IN OUR SERIES: **FROM THE TRENCHES:**

HOW TO WORK TOWARDS PHARMA COMPLIANCE FOR CLOUD COMPUTING–

WHAT DO FDA AND SIMILAR REGULATIONS MEAN FOR YOUR (CLOUD) IT DELIVERY ORGANISATION?

Martijn J – www.troopers.de – 2014 - www.ernw.de

THIS IS A PERSONAL ENDEAVOUR – SO PERSONAL INSIGHTS

SO WHAT I DO FOR WORK ENABLES ME TO SHARE THIS

HAD TO DO QUALIFICATION OF CLOUD COMPONENTS, SEARCHED AROUND, FOR ‘RE-USE’, NOTHING REALLY, SO CAME UP WITH SOMETHING MYSELF, AND THAT’S WHAT I WOULD LIKE TO SHARE!!

ABOUT ME

- Technically educated as construction engineer and -designer.
- 1997 turned into IT. *Yeah DTS CTS, Atalk, IPX/SPX ODI, DLSW+, TR etc*
- Last 11 years as 'consultant / architect' I took care of mostly bespoke and complex IT transformations for global pharma and manufacturing customers starting to be exposed quality and compliance since 2006.
- Ran a Middle-East Telco GRC project in 2012
- I currently work as Security Controls Assurance manager (?) for the Compliance department of a global Telco.

-FROM THE TRENCHES-

I have been working full time, in Pharma compliance for a few years now so by all means NOT a Compliance Industry expert!
However since I have described, designed, planned, implemented and tested quality for the conformance towards applicable regulations and company policies, from the standpoint of a technical guy that's exactly what I would like to share.

Combining these enhancements with a Telco security control mapping framework and Pharma tooling test automation ideas while we are at it.
Most of the principles are guidance for you, miles need to made….

WHAT IS THIS PRES ABOUT 1

- The translation of Pharmaceutical regulations (what regulations?) that could be projected to any (cloud-) related IT service into a quality management strategy and hands-on IT controls that could work for each one of us.
- How to bring compliance into the lifecycle of requirements, design, install and configuration plans etc. Furthermore we'll discuss different types of controls in service creation or delivery, be them administrative, technical, procedural controls.
- Usable quality assurance controls for People, Process and Technology, projected onto services (components). All this from practical experience. These controls might be there already to re-use (but not auditable) or might need to be created.
- Focus on the lower' IT people, processes, systems showing 'smart samples'.

WHAT IS THIS PRES ABOUT 2

- NOT a lecture about straight –up (?) Computer Systems Validation CSV, which is about making sure that Pharma application and information processing system are FDA compliant.
- There is already a lot of research material on the topic of CSV principles.
- Cannot be exhaustive 'trying to assure' the area of Cloud Orchestration as the world of Cloud automation is partially or greatly proprietary, and moving very fast.

(CLOUD COMPUTING DOES NOT EXIST, ITS ELASTIC COMPUTING I KNOW)

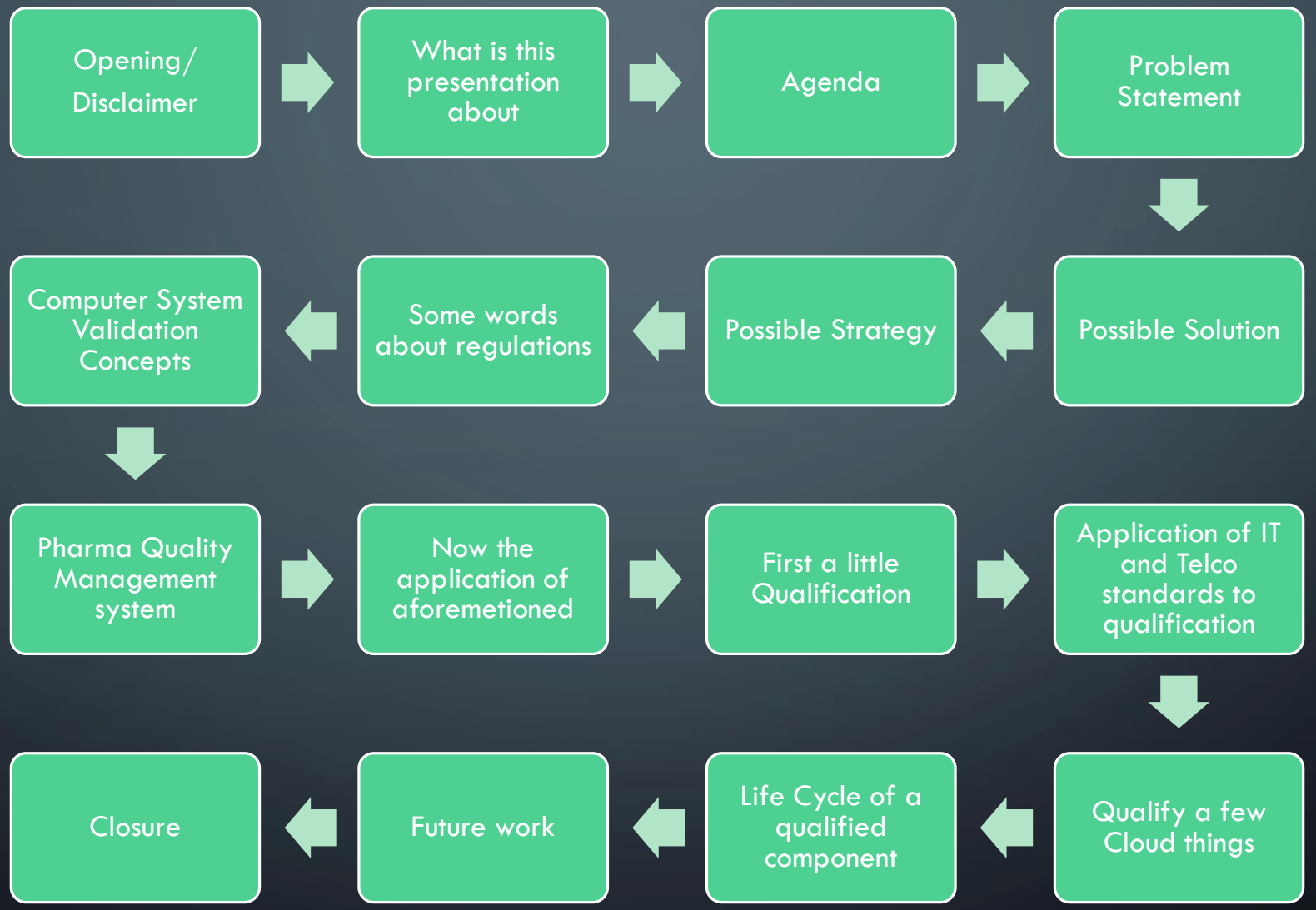
WHAT IS THIS PRES ABOUT –MARTIJN GET GOING!!!!-

