conformity

keeping it compliant

Outsourcing and the Cloud - Ensuring Quality and Compliance

Sion Wyn
Conformity Ltd.
+44 (0) 1492 642622
sion.wyn@conform-it.com

Overview

- Quality & Compliance in the Cloud
- Regulations and Guidance
- A Proposed Approach

Quality and Compliance in the Cloud

- Ensuring **patient safety, product quality, and data integrity…**

- …while exploiting the potential benefits of cloud computing (and wider aspects of outsourcing)

Sources of Information…

National Institute of Standards and Technology

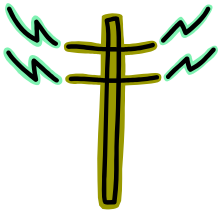
U.S. Department of Commerce

http://www.nist.gov

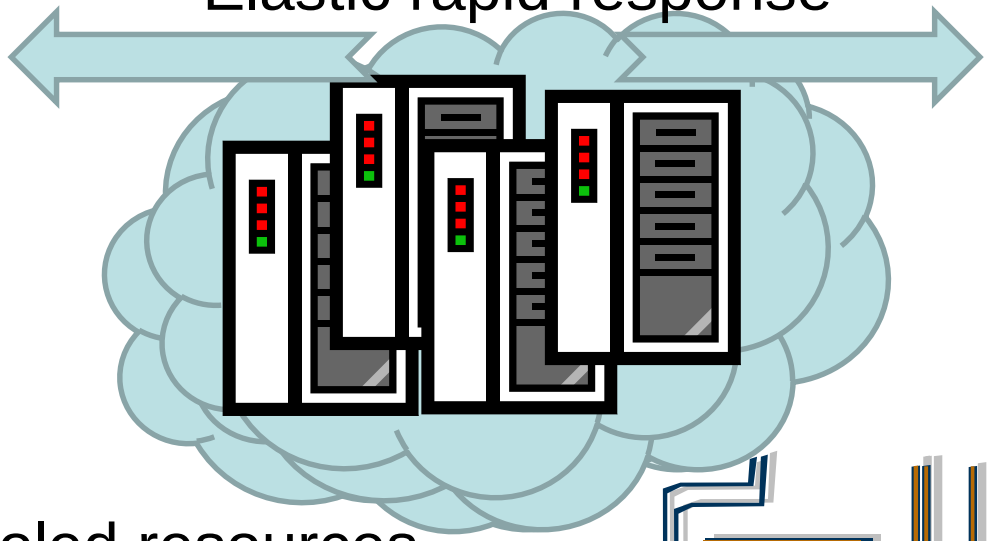
www.enisa.europa.eu

https://cloudsecurityalliance.org

"*Cloud computing is the utility of the future*"

