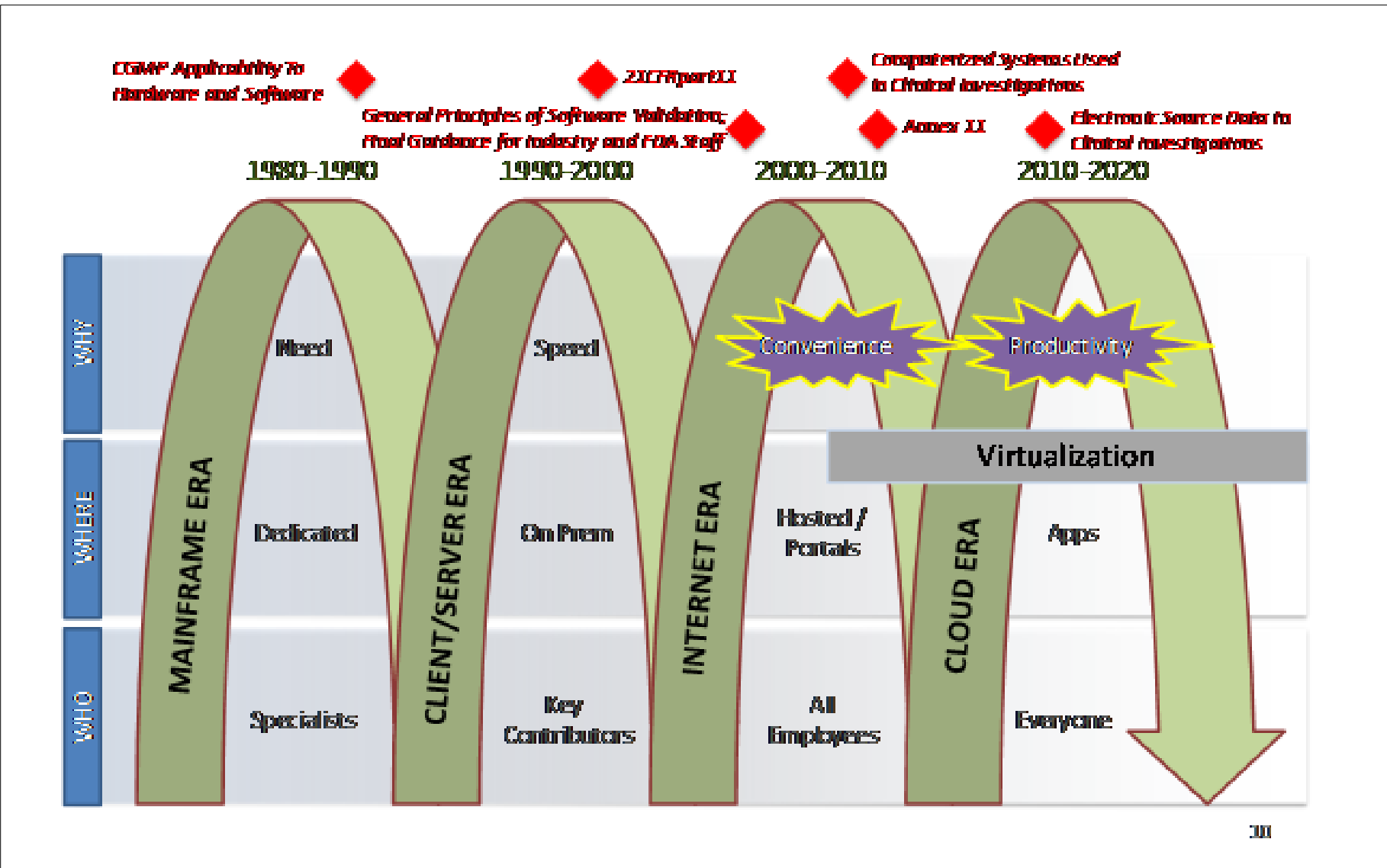


Project - Cloud Adoption in Regulatory Environments

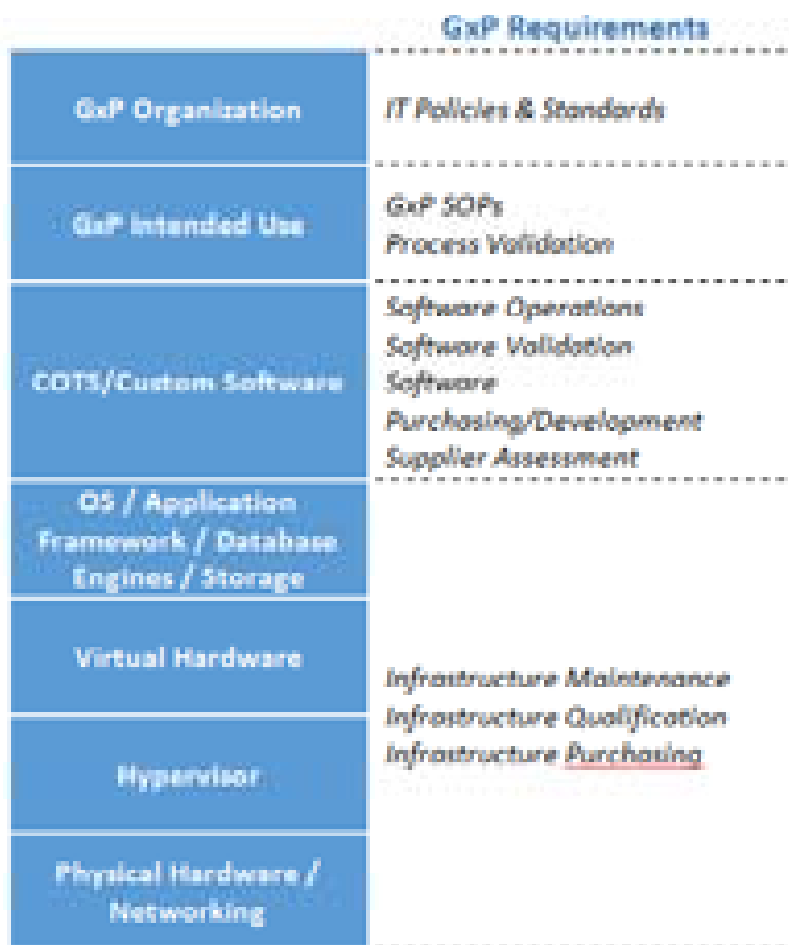
Anders Vidstrup, NNIT A/S - Chris Whalley, Amazon Web Services - Dan Dziadiw, Merck - Suzanne Studinger, Quality Assurance Studinger - Tony Hower, Medidata Solutions Inc - Robert Streit, Johnson & Johnson
Martijn Van Beelen, GSK - Evjatar (Evi) Cohen, Applan Corporation - Andrew Matteson, Applied BioMath

Cloud is a phase in the rapid evolution of information technology



Cloud Service Model

The following graphic depicts the basic elements of such an overall virtualized computer system in a "total stack" format geared toward GxP and its high-level aspects that are dealt with elsewhere in the framework.



The Cloud Service Customer Regulated Company

The following areas are important for the Customer to be aware of, when using Cloud Solutions:

- Accountable!
- Qualify* direct supplier(s)/Cloud Service Provider's in context of solution.
- Business and process risk determination.
- IT quality, data integrity and security risk determination.
- Quantify organization'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)/Cloud Service Providers must design and *validate* [their pieces of the] solution based on good engineering practices.
- The accountable Cloud Service Customer must *validate* the entire solution for its intended use.
- A risk-based approach should be used throughout the lifecycle – right along the supply chain.