- ‘assuring quality leading to compliance’
- And yes you need documentation
- ‘we have built it’
- ’yes we used our config guide’
- ‘ofcourse I have tested it’

HIGH-LEVEL AGENDA

- Problem statement
- Computer Systems Validation for Cloud Computing
- Quality Management Systems and (Modern) networking
- Qualification
- Application of Telco standards
- Lets qualify some cloud components
- Future work and such

>>> 'THE FLOW' OF THE PRESENTATION >>>



PROBLEM STATEMENT

- What regulations, policies
- Who is the regulated entity
- What does FDA compliance in IT mean to whom
- Vendors
- How to comply
- Scope
- Cloud computing

PROBLEM STATEMENT, NOW HANDS-ON

- How much quality is enough compliance?
- Need to assure fit for purpose, auditability, traceability
- What type of and how many controls to choose
- From what planes, layers, dimensions
- How to measure quality for compliance
- Now make it Cloud Computing?

SOLUTION IDEAS

- Types of Business processes and operating countries dictate applicable regulation
- Your company or your customer is the regulated entity, who develops and manufactures drugs
- All Personnel, all Processes and (supporting) systems servicing the Pharma business processes are in scope
- Need to fully understand the organisation supporting the service, personnel and their processes in use
- 3rd Party vendor assurance
- Need to understand what components are in Pharma IT, physical and virtual
- Taking into account possible vectors and threats
- Re-use Existing installation and operational procedures

STRATEGY IDEAS

- Scan the organisation for support personnel and their processes
- 3rd Party vendor assurance via assessment (at least)
- Scan the live system and documentation for Pharma IT systems and components, physical and virtual
- Assure the different components from installation and operational perspective
- Need a (security) framework to (re) identify tests for critical controls

REGULATIONS

REGULATORY COMPLIANCE

- In Pharma, the primary regulations regard drug manufacturing, clinical research & development and impacts in the laboratory
- FDA (the US Food and Drug Administration)
- GxP – Good Clinical / Laboratory / Manufacturing Practices
- 21 CFR Part 11 – electronic records and signatures

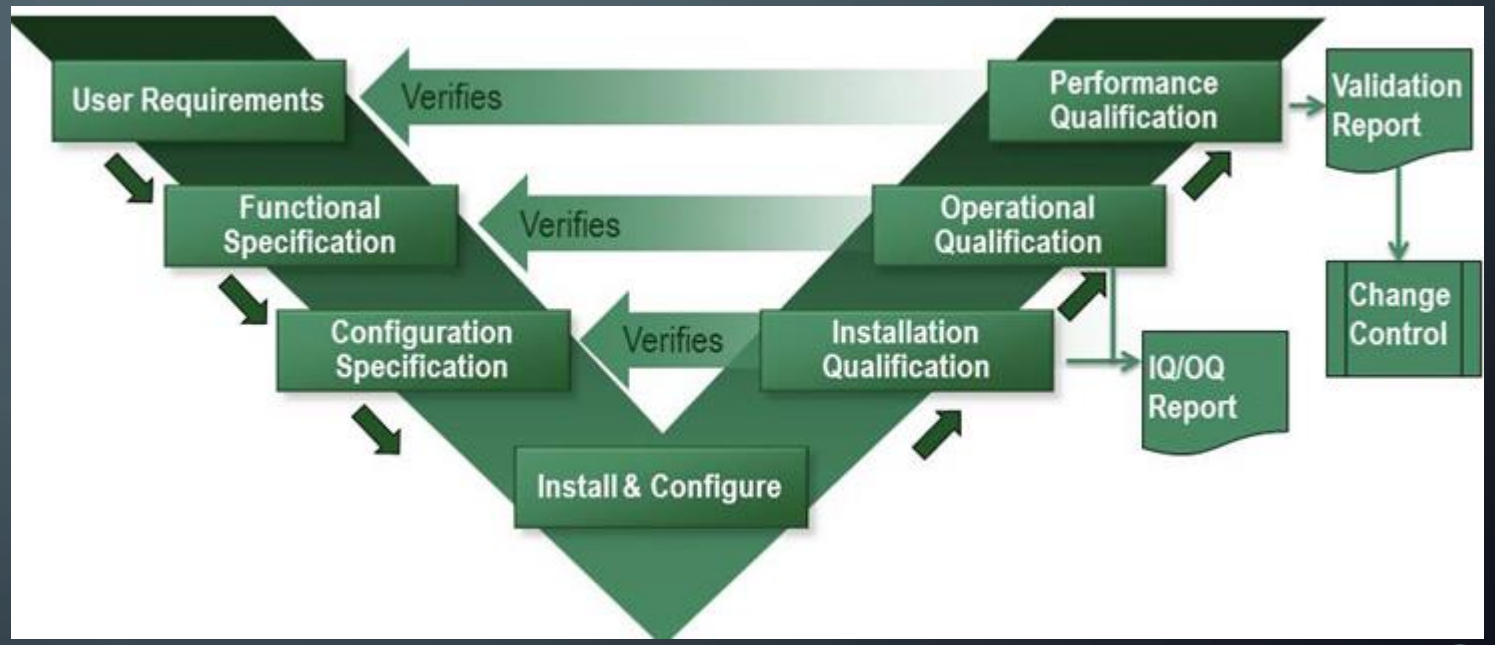
COMPUTER SYSTEM VALIDATION CONCEPTS

SOME CONCEPTS BEFORE WE GO FURTHER

- CSV
- QMS(M)
- Records
- Qualified
  - people,
  - process,
  - systems (actual and supporting tools)

WHAT IS CSV COMPUTER SYSTEMS VALIDATION

- Validation V
- Tell the whole story
- How do we do that in practice?