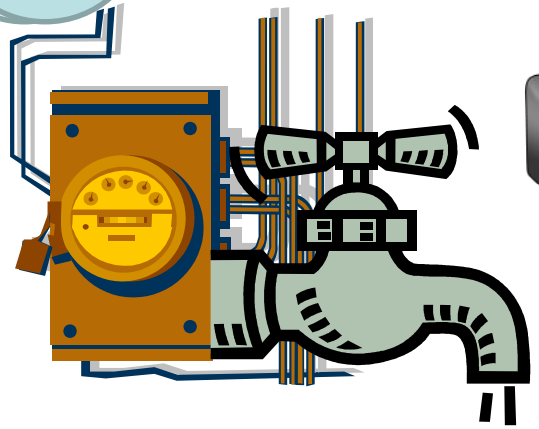


Elastic rapid response



Wide access

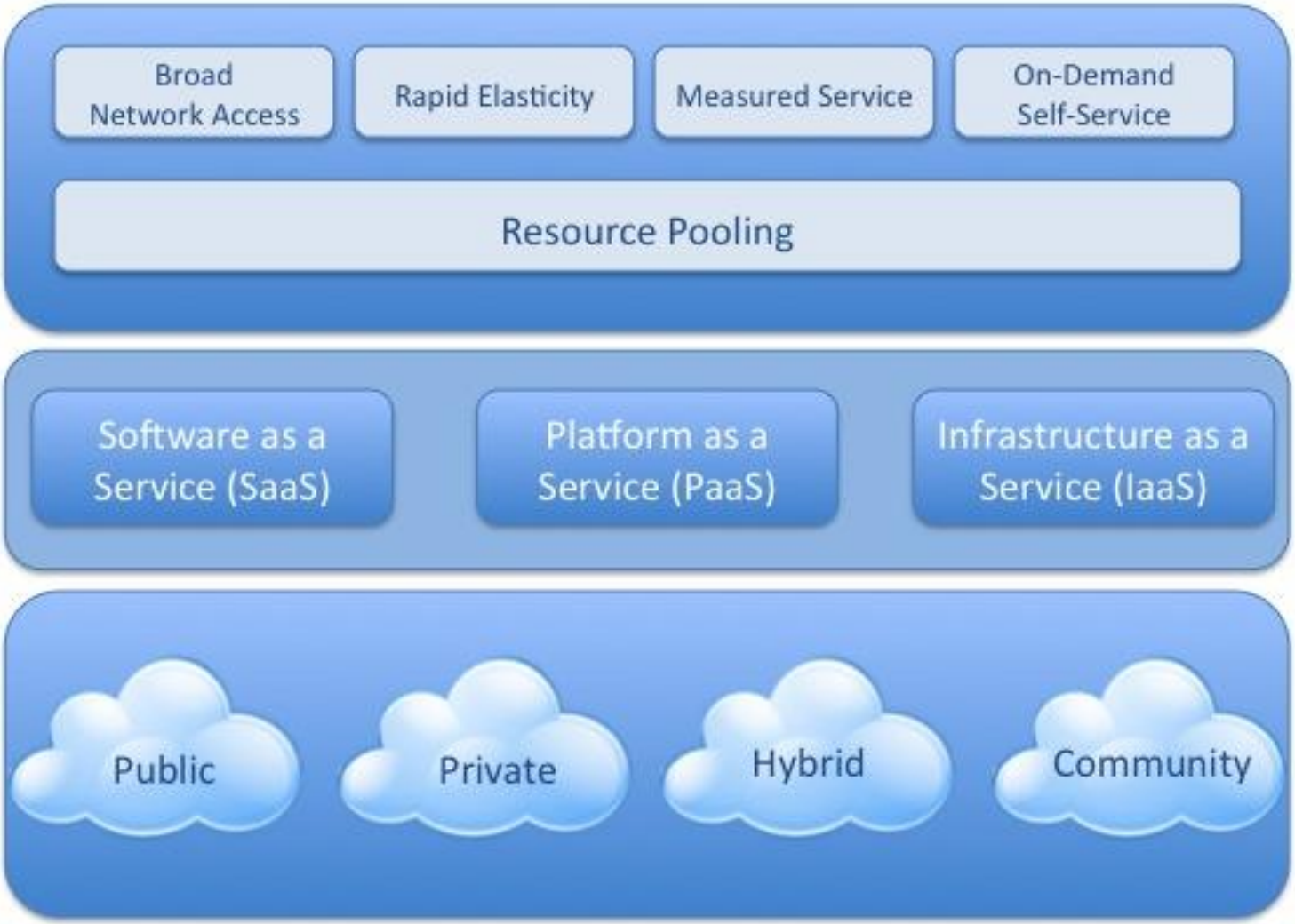
Pooled resources



On-demand, measured, self-service

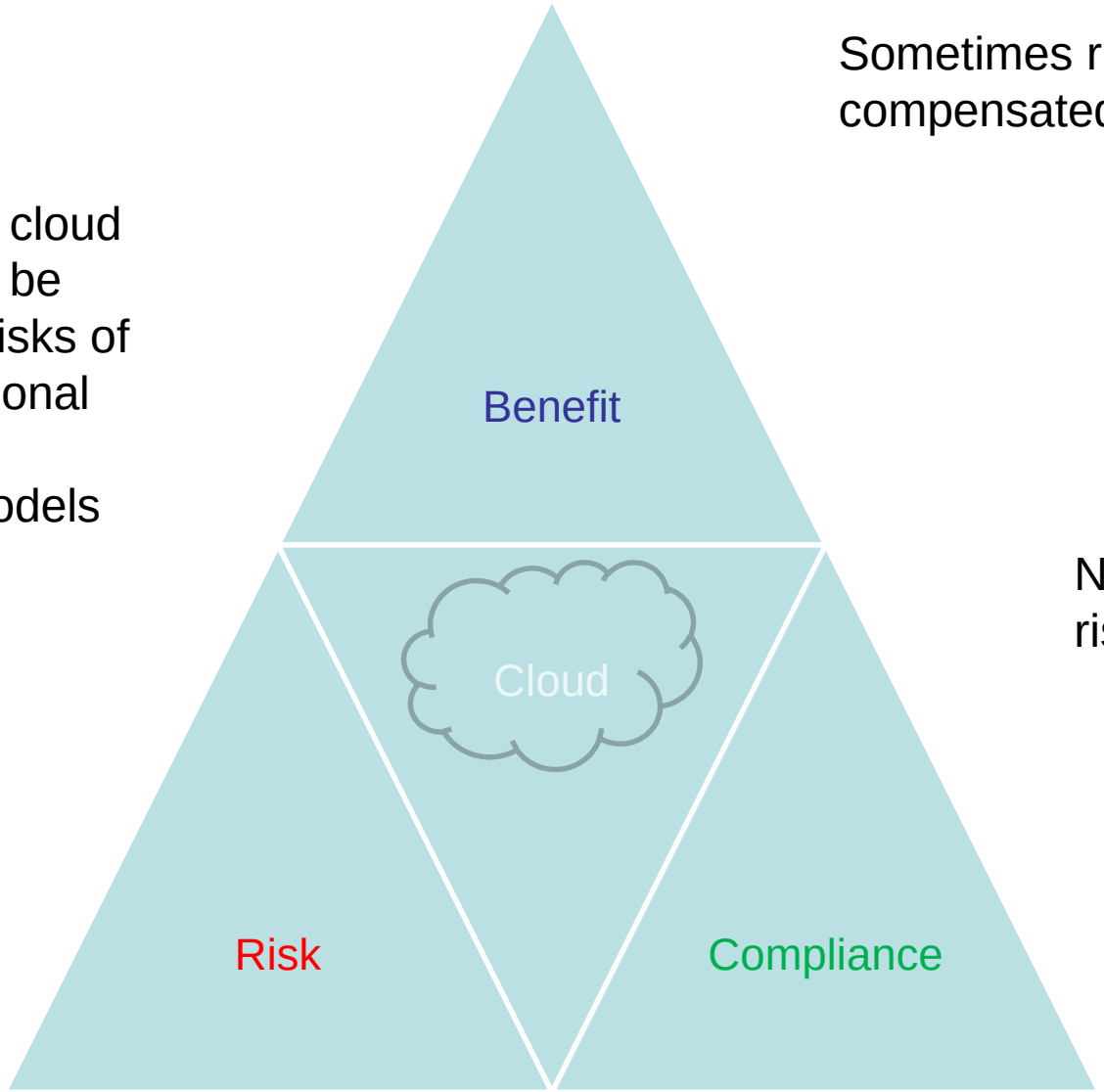
Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Sometimes risk is compensated by opportunity

The risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models



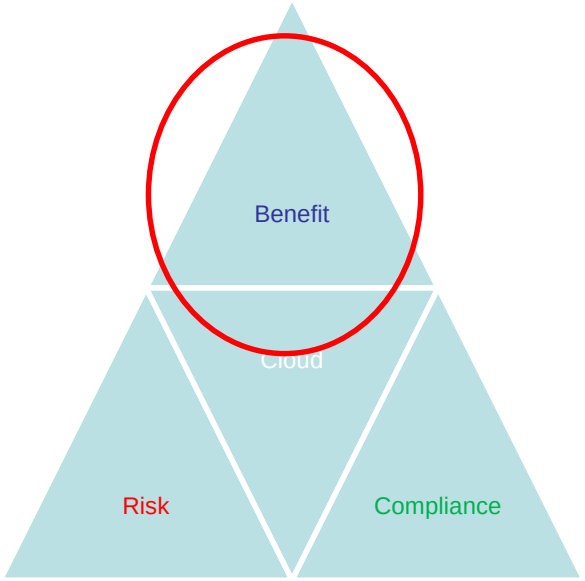
Need to balance risk vs. benefit

Risks

- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks

- Management interface compromise
- Data protection
- Insecure data deletion
- Malicious insider

