Auditing GxP Critical Computerized Systems

ISACA Italia

February, 17, 2010

Milano, Italy

Objectives

- Understanding the Validation Process
- How to audit GxP critical Computerized Systems
- Inspection Readiness

Can be used from two different point of views

- *Auditor: how to prepare the audit*
- *Auditee: how to be prepared for the audit*

Roadmap

- Introduction
- Regulations & Guidelines
- Governance
- System Inventory
- People
- System Lifecycle
- Change Management
- Incident Management
- Risk Management
- Security
- Supplier Management
- Inspection Readiness
- Q&A

Introduction

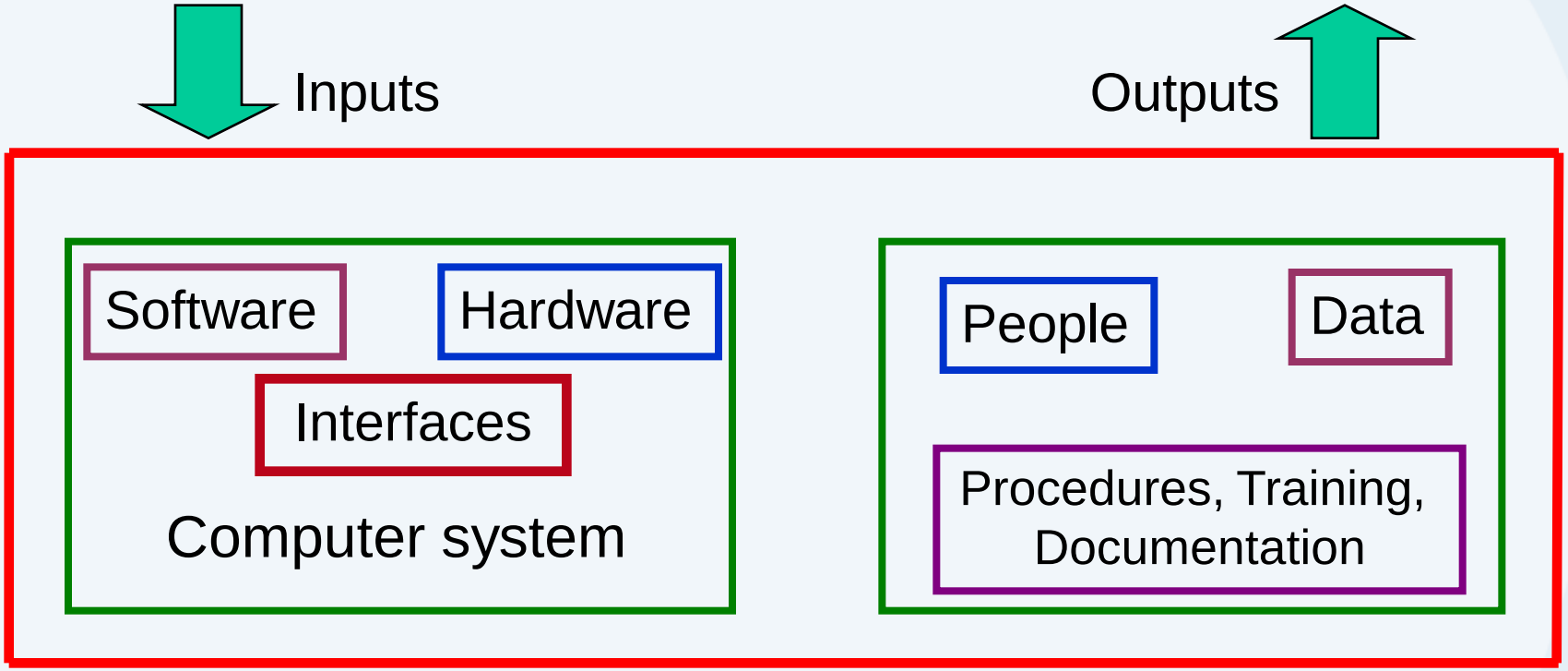
Definitions

Introduction

- What is a Computerized System ?
- What is therefore Computerized Systems Validation ?
- Why Computerized Systems Validation ?

What is a Computerized System ?

Not only HW and SW, but also users, administrators, business processes, SOPs, ….



COMPUTERIZED SYSTEM

What is Computerized Systems Validation ?

Computerized Systems Validation is:

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

Why CSV ?

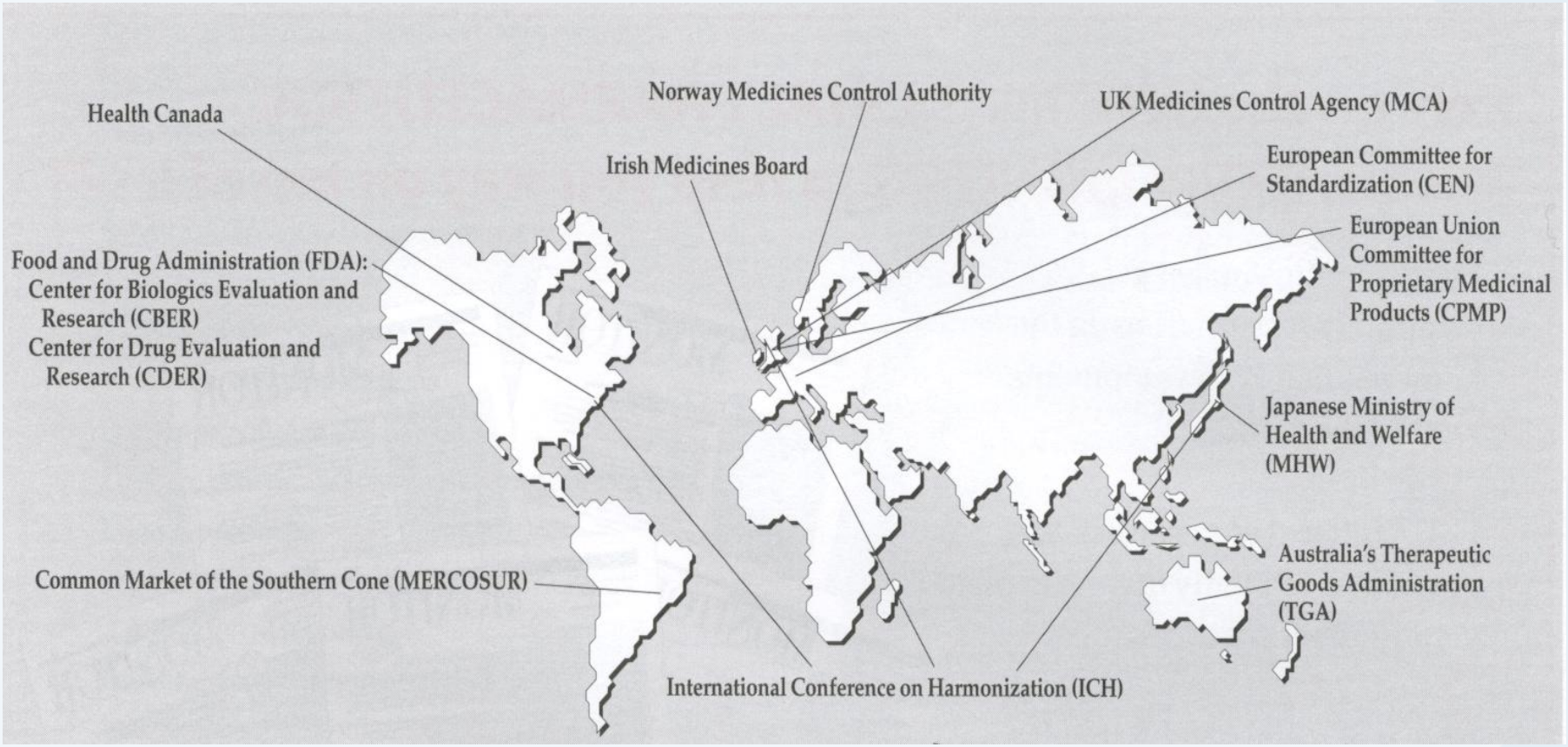
- Ensure the use of system is safe for the
  - quality of the product
  - health of the patients
- Get confidence in Data produced by the system
- Compliance with regulations
- Assure “Inspection Readiness”
- Confidence of patients to products
- Avoid negative publicity
- Maximise business benefits to be derived from IT systems

GxP

- **GXP == Good x Practices**
- **Good Manufacturing Practice**
- **Good Laboratory Practice**
- **Good Clinical Practice**
- **Good Distribution Practice**
- **. . .**

Regulations & Guidelines

A lot of regulatory agencies pay increasing attention on computerised systems ….



