Taking Compliance to the Cloud –
Using ISO Standards (tools and techniques)

Weather Report – Cloudy with a Chance of Risk

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 methodologies have a wide range of solutions and definition 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 consequences'. The scope of this Risk Assessment has been developed in conjunction with DevOps (Development-Operations) teams in the context of the following factors -

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

- 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 are the security and privacy requirements to be addressed? To complement the ISO standards, best practices are described for conducting Risk Assessments and protecting Personally Identifiable Information (PII) for newly-offered cloud services. Methodologies assessedt include FAIR [4], the CSA Cloud Control Matrix (CCM)[2], ENISA[1], NIST and vendor-supplied risk-assessment tools. How do we tailor a complicated compliance spreadsheet, industry standards and risk assessment 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 risk assessment, several widely published sources have been evaluated. A brief list of recommended cloud security recommendations is given here -

European Union Agency for Network & Information Security (ENISA)

A 2009 Risk Assessment report by ENISA includes contributions from a group of subject matter experts comprising representatives from Industry, Academia and Governmental Organizations, and provides a risk assessment of cloud computing business model and technologies. While the report provides a set of practical recommendations it is a 125-page documents of comprehensive discussion and analysis [1]. In the Cloud Security Guidelines, a list of the Top 8 Cloud Security Risks describes the findings of the ENISA Cloud Computing Risk Assessment. This report is widely discussed by online analyst blogs and articles.[1]

ENISA Tops 8 Cloud Security Risks
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

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

The Cloud Security Alliance (CSA) is recognized as the leading group of industry, academia and government entities dedicated to the awareness and recommendations of cloud security best practices[2]. CSA operates, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program for cloud security by providing guidelines for self-assessment, 3rd-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

[1] https://cloudtweaks.com/2015/03/top-cloud-security-risks/

[2] https://cloudsecurityalliance.org/about/

National Cyber Security Centre (NCSC UK) Cloud Security Principles

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

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

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

<table>
<tr><th colspan="2">Cloud Security Principle</th></tr>
<tr><td colspan="2">Data in transit protection</td></tr>
<tr><th>Description of the Principle</th><th>Why this is important</th></tr>
<tr><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>
</table>

ISO Standards for Cloud Security and Privacy

The international standard for information security, ISO/IEC 27001, was first published by the ISO and IEC in 2005 and was revised in 2013. The adoption of ISO/IEC 27001 is an effective way to put in place an information security management system (ISMS) to ensure that a company's objectives remain current and our processes, policies and controls are continually improved. ISO27001 is part of a family of information security guidance which provides enhanced and additional controls. Examples include -

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
ISO22031 – Business Continuity Management

For the risk assessment described in this article, ISO 27001, ISO 27005, ISO 27017 and ISO 27018 were utilized[3].

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 and customer, on who is responsible for what. Recognition that some security responsibilities with provider, some with customer, some shared [6].

- CLD.6.3.1: Requires agreement that information security roles associated with cloud services that are shared between cloud service provider 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 personally identifiable information (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 (SMB) there are a subset of controls to be considers.

- Establish control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII)

- 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 -

[3] See NoticeBored ISO standards portal - http://www.iso27001security.com/

- PII Principal
    - Person to whom the Personally Identifiable Information (PII) belongs or relates
- PII Controller
    - Privacy stakeholder that determines purposes and means for processing PII other than persons who use data for personal purposes
- PII Processor
    - 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:

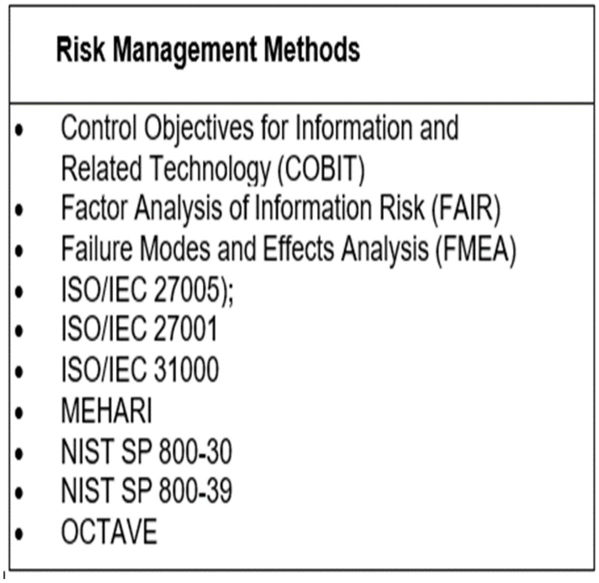
- Providing customers with the means to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- Informing customers as required by law to disclose any of their data, unless the Data Processer are prohibited from doing so
- Details of disclosures must be recorded
- Informing customers if sub-contractors 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