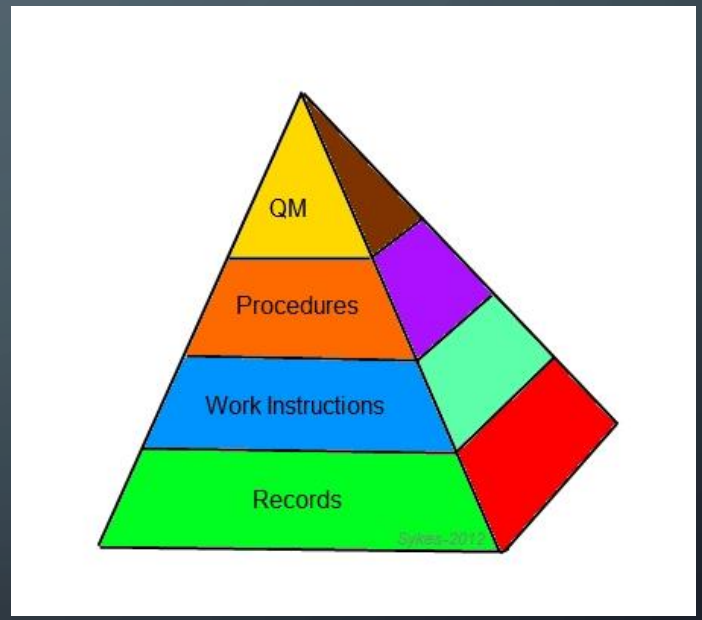


http://www.spkaa.com/wp-content/uploads/2011/04/CSV-process.jpg

QUALITY MANAGEMENT SYSTEM 1/2

Just a few QMS 'basics'

- QM
- Procedures
  - Qualification Plan,
  - Standard operating Procedure
- Work Instruction
  - DQ/IQ/OQ/PQ
- How do we do that in practice?



http://mnasq.org/benchmarq/2012/may/pyr_img001.jpg

QUALITY MANAGEMENT SYSTEM 2/2

- Qualification plan (QP) - describes qualification activities, quality requirements and documented evidences needed to qualify a 'Pharma' System. A 'Pharma' System may include its underlying software application, software elements and hardware components.
- Standard Operating Procedure (SOP) – defines the activities required to qualify devices (components) that service 'Pharma' services.
- Installation Qualification (IQ) – checks whether the System is installed and configured as per its design specifications
- Operational Qualification (OQ) – demonstrates that the System operates as per its functional specifications
- Performance Qualification (PQ) – demonstrates (where possible) that the System performs according to a specification appropriate for its routine use

A 'PHARMA' QUALITY MANAGEMENT SYSTEM

Pillars	Explanation
Qualified Persons	▪ Work effort must be performed by qualified resources to ensure compliance ▪ If it wasn't documented, it wasn't done (e.g. training, installation, etc.)
Consistent and Replicable Processes	▪ Provides leverage and scale across delivery teams ▪ Documented standards and processes define the baseline for compliance
Standardized Systems	▪ Provides leverage and scale across delivery teams ▪ Enables repeatability in system functionality, controls and document retention ▪ Validated systems are key element for compliance ▪ Streamlines assurance activities

A 'PHARMA' QUALITY MANAGEMENT SYSTEM

Pillars	What components
Qualified Persons	▪ Training records and management tools ▪ On-boarding and off-boarding records ▪ Access control lists, reviews and reporting ▪ Qualified Persons ▪ Subject Matter Experts in regulatory regimes
Consistent and Replicable Processes	▪ Controlled and standard document management ▪ **Standard device qualification methodology** ▪ Quality Management Manual (QMM) ▪ Control Self Assessments and frameworks ▪ Monitoring and metrics reporting
Standardized Systems	▪ Validated systems ▪ Organization-wide system stacks ▪ Service design standards ▪ Operating model Quality Gates

FOCUS ON QUALIFICATION ONLY!

