



Auditing of GxP Critical Computerised Systems

PharmConf 2010 - München

GlaxoSmithKline worldwide

- GSK was formed in 2001 through the merger of Glaxo Wellcome and SmithKline Beecham
- Operations in over 120 countries and products sold in over 150 countries
- More than 99,000 employees worldwide
- Total turnover £ 28.4 billion, market share of 4.7%



GSK Italian Sites

2 Manufacturing sites, 1 CH site & 1 Head Office



- Manufacturing (Verona e Parma)
- Administration (Verona)
- Consumer HealthCare (Baranzate-MI)

Parma manufacturing site



Verona manufacturing site




- GSK has operated in Italy since 1932
- About 2,300 employees
- Total export €129m (€ 75,8m from production)
- 74 clinical trials managed by GSK Italy in 2009
- Verona and Parma: FDA certified manufacturing facilities exporting to over 120 countries worldwide, including US, Japan and China
- Total area covered: Verona 22,000 m² and Parma 32,000 m²
- Both plants are specialized in sterile products: 95m ampoules and 83m vials in 2009

Objective of this presentation

How to prepare audits of computerised systems supporting GxP critical processes

- Can be used from two different point of views
 - Auditor: how to prepare the audit
 - Auditee: how to be prepared for the audit
- for Internal Audits
- for Supplier Audits

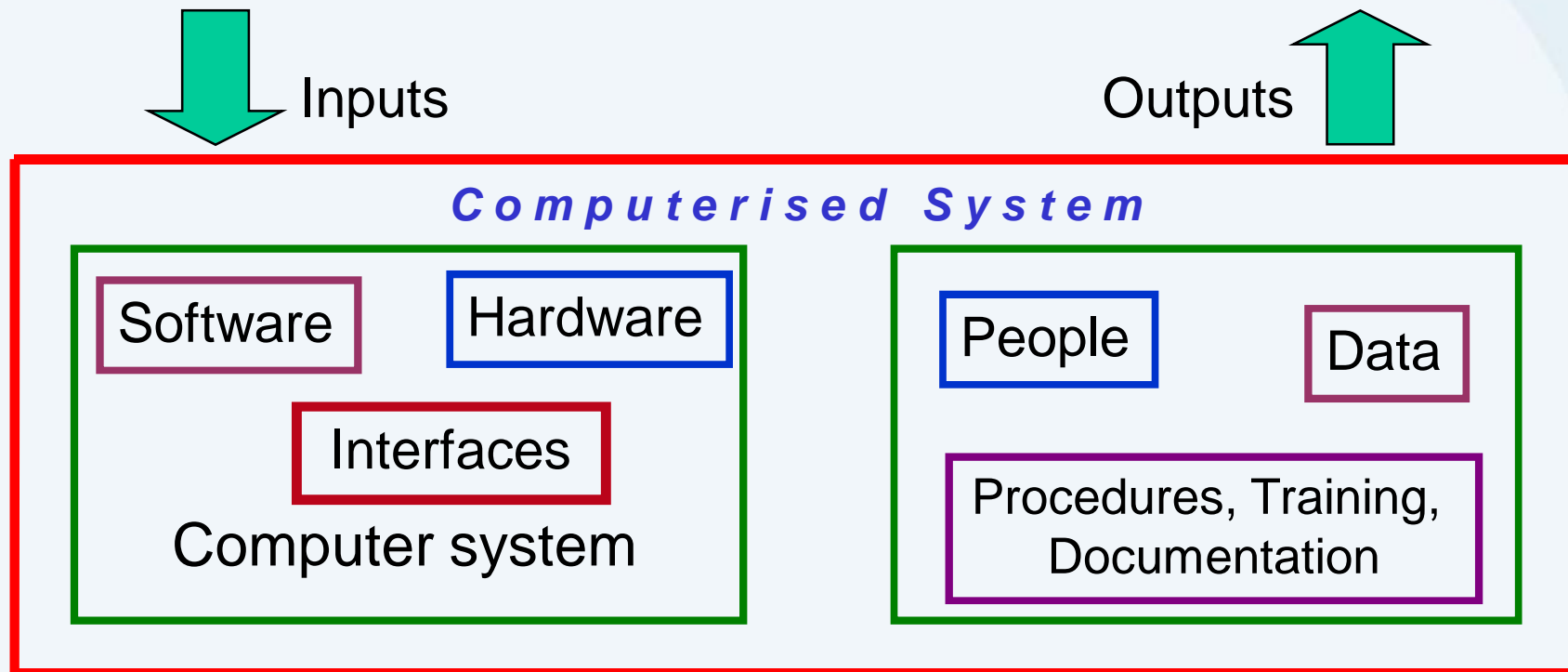


**Computerised System
&
Computerised Systems Validation**

Computerised System Validation

- A **ongoing** process ...
- of establishing **documented evidence**
- to provide a **high degree of assurance**
- that a **computerised system** (and its components)
- will consistently perform to **predetermined specifications**

