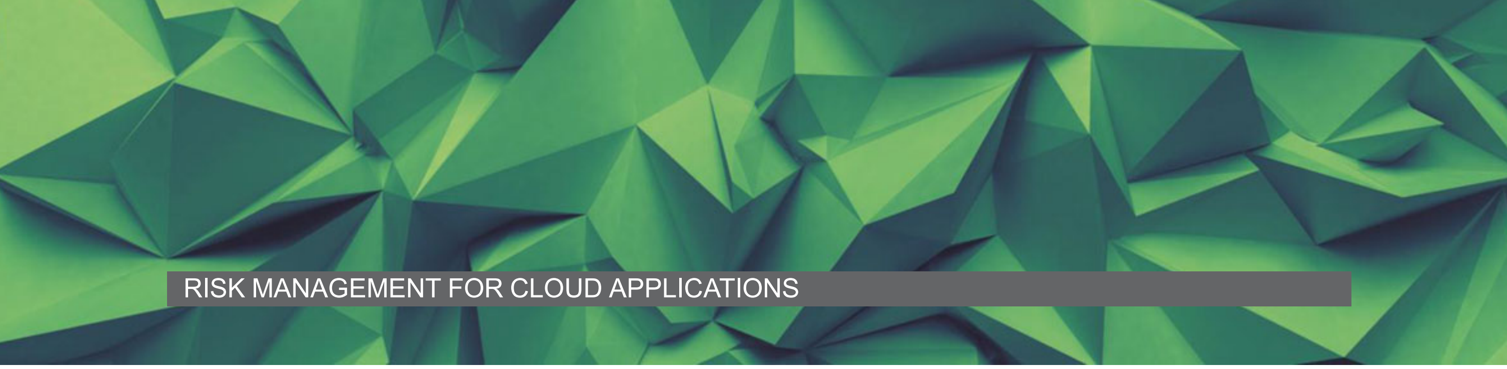


Taking Compliance to the Cloud—Using ISO Standards (Tools and Techniques)

Tim Weil
Alcohol Monitoring Systems
(SCRAM Systems)

WEATHER REPORT—CLOUDY WITH A CHANCE OF RISK

Risk assessment is an essential part of managing IT resources in nearly all applications, but successful risk management depends on adapting to the rapid changes in IT. One of the biggest changes in recent years has been the move to cloud computing to improve efficiency and reduce costs. The migration to cloud systems brings with it a need to update risk management practices as well. To help readers navigate this ever-changing landscape, this paper presents a risk-assessment approach for cloud computing software as a service applications derived from the ISO 27001 Information Security Management System (ISMS) standard and complemented by ISO practices for Cloud Security and Protecting Personal Information in the Cloud.

Risk assessment (RA) methodologies have a wide range of solutions and definitions in our industry and a key part of an ISMS is the management of risk. A simple model used in this exercise conforms to a definition of risk (per ISO standards) as "*the combination of the probability of an event and its consequence or the possibility that a particular threat will exploit a particular vulnerability of a data processing system"* (https://www.oxebridge.com/emma/dis-of-iso-9001introduces-a-fifth-definition-of-risk/). The scope of this RA has been developed in conjunction with Development Operations (DevOps) teams in the context of the following factors.

- How do we create a process that will create quality management methods that reduce process cycle time, reduce costs, increase application reliability, increase customer satisfaction, and increase profits?

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

- What areas need to be addressed to have a solid Dev/Ops concept for production deployments of our new cloud applications?
- What are the contractual obligations for privacy and security supporting the cloud-based applications?

To certify cloud applications (SaaS) and infrastructure services (IaaS), organizations must change. Traditional data center audits (PCI, HIPAA, FISMA, ISO 27001) are challenged by the risks, management, and security boundaries presented by moving commercial services to the cloud. What security and privacy requirements are to be addressed? To complement the ISO standards, best practices are described for conducting RAs and protecting personally identifiable information (PII) for newly offered cloud services. Methodologies assessed include FAIR,[4] the CSA cloud control matrix,[2] European Union Agency for Network and Information Security (ENISA),[1] NIST, and vendor-supplied risk-assessment tools. How do we tailor a complicated compliance spreadsheet, industry standards, and RA methods to get the job done? Get ready for another technology disruption.

TOP SECURITY AND PRIVACY THREATS IN THE CLOUD

To structure the approach for the cloud RA, several widely published sources have been evaluated. A brief list of recommended cloud security recommendations is given here.