Regulations
(description thx to Wikipedia)

- AIFA www.agenziafarmaco.it
  - Agenzia Italiana del Farmaco
  - Decreto Legislativo 24 Aprile 2006 n. 219 - Attuazione della direttiva 2001/83/CE (e successive direttive di modifica) relativa ad un codice comunitario concernente i medicinali per uso umano, nonché della direttiva 2003/94/CE

Regulations
(description thx to Wikipedia)

- Eudralex www.ema.europa.eu
  - EudraLex is the collection of rules and regulations governing medicinal products in the European Union
  - Volume 1 - EU pharmaceutical legislation for medicinal products for human use
  - Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use
  - Volume 9 - Guidelines for pharmacovigilance for medicinal products for human and veterinary use
  - COMMISSION DIRECTIVE 2003/94/EC of 8 October 2003 laying down the principles and guidelines of good manufacturing practice in respect of medicinal products for human use and investigational medicinal products for human use

Regulations
(description thx to Wikipedia)

- MHRA www.mhra.gov.uk

  - The Medicines and Healthcare products Regulatory Agency (MHRA) is the UK government agency which is responsible for ensuring that medicines and medical devices work and are acceptably safe.

    The agency was formed on 1 April 2003 with the merger of the Medicines Control Agency (MCA) and the Medical Devices Agency (MDA). It is an executive agency of the Department of Health.

  - Rules and Guidance for Pharmaceutical Manufacturers and Distributers (aka ‘Orange Book’)

Guidelines
(description thx to Wikipedia)

- ICH www.ich.org
  - The International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) is a project that brings together the regulatory authorities of Europe, Japan and the United States and experts from the pharmaceutical industry in the three regions to discuss scientific and technical aspects of pharmaceutical product registration.
  - Q7: Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients
  - Q9: Quality Risk Management
  - Q10: Pharmaceutical Quality System

Regulations
(description thx to Wikipedia)

- FDA , US Code of Regulations, Title 21: Food and Drugs
  - 21 CFR Part 11 – Electronic Records, Electronic Signatures
  - 21 CFR Part 58 - Good Laboratory Practice for Nonclinical Laboratory Studies
  - 21 CFR Part 210 - Current Good Manufacturing Practice in Manufacturing, Processing, Packaging or Holding
  - 21 CFR Part 211 - Current Good Manufacturing Practice for Finished Pharmaceuticals
  - Medical Devices 21 CFR Part 820 - Quality System Regulation

Guidelines
(description thx to Wikipedia)

- PIC/S www.picscheme.org
  - The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme is meant as an instrument to improve co-operation in the field of Good Manufacturing Practices between regulatory authorities and the pharmaceutical industry.
  - Guidance on Good Practices for Computerized Systems in Regulated “GxP’ Environments (PI 011-3) September 2007

Guidelines
(description thx to Wikipedia)

- GAMP Richtlinien www.ispe.org
  - is a trademark of the International Society for Pharmaceutical Engineering (ISPE). The ISPE's guide The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture describes a set of principles and procedures that help ensure that pharmaceutical products have the required quality.

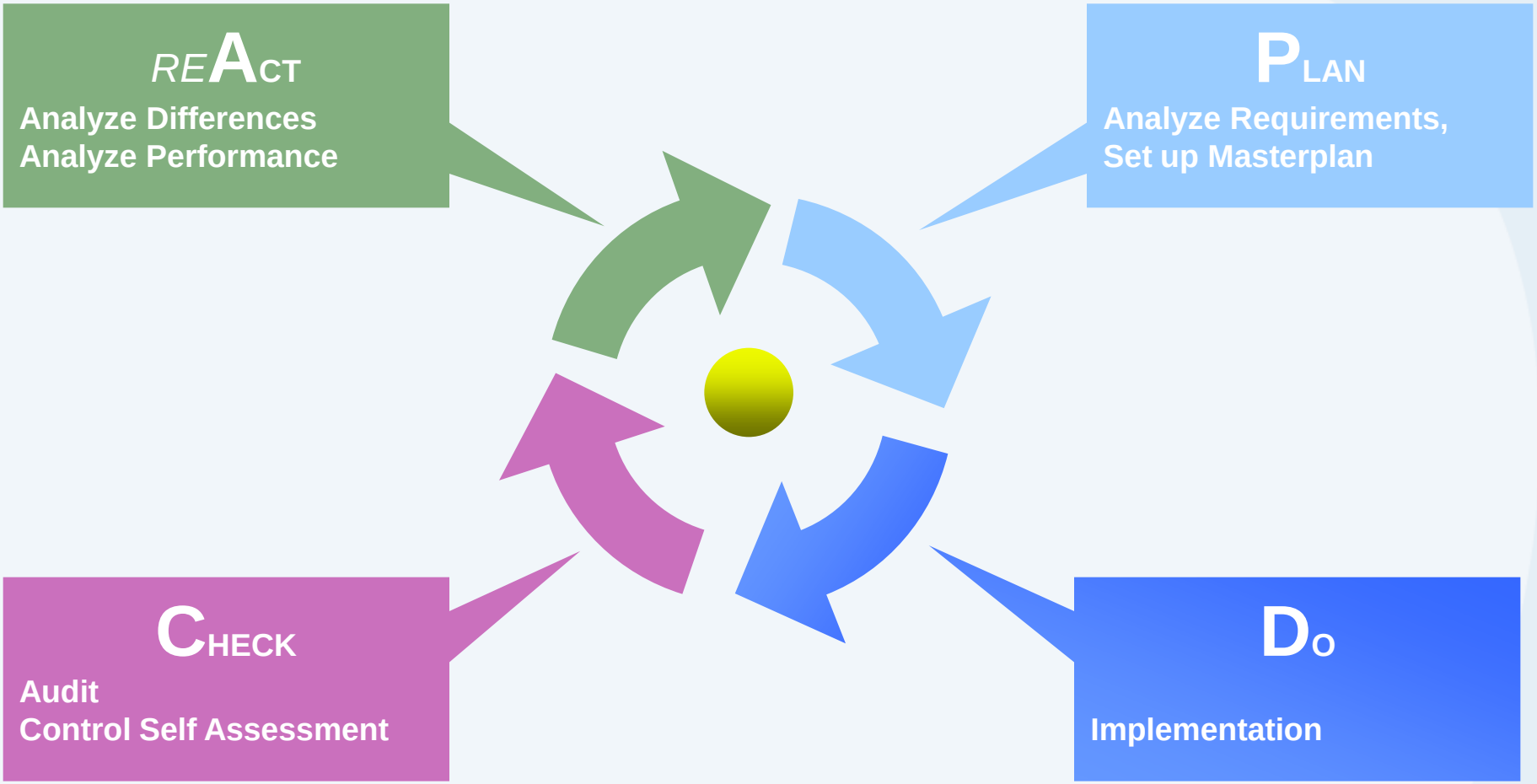
  - GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems

Q7: Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients

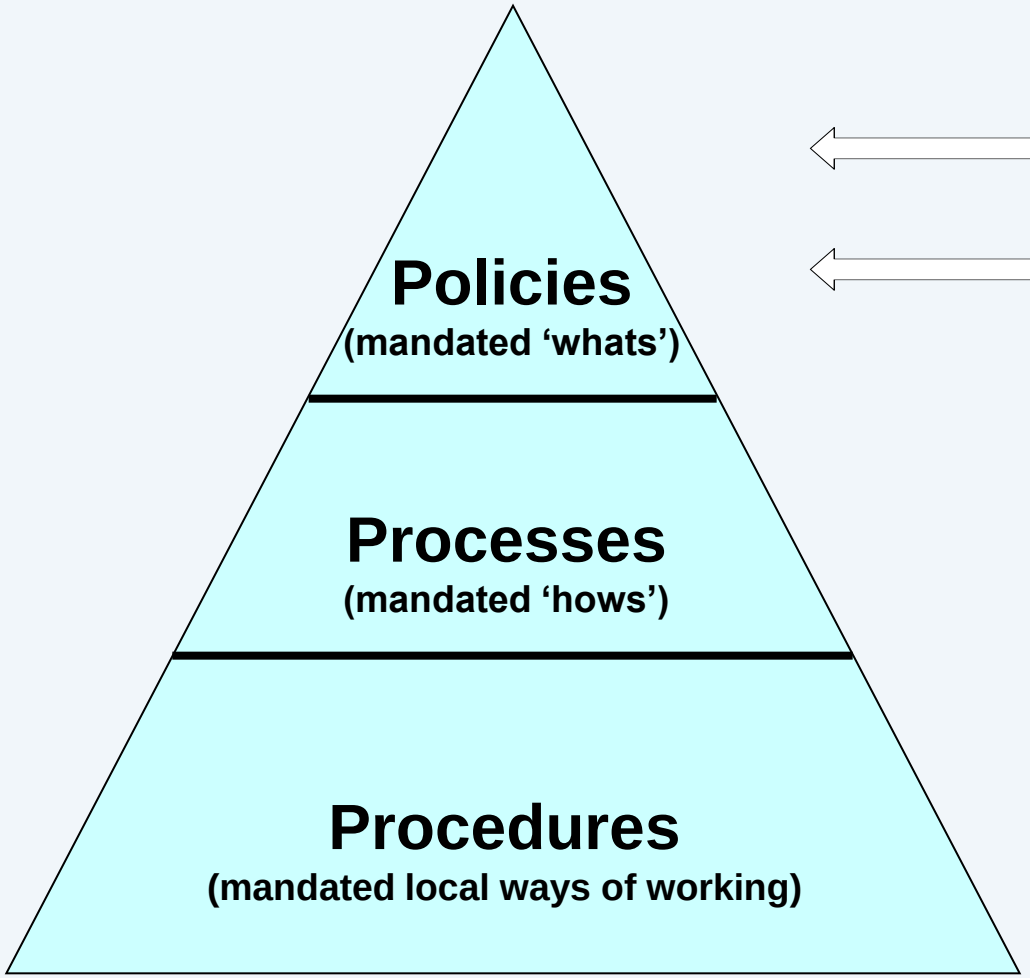
- **5.4 Computerized Systems**
  - 5.40 GMP related computerized systems should be validated. The depth and scope of validation depends on the diversity, complexity and criticality of the computerized application.
  - 5.41 Appropriate installation qualification and operational qualification should demonstrate the suitability of computer hardware and software to perform assigned tasks.
  - 5.42 Commercially available software that has been qualified does not require the same level of testing. If an existing system was not validated at time of installation, a retrospective validation could be conducted if appropriate documentation is available.
  - 5.43 Computerized systems should have sufficient controls to prevent unauthorized access or changes to data. There should be controls to prevent omissions in data (e.g. system turned off and data not captured). There should be a record of any data change made, the previous entry, who made the change, and when the change was made.