Computerised System



There are no laws to regulate Computer Systems Validation, but . . .

Guidelines and recommendations used by auditors in order to understand the validation status of IT systems

Particularly interesting are

- ICH - International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use
- PIC/S - Pharmaceutical Inspection Cooperation Scheme
- GAMP5 - Good Automated Manufacturing Practices

exporting products to US market

- FDA Guidelines

Auditing

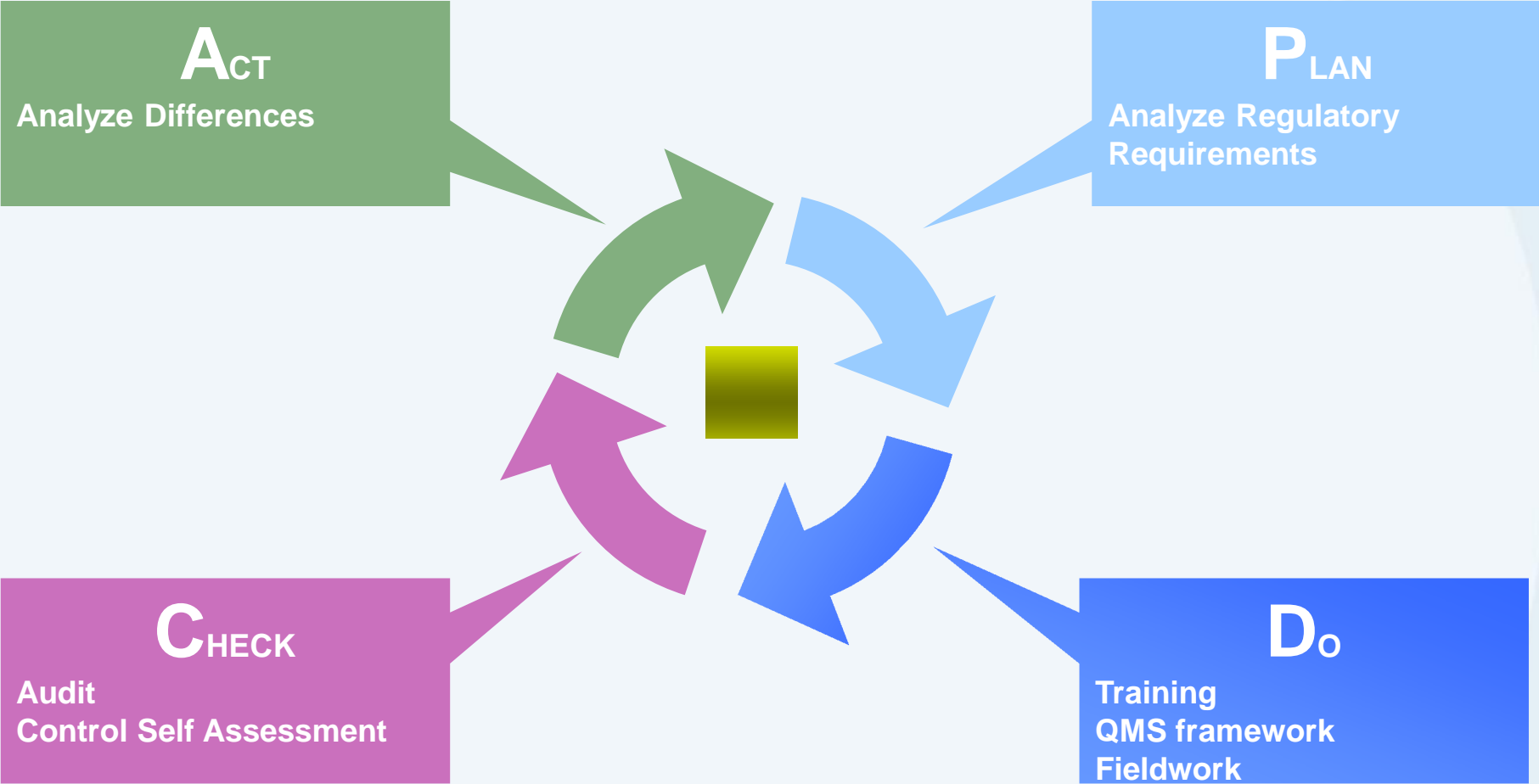
Risk and Audit Universe

Inventory of audit areas
Business Processes and their risks
Maintained regularly
Used in the audit planning process.