European Union Agency for Network and Information Security

A 2009 RA report by ENISA includes contributions from a group of subject matter experts comprising representatives from industry, academia, and governmental organizations and provides an RA of cloud computing business model and technologies. While the report provides a set of practical recommendations, it is a 125-page document of comprehensive discussion and analysis.[1] In the cloud security guidelines, a list of the top eight cloud security risks describes the findings of the ENISA cloud computing RA. This report is widely discussed by online analyst blogs and articles (https://cloudtweaks.com/2015/03/top-cloud-security-risks/).

ENISA Top Eight Cloud Security Risks
Loss of governance
Vendor lock-in
Isolation failure (multitenancy)
Compliance risk
Cloud provider compliance evidence
Cloud provider audit by cloud customer
Management interface compromise
Data protection
Insecure or incomplete data deletion
Malicious insider

Cloud Security Alliance (CSA)—The Dirty Dozen: 12 Top Cloud Security Threats (2018)

The CSA is recognized as the leading group of industry, academia, and government entities dedicated to the awareness and recommendations of cloud security best practices (https://cloudsecurityalliance.org/about/). CSA operates the CSA Security, Trust, and Assurance Registry, which is a three-tiered provider assurance program for cloud security by providing guidelines for self-assessment, third-party audit, and continuous monitoring. The CSA consortium publishes an annual list of threat vectors applicable to the cloud computing environments.[2]

Cloud Security Alliance—12 Top Security Threats (2018)
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

National Cyber Security Centre (NCSC U.K.) Cloud Security Principles

The U.K. NCSC office, established in 2016, publishes a set of 14 design principles for building confidence and transparency in cloud-computing systems.[3]

National Cyber Security Center Cloud Security Principles
Data in transit protection
Asset protection and resilience
Separation between users (multitenancy)
Governance framework
Operational security
Personnel security
Secure development
Supply chain security
Secure user management
Identity and authentication
External interface protection
Secure service administration
Audit information for users
Secure use of the service

The structure of the NCSC cloud portal lends itself to a methodical review of these best practices by providing questions to be addressed for each subject. An example is given here (https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles).

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.

ISO STANDARDS FOR CLOUD SECURITY AND PRIVACY

Using the international standard for information security, i.e., ISO/IEC 27001, is an effective way to put in place an ISMS so that company objectives remain up to date and that processes, policies, and controls are continually improved.

ISO27001 is part of a family of information security guidance that provides enhanced and additional controls. The following are the examples.

ISO27002—More detail on all of the ISO27001 Annex A controls.
ISO27005—Risk assessment.
ISO27017—Application to cloud services.
ISO27018—Protection of PII in the cloud.
ISO22031—Business continuity management.

For the RA described in this paper, ISO 27001, ISO 27005, ISO 27017, and ISO 27018 were utilized (see notice board ISO standards portal—http://www.iso27001security.com/).

ISO 27017—Cloud Risk Management

The 27017 Annex A standard extends the control sets from ISO 27001 with an additional 37 control enhancements. Clarity is required between both cloud service provider (CSP) and customer on who is responsible for what. Following are the areas of security responsibilities with provider, some with customer, and some shared.[6]

- CLD.6.3.1: Requires agreement that information security roles associated with cloud services that are shared between CSP and customer have to be clearly laid out, recorded, and communicated.
- CLD.8.1.5: Clarity around what happens to assets in the cloud when the contract/agreement between the customer and provider is terminated.
- CLD.9.5.1: Provider must protect and separate the customer's virtual environment from other customers and external parties.
- CLD.9.5.2: Both provider and customer ensure virtual machines are configured and hardened to meet the security requirements of the organization.
- CLD.12.1.5: Lays out details on customer's responsibility to define, document, and monitor administrative operations and procedures related to the cloud environment.
- CLD.12.4.5: Lays out how the provider should facilitate the customer ability to monitor activity within their cloud computing environment.
- CLD.13.1.4: Addresses build standards and configurations that should be consistent so that the virtual network environment is in line with information security policies around the physical network.

ISO 27018—Protection of PII in Public Clouds

The ISO 27018 privacy requirements in the public cloud can be used as a “best practices” guidance standard for protecting PII. For small/medium businesses, there is a subset of controls to be considered.

I. Establish control objectives, controls, and guidelines for implementing measures to protect PII.
II. ISO 27018 guidelines are based on ISO 27002, but takes consideration of the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

ISO 27018 key definitions include the following:

I. PII Principal
   A. Person to whom the PII belongs or relates.
II. PII Controller
   B. Privacy stakeholder that determines purposes and means for processing PII other than persons who use data for personal purposes.
III. PII Processor
   C. Stakeholder that processes PII on behalf of and in accordance with the instructions of the PII controller.