NOW THE APPLICATION

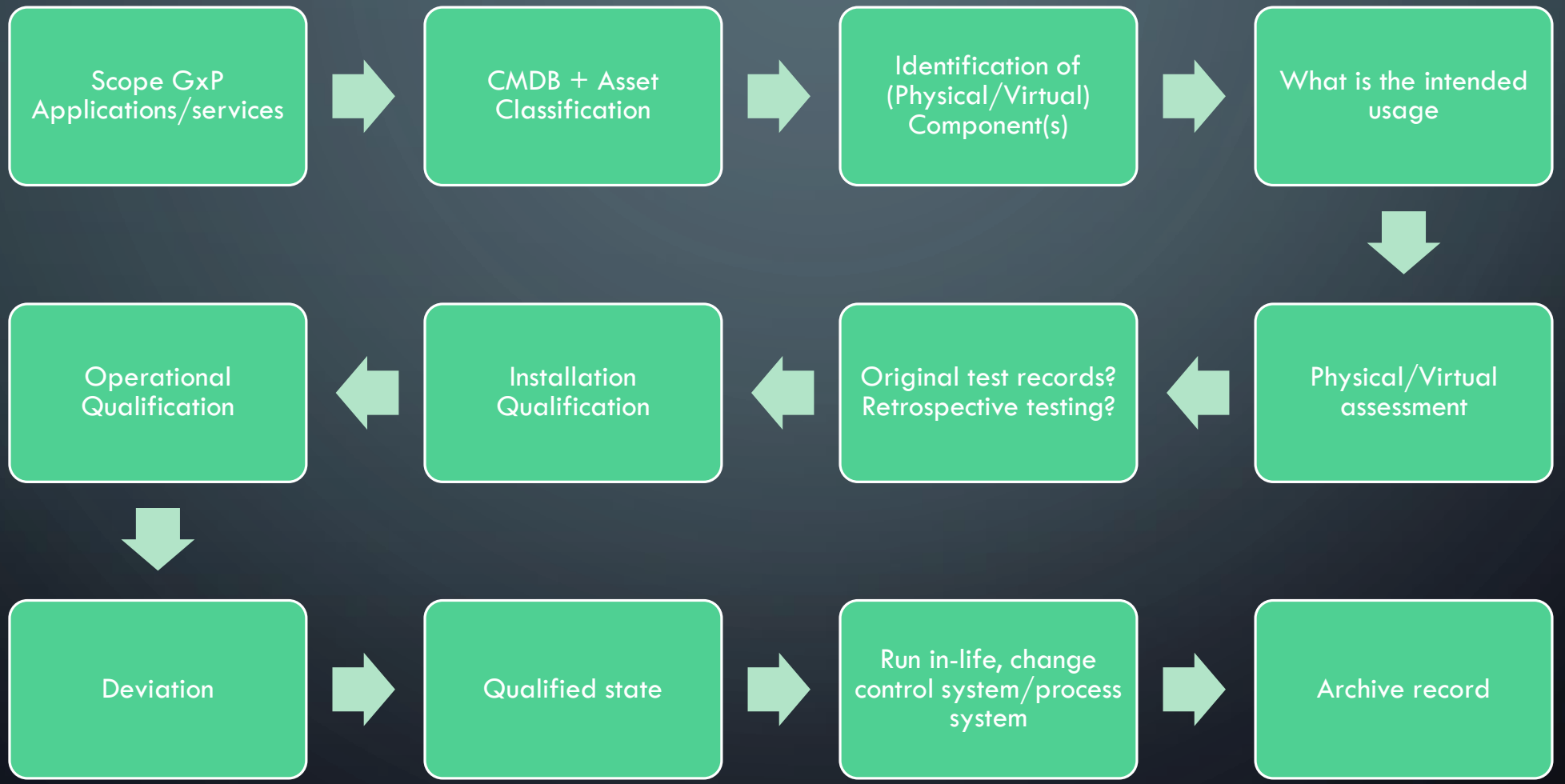
QUALIFICATION OF DATA CENTER AND CLOUD COMPONENTS

- Data Center and Cloud components
- Networks systems applications
- How do we do that in practice?
- Where would you be able to automate testing?