Governance

Validation Strategy
(Deming or PDCA cycle)



Validation Framework



Validation Governance

- Strategy
- Validation Framework (QMS)
- Clear Roles & Responsibilities
- Training
- System Inventory
- Supplier Management
- Record Retention Policy
- IT Governance

Document Management

- Applicable for all phases of the lifecycle
- Defined in the QMS (Standard Documents, Templates)
- Clear definition who approves and why
- Version Control, Motivation for Versions
- Storage in a way to avoid unintended and unauthorized change
- Definition of Record Retention Policy

System Inventory

System Inventory

- System Register

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

- System Description
- Periodical Review

People

People

Human resources are the key of a solid working computerized 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

Training

All persons involved in development, maintenance, use and validation must be trained to peform their assigned tasks

- Procedures
- Documentation
- Training is Up to Date
- Evaluation on Effectiveness
- Control of Training Activities

Roles & Responsibilities

- Process Owner
- System Owner
- QA
- SME - Subject Matter Expert
- Supplier
- End User

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

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”

Role of QA

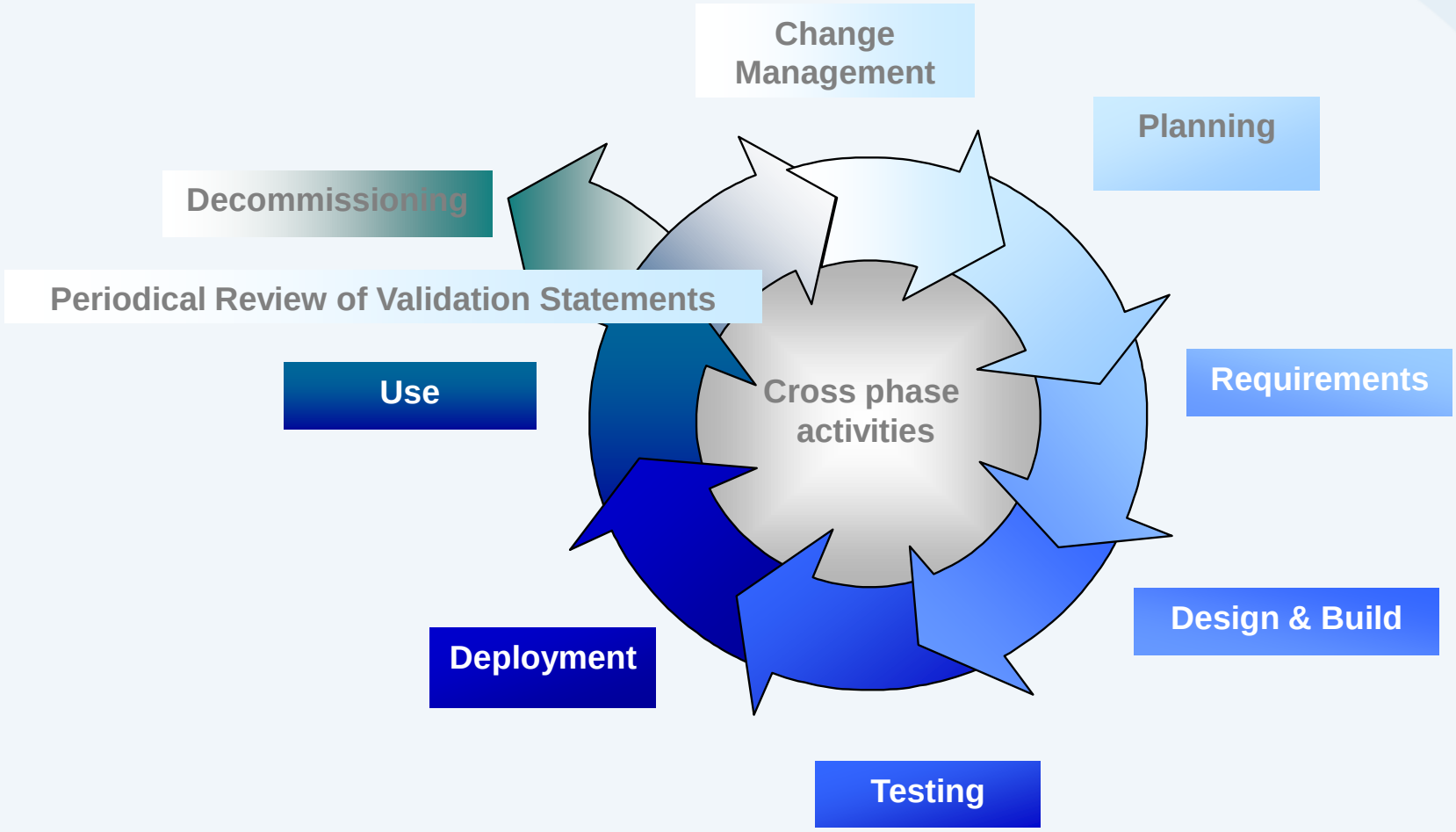
- Assure correct interpretation of GxP and regulatory aspects
- Be point of contact in case of inspections
- Coordinate validation activities
- Assure application of QMS standards
- Verify status of validation of computerised systems
- Support business in question of QMS/validation
- Approve documents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