As outlined in the ISO 27018 standard, the data processor has the following responsibilities.

- Providing customers with the means to meet their obligations under law in activities, such as accessing, amending, and erasing individuals’ PII.
- Informing customers as required by law to disclose any of their data, unless the data processers are prohibited from doing so.
- Details of disclosures must be recorded.
- Informing customers if subcontractors are processing their PII.
- Informing customers if their PII is subject to unauthorized access.
- To identify which country or countries are storing the customer’s PII.

RAs FOR CLOUD APPLICATIONS

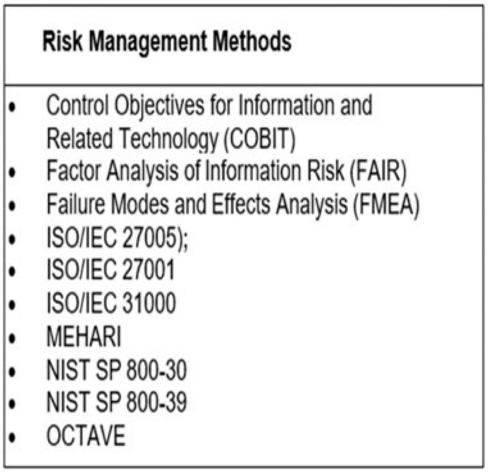
This process-based RA exercise was conducted against the hybrid cloud architecture components of Azure-based application systems (SaaS) and back-end data center system interfaces. An assessment of risk has been based on a consensus understanding of the current ISO 27001 ISMS and the new applications described here. Applicable standards (e.g., ISO 27001, ISO 27017 Cloud Security, and ISO 27018 Protecting PII in the Cloud) were considered, as well as management and organization impact from the adoption of Azure cloud technologies.

RAs for Cloud Applications—Where to Get Started?

In performing the cloud RA, determining the compliance specific context provides different reasons why the RA has been conducted. Different commercial control frameworks are listed here which may be applicable to your organization, such as industry/commercial solutions (such as ISO 27001/27002, PCI, NIST, NERC CIP). Alternatively, governmental compliance standards such as FISMA, FedRAMP, NIST, DFARS, CJIS, and HIPAA may also be addressed.

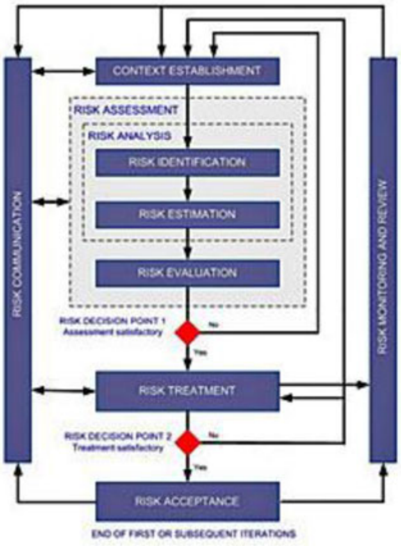
Best Practices Cloud Security and Privacy Risk

The RA and recommendations given below address security domains appropriate for the general scope of SaaS security in the Azure environment. In conversations with Dan Blum, Security Architect Partners a reasonable set of risk assessment questions came to my attention[7]



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



ISO 27005 Information Security Risk Management Process

1. Security governance, supplier management, and risk management: What governance, supplier management, and risk management organizational structures should be in place, and how should supporting processes and controls be right sized for the organization?
2. Application security: How should a company protect its applications from cyberattacks (i.e., OWASP top 10), ensure application program interface (API) security, and securely integrate on-premise system components with components in the Microsoft Azure environment?
3. Network security: How should the hybrid cloud applications environment be layered with traditional network security?
4. Data Security: How should customer data and personal information be protected (e.g., encryption, tokenization, obfuscation, data leakage prevention, etc.)?
5. Identity and access management: How should IAM technologies and practices be integrated?
6. Security monitoring: What monitoring technologies and practices are required?
7. Incident response: What processes and communication protocols are required to react and respond in the event of a data leakage event or other incidents?
8. Business continuity/Disaster recovery: How can the availability and resiliency of the hybrid cloud service be assured?