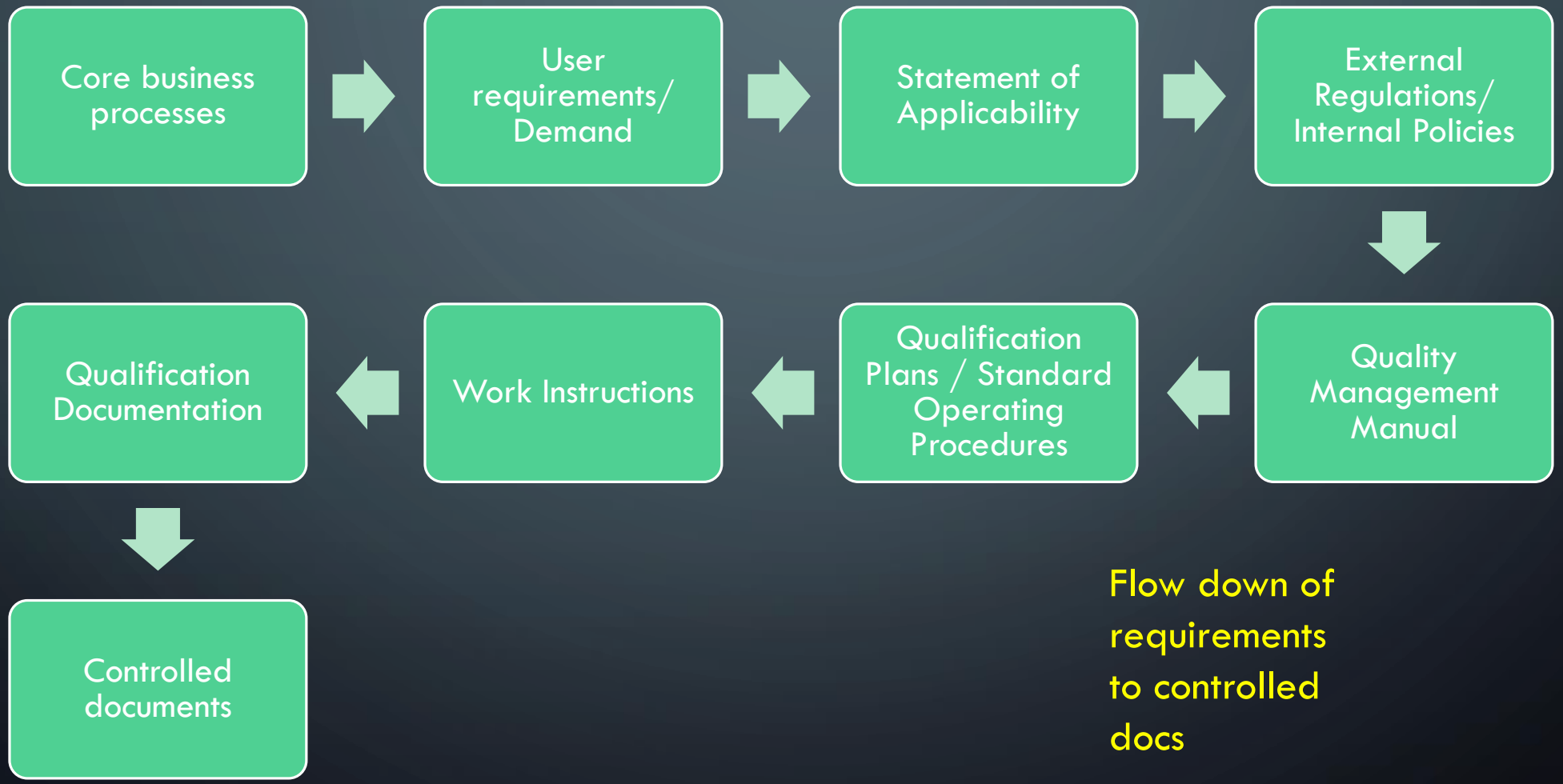
QUALIFICATION OF DATA CENTER AND CLOUD COMPONENTS

- I'll keep this one condensed!
- Check Data center physical, security, DR certifications
- Security controls pipe into Pass/Fail criteria on the device Installation Qualification test steps!
- You can do separate DC Qualification
- Say assessment, not audit.

BASELINE: QUALIFICATION OF COMPONENTS



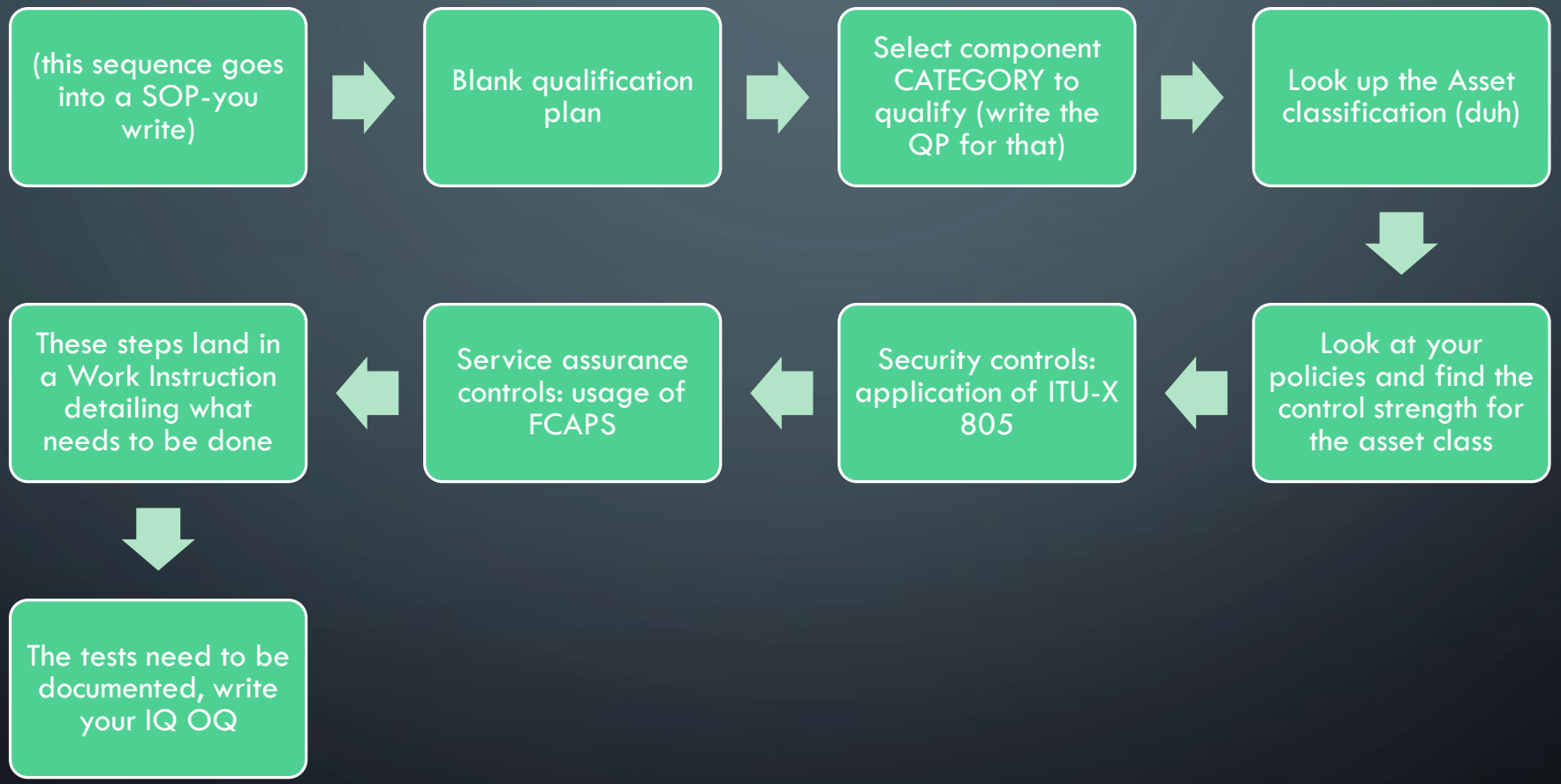
TRENCHY: FULL PICTURE – QUALIFICATION GOVERNANCE EXAMPLE



Flow down of requirements to controlled docs

THE APPLICATION OF IT AND TELCO ‘TECHNICAL‘ STANDARDS TO MAKE QUALIFICATION EASIER

THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER



THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER

- FCAPS is an ITU standard model for enterprise management.
- The five FCAPS domains are:
  - Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management

THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER

- FCAPS
  - Fault Management
    - Design and configure Tooling for Faults
  - Capacity Management
    - Design and configure Tooling for Capacity
  - Accounting management
    - Design and configure Tooling for Accounting and access
  - Performance Management
    - Design and configure Tooling for Performance
  - Security Management
    - Design and configure Tooling for Security and Management access

THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER

- ITU-T X.805
  - SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS
  - Security architecture for systems providing end-to-end communications
    - Security dimensions
    - Security planes
    - Security threats

THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER

- ITU-T X.805 Security dimensions
  - Access control
  - Authentication
  - Non-repudiation
  - Data confidentiality
  - Communication security
  - Data integrity
  - Availability
  - Privacy
- ITU-T X.805 Security planes
  - User/data plane
  - Management plane
  - Control plane
- ITU-T X.805 Security layers
  - Infrastructure Security Layer
  - Services Security Layer
  - Applications Security Layer

THE APPLICATION OF IT AND TELCO 'TECHNICAL' STANDARDS TO MAKE QUALIFICATION EASIER

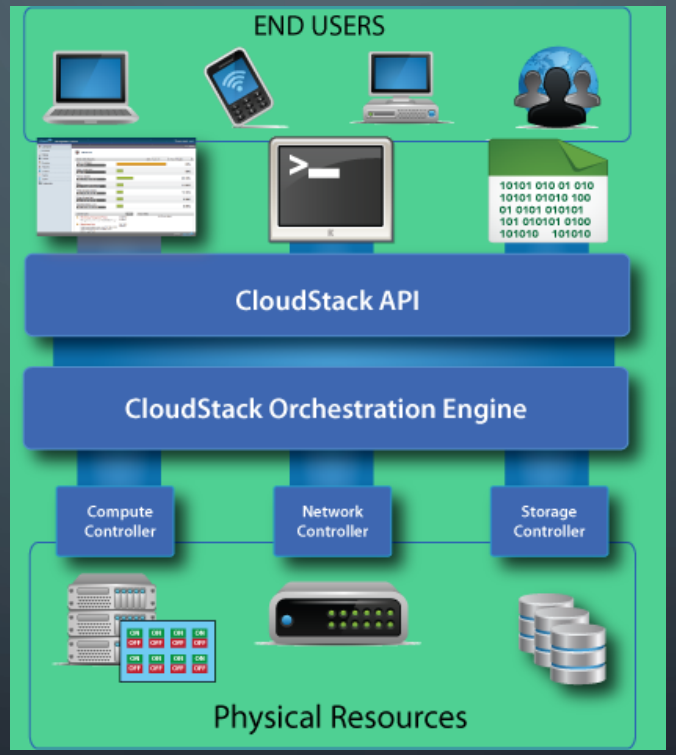
- Applying FCAPS to OQ testing, use the methodology to include teststeps for
  - Define faults, watermarks exception handling
  - Fault Management
    - NMS polls/listens for device faults, mutual configuration
  - Capacity Management
    - Include teststeps checking NMS monitors and generates capacity alerts, mutual configuration
  - Accounting management
    - Access management, logging access, authorisation review
  - Performance Management
    - Include teststeps checking NMS monitors and generates capacity alerts, mutual configuration
  - Security Management
    - Management, Monitoring, etc etc
    - Exception handling

TRENCHY: 'QUALIFICATION OF CLOUDPORTAL PRESENTED USER CLOUDMANAGEMENT AUTOMATED FUNCTIONS' INTERSECTION BETWEEN ITU X-805 AND IQOQ

	User/data plane	Management plane	Control plane
Security dimensions	Security threats		
Access control	• destruction of resources		
Authentication	• modification of information;		
Non-repudiation			
Data confidentiality	• loss of information and/or resources;		
Communication security	• disclosure of information		
Data integrity			
Availability	• interruption of services		
Privacy			

CONFIDENTIALITY
INTEGRITY
AVALABILITY

TRENCHY: 'QUALIFICATION OF CLOUDSTACK??? WHAT'S THAT?



http://philippe.scoffoni.net/wp-content/uploads/2012/02/cloudstack-oss-product_archtiecture.png

TRENCHY: 'QUALIFICATION OF CLOUDSTACK??? WHAT'S THAT?

- We'll do 2 parts in this talk
  - The core functions - fiddle with VM and 'side' features
  - The Virtual layer – servers, network, storage

http://philippe.scoffoni.net/wp-content/uploads/2012/02/cloudstack-oss-product_archtiecture.png

TRENCHY: ‘QUALIFICATION THE CORE FUNCTIONS - FIDDLE WITH VM AND ‘SIDE’ FEATURES

http://philippe.scoffoni.net/wp-content/uploads/2012/02/cloudstack-oss-product_archtiecture.png

TRENCHY: 'QUALIFICATION OF CLOUDPORTAL PRESENTED USER CLOUDMANAGEMENT AUTOMATED FUNCTIONS' OVERVIEW – QUALIFICATION PLAN LEVEL

TRENCHY: 'QUALIFICATION OF CLOUDPORTAL PRESENTED USER CLOUDMANAGEMENT AUTOMATED FUNCTIONS' PART 1- GENERAL (WORK INSTRUCTION LEVEL)

Work includes and functions IQ tested are

- Template documentation work
- Account manipulation
- VM manipulation
- Manipulate firewall
- Manipulate pri/sec storage

Work includes and functions OQ tested are

- Cloudmanagement Qualification - Cloud Platform Test Plan (automated)
- Pipeline Pilot V9 protocol loaded on PCVM manipulation
- Start protocol
- Capture output and formally archive
- QP compares output

TRENCHY: 'QUALIFICATION OF CLOUDPORTAL PRESENTED USER CLOUDMANAGEMENT AUTOMATED FUNCTIONS' PART 2 INSTALLATION QUALIFICATION (IQ)

Template documentation work

- Qualified person retrieves new template, populate document fields
- Document Other/ALL test parameters:

Account manipulation

- Within customer account,
- addition of test user account
- Login with test account

VM manipulation

- Start VM
- Acquire External IP Address
- Retrieving image

(VM manipulation)

- Delete VM
  - Is the VM really deleted?
  - Is storage really deleted?
- Manipulate firewall
  - Creation of a firewall rule
  - Creation of a port forwarding rule
- Manipulate pri/sec storage
  - Primary storage
  - Secondary storage
  - etc