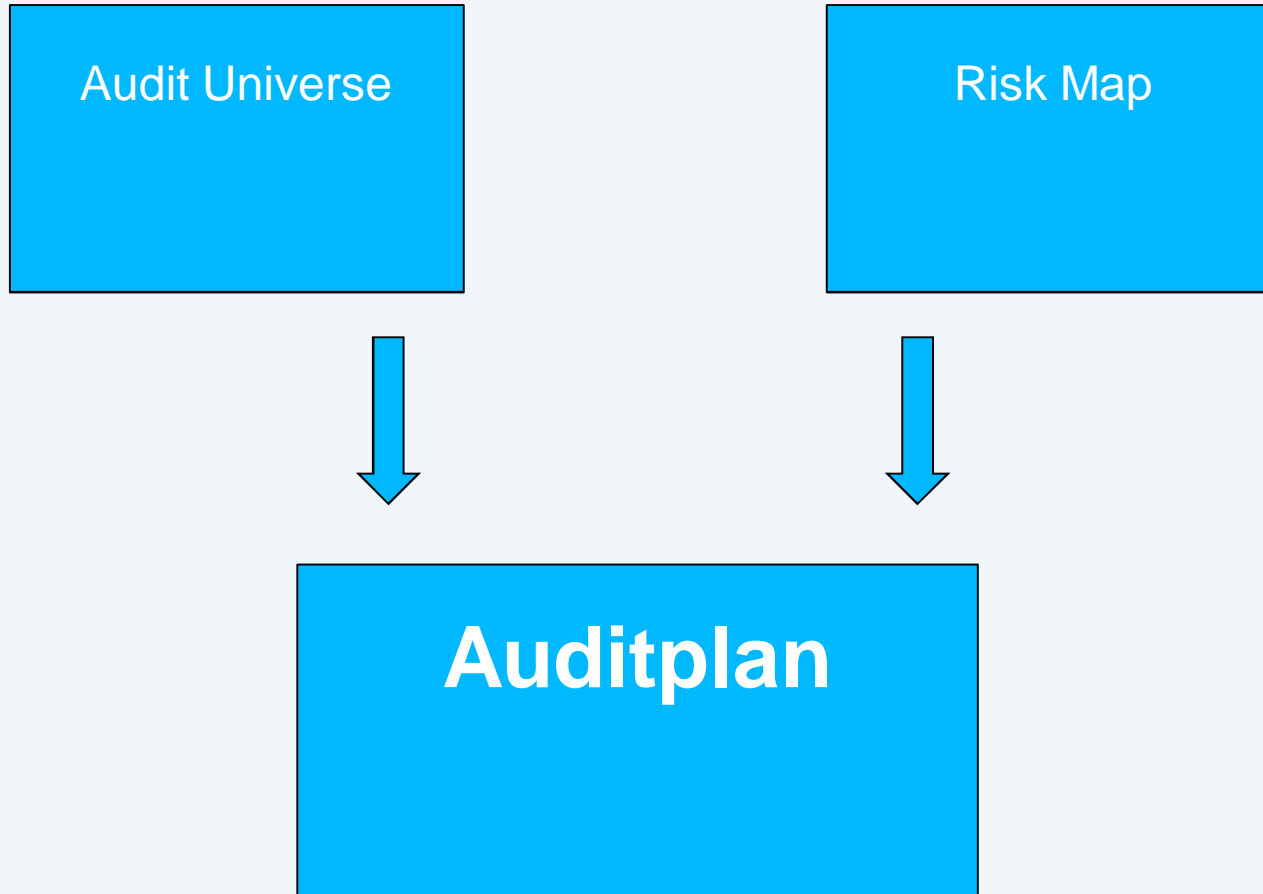
*Copyright :
Max-Planck-Institut
für Astrophysik*

