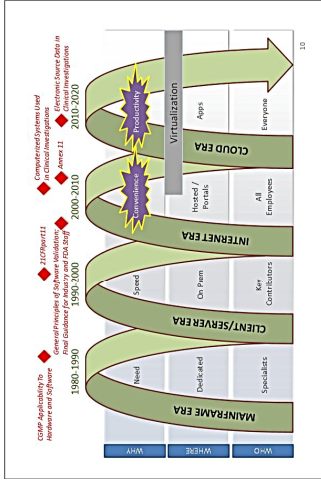


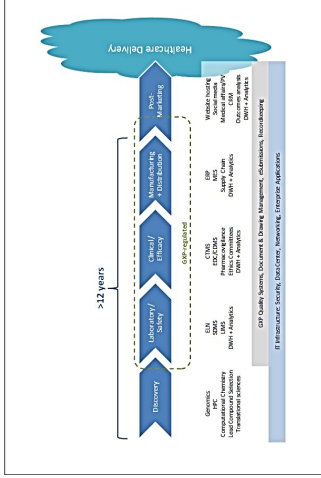
A Framework for the Adoption of Cloud Services in the Life Science Industry

Anders Vidstrup, IT Quality & Security Subject Matter Expert, NNIT A/S
Elford, Director, ISO 15 Security, Randi Rasmussen, Amazon Web Services
Chris Whalley, IT Risk & Compliance, and Health & Safety, Merck
Dan Dradiw, Director, IT Compliance & Risk Mgmt, Supplier Mgmt & Managed Services, Merck
Geoff Low, Lead System Architect, Medidata Solutions Inc
Rich Levin, Director, Clinical Development IT, Pfizer Inc
Rocco Timpano, Senior Director, IT Risk Management & Compliance, Pfizer Inc
Suzanne Studinger, Quality Assurance Studinger
Tony Hewer, Senior Quality & Regulatory Affairs Director, Medidata Solutions Inc
Walter Joppy, Vice President, IT Quality & Compliance, Johnson & Johnson
Robert Strelt, Senior Manager, Quality & Compliance possessing, Johnson & Johnson

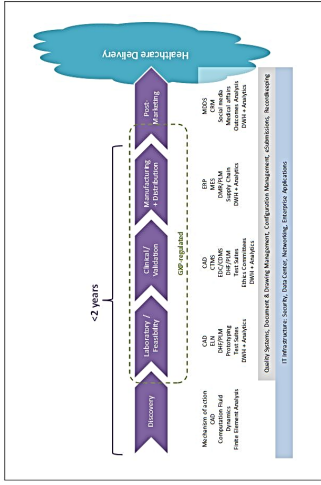
Cloud is a phase in the rapid evolution of information technology



Cloud-based Systems + Drug/Biologic Development



Cloud-based Systems + Medical Device/App Development



What are the barriers/challenges?

Ensuring adequate performance. The inherent limitations of the Internet apply to cloud computing. These performance limitations can take the form of delays caused by demand and traffic spikes, slowdowns caused by malicious traffic/attacks, and last mile performance issues, among others.

Ensuring adequate security. Many cloud-based applications involve confidential data and personal information. Therefore, one of the key barriers cloud providers have had to overcome is the perception that cloud-based services are less secure than desktop-based or in-house based services.

Ensuring basic mind-set and understanding of terminology. The cloud as a term is often understood as web-applications. It is important to appreciate that cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Ensuring diversified controls, roles and responsibilities. It is critical that organizations working on cloud solutions understand what their responsibilities are within each service model – client, supplier, sub-suppliers, also called the IT Supply Chain.

Ensuring a Quality Management System is fit for purpose. Each organisation in the IT Supply Chain must have a QMS that reflects its regulatory responsibilities and the technology solutions' capabilities.

The initial validation ensures that the solution is fit for intended use (and "inspection ready")

- After that, both the consumer and the supplier(s)/providers must sustain this fitness for use and inspection readiness.
- The ongoing operation and maintenance of a cloud solution requires that:
 - Documentation is always up to date.
 - Roles and responsibilities maintained.
 - Agreements with supplier/providers maintained – down the supply chain.
 - Operational controls are maintained by parties in the supply chain - around the IT Supply Chain.
 - Incident and problem management.
 - Change management and change control.
 - IT security management.
 - Security management.
 - Business continuity.
 - Disaster and recovery management.
 - Configuration management and related configuration review.
 - Document management.
 - Supplier/provider due-diligence.

Overall Regulatory Expectations

- Agencies will exercise enforcement discretion in regard to certain regulations - e.g. 21 CFR Part 11.
- Agencies will continue to enforce all predicate rule requirements, including requirements for recordkeeping.
- Requirements for validation:

- Accurate and complete records
- Protection of records
- Limiting system access
- Operational system checks
- Authority checks
- Device checks
- Training

The Consumer:

- Accountable
- Qualify direct supplier(s)/providers in context of solution.
- Business and process risk determination.
- IT quality, data integrity and security risk determination.
- Quantify organisation's level of maturity and skills.
- Adopt a risk-based validation strategy.
- Plan and execute such validation – ongoing

Design and Validation of a the solution:

- Supplier(s) must design and validate [their pieces of the] solution based on good engineering practices.
- The accountable consumer must validate the entire solution for its intended use.
- A risk-based approach should be used throughout the lifecycle – right along the supply chain.

Essential Characteristics

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Service Models

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own created applications using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have common concerns. It may be owned, managed, and operated by the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, government agency, or other organization, and it may exist on or off premises.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data, applications, and services to be shared between them.

Output from the working group

Ongoing development and refinement of framework

"Continuous publication"

Adopting industry practice and experience

Emerging guidances from regulated agencies

Table of Contents	
1	Introduction
2	Cloud Services
2.1	Essential Characteristics of Cloud Services
2.2	Cloud Service Models in Cloud Context
3	Cloud Services in the Life Science Industry
3.1	Cloud Considerations for Cloud Consumers and Managers
3.2	Organizational Policies and Standards
3.3	System Controls
4	Supplier Controls
5	Appendices
6	References