TRENCHY: 'QUALIFICATION OF CLOUDPORTAL PRESENTED USER CLOUDMANAGEMENT AUTOMATED FUNCTIONS' PART 3 OPERATIONAL QUALIFICATION (OQ)

- Procedure used Cloudmanagement Qualification - Cloud Platform Test Plan (automated) (need to be defined and created)
- OQ tests cover the operation of the instances of Citrix CloudPlatform targeted (AZ') as installed in your Cloud environment.
- CloudPlatform will be tested through the API via Pipeline Pilot.
- Checking via PP output and manual verification in Vcenter for VM's +storage browser
- (fill in what you have)

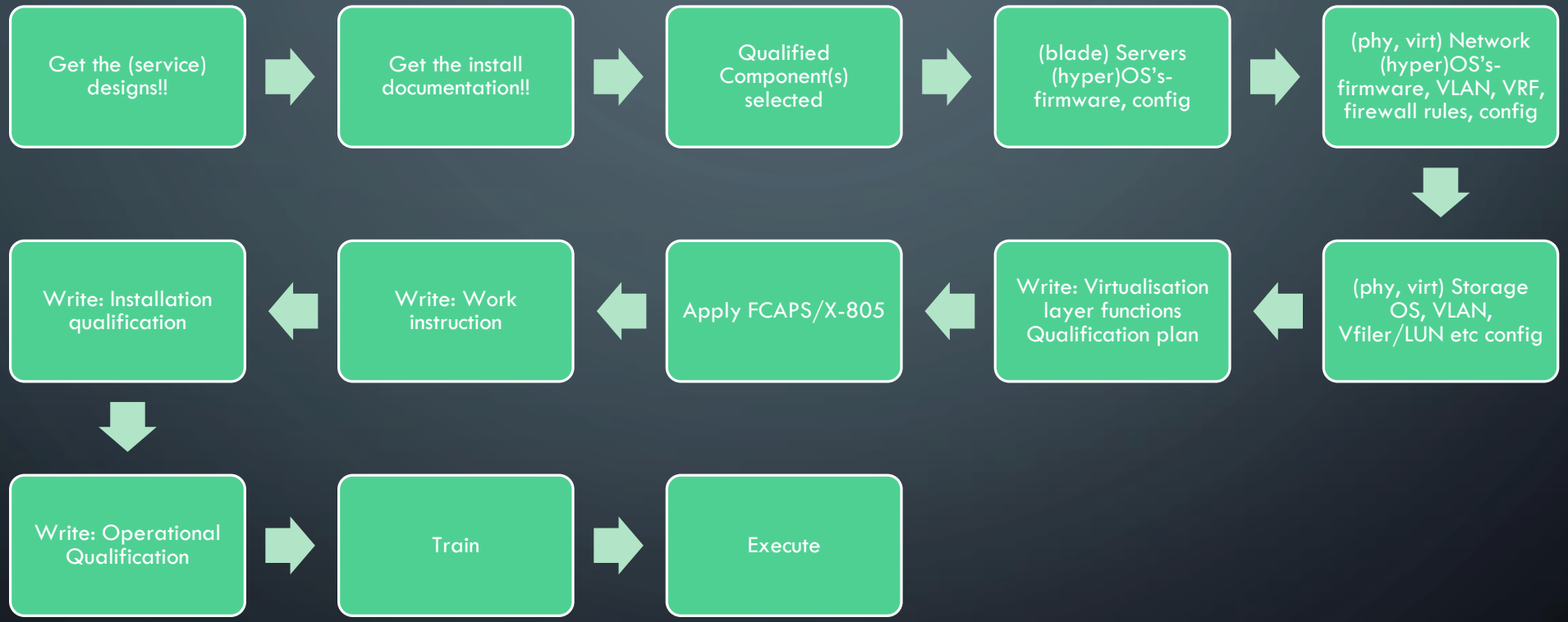
Pipeline Pilot V9 protocol loaded on PC

- Start protocol 'CloudPlatform Testing V1'
- VM launch: cstestaapi4
- VM stop: csteststopstart
- VM start: csteststopstart
- VM destroy: cstestkaput
- Archive excel Output file written as part of the protocol

TRENCHY: ‘QUALIFICATION OF THE VIRTUAL LAYER – SERVERS, NETWORK, STORAGE

http://philippe.scoffoni.net/wp-content/uploads/2012/02/cloudstack-oss-product_archtiecture.png

TRENCHY: 'QUALIFICATION OF THE VIRTUAL LAYER – SERVERS, NETWORK, STORAGE OVERVIEW – QUALIFICATION PLAN LEVEL



TRENCHY: ‘QUALIFICATION OF THE VIRTUAL LAYER – SERVERS, NETWORK, STORAGE
PART 1/2- (WORK INSTRUCTION LEVEL-IQ/OQ CONDENSED)

- Network infrastructure
- Hypervisor and supporting services
- Servers for additional services
- Management

Network infrastructure

- WAN
  - Inter-platform connectivity
  - Customer connectivity
  - Management connectivity
- LAN
  - Configuration of User, Management, storage networks
- Management
  - Management and monitoring of the individual devices

Hypervisor and supporting services

- Vspherex SQL database
- Separation between ‘different domains’ networks
- Vspherex SQL database
- Separation between ‘different domains’ networks

Servers for additional services

- X jump server
- Windows patching server
- Linux utility server

Servers for additional services

- VMA, HDA
- Post install work /tidy up

Management

- Management and monitoring of the individual devices.