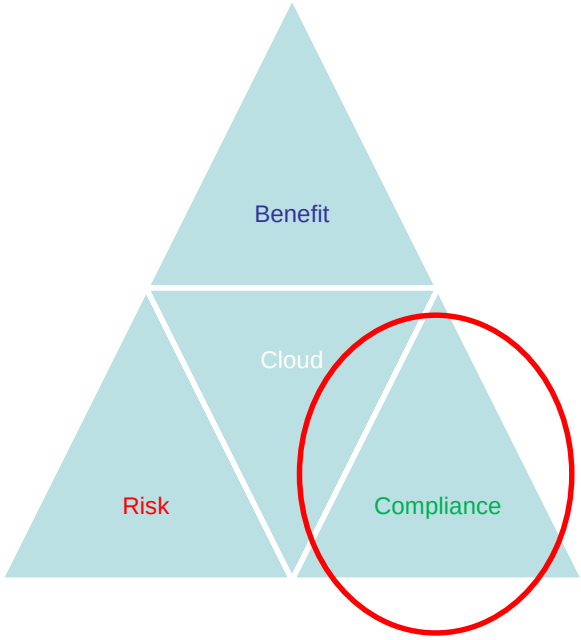
Identified by enisa European Network and Information Security Agency



Benefits

- Pay per use
- Scalability
- Down-time
- Security
  - benefits of scale
  - a market differentiator

- Tools, techniques, resources
- Audit and evidence-gathering
- Faster, more effective updates
- Audits and SLAs force better risk management
- Benefits of resource concentration



Compliance

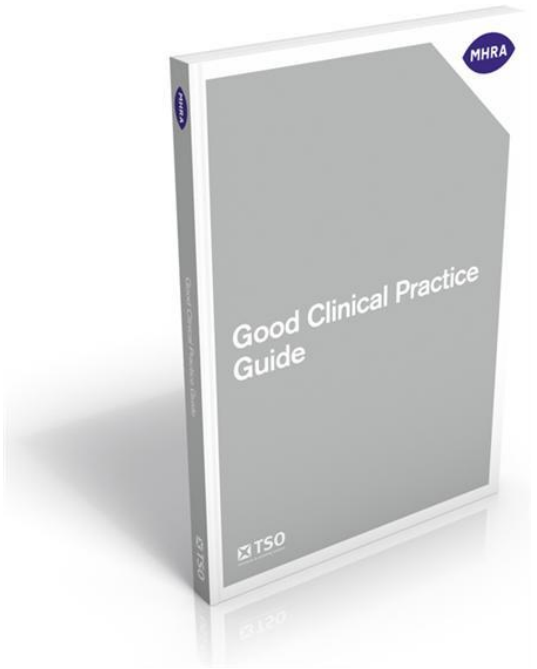
EU

FDA

UK Medicines and Healthcare products Regulatory Agency

GCP Guidance

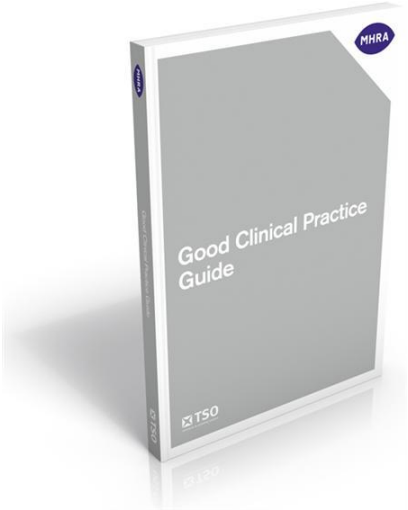
- **Good Clinical Practice Guide (2012)**
- UK Medicines and Healthcare products Regulatory Agency (MHRA)



GCP Guidance

- **Good Clinical Practice Guide (2012)**
- Section 14.5 Computer Systems Validation

- Principles:
  - Appropriate controls through the life cycle
  - Documentation available to support application of controls
  - System is fit for purpose and performs reliably and consistently as intended