IT Supply Chain in the Cloud Era

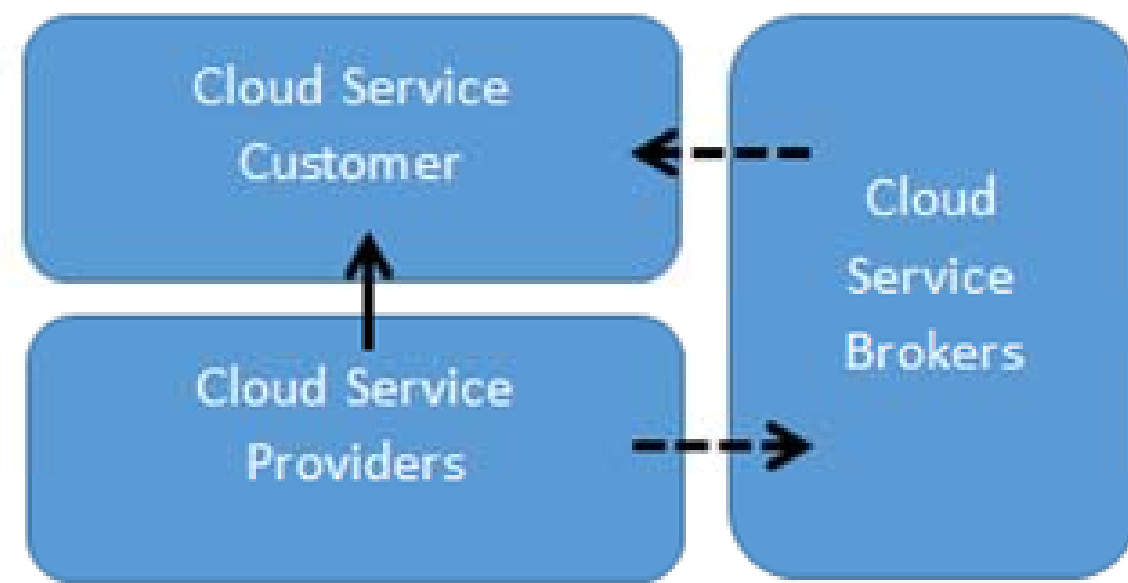
The Supply Chain of IT resources has grown over time from a simple, direct relationship between a purchaser and supplier to a set of relationships between purchasers, product suppliers, and service providers, as well as their downstream suppliers. The growth of Internet-based services and loosely coupled web services has further increased the complexity of computerized systems provisioning. The ability to manage this IT supply chain is now a critical success factor in business operations and compliance.

The terms used in cloud system roles are rapidly evolving as the cloud marketplace evolves, and for the purposes of this framework we have identified the basic roles based, here, from NIST and ISO.

- Cloud Service Customer - Party which is in a business relationship for the purpose of using cloud services.
- Cloud Service Provider - Party which makes cloud services available.
- Cloud Service Broker - Cloud Service Partner that negotiates relationships between Cloud Service Customers and Cloud Service Providers.

An organizational entity can play more than one role at any given contractual situation.

The figure to the right provides a simplistic model.



Output from the working group

In adopting cloud-based solutions for GxP workloads, understanding the essential characteristics of cloud services and solutions is important for determining the applicability of GxP requirements to specific Cloud Service Providers and/or cloud-based solution models.

It is essential for compliance with e.g. 21 CFR Part 11, FDA guidance on Data Integrity and EU Annex 11, that controls are in place when using different Cloud Services and Cloud Service Providers.

The main conclusion is that despite technology having undergone many evolutionary steps, the fundamental principles associated with regulatory predicate rules and good engineering practices still, very much, apply and can be fully exploited.

