

LIVE WEBINAR:

# How to Build and Qualify the Cloud for Regulated Applications: A Case Study

Host: Paul Fenton  
Presented by Gianna De Rubertis & Samuel Collier





# Presenters



## Director, Professional Services

- At Montrium since 2008
- Validation & Compliance Expert



## Product Integration & Deployment Coordination

- At Montrium since 2010
- Microsoft Azure SME



montrium  
where people · processes · technology connect



# Today's focus

- Introduction to Regulated Cloud
- Why Microsoft Azure?
- What did we qualify it for?
- What approach did we take?
- Technical and Procedural Steps
- Realizing true benefits in the cloud
- Conclusion & Recommendations





# Introduction to the regulated cloud

- **Many factors** are pushing the Pharmaceutical industry to adopt new strategies for computerized systems
- The need to maintain **quality, compliance, agility** and **flexibility** is still there
- **Cloud computing = New IT paradigm**
- Cheaper, Faster, More scalable, High availability, Better DR
- **No clear regulatory guidance** (yet)
- Dilemma: Innovation versus Compliance



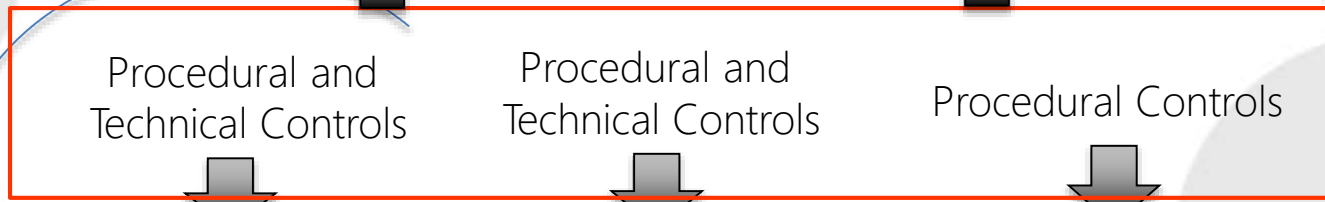


# Compliance challenges

- Pharma industry has typically been conservative and risk averse in relation to computerized systems compliance
- Pharma has very specific requirements around quality and compliance – cloud providers may not be pharma specific
- Traditional qualification focused on individual machines and specific hardware/software
- How to clearly identify and document system components
- Shared resources – unclear ownership
- Who is responsible for what
- Change control



# A New Paradigm



Cloud Vendor

SaaS Vendor

PharmaCo

Roles and Responsibilities

Roles and Responsibilities



Quality Agreement / SLA

Quality Agreement / SLA

Cloud=1 Large Machine





# Why we chose the Cloud?

- Can be deployed quickly
- Flexible pricing models
- Allows for significant scaling
- Allows for operational efficiencies
- Reduces Capex
- Alleviates internal IT burden
- Improves availability and disaster recovery





# Why we chose Microsoft Azure?

- Multiple data centers worldwide
- Significant capacity
- Certified through ISO and SOC
- Our team is trained and certified
- Competitive pricing
- Existing knowledge through the white paper we authored with Microsoft







# What approach did we take?

Define  
Needs

Implement  
Controls

Due  
Diligence

Qualify

Migrate

Monitor



montrium  
where people · processes · technology connect

1

Define needs, analyse risks  
and determine service &  
deployment models





# What we needed from the cloud

- A flexible, highly redundant infrastructure
- Easy to manage, with secure administrator access.
- Support for Microsoft Windows Server, SharePoint, Montrium Connect Applications.
- A transparent cloud framework which allowed visibility on data location, configuration, etc to support validation.
- Allowed the level of control required to meet compliance with regulations.





# Deployment Options With Azure

Within the Microsoft stack, there were several options for going Cloud:

- **SaaS – Software as a Service**

- Ex: Office 365. An application is available for use, however only minimal customizations are supported, and level of control over the application is low.

- **PaaS – Platform as a Service**

- Ex: Azure SQL. PaaS provides a data platform ready to use and develop cloud applications, however some limitations in application support apply.

- **IaaS – Infrastructure as a Service**

- Allows provision of network infrastructure, servers, cloud services on a highly flexible delivery platform.





# Why we chose IaaS?

The Azure IaaS provided the right balance of Cloud benefits while keeping the level of control we needed.

- Allowed flexibility to move applications to the cloud, while still retaining legacy system in our qualified Datacenter
- Still provided ease of management and scalability, with the security and access levels we needed.
- Completely Transparent to existing user base
  - No change of login credentials
  - No change to existing emails





# Determining a Deployment Model: Hybrid vs. Full Cloud

## Full Cloud

- Great for brand new environments
- No need for pre-existing infrastructure
- Start Fresh with no legacy applications

## Hybrid Cloud

- Allows quick adoption of core cloud benefits
- No need to decommission currently validated components
- Greater flexibility for legacy components
- Seamless transition for End Users





# Understanding the Risks

The risks we knew...