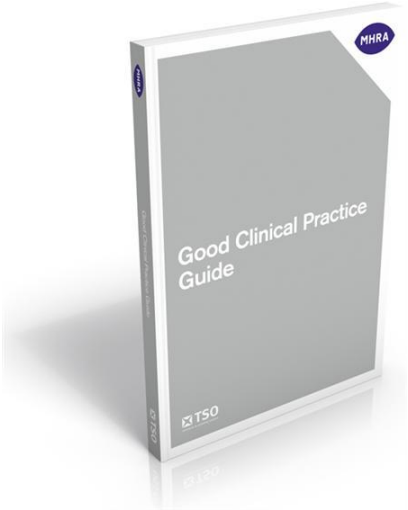


Refers to GAMP 5 …

GCP Guidance

- **Good Clinical Practice Guide (2012)**
- Section 14.5 Computer Systems Validation

- Other Considerations:
  - System backup
  - System security
  - Interaction between systems
  - Audit trails
  - Continued accessibility
  - Training of staff



GCP Guidance

- **Good Clinical Practice Guide (2012)**
- Section 14.5 Computer Systems Validation
  - "The above considerations apply if the system is hosted on the server of the sponsor or of the vendor, or if it hosted in a so-called 'cloud' space…"
  - "…it must meet the requirements for managing and storing data for clinical trials."

Key Considerations

- Technical / Quality Agreements
- Approved supplier status
- Change control and validation
- Data security
- Data access and retention

Data Storage and Access

- Do you know where your data is stored?
- If in a third country, what further considerations must be made, e.g. legislation on data privacy and misuse?
- Do you understand the potential restrictions on access to the data?
- Can you move the data to another provider without data loss or corruption?

Data Storage and Access

- What security aspects are in place?
- Is your data stored in a private dedicated storage area, or is it intermixed with other users data?
- Who else has visibility of your data?
- Is there secure access to your data?
- What guarantees are available with respect to lost or corrupted data?

Data Storage and Access

- What are the arrangements for backup and system / data restoration?
- Under what circumstances can your data be deleted by the service provider?
- What are the implications with respect to your data and your ability to maintain regulatory compliance should the service provider become insolvent or be taken over by another provider?

“FDA Want to Understand…”

- What systems are currently outsourced?
- What issues or concerns have come up?
  - What resolutions/mitigations were employed?
- Common terminology and definitions for outsourcing IT systems
- What type of systems will be outsourced in the future?

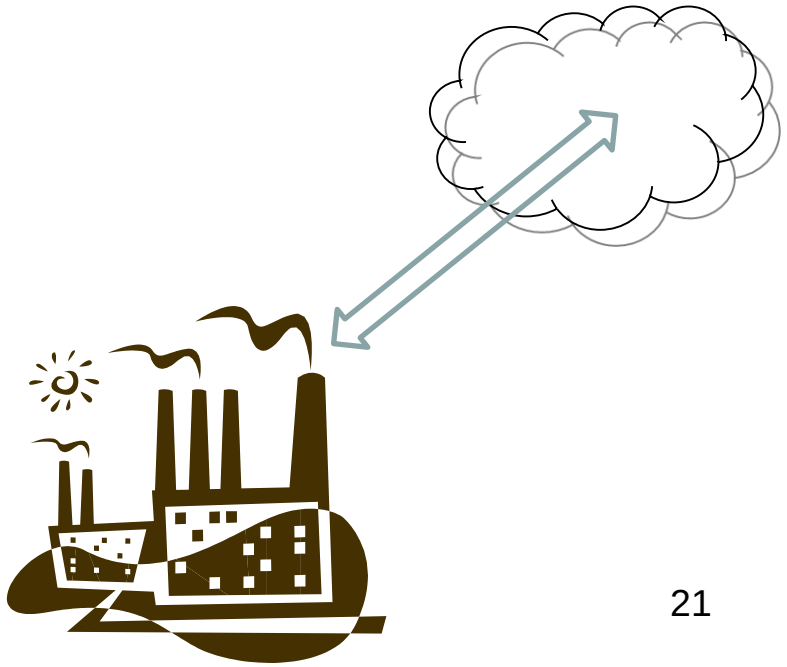
“FDA are interested in…”

- Integrity of the data is assured
- Risks clearly identified & mitigated
- Client/Provider Contracts
- Provider Quality Systems
- SOPs, validation, change control, training
- Cyber-security for Networked Systems
- Data Backup/Recovery
- Audits of Providers by FDA/Clients

So…

- Same requirements
- Same activities
- Same controls

…but distributed differently…



EU GMP Annex 11

Volume 4, EU Guidelines to Good Manufacturing Practice

Annex 11 - Computerised Systems

Revision came into operation: 30 June 2011

Requirements, but also solutions!