In the current edition of the framework, the following topics have been further elaborated and outlined in documents on their own:

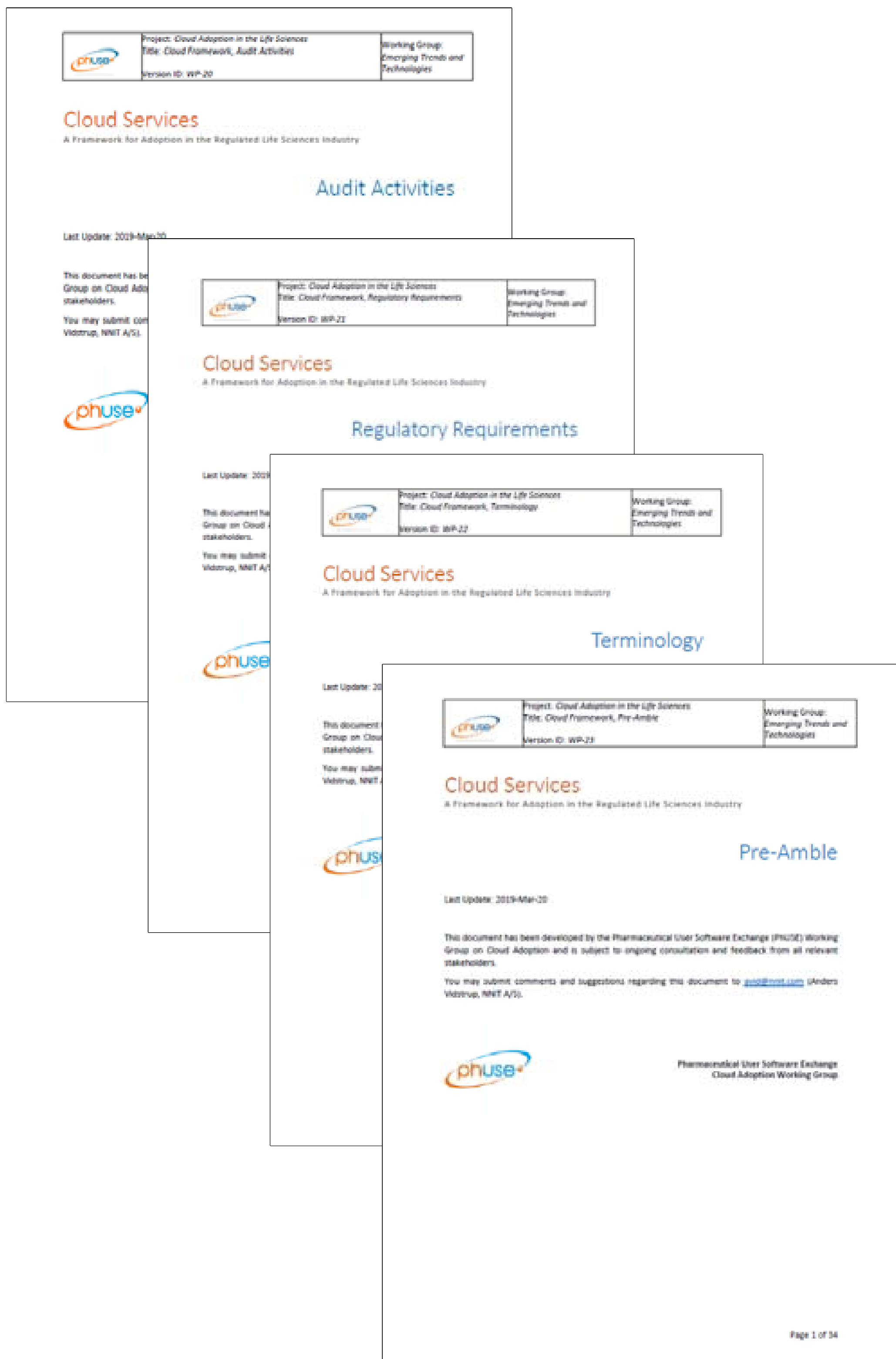
- Cloud Services – Pre Amble (main document)
- Cloud Services – Terminology
- Cloud Services – Audit Activities
- Cloud Services – Regulatory Requirements

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

Both the Cloud Service Customer and the supplier(s)/Cloud Service 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, include Data Integrity
- Roles and responsibilities maintained.
- Agreements with supplier/providers maintained – down the supply chain.
- Operational controls are maintained by parties in the supply chain - around:
 - Incident and problem management.
 - Change management and change control.
 - IT quality risk management.
 - Security management.
 - Business continuity.
 - Disaster and recovery management.
 - Configuration management and related configuration review.
 - Document management.
 - Supplier/Service Cloud Provider due-diligence.