Validation Strategy

(Deming or PDCA cycle)



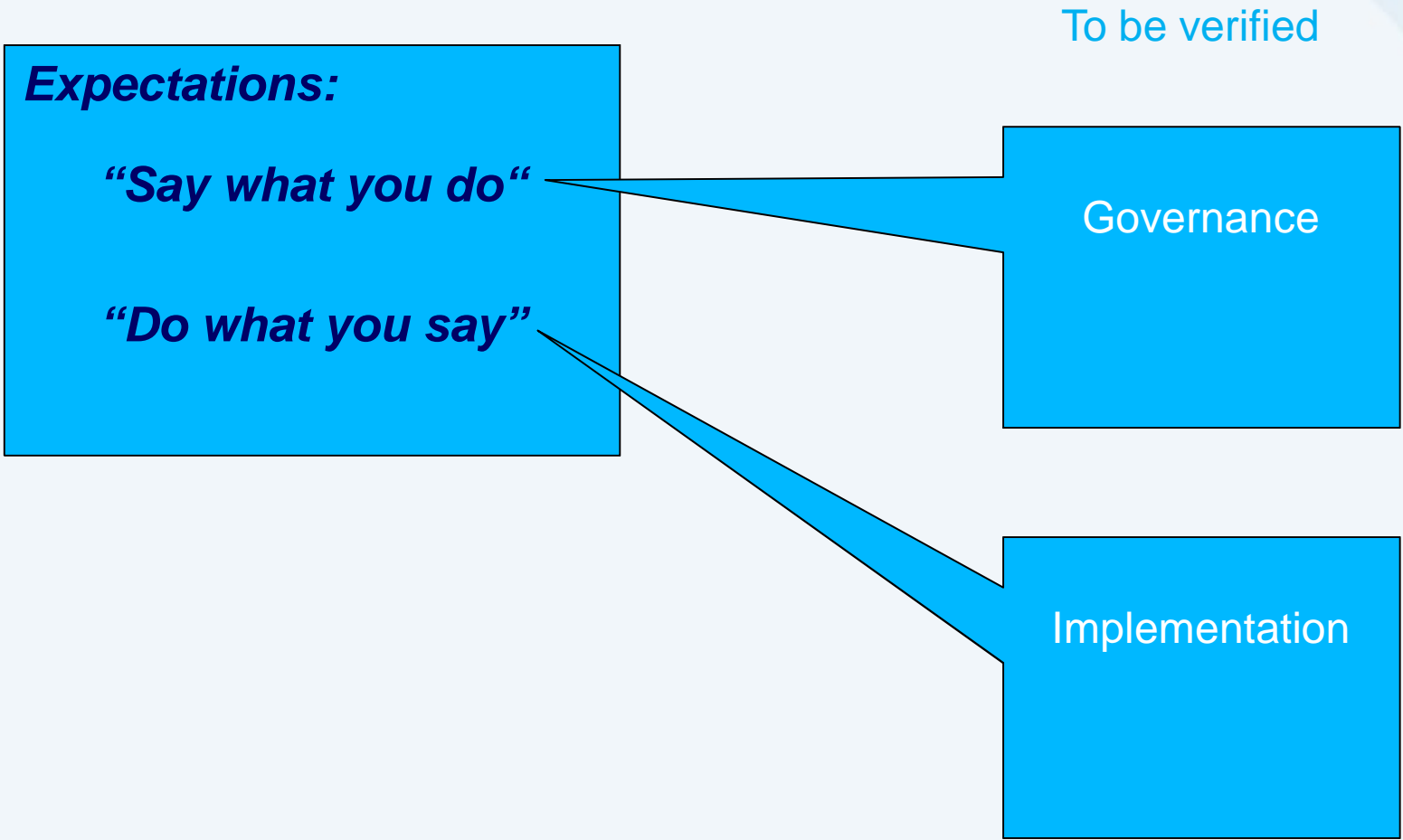
Audit Plan





Audit Checklist

Audit Approach



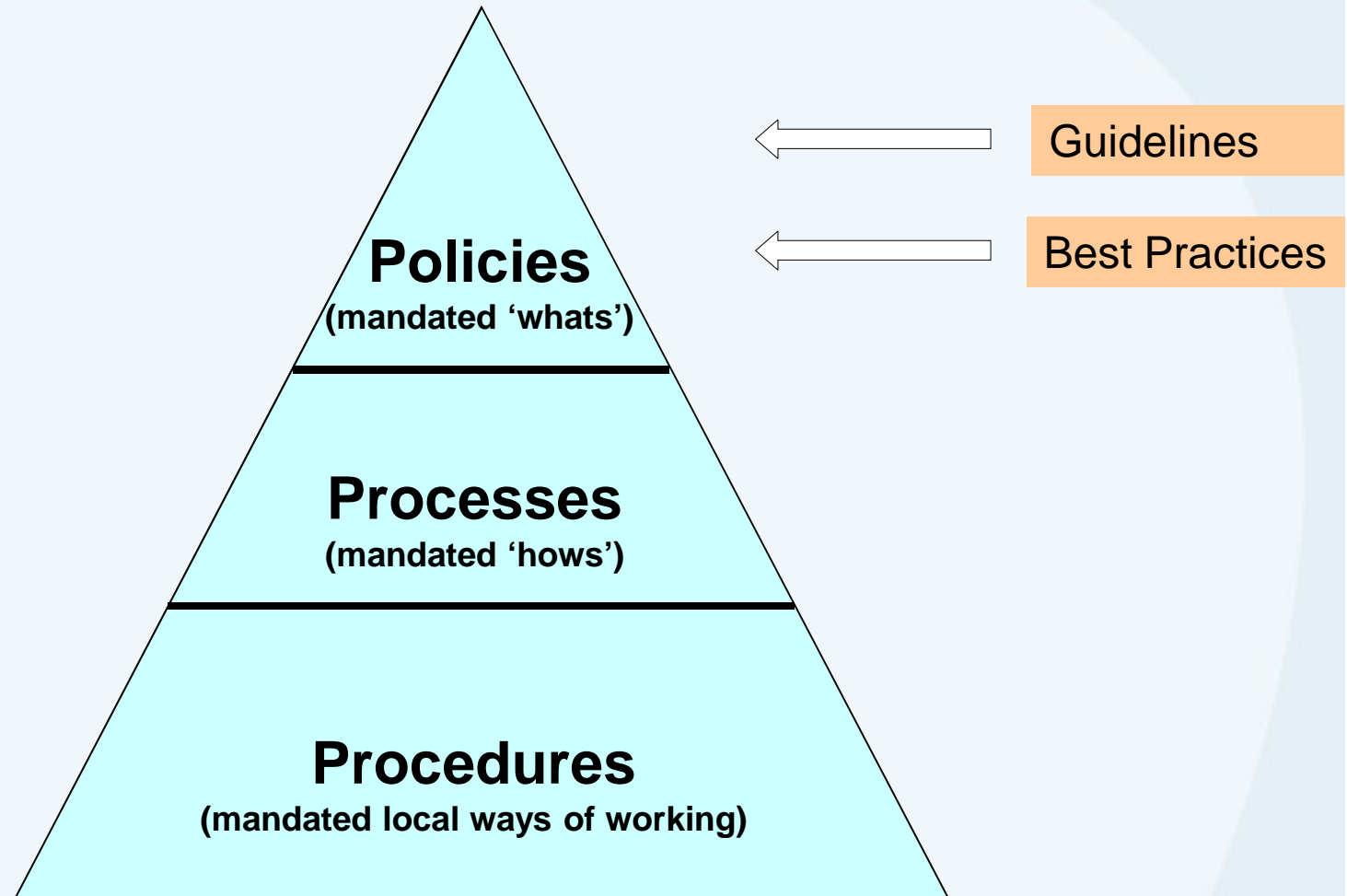
Audited Areas

- Governance: QMS – Policy – Process – Procedure – Operating Guideline
- Computerised Systems Lifecycle
- Document Management System
- Datacenter
- Back & Recovery
- Disaster Recovery
- Security
- Outsourced Services
- ERES / 21 CFR 11 Compliance



Governance

QMS Framework



System Overview

- System Register

System Name	System ID	Description	Validation Status	Contacts	Documents (Location)
.....					