Quality Risk Management

- ***Risk management*** *should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality.*
- *Decisions on the extent of* ***validation*** *and* ***data integrity controls*** *should be based on a justified and documented risk assessment of the computerised system.*

Revised Annex 11

Suppliers and Service Providers

- ***When*** *third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing…*

Revised Annex 11

Suppliers and Service Providers

- *[**Then**]…formal agreements must exist between the manufacturer and any third parties and these agreements should include clear statements of the responsibilities of the third party.*

Typically Service Level Agreements (SLAs) or similar

Revised Annex 11

ICH Q10 - Useful Guidance

- The pharmaceutical company is ultimately responsible for assuring the control of outsourced activities...

Assessing suitability and competence prior to outsourcing operations…

Defining the responsibilities and communication processes for quality-related…in a written agreement…

Monitoring and review of the performance…

ICH Q10 – Pharmaceutical Quality System
(ICH - The International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use. (www.ich.org)

Data Integrity/Security Controls

- Access Control
- Interfaces
- Entry of critical data
- Backups
- Data Migration
- Archiving and long term retention of data
- Electronic records and signatures

Revised Annex 11

Other Operational Controls

- Periodic Evaluation
- Change Management
- Configuration Management
- Incident Management
- Business Continuity

Revised
Annex 11

So…Cloud Provider Management

- Assess the risks
- Define quality requirements
- Assess provider
- Define and agree responsibilities (SLA)
  - Which controls?
  - Where applied
  - Who is responsible?
- Monitor and review performance

Many Variables

- Use (the process supported)
- Content (the data managed)
- Service model (e.g. SaaS, IaaS)
- Deployment model (e.g. private, public)
- Nature and capability of provider(s)

The risks will vary,
so also detail and extent of controls

Initial Assessment

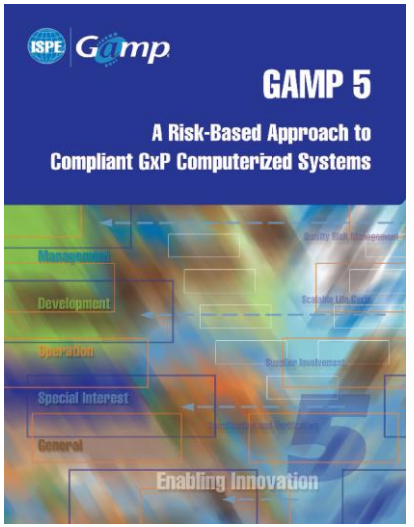
- Define Scope (Exactly what are we dealing with?)
  - Data / Records
  - Applications / Functions / Processes

Initial Assessment

- Initial Risk Assessment (how important is it and why?)
  - How would you be harmed if..
    - the asset became widely public and distributed?
    - a cloud provider employee accessed the asset?
    - the process or function were manipulated by an outsider
    - the process or function failed to provide expected results?
    - the information/data was unexpectedly changed?
    - the asset were unavailable for a period of time?
    - the asset were lost?

GAMP® 5

- Guidance includes:
  - Life Cycle activities and controls
  - Quality Risk Management
  - Supplier Assessment



GAMP® GPGs

- Other GAMP® Good Practice Guides also relevant…

- Electronic records and signatures
- Operation of GxP systems
- E-data archiving

See www.ispe.org/publications

GAMP Good Practice Guide:

A Risk-Based Approach to Compliant Electronic Records and Signatures

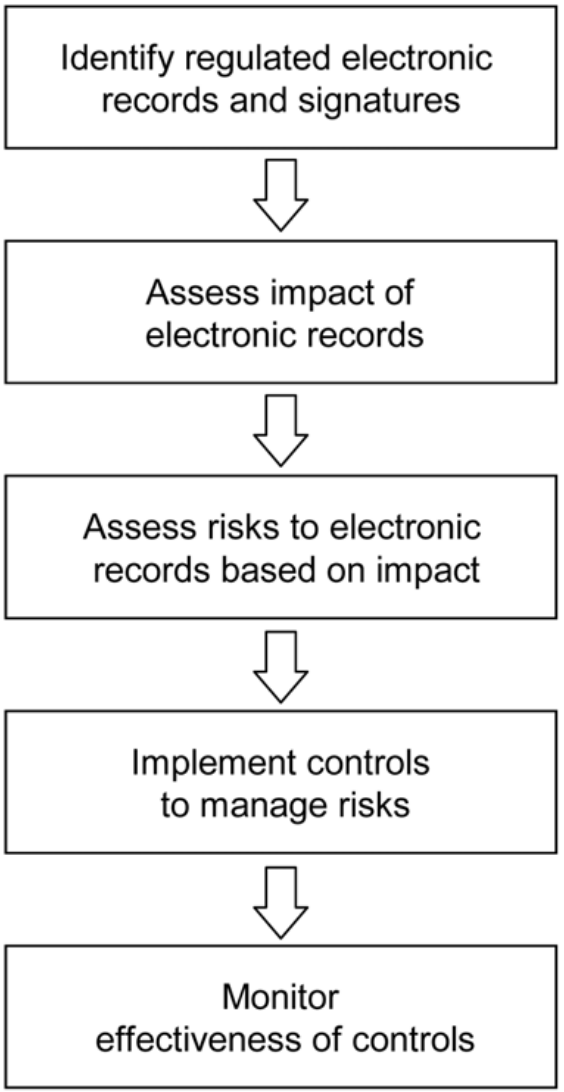
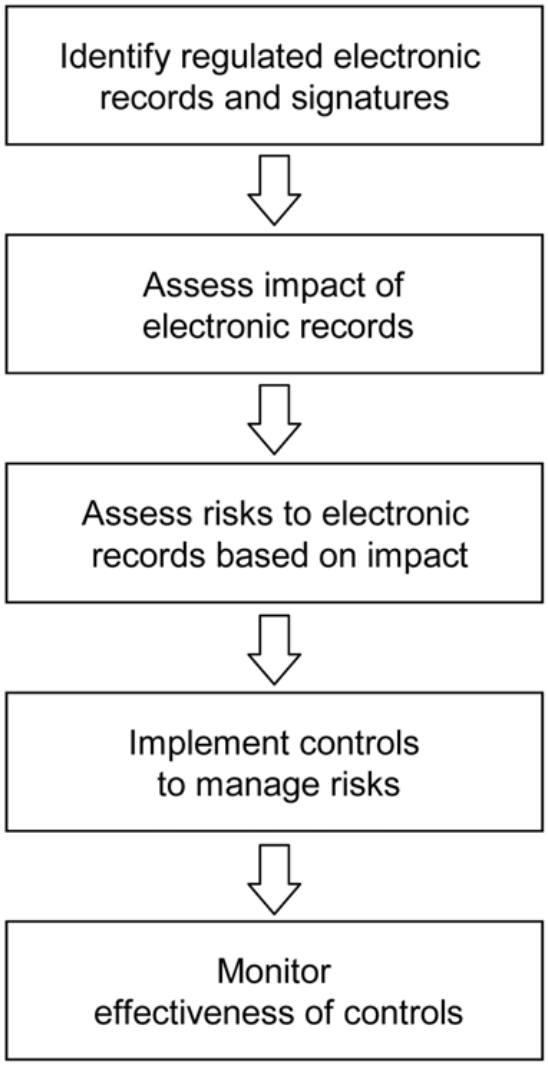


