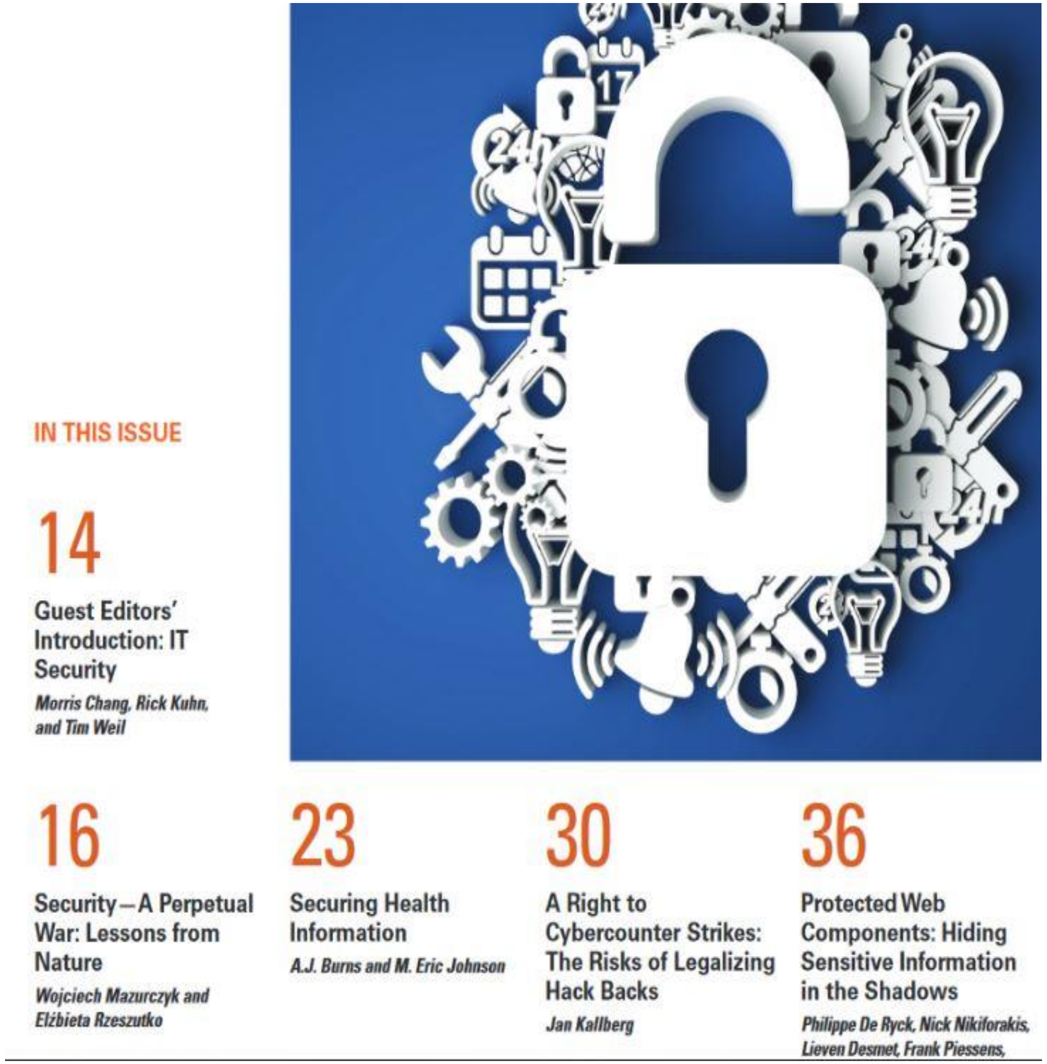
EDITORS: Rick Kuhn, US National Institute of Standards and Technology, kuhn@nist.gov
Tim Weil, Scram Systems, tweil.ieee@gmail.com

VPKI Hits the Highway

Secure Communication for the Connected Vehicle Program

Tim Weil, SCRAM Systems

IT Professional Security Issue (2015 vs 2018)



IN THIS ISSUE

14
Guest Editors' Introduction: IT Security
Morris Chang, Rick Kuhn, and Tim Weil

16
Security—A Perpetual War: Lessons from Nature
Wojciech Mazurczyk and Elżbieta Rzeszutko

23
Securing Health Information
A.J. Burns and M. Eric Johnson

30
A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs
Jan Kallberg

36
Protected Web Components: Hiding Sensitive Information in the Shadows
Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens,