TOOLS AND TECHNIQUES

The processes reviewed for the cloud RA briefly summarized:

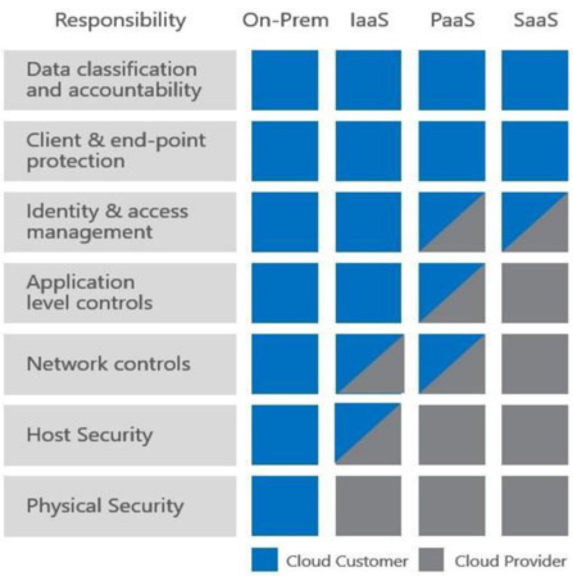
- cloud security shared responsibilities;
- CSP governance responsibilities;
- application-specific ISMS controls.

CLOUD SECURITY SHARED RESPONSIBILITIES

Different cloud service models affect the ways that responsibilities are shared between CSPs and customers1. The industry recognizes the following three primary cloud service models:

1) infrastructure as a service (IaaS);
2) platform as a service (PaaS);
3) software as a service (SaaS).

The figure shows how customers and providers share the identity and access management responsibility for Azure (an IaaS/PaaS offering). It also shows how customers and providers share the application-level controls and network controls for Azure (https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/).



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

Assessing a Cloud Security and Privacy Policy

A sampling of the documentation and controls has been evaluated. A representative list of control testing areas is given here.

ISO 27017 / 27018 Control Overlay (ISO 27001 Annex A).

I. A.05 Security policy
A. A.05.01 Information security policy
B. A.05.01.01—Policies for information security
II. A.06 Organization of information security
A. 06.01 Internal organization
B. 06.01.01—Information security roles and responsibilities
III. CLD.6.3—Relationship between cloud service customers and CSPs
IV. A.08 Asset management
A. A.08.01 Responsibility for assets
B. A.08.01.01 - Inventory of assets
C. A.08.02 Information classification
D. A.08.02.02—Labeling of information
V. A.09 Access control
A. A.09.02 User access management.

Azure Assessment Checklist

The cloud RA conducted an architecture component review of the applications and functional design. The tables shown here are components of the software as service architecture in Azure, which were reviewed for the RA.

Azure Assessment Checklist
Database services
SQL server database
MongoDB (NoSQL database)
Personal identifiable information
Access control and identity management
Privileged user accounts
Azure services
App services
WebApp
WebApi
Content delivery network
Azure infrastructure services
Storage
Service bus messaging
Traffic manager
Application insights
Visual studio team services (deploy software to Azure)
Azure deployment groups
Kudu (Git deployments to Azure services)
Azure app service deployment
VSTS to Azure deployment (compliance platform)
RA and treatment process
Appendix—Network diagrams
Appendix—Functional services
Appendix—High-level asset description (by departments)
High-level asset description—Network Development (NetDev)
High-level asset description—Network Operations (NetOps)
High-level asset description—Customer service
Application subsystems and third-party software
Appendix—Core services functional services
Middleware functional services and component subsystems
Middleware URLs and software components
Core services inventory (data center assets)
Appendix—Privacy policy (cloud apps)

Summary Findings and Risk Mitigations

This RA tables were derived from applying ten of the applicable NCSC cloud security principles to the Azure cloud applications using the interview methods described in this paper. Proposed control remediation and applicable cloud security/privacy clauses are shown as follows.

Risk Summary	**Risk Description**	**Existing Controls**	**Annex A / ISO 27017-18 Control Reference**
Data in transit protection	The 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)	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.	Access controls for MongoDB and SQL Server PII data in Azure Microsoft Azure Risk Assessment Diagnostic tool (Information Management)	A8.1.1 Inventory of assets (PII) A.8.2.1 Classification 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.	Microsoft Azure Risk Assessment Diagnostic tool	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 27001 ISMS for SaaS Applications	A.5 Information security policies
Operational security	The service can't be operated and managed securely to impede, detect or prevent attacks against it.	Application Insights (Azure) is used for cloud monitoring in development	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.	Contract with Microsoft Azure services Microsoft Azure Risk Assessment Diagnostic tool (Vendor Management)	A.15 Supplier relationships
Secure user management	Unauthorized people may be able to access and alter consumers' resources, applications and data.	Microsoft Azure Risk Assessment Diagnostic tool (Access Control)) Software Release Process for Cloud Applications	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.	Microsoft Azure Risk Assessment Diagnostic tool (Network Control)	CLD.12.1.5 Administrator's operational security
Secure service administration	An attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	Microsoft Azure Risk Assessment Diagnostic tool (Access Control)	A.9 Access control
Audit information for users	Consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	Microsoft Azure Risk Assessment Diagnostic tool (Logging and Monitoring)	A.12.4 Logging and monitoring CLD.12.4.5 Monitoring of Cloud Services

