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
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.
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).
Now What?

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

Private Cloud

Community Cloud

Public Cloud

Deployment Models

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
- Resource Pooling
- Measured Service
- Rapid Elasticity

Common Characteristics

- Massive Scale
- Homogeneity
- Virtualization
- Low Cost Software
- Resilient Computing
- Geographic Distribution
- Service Orientation
- Advanced Security
General Cloud Structure (SaaS PaaS, IaaS)

![Diagram of cloud computing structure showing service and deployment models.](image-url)

*Figure 1—NIST Visual Model of Cloud Computing Definition*
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

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)
Microsoft Azure Resources and Services (examples)
Amazon Cloud Resources and Services (examples)

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

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

Business Applications
- Alexa for Business
- Amazon Chime
- WorkMail

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

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

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


• Loss of Governance
• Vendor Lock-In
• Isolation Failure (multi-tenancy)
• Compliance Risk
  o Cloud Provider Compliance Evidence
  o 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

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
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

<table>
<thead>
<tr>
<th>Cloud Security Principle</th>
<th>Description of the Principle</th>
<th>Why this is Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data in transit protection</td>
<td>User data transiting networks should be adequately protected against tampering and eavesdropping.</td>
<td>If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.</td>
</tr>
</tbody>
</table>
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)

Elements of risk assessment

<table>
<thead>
<tr>
<th>Risk identification</th>
<th>Risk owner</th>
<th>Risk analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Threat</td>
<td>Vulnerability</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>NIST SP 800-30 Risk Assessment</th>
<th>ISO 27005 Information Security Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Characterization</td>
<td>Context Establishment</td>
</tr>
<tr>
<td>Threat Identification</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Vulnerability Identification</td>
<td>Risk Analysis – Risk Identification</td>
</tr>
<tr>
<td>Control Analysis</td>
<td>Risk Analysis – Risk Estimation</td>
</tr>
<tr>
<td>Likelihood Determination</td>
<td>Risk Evaluation</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Risk Treatment</td>
</tr>
<tr>
<td>Risk Determination</td>
<td>Risk Acceptance or</td>
</tr>
<tr>
<td>Control Recommendation</td>
<td>Risk Monitoring and Review, Communication and Redo</td>
</tr>
</tbody>
</table>
Risk Assessment Methods in the ISO 27001 Implementation (PDCA)
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

NIST SP 800-30 Risk Model
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.**
ISO/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!*

9/10/2019
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


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.

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:

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

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.

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

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

9/10/2019
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.
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

<table>
<thead>
<tr>
<th>Risk Summary</th>
<th>Risk Description</th>
<th>Proposed control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data in transit protection</td>
<td>The integrity or confidentiality of the data may be compromised while in transit.</td>
<td>User data transiting networks is adequately protected against tampering and eavesdropping by (SSL, TLS, VPN)</td>
</tr>
<tr>
<td>Asset protection and resilience</td>
<td>Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.</td>
<td>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)</td>
</tr>
<tr>
<td>Separation between users</td>
<td>Service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer’s data or service.</td>
<td>A malicious or compromised user of the service shall not be able to affect the service or data of another.</td>
</tr>
<tr>
<td>Governance framework</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Operational security</td>
<td>The service can’t be operated and managed securely in order to impede, detect or prevent attacks against it.</td>
<td>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.</td>
</tr>
<tr>
<td>Supply chain security</td>
<td>It is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.</td>
<td>The service provider shall ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.</td>
</tr>
<tr>
<td>Secure user management</td>
<td>Unauthorised people may be able to access and alter consumers’ resources, applications and data.</td>
<td>Your provider shall make the tools available for you to securely manage your use of their service.</td>
</tr>
<tr>
<td>Identity and authentication</td>
<td>Unauthorized changes to a consumer’s service, theft or modification of data, or denial of service may occur.</td>
<td>All access to service interfaces shall be constrained to authenticated and authorized individuals.</td>
</tr>
</tbody>
</table>

9/10/2019
## Summary Cloud Risk Scoring (Pre-Treatment)

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

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

![Pizza as a Service Diagram]

*Figure 1–7. Pizza as a Service*

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


References Used in This Presentation


  https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.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
A Writer’s Life –

Tech Day VI

A Writer’s Life –

Risk Assessment Methods for Cloud Computing Platforms

Timothy Weil
Audit and Compliance
Alcohol Monitoring Systems
Longmont, USA
tweil@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 Standards; cloud computing; information security; risk management; risk assessment

1. 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 Optex™, 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 (SCRAM® and SCRAM® OPT®). Since 2016, SCRAM Systems has received ISO/IEC 27001:2013 certification for Alcohol Monitoring, Offender Management, and Judicial Management services in SCRAM® 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

TABLE OF CONTENTS

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

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 Cavagnile, Wojciech Mazarczyk, 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 Proença

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 Khojaly

Columns and Departments

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

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