Risk Assessments for Cloud Applications

This process-based risk assessment exercise was conducted against the hybrid cloud architecture components of Azure-based application systems (SaaS) and back-end data center system nterfaces. 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

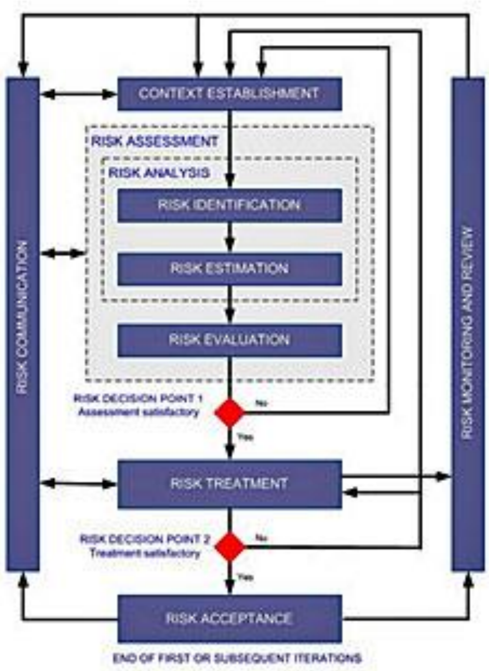
Risk Assessments for Cloud Applications – where to get started?

In performing the Cloud Risk Assessment (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. Industry/Commercial solutions such as (ISO 27001/27002, PCI, NIST, NERC CIP). Alternatively, Governmental Compliance Standards such as (FISMA, FedRAMP, NIST, DFARS, CJIS, HIPAA) may also be addressed.



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

Best Practices Cloud Security and Privacy Risk

Risk assessment and recommendations given below address security domains as appropriate for the general scope of SaaS security in the Azure environment:

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 (DLP), 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 used for the cloud risk assessment briefly summarized here

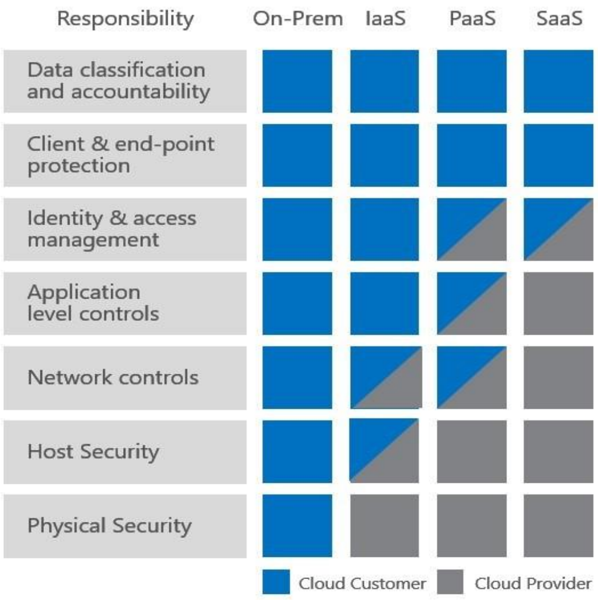
- Cloud Security Shared Responsibilities
- Cloud Service Provider Governance Responsibilities
- Application specific ISMS Controls

Cloud Security Shared Responsibilities

Different cloud service models affect the ways that responsibilities are shared between cloud service providers (CSPs) and customers1. The industry recognizes 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[4].



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 view of documentation used a sampling of the controls which have been evaluated. A representative list of control testing area are given here.

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

- A.05 Security policy
  - A.05.01 Information security policy
  - A.05.01.01 – Policies for information security
- A.06 Organization of information security
  - A.06.01 Internal organization
  - A.06.01.01 – Information security roles and responsibilities
- CLD.6.3 – Relationship between cloud service customers and CSPs

[4] https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

- A.08 Asset management
  - A.08.01 Responsibility for assets
  - A.08.01.01 - Inventory of assets
  - A.08.02 Information Classification
  - A.08.02.02 – Labelling of information
- A.09 Access Control
  - A.09.02 User access management