Risk Summary	Risk Description	Risk Type	Proposed Controls	Risk Level
Data in transit protection	The integrity or confidentiality of the data may be compromised while in transit.	Confidentiality	User data transiting networks is adequately protected against tampering and eavesdropping by (SSL, TLS)	Medium
Asset protection and resilience	Inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.	Integrity	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 Public Cloud)	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	A malicious or compromised user of the service shall not be able to affect the service or data of another. Multi-tenancy for SaaS applications shall be implemented	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	ISO 27017 (Cloud Security) and ISO 27018 (PII Protection in the Public Cloud) are recommended for limited adoption.	High
Operational security	The service can't be operated and managed securely to impede, detect or prevent attacks against it.	Integrity	The service needs to be operated and managed securely to impede, detect or prevent attacks. Good operational security shall not require complex, bureaucratic, time consuming or expensive processes.	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	The service provider shall ensure that its supply chain satisfactorily supports all the security principles which the service claims to implement.	Medium
Secure user management	Unauthorized people may be able to access and alter consumers' resources, applications and data.	Confidentiality	Your provider shall make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data.	Medium
Identity and authentication	Unauthorized changes to a consumer's service, theft or modification of data, or denial of service may occur.	Integrity	All access to service interfaces shall be constrained to authenticated and authorized individuals.	Medium
Secure service administration	An attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	Confidentiality	Manage the risks of privileged access using a system such as the 'principle of least privilege' Understand how management interfaces are protected and what functionality they expose	Medium
Audit information for users	Consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	Integrity	The Cloud Service Provider shall protect the audit information provided for consumers, determining how and when it will be made available, the format of the data, and the retention period associated with it	Medium

CONCLUSION

The RA approach of this paper is provided as a “tool in the toolbelt” in the process of obtaining ISO 27001 certification for cloud-based applications. The methods and techniques of this paper were conducted over a three-month period and have been peer reviewed at the recent Certified Infosec Conference 2018 (http://certinfosec.org) attended by an international group of compliance and audit professionals. By those standards, perhaps it can be used broadly across different CSPs. In closing, the remarks of my information security colleague Walt Williams must be read.

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

Most people do not understand that asset management risk management models have been failing us for years, and we are 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, which is in scope for the data privacy laws, are not an asset for any organization. It is an asset for various individuals. This information does not bring the organization any value, and because of that, it is often not protected.

The data simply have not 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 do not lead to organizations protecting all the data, just the data that drive business value, and therefore, we fail.

REFERENCES

1. “European Union Agency for Network and Information Security (ENISA) cloud security guidelines.” 2012. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
2. Cloud Security Alliance, “The dirty dozen: 12 top cloud security threats,” 2018. [Online]. Available: 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
3. “Implementing the cloud security principles,” 2016. [Online]. Available: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
4. “13 effective security controls for ISO 27001 compliance,” Microsoft Azure, White Paper. [Online]. Available: https://azure.microsoft.com/en-us/blog/13-effective-security-controls-for-iso-27001-compliance/
5. C. Singh Rastogi, “Cloud risk assessment using FAIR.” Mar. 2013. [Online]. Available: http://ijcst.com/vol41/1/adesh.pdf
6. M. Fuller, “Information security and data privacy in the cloud,” *Coalfire*, p. 33, Oct. 2017.
7. D. Blum “Security architects partners,” Available: https://security-architect.com/about-us/our-team/

ABOUT THE AUTHOR

Tim Weil is a Network Project Manager for Alcohol Monitorings Systems (Littleton, CO). He is a Senior Member of IEEE and Cybersecurity Editor for IT Professional magazine. Tim is an industry-certified security professional (CISSP/CCSP, CISA, PMP) and an experienced auditor of enterprise security systems (federal, commercial). He can be reached at trweil@ieee.org