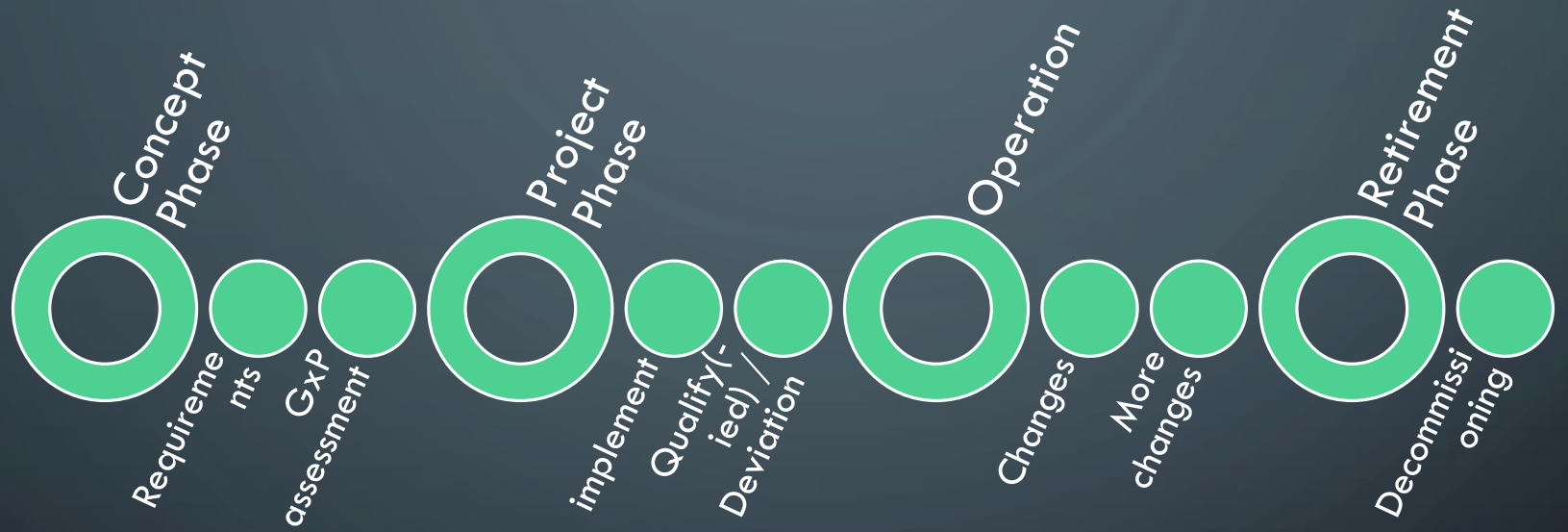
Storage

- vFiler
  - Separation between ‘different domains’ storage vFilers
  - Separation between ‘different domains’ storage VIF’s
- NFS
  - NFS shares made available to the ESXi hosts
- Management
  - NetApp Operations Manager
  - Management of the individual devices

Computing

- Management
  - Cisco UCS Manager
  - Management and monitoring of the individual device

TRENCHY: FULL PICTURE – LIFECYCLE OF A QUALIFIED COMPONENT



Possibly existing component or new install

Retention or safe disposal

Where did the old hard disk end up?? Ebay?

To a model on www.ispe.org

FUTURE WORK

Look deeper into assuring the quality, repeatability, functionality of:

- 'black box' CloudStack functions not touched yet
  - (why not apply FCAPS on deamon(s) and services!) eeeh yes document - document.
- Investigate Other cloud computing functions like '*assuring quality leading to compliance' for* object storage and end-user application library
  - In the future

CLOSURE

- Recap
  - I have shared how to utilise a framework to test quality for the conformance towards applicable regulations and company policies, from the standpoint of a technical guy, with some ideas to optimize, reuse, smarten and enhance testing (qualification)
  - Combining with a Telco security control mapping framework and Pharma tooling test automation ideas should give you the tools to write your own (smart) qualification strategy.

CLOSURE

- Questions
- Ask me at martijnmichiel@hotmail.com

REFERENCES

Troopers References, virtualisation, Cloud, Compliance or all together ;-)

- Just a quick list maybe I miss a colleague, do check archives @ troopers website
- Troopers 2008 - ERNW_ESX-In-Security
- Troopers 2009 -
- Troopers 2010 - TROOPERS10_Clobbering_the_Cloud_Marco_Slaviero
- Troopers 2011 - TR11_Gall_Lueken_Security_and_regulatory_requirements_for_cloud_offerings
- Troopers 2012 - TR12_Day01_Leithner_Cloud_Storage_Security_and_Privacy
- Troopers 2013 – A LOT of presentations from talks and workshops, additional files, go grab them!

REFERENCES

External References

- ISPE, the International Society for Pharmaceutical Engineering.
- http://www.ispe.org/home
- 21CFR11
- http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11
- http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=1002.11
- GAMP
- http://www.ispe.org/index.php/ci_id/2652/la_id/1.htm
- EU version
- http://ec.europa.eu/health/documents/eudralex/vol-4/
- http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf
- X.805 : Security architecture for systems providing end-to-end communications
- http://www.itu.int/rec/T-REC-X.805-200310-I/en
- http://en.wikipedia.org/wiki/FCAPS

BACKUP

A LITTLE HIPAA REF 1

HIPAA Security Rule

- The HIPAA Security Rule specifically focuses on the safeguarding of EPHI.
- In general, the requirements, standards, and implementation specifications of the Security Rule apply to entities working with EPHI.

- Ensure the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

A LITTLE HIPAA REF 2

Security Rule Organization

- Security standards: General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

However, regardless of whether a standard includes implementation specifications, covered entities must comply with each standard.

- A required implementation specification is similar to a standard, in that a covered entity must comply with it.
- For addressable implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment

IMPORTANT PHARMA REGULATIONS

- GxP regulations – at 21 CFR Parts 58, 210 and 211
- Computer system validation principles defined in 21 CFR Part 11 and the guidance to companies who manufacture or sell drugs in the US
- Easy to replicate by other oversight bodies
- Most everyone wants to sell their products in the world's largest market
- Therefore, they MUST apply these principles in their environments; however, how they do so varies greatly
- EU Directives
- Directives 2004/9/EC, 2004/10/EC - GLP
- Directives 2001/20/EC, 2005/28/EC - GCP
- EU Directive 95/46/EC – Data Protection

TRENCHY: FULL PICTURE – OUTSOURCING GOVERNANCE EXAMPLE