Azure Assessment Checklist

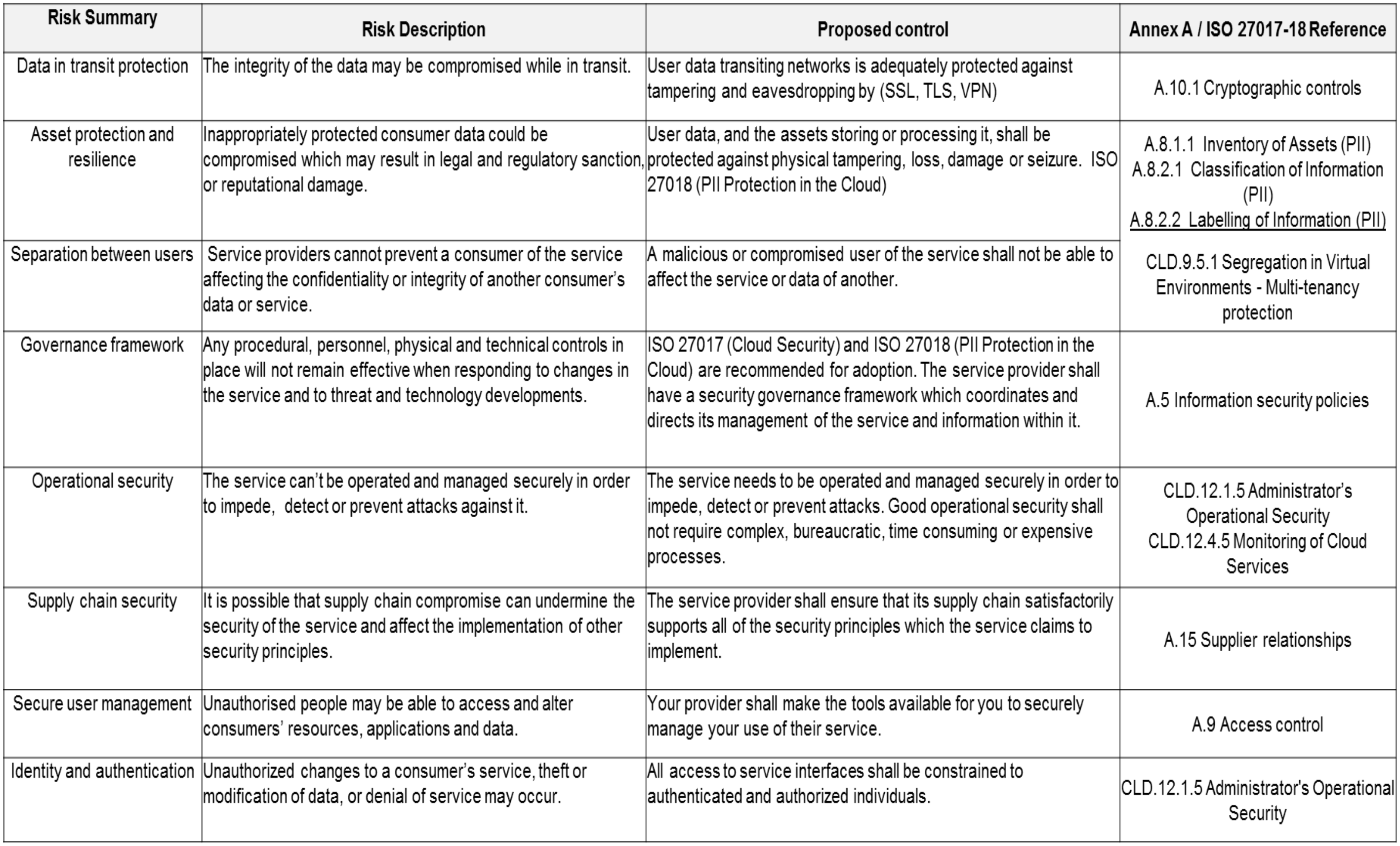
The Cloud Risk Assessment conducted an architecture component review of the applications and functional design. The tables shown here are components of the Software as a Service architecture in Azure which were reviewed for the risk assessment.