- System Description

People

Human resources are the key of a solid working computerised system, therefore following documents should be in place:

- Organizational Charts
- Role Descriptions
- Training Matrix – training per role
 - technical
 - SOPs
 - regulation, laws, ..
- Documentation of Training Records
- CV

Example: Role of Business

- Assure that all computerised systems are
 - Correctly validated
 - Used in compliance of their validation status
 - Maintained in a validated status
- Collaborate at validation activities
- Assure that all business roles are adequately prepared
- Assure correct usage of computerised systems
- Be “inspection-ready”

Example: Role of QA

- Assure correct interpretation of GxP and regulatory aspects
- Be point of contact in case of inspections
- Coordinate validation activities
- Assure application of QMS standards
- Verify status of validation of computerised systems
- Support business in question of QMS/validation
- Approve documents of validation

Example: Role of IT

- Assure that development, maintenance and change management of computerised systems are compliant with QMS standards
- Maintain Computerised Systems Registry
- Support Business in case of inspections

Audit Checklist

Does a Quality Policy exist ?

Yes No

Comments or referral to external Document:

Does a Quality Management System exist ?

Yes No

Comments or referral to external Document:

Does a separate QA function exist ?

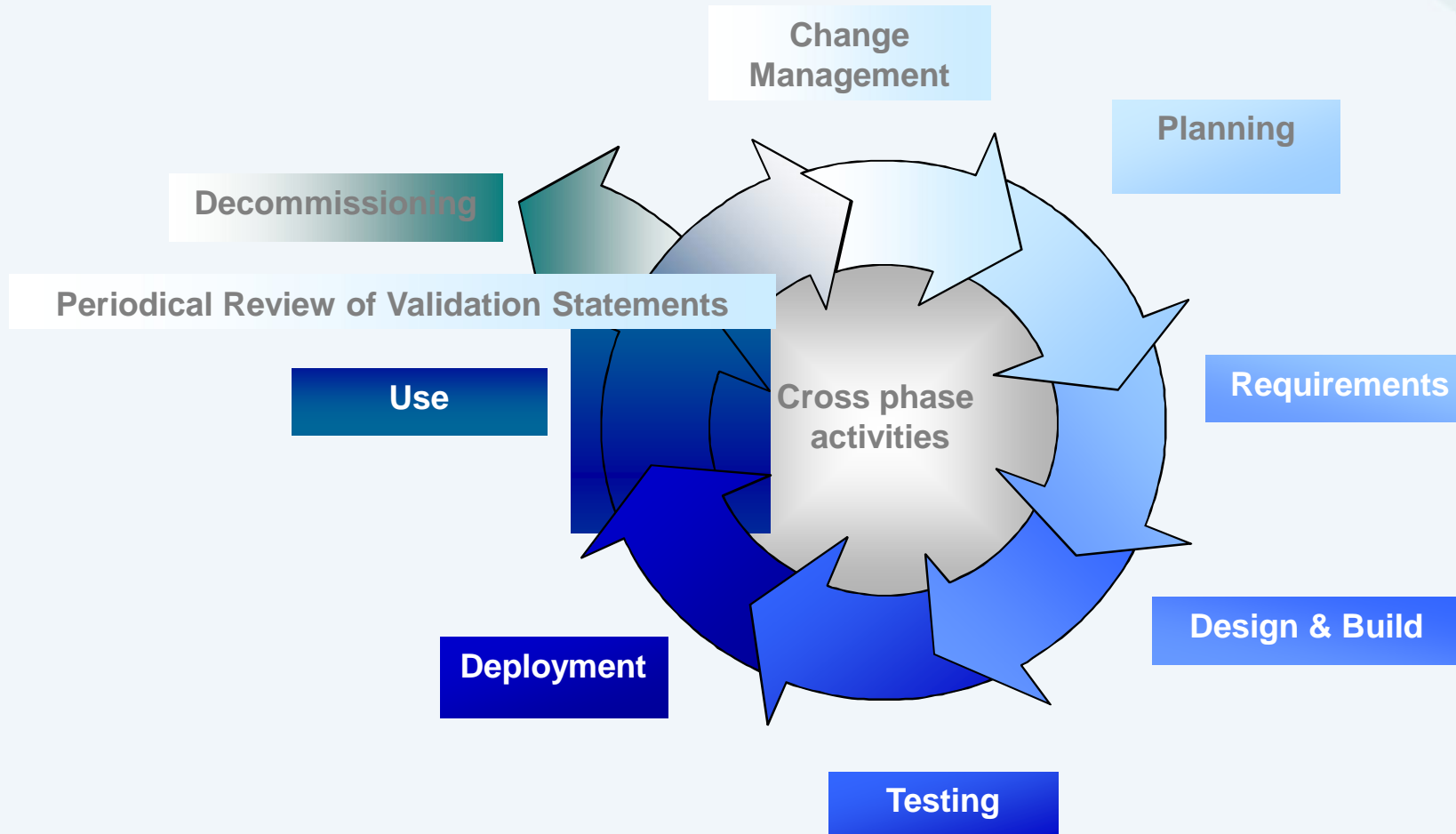
Yes No

Comments or referral to external Document:



Computerised System Lifecycle

Computerised Systems Lifecycle



Audit Checklist

Does a model for system life cycle exist ?