Regulatory requirements traced to IT terms and Cloud Services

Topic	Regulations	MAAS	PAAS	SAAS
Audit Trail, Electronic records	21 CFR Part 11, §11.10(a) and 11.10 (e) Annex 11, §8.2, §9 and §12.4		X	X
Audit Trail, Time stamp	21 CFR Part 11, §11.10 (e) Annex 11, §8.2, §9 and §12.4	X	X	X
Audit Trail, Record Management	21 CFR Part 11, §11.10(a) 21 CFR Part 11, §11.10(c)		X	X
Backup	21 CFR part 211, §211.68(b) Annex 11, §7.2	X	X	X
Change and Configuration Management	21 CFR Part 11, §11.10(k)(2) Annex 11, §1, §4.2 and §10	X	X	X
Change and Configuration Management, System overview	Annex 11, §4.3			X

Topic	Regulations	MAAS	PAAS	SAAS
Incident and Problem Management	21 CFR Part 11, §11.300(d) Annex 11, §13	X	X	X
Periodic Review	21 CFR part 211, §211.22 (implicit by cGMP) Annex 11, §11	X	X	X
Personnel Qualification, electronic signature	21 CFR Part 11, §11.10(j) Annex 11, §2 and §14	(X)	(X)	X
Personnel Qualification, general	21 CFR Part 11, §11.10(i) Annex 11, §211.25(a)	X	X	X
Physical Security	21 CFR part 211, §211.28 (and §211.122(d)) Annex 11, §7.1, §12.1 and §12.3	X	X	X
Record Management, availability	21 CFR Part 11, §11.10(b) and §11.10(c) Annex 11, §7.1, §8.1, §8.2 and §17	X	X	X

Topic	Regulations	MAAS	PAAS	SAAS
Record Management, electronic signature	21 CFR Part 11, §11.50(a), §11.50(b) and §11.70 Annex 11, §14	(X)	(X)	X
Record Management, general	21 CFR Part 11, §11.10(h) 21 CFR part 211, §211.180 and §211.182 Annex 11, §1, §5, §7.1, §9, §12.4 and §17	X	X	X
Remote Access, e.g. in clinical trials	21 CFR Part 11, §11.10(f) and §11.10(g) Annex 11, §9 and §6	X	X	X
Systems Development, general	21 CFR Part 11, §11.10(e) Annex 11, §1, §4.1, §4.2, §4.4, §4.6 and §4.7	(X)	X	X
Systems Development, Incident- and problem management	21 CFR Part 11, §11.10(h) Annex 11, §4.2 and §13	X	X	X

Topic	Regulations	MAAS	PAAS	SAAS
Systems Development, Infrastructure	21 CFR Part 11, §11.10(a), §11.10(d), §11.100(a) and §11.200(a) Annex 11, §1, §4.1, §4.2, §4.4, §4.6 and §4.7	X	X	X
Third Party Management	21 CFR part 820, §820.22 and §820.50 Annex 11 - §3.1	X	X	X
User Access Management, general	21 CFR Part 11, §11.10(d), §11.10(g), §11.100(b), §11.300(a), §11.300(b), §11.300(c), §11.300(d), §11.300(e) Annex 11, §12.1, §12.2, §12.3, §15	X	X	X
User Access Management; electronic signature identity	21 CFR Part 11, §11.200(a) and §11.200(b)	(X)	X	X
User Access Management; Record Management	21 CFR Part 11, §11.100(a)	X	X	X