System Lifecycle

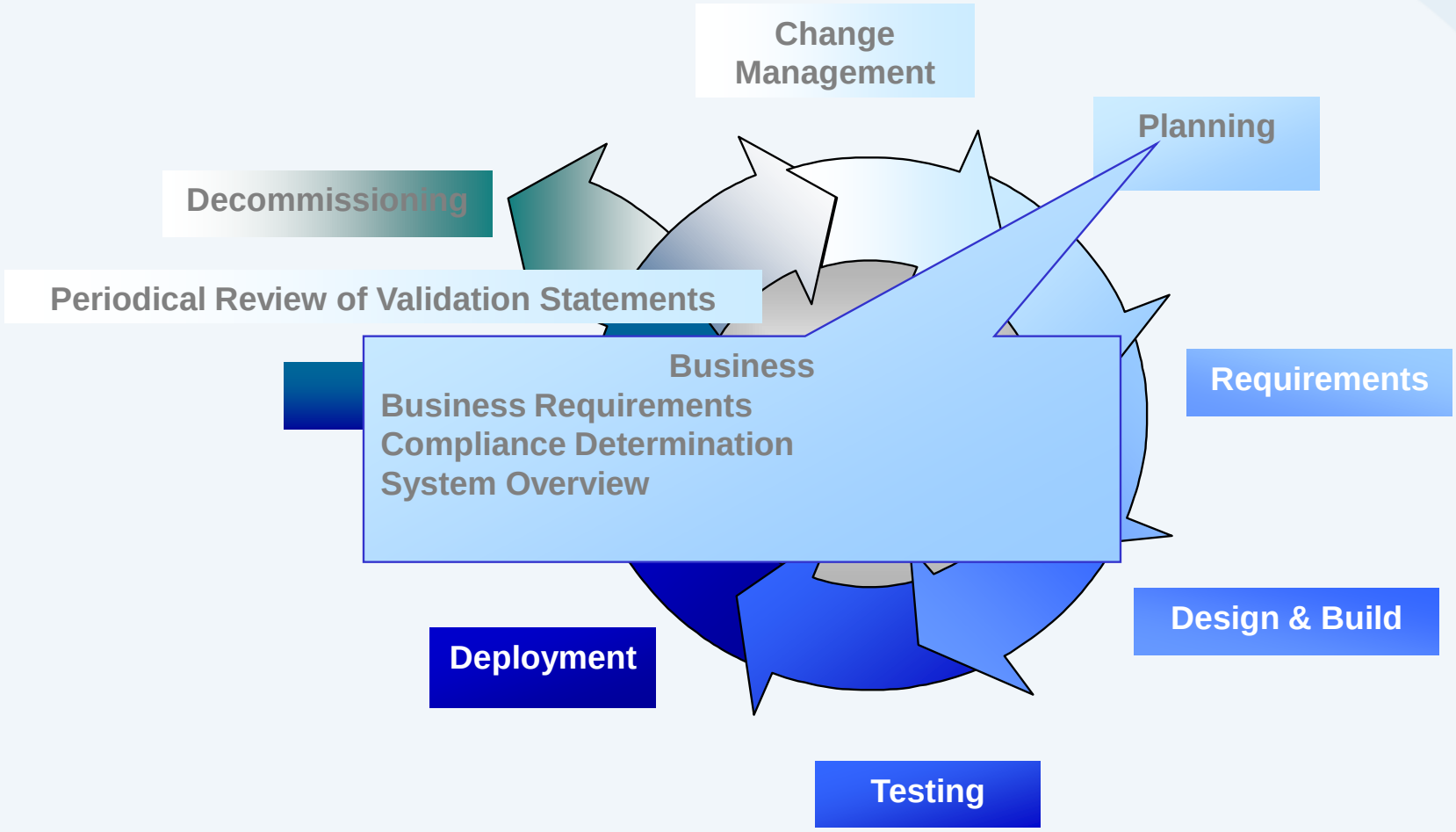
System Lifecycle

- Planning
- Design
- Operation
- Retirement

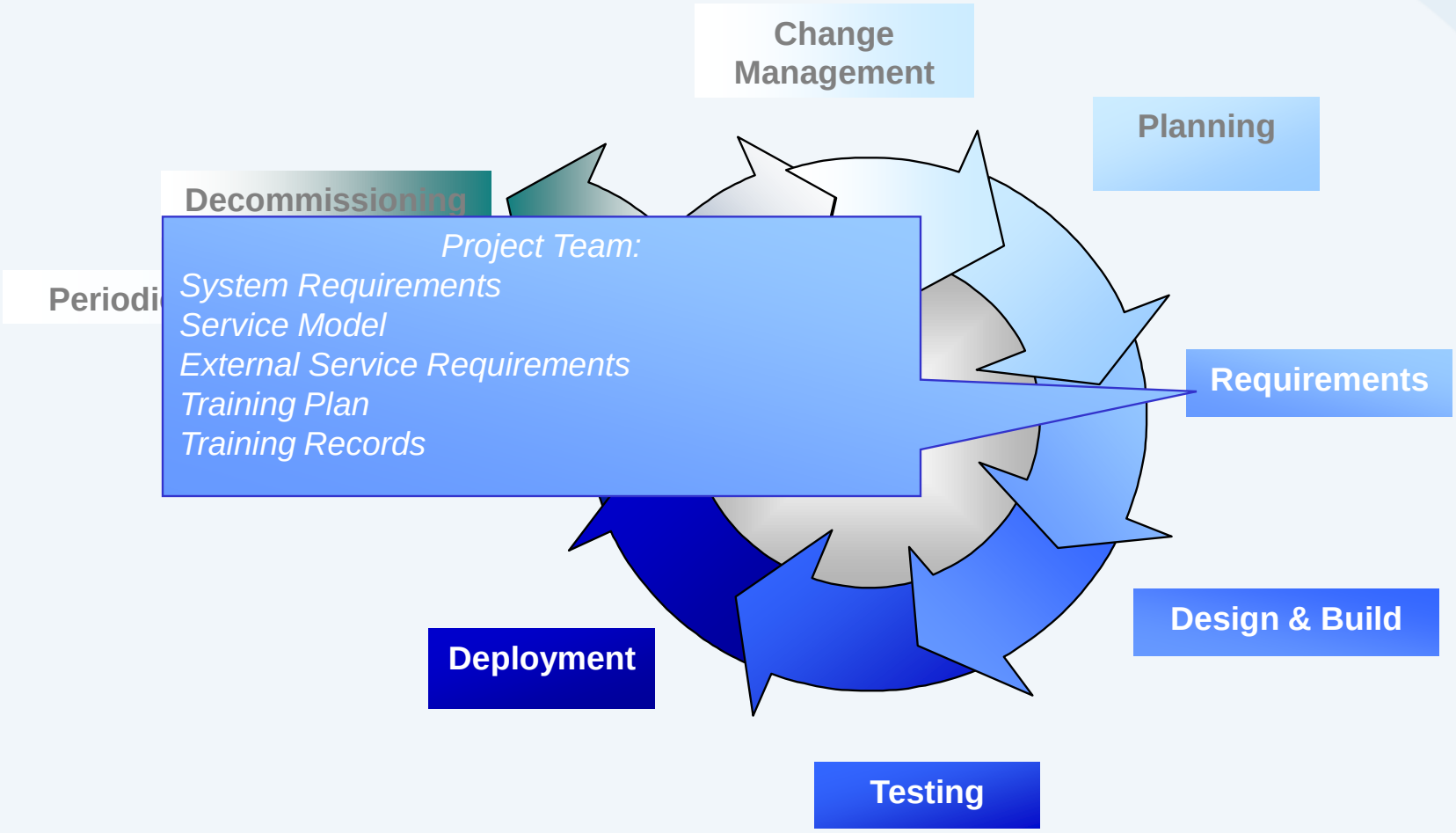
System Lifecycle



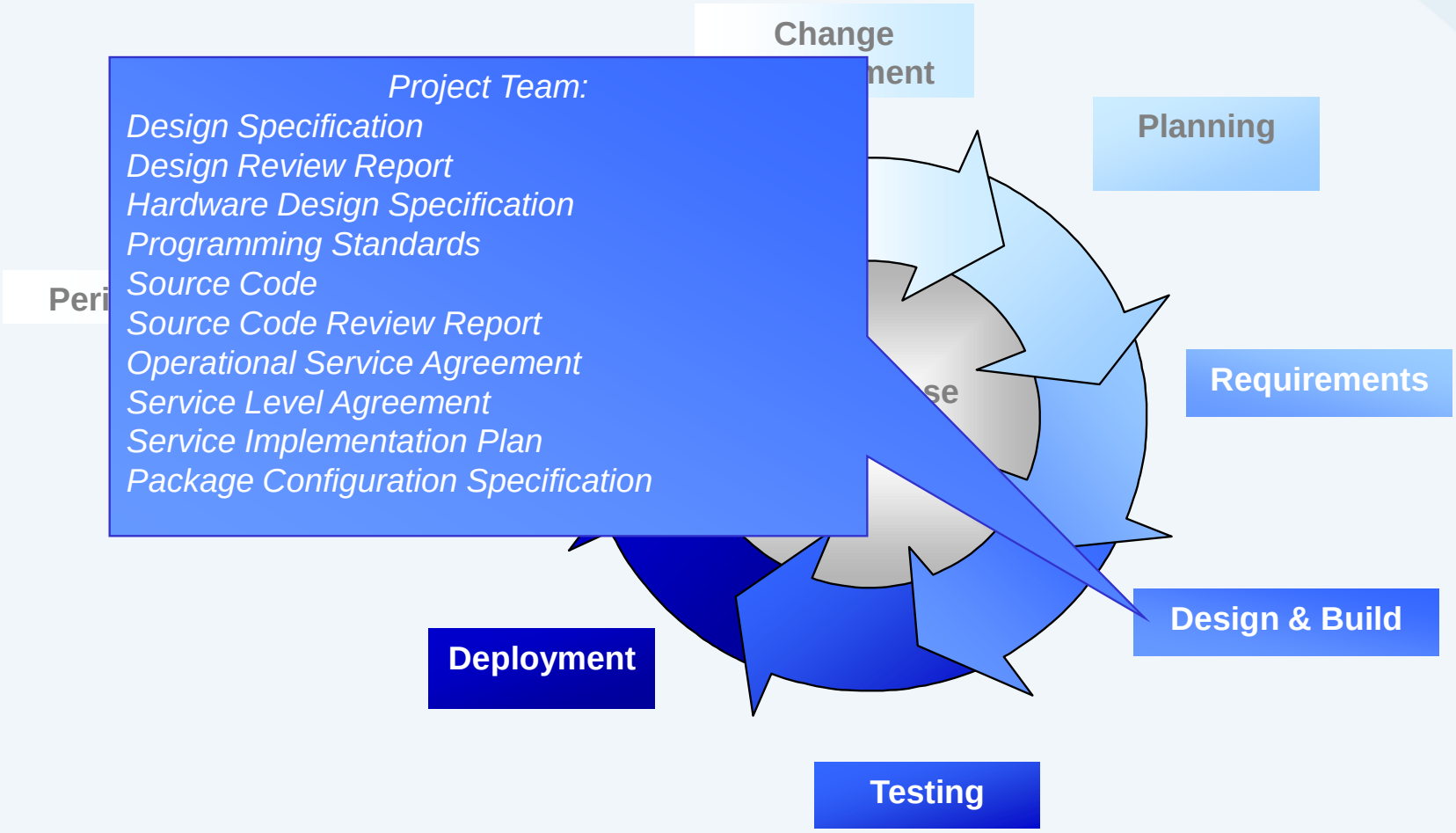
System Lifecycle



System Lifecycle

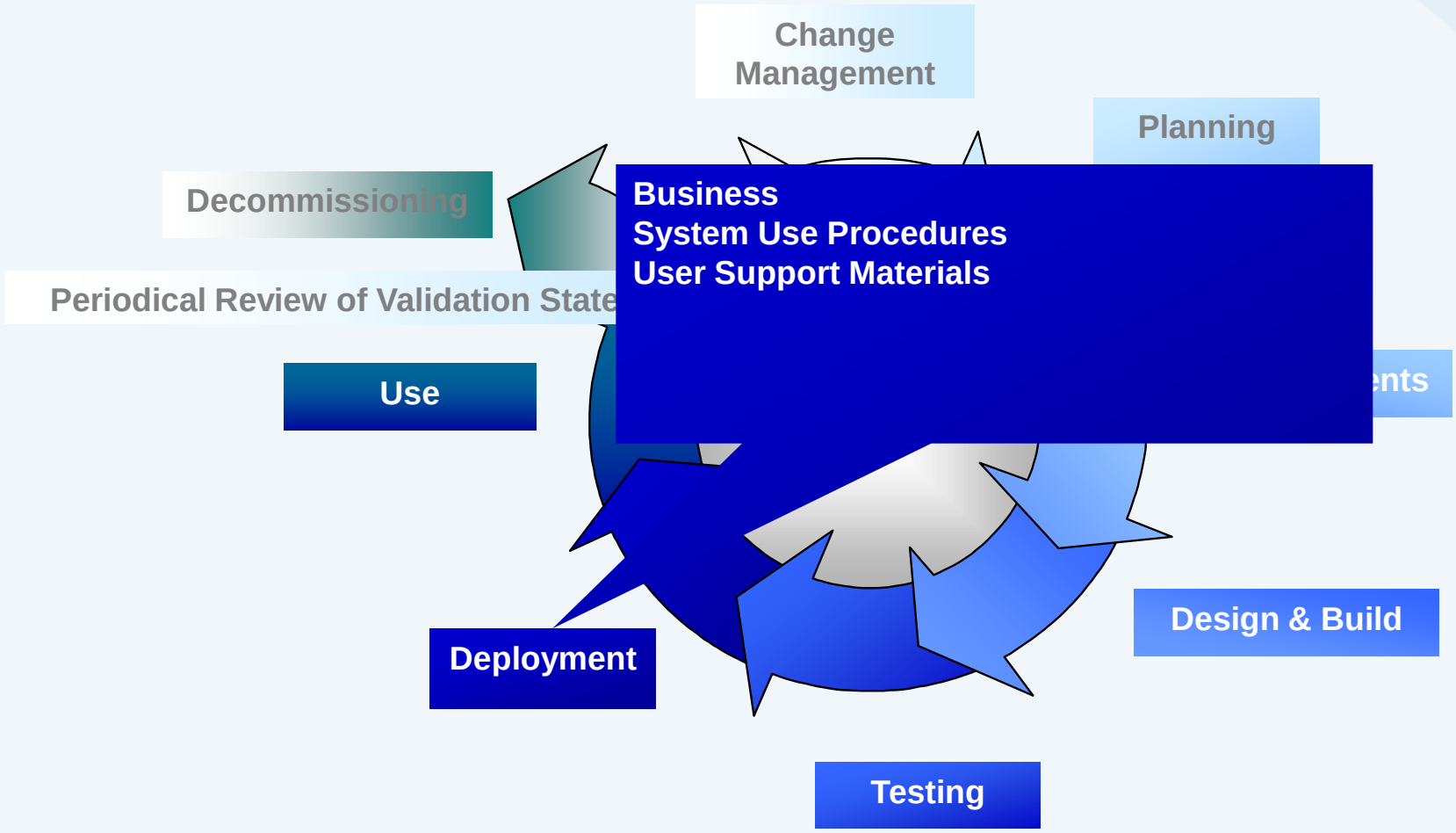


System Lifecycle

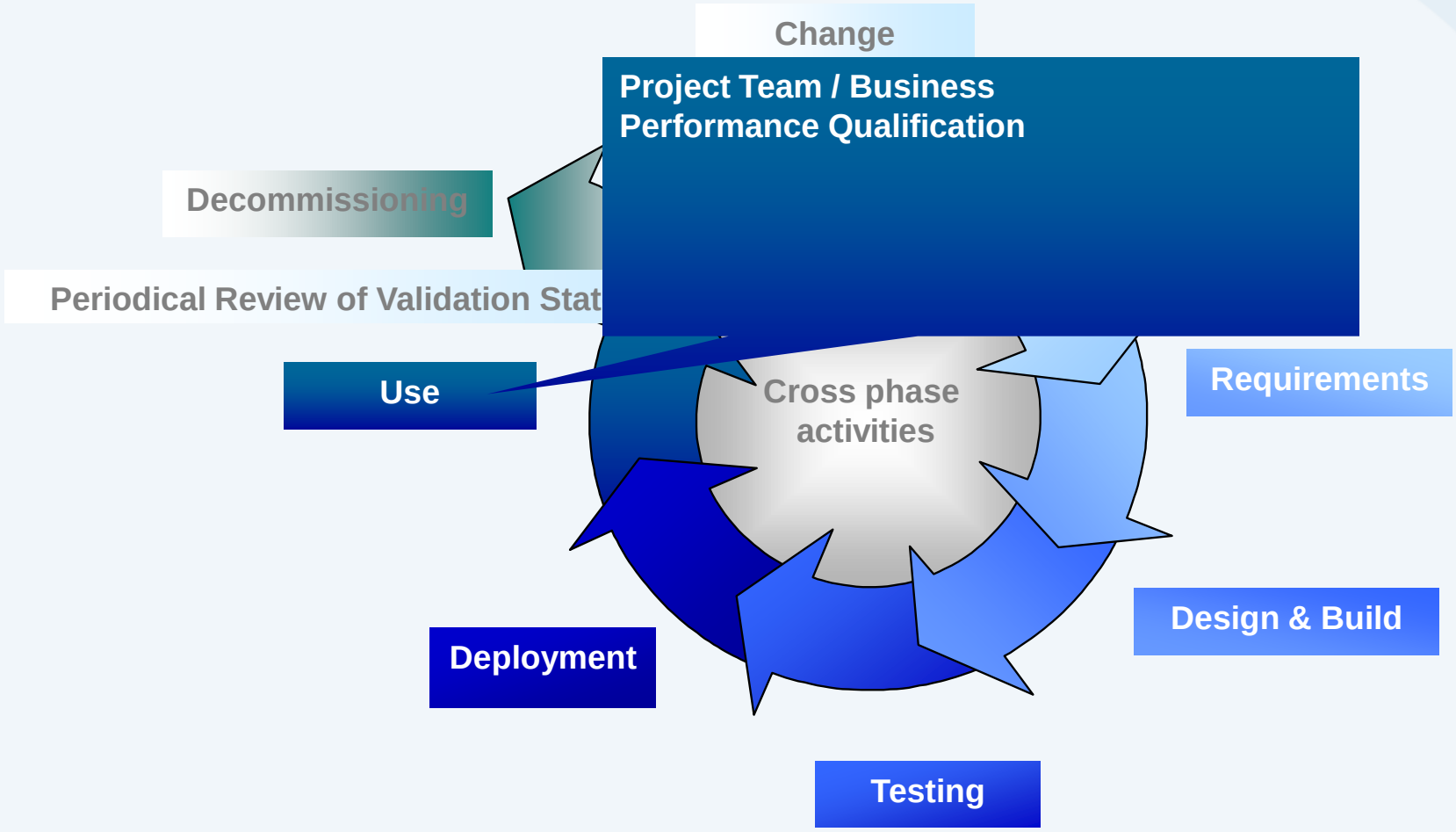


System Lifecycle

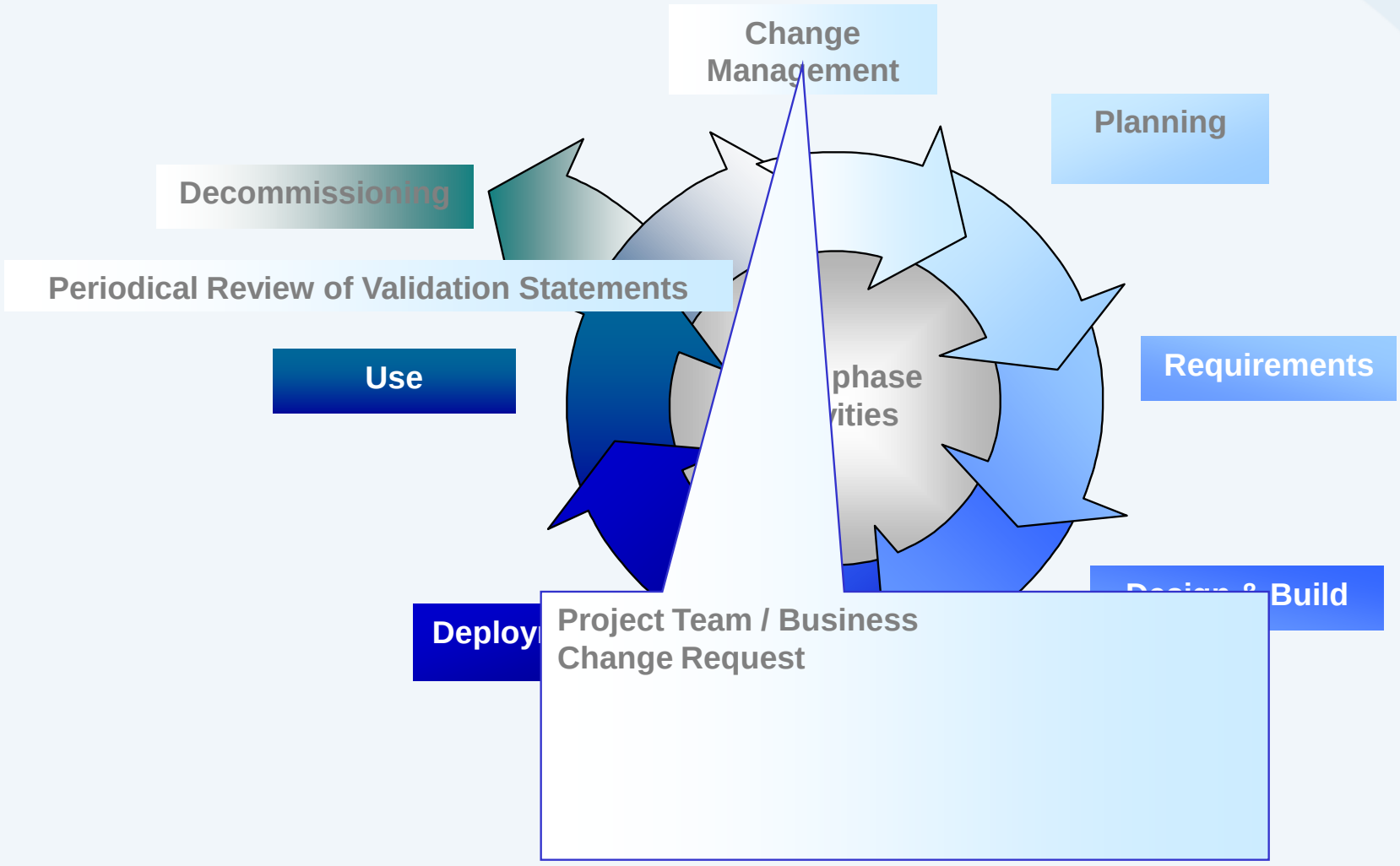
System Lifecycle