Yes No

Comments or referral to external Document:

Are all involved employees adequately trained ?

Yes No

Comments or referral to external Document:

Does a QA function audit the life cycle ?

Yes No

Comments or referral to external Document:



Document Management System

Audit Checklist

Does a document management system exist ?

Yes No

Comments or referral to external Document:

Is the reason for each signature documented ?

Yes No

Comments or referral to external Document:

Are the approver independent from the author ?

Yes No

Comments or referral to external Document:

Record Retention

Where is documentation stored ...

...



Data Center

Datacenter

- How is access to the data centre controlled ?
- Are all entries to the datacenter controlled (windows, ...) ?
- Any procedures in place for entry to data centre (training) ?
- Is there a printed list of personnel that have access to the data centre?
How often is this list checked ?
- Is there any audit trail of accesses ?
- Is Data Center protected form environmental hazards (power failure, fire, flood, overheating,theaft, etc.) ?
- Supplier Audit: are there separate areas for each customer ?



Back & Recovery

Backup & Recovery

- Any procedures in place for backup (training) ?
- Is there a backup log in place to check for failures etc?
- Are backups restored at regular intervals to check the integrity of the data ? Are these checks documented ?
- What measures are in place to prevent unauthorised access to backup media ?
- Are copies of software backups located on-site and/or off-site?
- Are off-site copies stored at a safe distance ?
- Are backups regularly restored to test the integrity ?



Disaster Recovery

Disaster Recovery

- Are procedures in place for disaster recovery (training) ?
- Are these procedures regularly tested (is there a log) ?
- Are systems supporting critical processed build redundantly ?
- Are the redundant systems stored at a secure distance ?



Security

Security

- Does a security policy exist ?
 - Is personell appropriately trained ?
 - Does a risk assessment process exist ?
 - Are responsibilities clear defined ?
 - User awareness of security / acceptable use of IT resources ..
 - Is there a password policy ?
 - Is there a system against malicious software ?
 - Intrusion Detection System ...
-
- see also backup & recovery / desaster recovery



Still Some Hints



Outsourced Services

External Suppliers

- Responsibility cannot be outsourced
- Rules in Place (SOPs)
- Validation Documentation
- Audits – Inspections of External Suppliers
 - supplier audit from customer
 - external authorities (FDA, health agency,...)



Retrospective Validation

Retrospective Validation

- Should not exist
- Should it happen however better to have a plan
- Risk Assessment
- Use / not Use Decision
- System Release Notification



Central Applications local deployed

Central Application – local deployed

- Central Validation maybe not applicable locally
- Intended Use
- Local Legislation
- Additional Validation Activities (a.e. Printer)
- Deployment Plan
- Deployment Report



User Side Computing

User Side Computing

What is USC

Tools and Application which allow users to write applications, for example: Excel, Notes, Access, shell scripts but also HTML files with embedded JavaScript, etc.

Risk of USC

Application Development of IT well regulated, well documented, subject of change management, done by trained persons. Users normally none of the before mentioned. Therefore the risk is applications not centrally known, not under control and not sure to be working.

User Side Computing

Control Tools

- **Clear Guidelines, SOPs of what users should do/ should not do**
- **User training regarding Computer System Validation.**
- **Control Self Assessments which allows user to self assess eventual risks.**
- **Internal Audits to verify correct user behavior and offer consulting to users.**



Audit Readiness

Audit Readiness

- have in place all documentation
 - checklist (maybe “audit SOP”)
 - “technical” documentation
 - correct record retention
- have well prepared persons
 - audit coordination
 - correct persons informed / available
 - specific audit preparation

Audit Readiness

- all necessary infrastructure in place
 - rooms (control centre, documentation room, audit room)
 - communication infrastructure in place



Questions & Answers



**any later questions / comments
to:
reinhard.e.voglmaier@gsk.com**