- Authentication concerns for management access
- Unknown compatibility for third-party applications
- Validation documents for on-premise didn't cover cloud-specific parameters.

Before we could write a meaningful risk assessment, we needed to prove we could mitigate high level risks...





# Planning for Our Cloud

## Proof of Concept

- Essential, as cloud presented challenges which required configuration updates.
- Some configuration can only be done on initial provisioning; cannot be altered afterwards.(Cloud services, regions, affinity groups, etc)
- Proof of concept helped dry-run new documents such as cloud configuration specifications, as well as the environment and applications.

## Identified Additional Risks:

- Performance profiles of cloud were different than on-premise
- Specialized knowledge required for managing automation







# Planning for Our Cloud

Still a Dev-Test-Prod world, but;

- In the Cloud, the environments can be de-provisioned, re-provisioned on demand.
- Costs associated with Dev and Test are reduced.
- All the benefits, for less.

Provides an opportunity to fully adapt to the Cloud

- New components and configuration required which does not exist on-premise.
- Cloud infrastructure simplifies provisioning, however automation is critical to success.



2

Implement appropriate internal procedural and technical controls





# Implementing Robust Controls

As with any system, an in-depth analysis identified key areas where controls are needed to mitigate risk.

- **Technical Controls** are required to implement system level measures to ensure the system functions as intended.
  - Example: Firewalls, Audit Trails, Authentication mechanisms
- **Procedural Controls** are required to mitigate risk when technical measure alone are insufficient
  - Example: Verification of Off-Site Backups, Change Controls





# The Technical Controls

- Two factor authentication required for management access
  - Though all management interfaces, not just Web Portal.
- Public endpoints closed, and access controlled via proxy array.
  - Direct connection off the internet are not allowed.
  - Additional firewalls and ACL's in place for tenant isolation
- Authentication of End Users via AD, where password policy is forced
  - (Lockouts, Bad Password Counts, Isolation and delegation of authority, etc)





# The Procedural Controls

- Some controls are very similar or the same as On-Premise applications.
  - Change Control
  - Logical Security
- Disaster Recovery
  - Very different in the cloud with Azure. A hybrid VM Disk redundancy (built-in), the Azure Backup vault in a different geographic region, and off-cloud traditional backups.
- New Work Instructions
  - Identify new work instructions for environment and application deployments are required for Cloud vs On-Premise.



3

Perform cloud provider due diligence





# “Qualification Guideline for Microsoft Azure”

- This white paper was published to assist Microsoft’s life science customers in establishing a qualification strategy for Microsoft Azure.
- Microsoft has been audited by third parties:
  - ISO/IEC 27001:2005 Certification
  - Service Organization Controls (SOC) Audit Reports
- Existing Microsoft customers may request access to these certifications and audit reports, subject to non-disclosure agreement (NDA) terms and conditions.





# Vendor Assessment

- The assessment was based on a review of third party audit reports of the Microsoft Azure platform and supporting infrastructure (Global Foundation Services).
  - We did not do a postal audit.
  - We did not do an on-site audit.
- Following Montrium's Vendor Management procedure, the outcome of the assessment was documented:
  - Microsoft is a qualified vendor.





# 4 Plan and execute qualification activities





# Steps to Regulatory Compliance

- 1. Risk Assessment**
- 2. Qualification Planning**
- 3. Specifications**
  - Requirements
  - System Description
  - Configuration Specifications
- 4. Verification / Testing**
  - Installation Qualification (IQ)
  - Operational Qualification (OQ)
- 5. Qualification Reporting**
  - Traceability Matrix
  - Qualification Summary Report





# Risk Assessment

- **Purpose:** To identify and manage risks that arise from failure of the system functions or components.
- The methodology is based on GAMP 5.
  - Identify GxP risk area.
  - For each risk area, identify risks and risk scenarios.
  - For each risk, assess Potential Harm, Likelihood, and Detectability.
  - Calculate Severity = Harm x Likelihood.
  - Calculate Risk Level = Severity x Detectability.
  - Describe measures already in place to mitigate the risk to an acceptable level (Low or Medium). Determine whether additional actions are required to mitigate the risk and describe them.



