As projects are dynamic in nature, the risk priorities may change throughout the life of the project. As per *Computer System Guideline* (**VAL-110**), risk assessment should be performed at the start of each computer system qualification. However, for a large system Risk Assessments may be conducted at several stages of the project. The number and timing of the assessments can be documented in the Validation Project Plan. For guidance, Risk Assessments may be undertaken following:

- The generation of the User Requirements Specification (URS)
- The Supplier Assessment and the development of the Functional Specification (FS)
- The completion of the Design Review prior to validation test
- Whenever any major changes are to be applied to the system.

Undertaking Risk Assessments at these stages will help define the user requirements and alternatives, aid the supplier selection process, and determine any mitigation steps or additional validation requirements for the project. The findings of early Risk Assessments should be reviewed at later key points in the project, to ensure that the assumptions and circumstances upon which they are founded are still valid.

For a small scale computer system a risk assessment at the start of the project may be sufficient.

As a minimum the System Owner, Validation / Technical Services and Quality Assurance in consultation with IT should approve the Risk Assessment documentation. Additional approvers may be added as required by the team and depending upon the phase of the project.

4.0 RESPONSIBILITY \ BUSINESS RULES

Risk Assessment is part of the overall responsibility of the project team or change control team members, however each member may take on a different role during the assessment exercise.

Typical responsibilities for conducting a Risk Assessment are detailed below:

- ***System Owner/Administrator***: The System Owner is defined as the person ultimately responsible for the operation of a system, and the data residing on that system.

- ***The System Owner*** is responsible for the investigation and evaluation of those risks identified as part of the GxP operational process and those risks identified as significant to the overall business process.

- ***IT Person Responsible for System***: Responsible for the investigation and evaluation of those risks identified as a result of the program configuration or implementation and those risks identified as a result of the infrastructure (hardware, network, peripherals, etc.) implementation.

- ***Validation / Technical Services Personnel***: Responsible for the investigation and evaluation of those risks associated with validation requirements of the system.

- Data integrity
- Release for sale documentation

The project team should look at each function or sub-function and make an assessment of the GxP impact. The outcome of their discussions should be documented on the assessment form.

If the assessment of a particular function or sub-function determines that there is no GxP risk, the justification for taking this viewpoint should be documented on the assessment form.

5.2.2 Identify Business Risk

A secondary element of the Risk Assessment process is to determine whether the system function or sub-function represents a risk to the business.

The types of risk to be identified include, but are not limited to:

- Equipment downtime
- Equipment damage
- Cost of replacement equipment parts
- Potential for injury (Health and Safety)

If the assessment of a particular function or sub-function determines that there is no business risk, the justification for taking this viewpoint should be documented on the assessment form.

5.2.3 Identify Risk Scenarios

Having determined that a particular function or sub-function may have a GxP or business risk associated with it, the assessment should proceed to identify the various risk scenarios (i.e. the events that identify the risks associated with use of the system). It is useful to consider for each event what the likely effect will be (note that each event may have more than one effect).

5.2.4 Assess Likelihood

The next stage is to determine the likelihood (frequency or probability) of an adverse event occurring. The approach requires the project team to consider the likelihood of the adverse event occurring within a given time period (day, month, year) or per a quantity of transactions, and assigning a value to that estimate the risk can be classified.

A suggested method of representing this is as follows:

Low	The frequency of the event occurring is perceived to be once per ten thousand transactions.
Medium	The frequency of the event occurring is perceived to be once per thousand transactions.

type of project organization preferred; the amount of education and training provided.

- ***Reconsider Amount of (Auditable) Built-in Quality***: Alter the amount of documentation that is approved and controlled; introduce or remove formal review points to reflect identified risk.

5.2.8.3 Modification of Validation Approach to Mitigate Risk

- ***Increased Testing***: Increase the scope and level of testing applied during various stages of the validation process, including the development of specialised testing aimed at the testing to failure of certain functions.

- ***Decreased Testing***: Decrease the scope and level of testing applied during various phases of the validation process due to the extremely low risk associated with occurrence and consequences of the fault conditions.

5.2.8.4 Eliminate Risk

- ***Avoidance***: The risks are so high that the new way of working should not be implemented.

The results of this phase of the assessment should be documented and used as justification for the validation approach. Details should include who is responsible for providing the mitigation effort.

5.3 Risk Assessment of Change

The Risk Assessment process should be used during the entire lifetime of the system. A process of Risk Assessment should be pursued at any time a major change is to be applied to the system. The application of the Risk Assessment technique as part of the Change Control process will allow the development of suitable mitigation strategies, to identify the verification and re-test activities to pursue before the change is put into operation.

5.4 Documentation of a Risk Assessment

Risk Assessments should follow site documentation structures. Risk Assessments for small-scale systems may be documented in the Validation Project Plan.

The Risk Assessment must, as a minimum, include the sections listed below. If there is no information relevant to a section, the statement "This section is not applicable to this Risk Assessment" should appear below the section heading, followed by a brief justification as to why the section has been omitted:

- Cover Sheets
- Introduction (including Purpose and Scope)
- System and Project Overview
- Risk Assessment