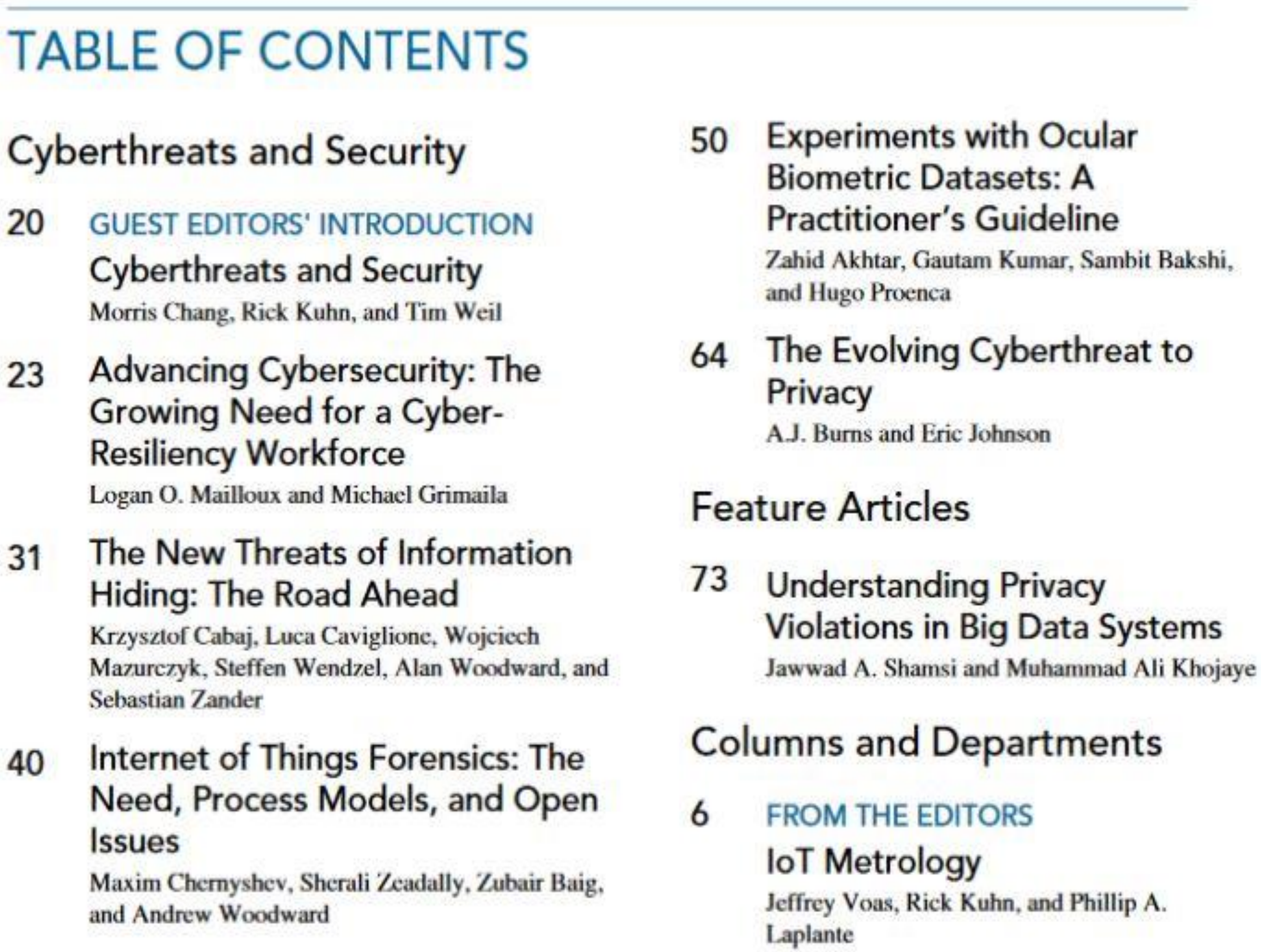


TABLE OF CONTENTS

Cyberthreats and Security

20 GUEST EDITORS' INTRODUCTION
Cyberthreats and Security
Morris Chang, Rick Kuhn, and Tim Weil

23 Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce
Logan O. Mailloux and Michael Grimaila

31 The New Threats of Information Hiding: The Road Ahead
Krzysztof Cabaj, Luca Caviglione, Wojciech Mazurczyk, Steffen Wendzel, Alan Woodward, and Sebastian Zander

40 Internet of Things Forensics: The Need, Process Models, and Open Issues
Maxim Chernyshev, Sherali Zeadally, Zubair Baig, and Andrew Woodward

50 Experiments with Ocular Biometric Datasets: A Practitioner's Guideline
Zahid Akhtar, Gautam Kumar, Sambit Bakshi, and Hugo Proenca