# Risk Assessment

Risk Area	Risk	Risk Scenario	Harm	Likelihood	Severity	Detection	Risk Level	Justification	Additional Action Required	Risk Mitigation Activity
Data Backup	Data Backup	Complete loss or corruption of data from primary data center due to force of nature or environmental protection failure (fire, flood, etc.).	High (3)	Low (1)	Med (3)	High (1)	Low (3)	A backup and restore procedure is in place and includes off-site data backup.	No	N/A
System Performance	Data Storage	Drives running out of space.	High (3)	Low (1)	Med (3)	High (1)	Low (3)	System is monitored for disk space usage. Automatic notifications are sent when threshold are reached.	Yes	Update Systems Maintenance procedure.





# Qualification Planning

- **Purpose:** To define the scope of qualification, required resources (including roles and responsibilities), and the quality assurance activities and deliverables that comprise the qualification effort.
- **Goal:** To generate objective and documented evidence that the Azure infrastructure has been installed and configured properly and functions according to specifications.





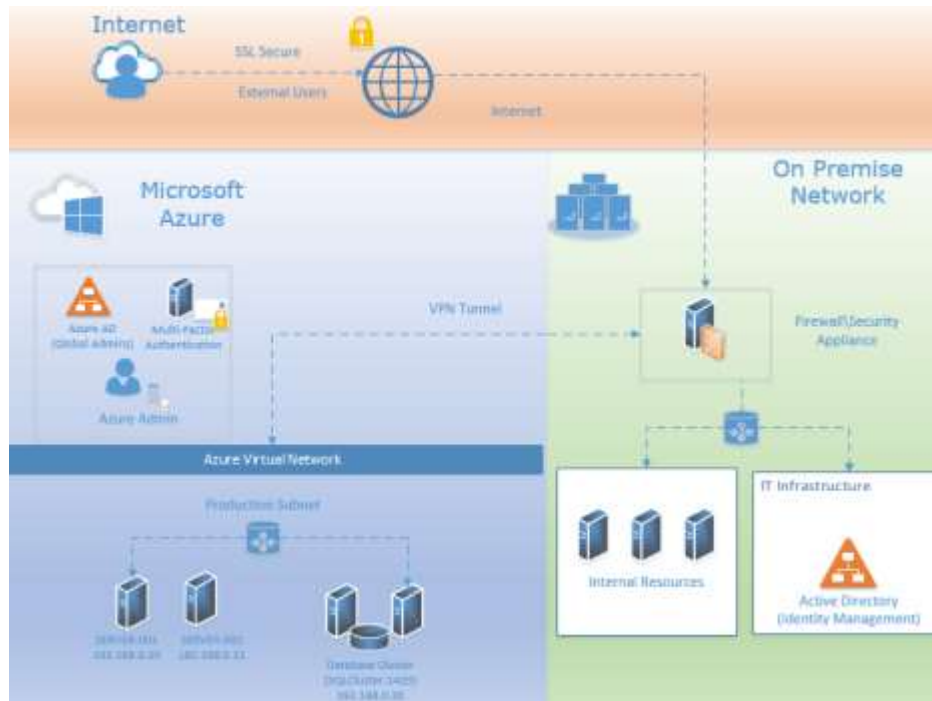
# Specifications (Requirements)

- **Purpose:** To define what Azure infrastructure should do in order to satisfy business needs and how Azure infrastructure should function in order to comply with applicable regulations.
  - **Business requirements:** System documentation, Training, Disaster recovery, Vendor management
  - **Functional requirements:** System monitoring, Data backup and recovery
  - **Security requirements:** Physical and logical security

Requirement ID	Requirement
REQ-AZU-0110	Access to the physical servers and related equipment (e.g. switches, hubs, routers, firewall) is controlled and monitored.
REQ-AZU-0420	Technical controls are in place for enforcing the use of strong passwords.

# Specifications (System Description)

- **Purpose:** To describe the main components of the Azure infrastructure and their interconnectivity.
  - Includes network diagram.





# Specifications (Configuration)

- **Purpose:** To define configurable system parameters and their assigned values that will allow the Azure infrastructure to operate as intended.


CS ID	Provider	Configuration	Enabled / Disabled	Configuration
CS-AUTH-010	AZT_MTCT_Admins_2 FA	Allow __ attempts during Multi-Factor Authentication call	Un-Checked	-
CS-AUTH-011	AZT_MTCT_Admins_2 FA	Say extention digits when prompting for extension (Server/SDK only)	Un-Checked	-
CS-AUTH-012	AZT_MTCT_Admins_2 FA	Caller ID Phone Number (US Phone Numbers Only)	N/A	8553308653
CS-AUTH-013	AZT_MTCT_Admins_2 FA	Two-Way Text Message TimeOut Seconds (Server/SDK Only)	N/A	60
CS-AUTH-014	AZT_MTCT_Admins_2 FA	Default One-Time Bypass Seconds	N/A	300