Figure 2.2: Managing Risks to Electronic Records

Taken as a model…

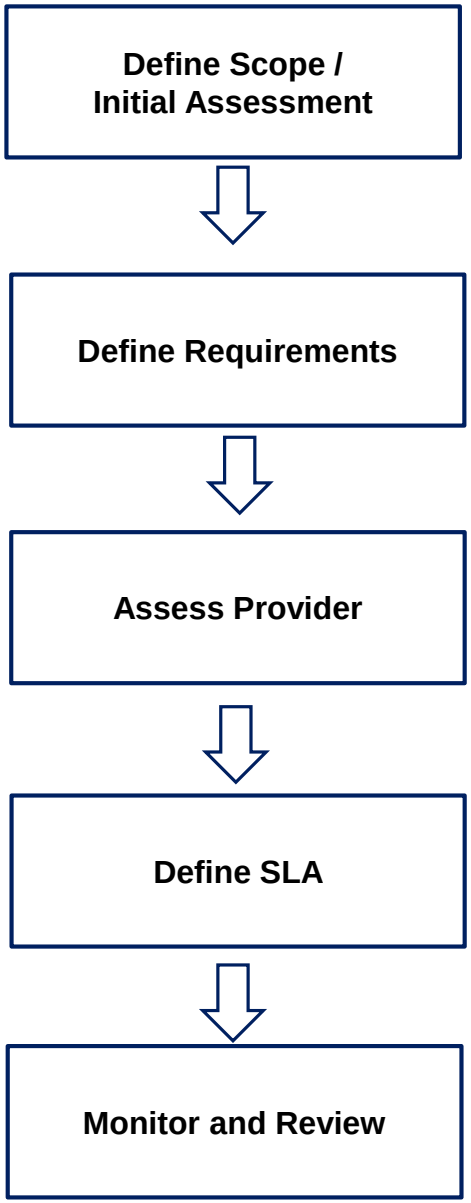
Record Risk Management



WHO IS RESPONSIBLE?

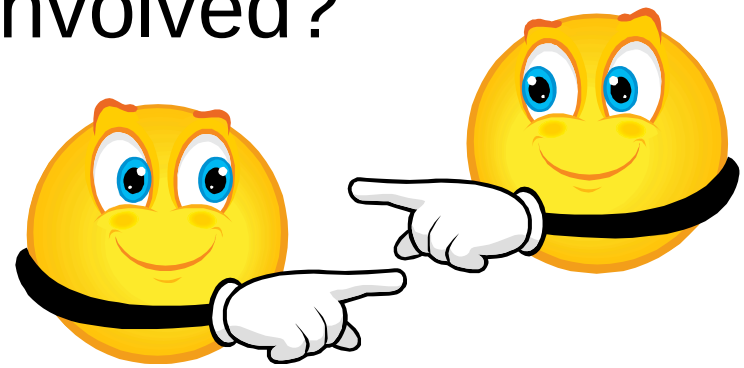
WHO ACTUALLY DOES IT?

Cloud Provider Management



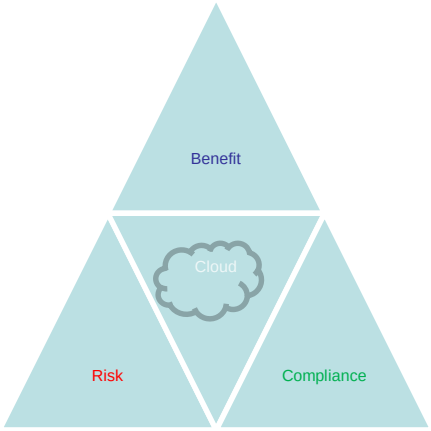
Challenges

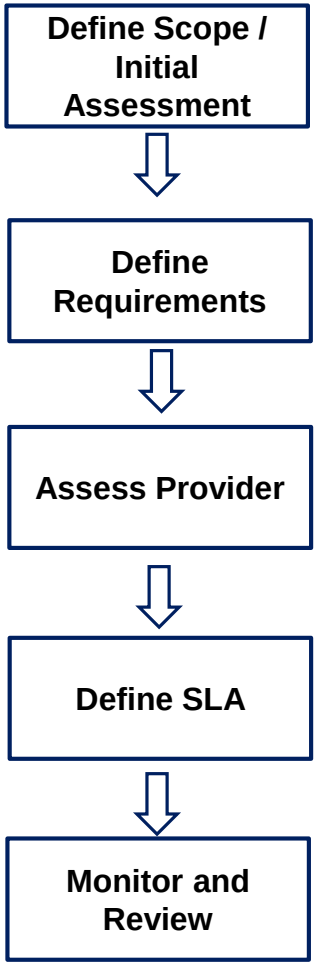
- Certifications and audits
- Big providers - not just GxP
- Chain of suppliers/providers involved?
- Responsibilities clear?
- Finger pointing?
- Complex – a lot to check
- Technologies and services change…



Conclusions

- Assess the risks
- Define quality requirements
- Apply appropriate controls
- Manage the provider(s)…through appropriate agreements





Sion Wyn
Conformity
+[44] (0) 1492 642622
sion.wyn@conform-it.com

conformity
keeping it compliant