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

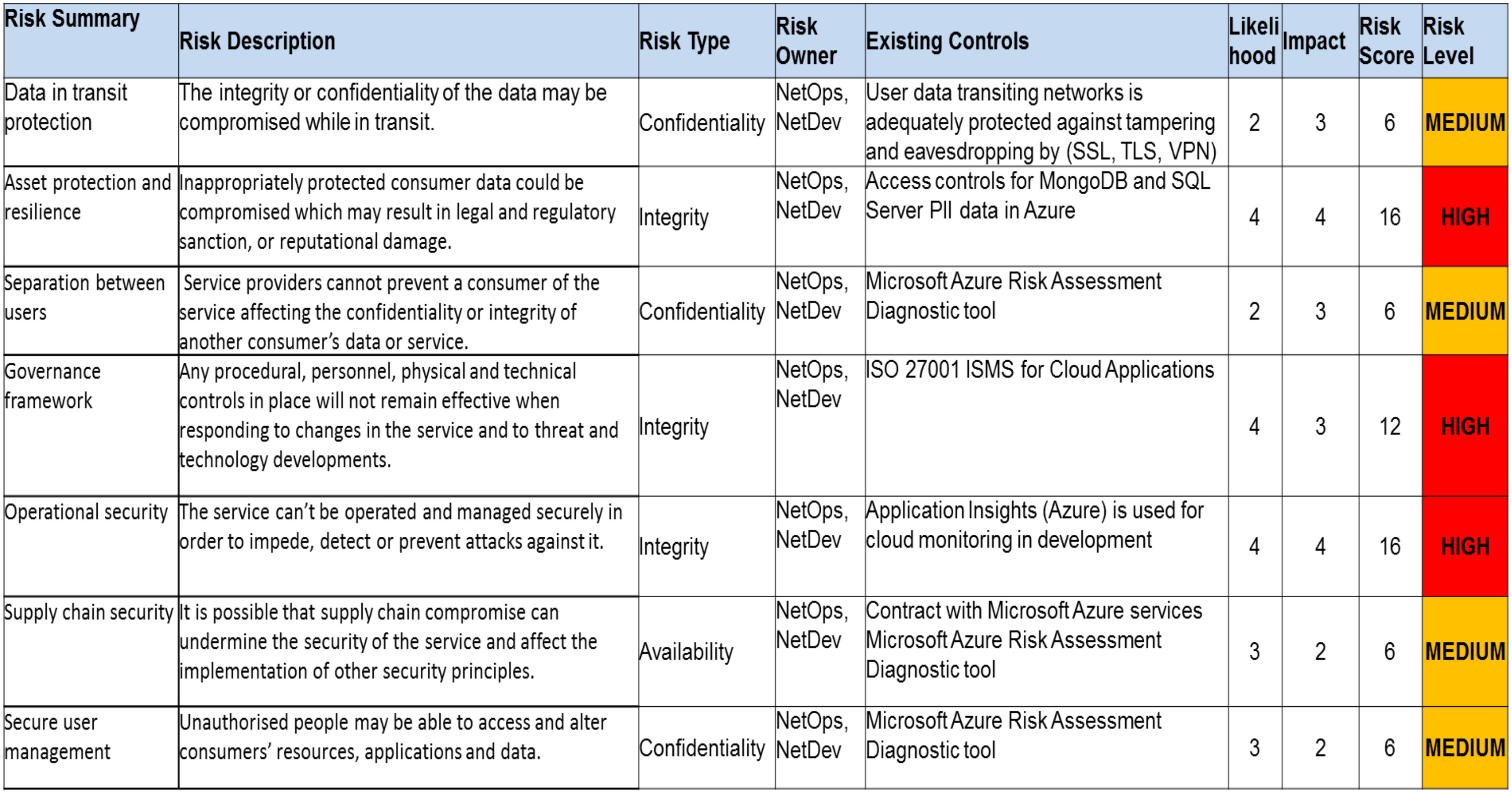
Azure App Service Deployment
VSTS to Azure Deployment (Compliance Platform)
Risk Assessment and Treatment Process
Appendix – Network Diagrams
Appendix – Functional Services
Appendix - High Level Asset Description (by Departments)
High Level Asset Description – Network Development (NetDev)
High Level Asset Description – Network Operations (NetOps)
High Level Asset Description – Customer Service
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 risk assessment tables were derived from applying 10 of the applicable NCSC Cloud Security Principles to the Azure cloud applications using the interview methods described in this article. Proposed control remediation and applicable Cloud Security/Privacy clauses are shown.



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



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

Conclusion

The risk assessment 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[5] attended by an international group of compliance and audit professionals. By those standards, perhaps it can be used broadly across different cloud service providers. In summary, the remarks of my information security colleague, Walt Williams must be read.

The Failure of Asset-Based Risk Assessments (Walt Williams)6

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.

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 therefore, we fail.

References

1. European Union Agency for Network & Information Security (ENISA) Cloud Security Guidelines - https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
2. 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
3. Implementing the Cloud Security Principles (NCSC) https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
4. 13 Effective Security Controls for ISO 27001 Compliance (Microsoft Azure White Paper) https://www.microsoft.com/en-us/download/details.aspx?id=50742
5. Cloud Risk Assessment Using FAIR (Rastogi, Chandra, Singh) - Online available - http://ijcst.com/vol41/1/adesh.pdf
6. Information Security and Best Practices for Privacy in the Cloud - Building Trust with ISO Standards and Codes of Practice, Michael Fuller (Coalfire) . Certified Information Security Conference (CISC16).

[5] http://certinfosec.org

[6] https://infosecuritymetrics.wordpress.com/

About Tim Weil

Tim Weil is a Senior Member of the IEEE and Security Editor for IT Professional magazine. In the areas of Vehicular Networks his work includes the IEEE 1609 (WAVE) standards, US DOT VII/Intellidrive and Connected Vehicle programs, author and speaker on topics in Security for Vehicular Networks (IEEE GLOBECOM). His interests include "Service Management for Vehicular Networks and Vehicular PKI. Weil is an industry-certified security professional (CISSP/CCSP, CISA, PMP) and chair of the IEEE Denver Communication Society Chapter. He can be reached at trweil@ieee.org.