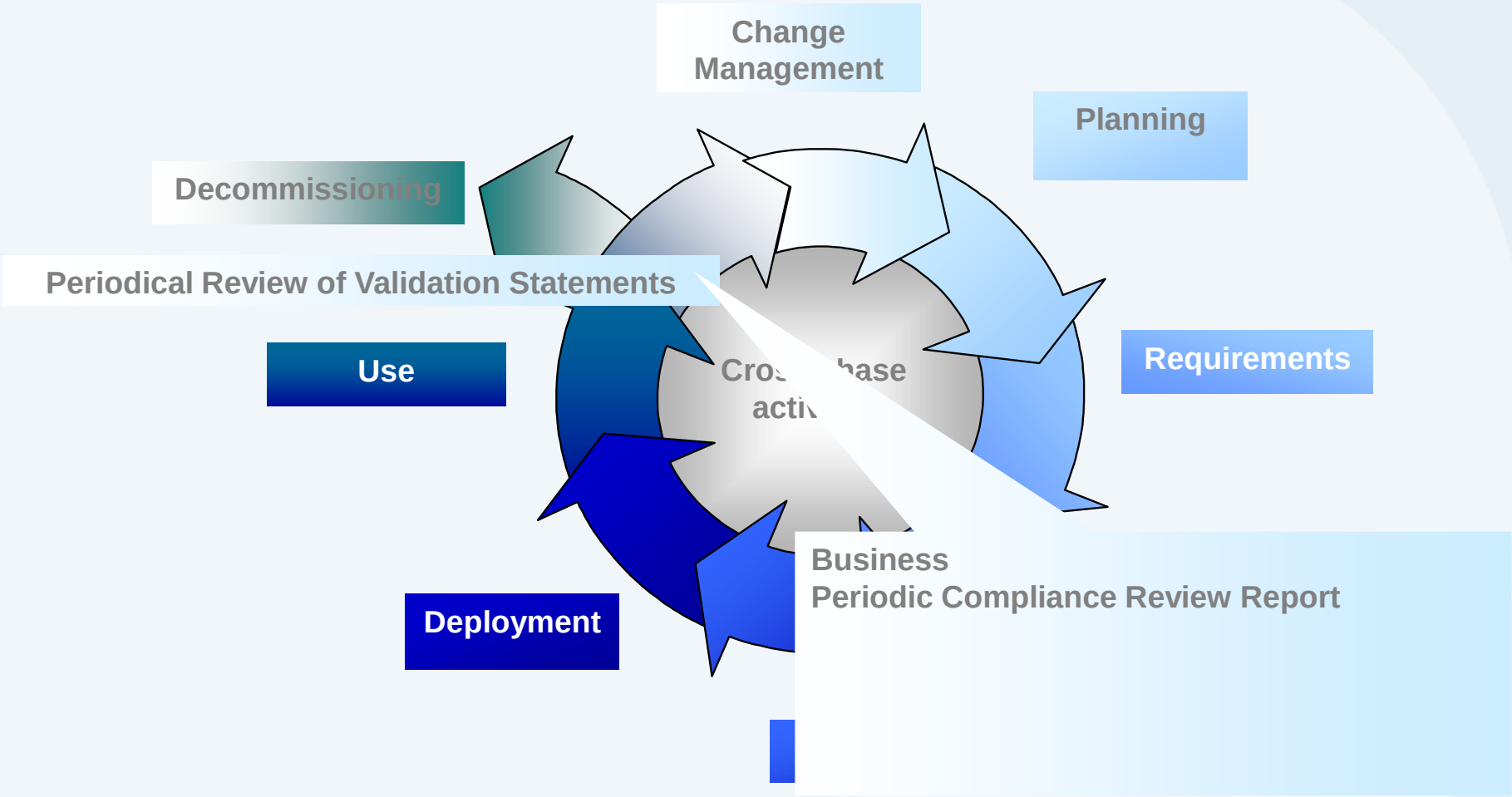
System Lifecycle



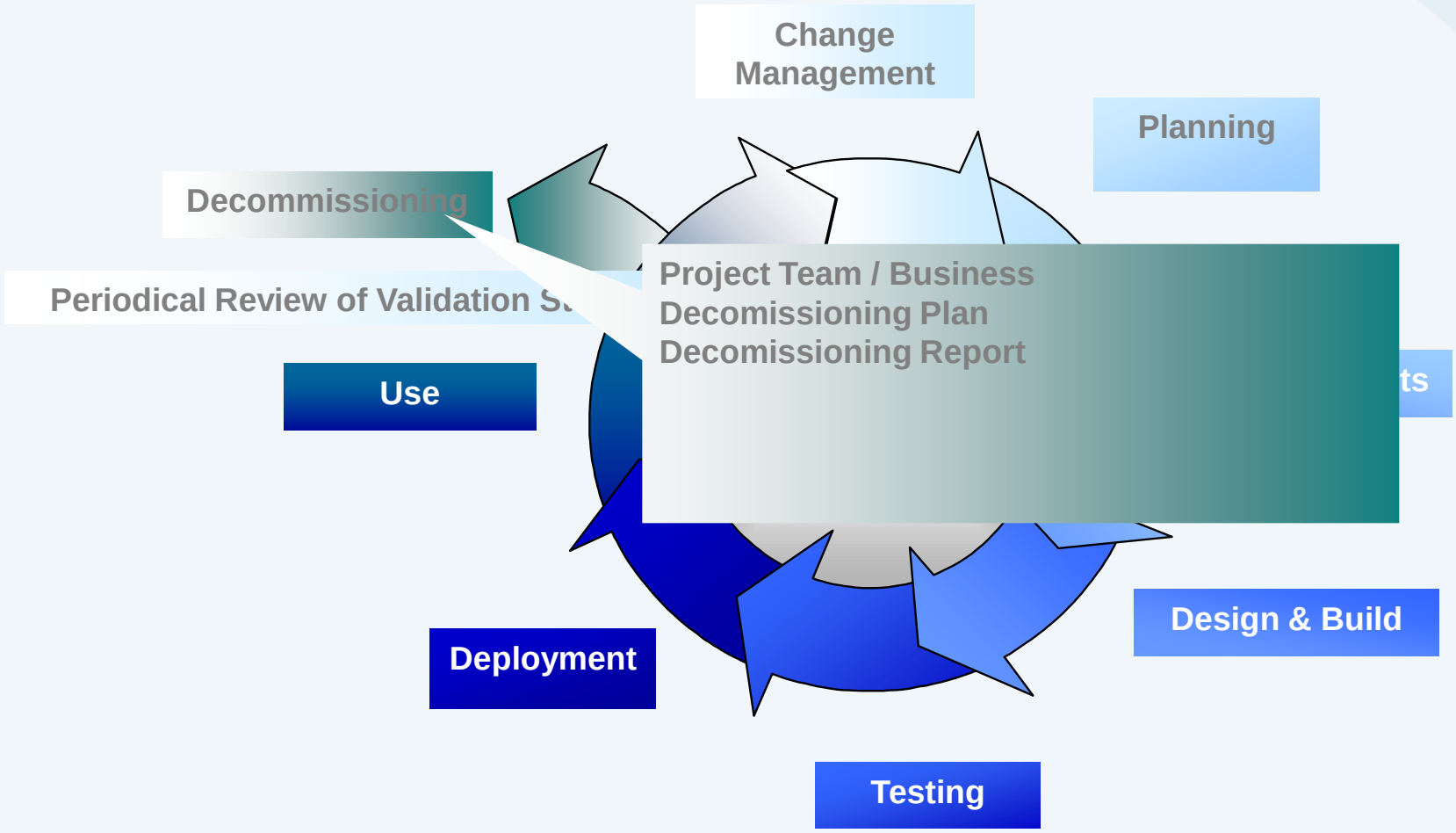
System Lifecycle



System Lifecycle



System Lifecycle



Scaling

Quite different Computerized Systems, ranging

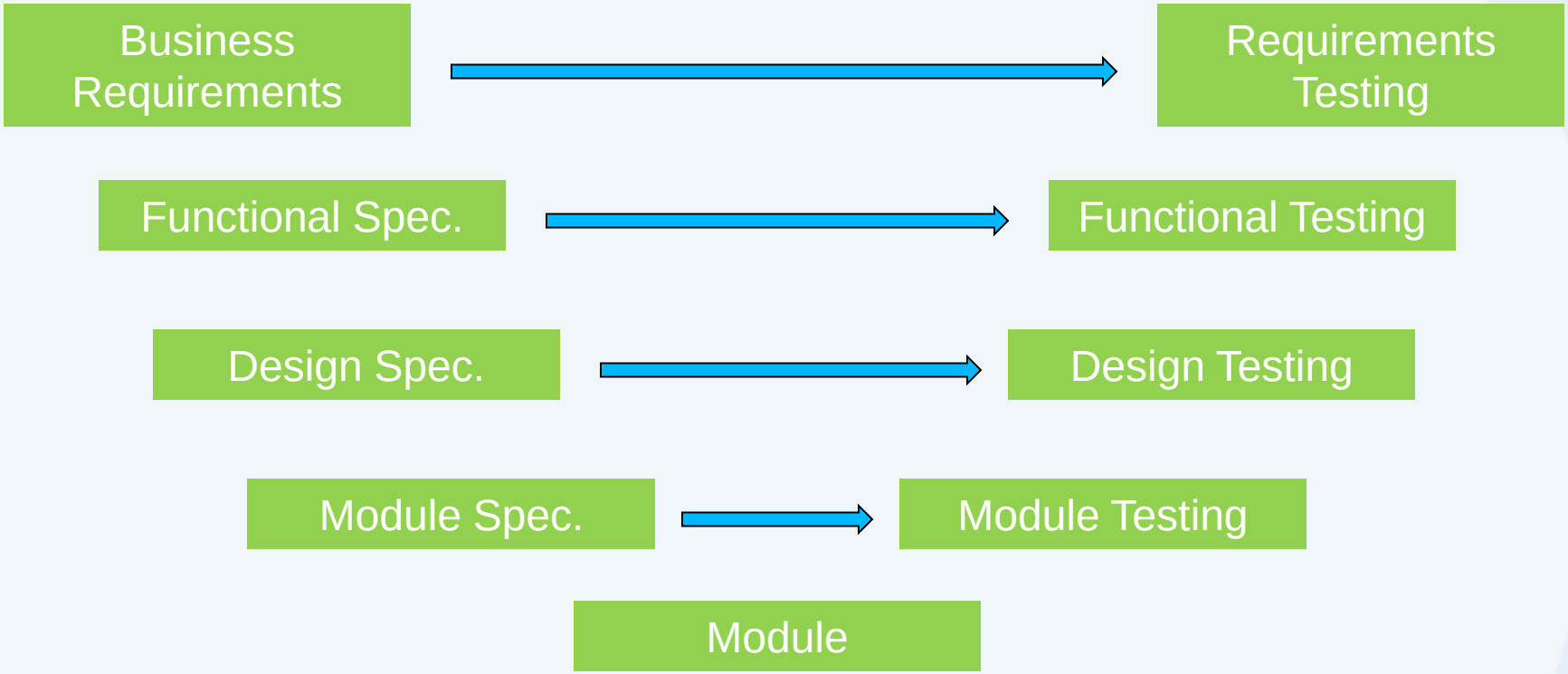
- From one single spreadsheet up to multi-tier application
- From single desktop up to multination application spanning continents.