64 The Evolving Cyberthreat to Privacy
A.J. Burns and Eric Johnson

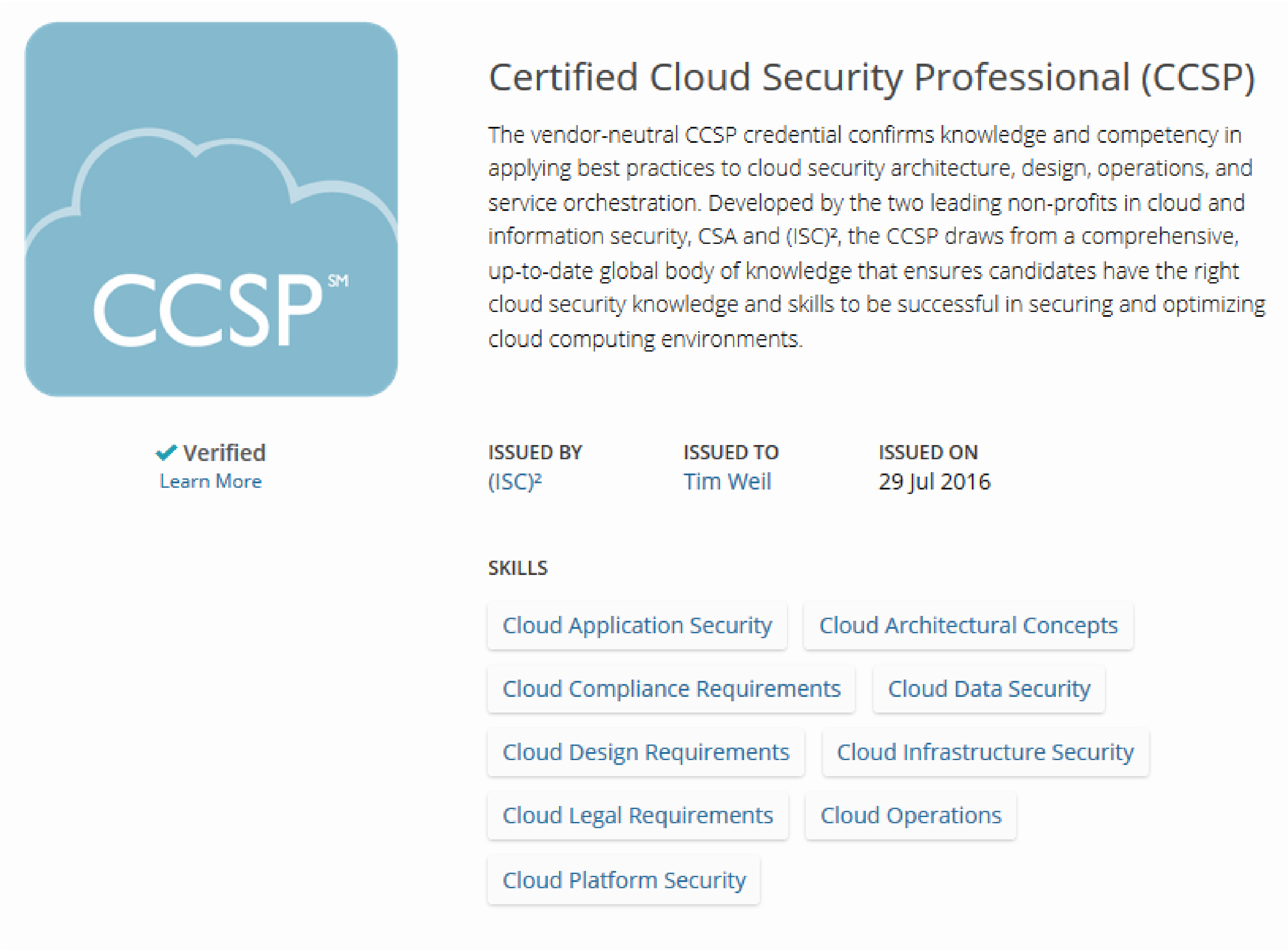
Feature Articles

73 Understanding Privacy Violations in Big Data Systems
Jawwad A. Shamsi and Muhammad Ali Khojaye

Columns and Departments

6 FROM THE EDITORS
IoT Metrology
Jeffrey Voas, Rick Kuhn, and Phillip A. Laplante

Certifying Cloud Security Practices



Certified Cloud Security Professional (CCSP)

The vendor-neutral CCSP credential confirms knowledge and competency in applying best practices to cloud security architecture, design, operations, and service orchestration. Developed by the two leading non-profits in cloud and information security, CSA and (ISC)^2, the CCSP draws from a comprehensive, up-to-date global body of knowledge that ensures candidates have the right cloud security knowledge and skills to be successful in securing and optimizing cloud computing environments.

✓ Verified
Learn More

ISSUED BY	ISSUED TO	ISSUED ON
(ISC)^2	Tim Weil	29 Jul 2016

SKILLS

Cloud Application Security
Cloud Architectural Concepts
Cloud Compliance Requirements
Cloud Data Security
Cloud Design Requirements
Cloud Infrastructure Security
Cloud Legal Requirements
Cloud Operations
Cloud Platform Security

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

Thank you for joining us!

Tim Weil – CISSP/CCSP, CISA, PMP
Network Project Manager
Alcohol Monitoring Systems

http://www.scramsystems.com
tweil@scramsystems.com
Linkedin - https://www.linkedin.com/in/tim-weil-a8b1952