1 Purpose

To define the requirements for the application of risk management principles to computerized systems.

2 Scope and Applicability

This Guideline is applicable to any operations sites, functions and departments undertaking work, or providing support services, required to meet Good Laboratory Practice (GLP), Good Clinical Practice (GCP), and Good Manufacturing Practice (GMP). Risk Management is mandatory for GxP computerized systems and should be considered for all others, especially those of high business risk.

This Guideline provides guiding principals applicable to the risk management of computerized systems. While the primary focus is applications, it may also be used with IT infrastructure platforms and process control systems.

3 Definitions

3.1 Risk management

The systematic and comprehensive identification and understanding of risk factors and their associated risks, together with a decision making process to implement appropriate controls.

- Aims to maximize potential opportunities, control uncertainties and minimize potential threats, thereby increasing the probability of achieving business objectives.
- Includes the conscious decision to accept risk.
- Is an ongoing (iterative process)

3.2 Computerized System

An assembled group of hardware components (including peripheral devices), firmware and software components, that are collectively designed to perform a specific function or group of functions.

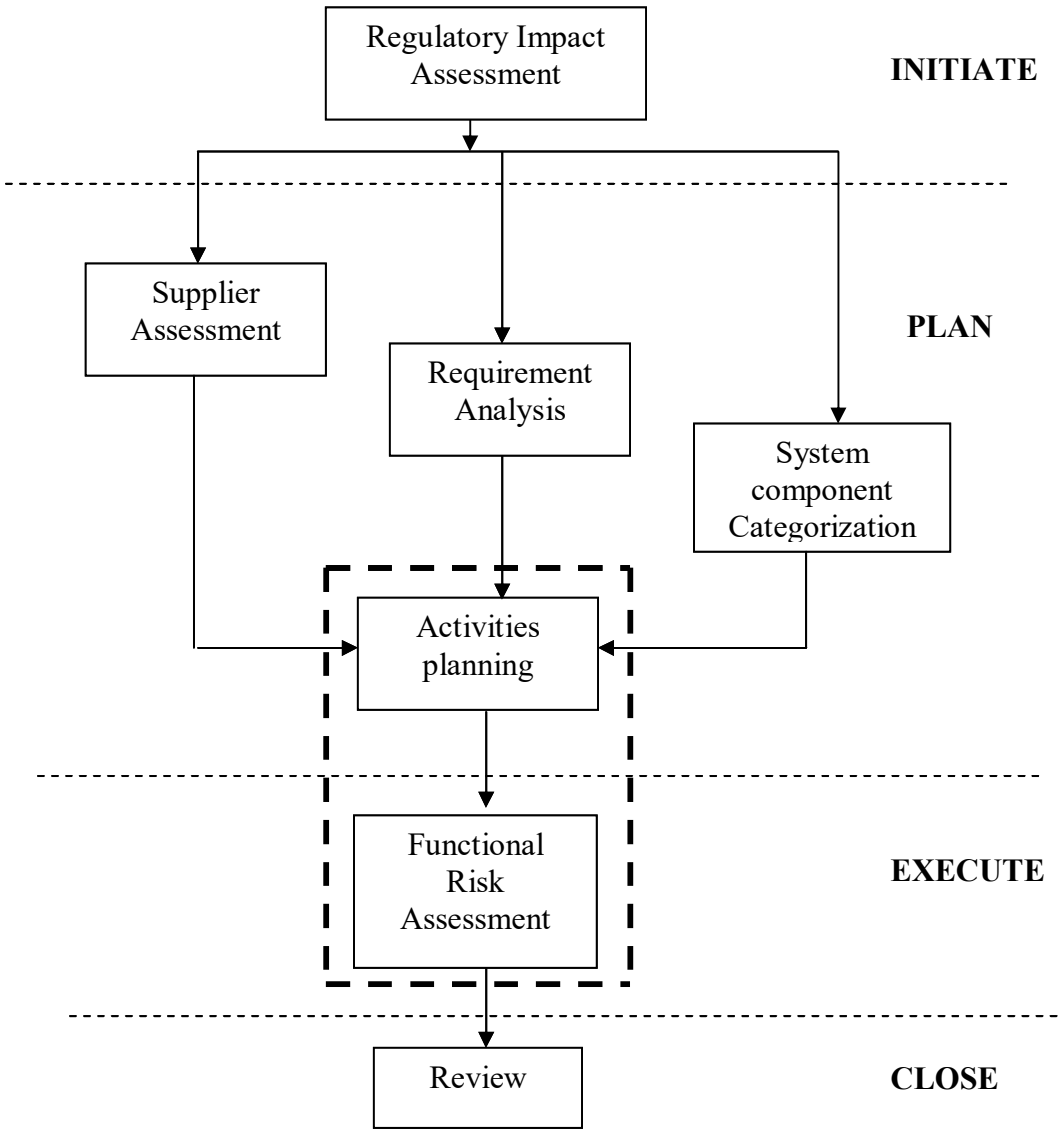
3.3 Technical Staff

Members of the technical community (typically from IS, but for some systems may be from operations, engineering or another group that performs development or support) who understands and represents the technical perspective.

3.4 Key User

A member of the business or functional group who currently uses the system on a day-to-day basis and has responsibility for representing users needs and the process use of the system.

Risk Management Activities



5.1 Regulatory Impact Assessment

Components of this activity:

- It is necessary to perform a regulatory impact assessment to determine if the computerized system has regulatory impact.

- The result of the Regulatory Impact Assessment (RIA) must be documented along with the rationale for any decisions taken.

It is necessary to perform a Regulatory Impact Assessment to determine if the computerized system has regulatory impact. To make this determination, the system's impact on product quality, patient safety and data integrity should be

validation effort required e.g. Testing, documentation, planning

5.3 Supplier Assessment

Components of this activity:

- If a supplier assessment is required, it must be conducted in accordance with appropriate guidelines.

Many computerized systems will utilize components purchased from external suppliers. The quality and reliability of these components will largely depend on the supplier. An assessment may be performed to determine their suitability in terms of systems development and support processes. This assessment is not mandatory but is strongly recommended. The decision to conduct this assessment will be based on the Regulatory Impact Assessment and the team's knowledge of the supplier and/or system components. The Vendor Assurance and Contractor database is a good reference source for audits of suppliers and vendors including IS.

The results of this activity will assist the team with activities planning and in scaling the testing activities as appropriate.

5.4 Requirements Analysis

Components of this activity:

- The requirements must be analyzed to determine the scope of testing and regulatory applicability.
- Once the requirements categorization is complete, the team must then decide on appropriate levels of testing to ensure that the computerized system operates properly to satisfy the business and regulatory needs.

The requirements must be analyzed to determine the scope of testing and regulatory applicability. It is important to determine which requirements have regulatory impact and to what degree. In order to determine this, they should be reviewed and categorized. Recommended categories for regulatory impact are direct, indirect and no impact.

It is also essential to determine the importance of requirements to the business process. Recommended categories are Essential, Important and Desirable.

Once the requirements categorization is complete, the team must then decide on appropriate levels of testing to ensure that the computerized system operates properly to satisfy the business and regulatory needs. The following grid may be used as a guide to help make this determination.

	No Regulatory Impact	**Indirect Regulatory Impact**	**Direct Regulatory Impact**
Essential	**EN**	**EI**	**ED**
Important	**IN**	**II**	**ID**
Desirable	**DN**	**DI**	**DD**