- From preconfigured system (plug & play) up to applications developed with several teams

Software Categories

- following GAMP 5 -

- Category 1 – Infrastructure Software
- (Category 2 – Not used any more)
- Category 3 – Non-configured products
- Category 4 – Configured products
- Category 5 – Custom Application

Traceability



Change Management

Objectives

- Avoid unintentional or unauthorized change

GXP

- Preserve validation status of the system

Type of Changes

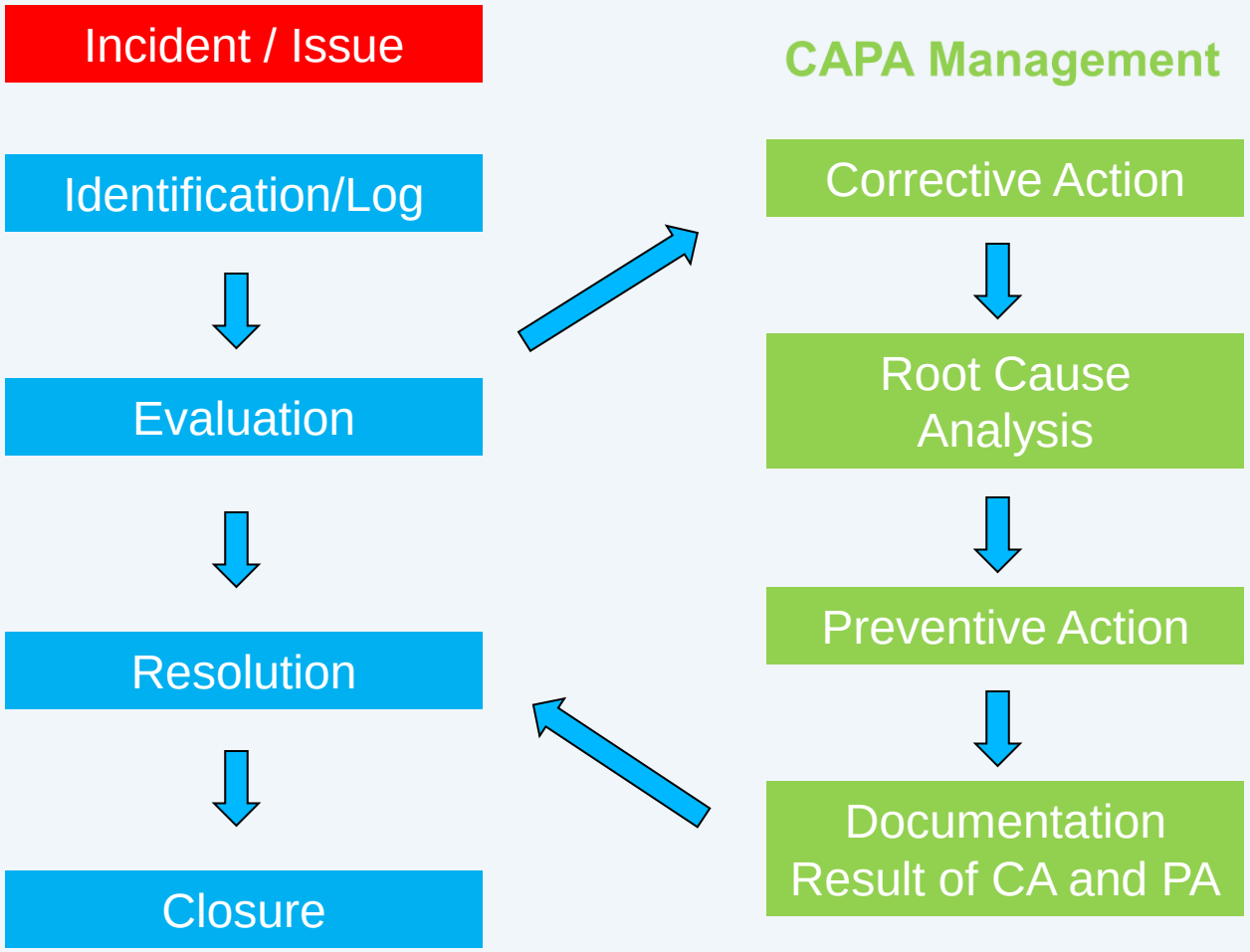
- IT, for example:
  - Changes in the Configuration
  - Changes in the Software
  - …
- Business Processes
  - Changes in the business process
  - Changes in the Use (as described in the User Requirements)

Change Management

- Applicable in the whole lifecycle of the system
- Clear Procedures describing Change Management
- Change Request + Validation Documents
- Changes registered in the System Register