# Verification / Testing (IQ: Installation Qualification)

- The IQ Protocol governs the execution, documentation, and acceptance of all testing necessary to demonstrate that Azure infrastructure components are installed properly and configured according to specifications.
- IQ Test Scripts:
  - Infrastructure Configuration Verification
  - Standard Operating Procedure Verification
  - System Documentation Verification



# Verification / Testing (OQ: Operational Qualification)

- The OQ Protocol governs the execution, documentation, and acceptance of all testing necessary to demonstrate that Azure infrastructure functions according to specifications and is fit for its intended use.
- OQ Test Scripts:
  - Connectivity to Virtual Machines (VMs)
  - Connectivity to the Azure Management Portal: Multi-Factor Authentication
  - Connectivity to the Microsoft Azure PowerShell: Multi-Factor Authentication
  - Password Management and Controls



# Qualification Reporting (Traceability Matrix)

- The Traceability Matrix serves as a tool for ensuring that documented requirements are met.
  - Maps specified requirements to test scripts and/or applicable procedures.

Requirements		Test Script	Procedure	Comments / Rationale for not testing
REQ-AZU-0110	Access to the physical servers and related equipment (e.g. switches, hubs, routers, firewall) is controlled and monitored.	N/A	N/a	Access to physical servers and related equipment housed within Microsoft Azure is managed by Microsoft and certified according to the principles of ISO/IEC 27001:2005. This was confirmed by Montrium during its vendor assessment of Microsoft (for Azure – Microsoft cloud platform).
REQ-AZU-0420	Technical controls are in place for enforcing the use of strong passwords.	VTS-08	N/A	Functional verification of this requirement was performed for accounts managed by Azure Active Directory (i.e. administrators in the Azure Management Portal).



# Qualification Reporting (Traceability Matrix)

- The Traceability Matrix also confirms the verification of controls which were implemented to manage identified risks.

Risk Mitigation Activity		Test Script	Procedure	Comments / Rationale for not testing
R0280	Periodic testing of backup data recovery and verification of backup logs for successful backup jobs completion.	VTS-02	Backup, Data Archiving and Data Recovery procedure	N/A



# Qualification Reporting (Qualification Summary Report)

- The Qualification Summary Report confirms that required deliverables were produced:
  - Document title, document ID, approval date
- The report summarizes the execution results of the IQ and OQ test scripts, including a summary of issues encountered and their resolution.
- The report includes a statement of acceptance for use.
- The report was approved prior to the Azure infrastructure being released for operational use.

# 5

Plan and execute migration activities





# Planning Migration Strategy

## Users

- Hybrid Cloud ensured migration of users would be a non-issue.

## Application

- In Proof of Concept, determined we could use our existing web portal to link to the cloud environment.
- Using IaaS and hybrid ensured a smooth transition to the Cloud infrastructure.
- Only configuration updates to match the cloud were required, rather than re-development of entire applications.



# 6

## On-going monitoring and management







# On-going Management

Cloud platforms means monitoring is critical;

- Cloud platforms (Montrium Connect included) typically have SLA (service level agreements) which mandate a high percentage of uptime.
- All components are redundant, so there is no single point of failure.
  - Azure VM's are provisioned in different fault and upgrade domains
  - Fault Domains: A fault domain is a set of hardware where a single point of failure exists
  - Upgrade Domains: An upgrade domain is a location in which upgrades to the underlying cloud fabric will be done at different times to ensure uptime.





# Realizing the True Benefits of the Cloud

A highly available, flexible infrastructure was qualified for our applications

- Applications were moved to the Azure cloud with minimal impact to existing clients
- Goal of highly available, robust platform was achieved with a combination of technical and procedural controls.
- Controlled access and Two-Factor authentication makes the platform more secure than traditional private cloud

Scalability is achieved through monitoring, however

- Cloud is built for scalability; both vertically and horizontally
- Scalability exists, but is not always automatic
  - VMs can Autoscale, but there are some catches
  - SharePoint servers can scale vertically on-demand





# Conclusions and Recommendations

- There is significant value to be had from leveraging cloud technology
- It is important to define a clear qualification process for the organization which will ensure that you collectively meet regulatory requirements
- This process should document activities performed by the cloud vendor
- Regular re-evaluation of controls will ensure ongoing compliance





# Contact Details

## Montrium Inc.

507 Place d'Armes, Suite 1050  
Montreal (QC)  
H2Y 2W8  
Canada  
+1.514-223-9153

## Montrium S.A.2A

Rue Adolphe Diederich  
L-5820 Fentange  
Luxembourg  
+352.20.88.01.30

[info@montrium.com](mailto:info@montrium.com)

[www.montrium.com](http://www.montrium.com)



montrium  
where people · processes · technology connect