Incident Management

Process

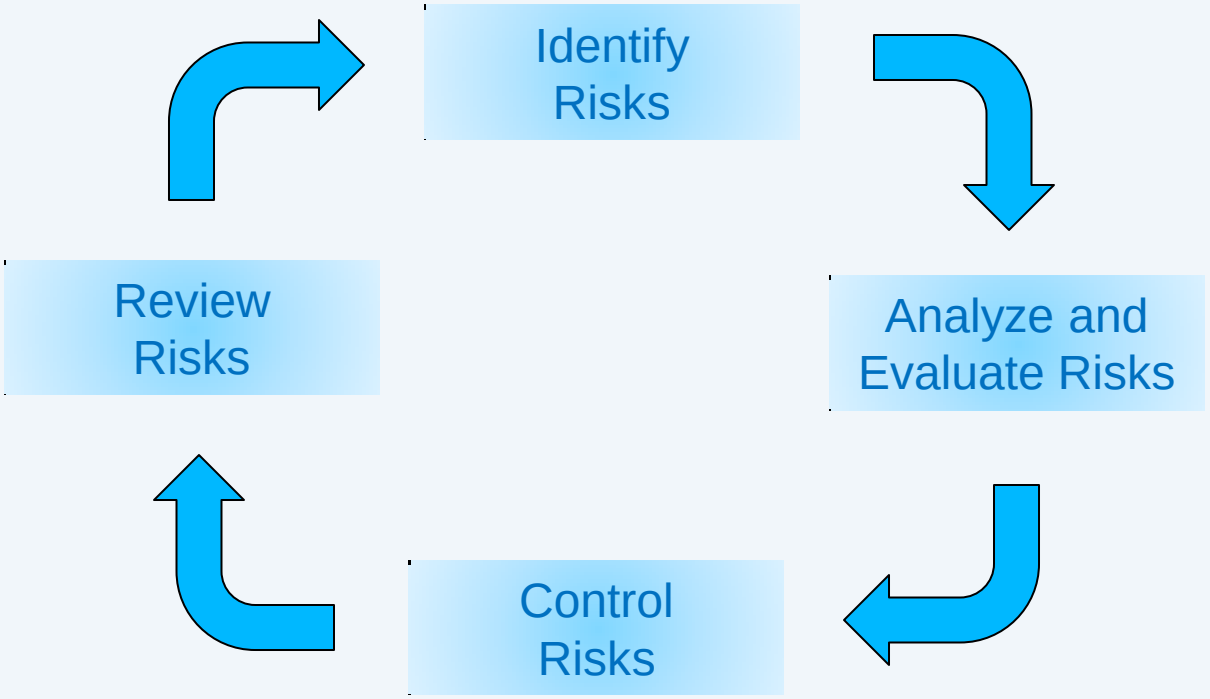

Incident / Issue
Identification/Log
Evaluation
Resolution
Closure
CAPA Management
Corrective Action
Root Cause Analysis
Preventive Action
Documentation Result of CA and PA

Incident Management

- Applicable in the whole lifecycle of the system
- Clear Procedures describing Incident Management
- Clear Responsibilities
  - System Owner: Process in place and used
  - Subject Matter Expert: Perform Actions / Write Documentation
  - Quality Assurance: Procedures followed / Actions taken

Risk Management

Risk Management



Eliminate by Design

Implement Controls

Accept Risk

Risk Management & CSV

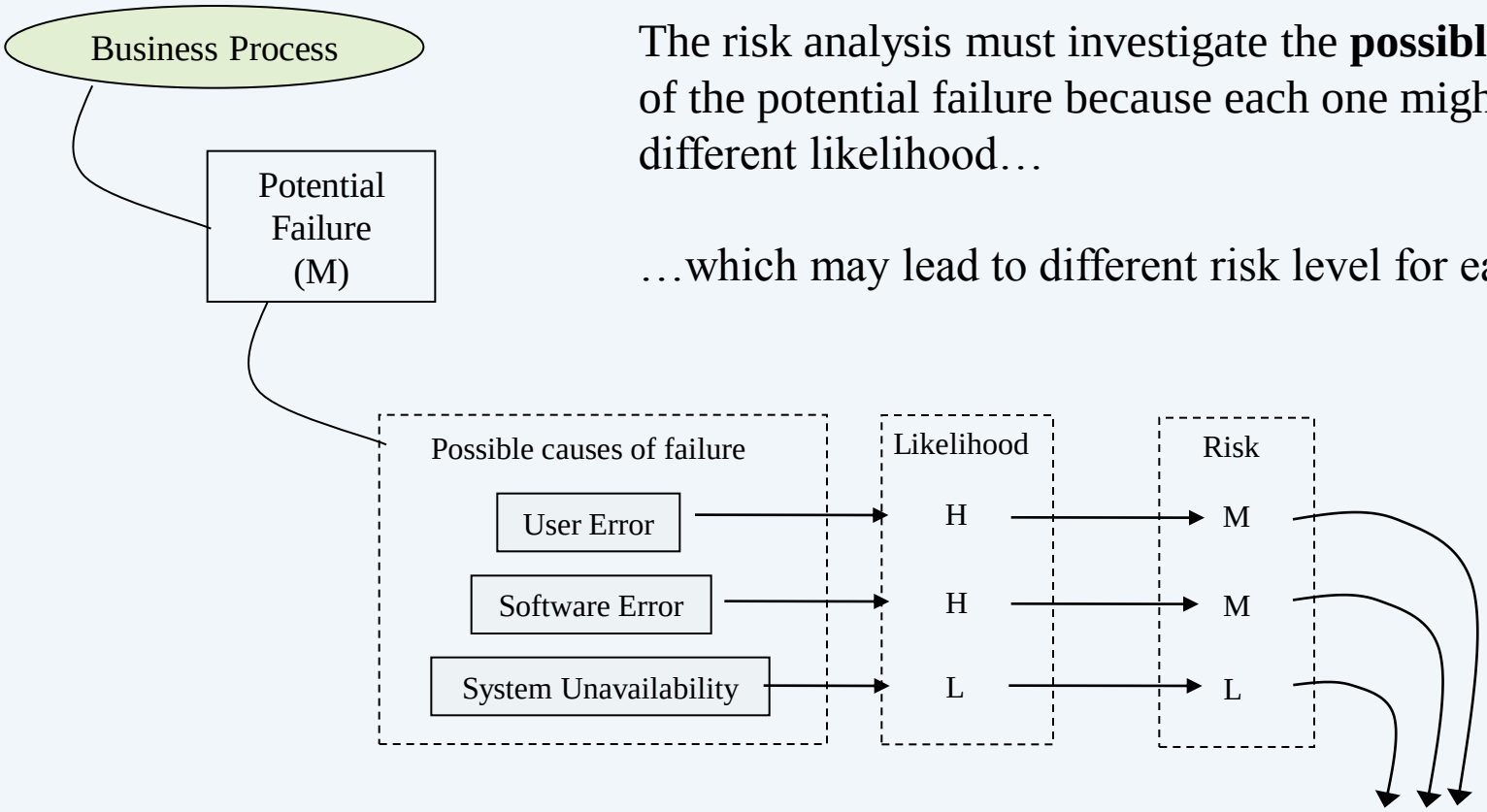
Risk Assessment

- Identify Risk
- Define Likelihood
- Identify Controls
- React
  - Accept
  - Mitigate
  - Remediate

Risk Rating

Risk Rating		Likelihood		
		Low	Medium	High
Consequence	High	M	H	H
	Medium	L	M	H
	Low	L	L	M

Risks and Causes



The risk analysis must investigate the **possible causes** of the potential failure because each one might have a different likelihood…

…which may lead to different risk level for each cause

Controls are later selected at the level appropriate to mitigate individual possible causes…

Security

Data Security

- Backup & Recovery
- Physical Access to IT Infrastructure
- Disaster Recovery
- Decomissioning

Supplier Management

Supplier Management / Outsourcing

- Responsibility can not be delegated / outsourced
- Defined Standards for suppliers
- Quality Standards to be verified via Supplier Audits

End User Applications

Tools and Applications which allow end users to write applications, for example:

- Databases (Access, MySQL, XML, …)
- Development Tools
- Spreadsheets
- Scripts
- Dynamic HTML (JavaScript)

Risks of End User Applications

- Missing Quality Standards in
  - Planning
  - Development
  - Implementation
  - Maintenance

Risks of End User Applications

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.

Control Tools

- Clear Guidelines, SOPs of what users should do/should not do
- User training regarding Computer System Validation.
- Risk Assessment of the business processes
- Control Self Assessments
- Internal Audits to verify correct user behavior and offer consulting to users.

Inspection Readiness

Problems

All Systems correctly validated, but …..

- Preparation for Audit may require too much resources
- Sometime insufficient time caused by short term notifications
- People not prepared for unusual situations

Inspection Readiness

- Checklist for Audit
- Clear Responsibilities for Audit Governance
- Logistics defined (rooms and facilities)
- Training of Key Contacts
- Tests (Walkthrough , Mock Audit)

Questions & Answers

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