Procedure

1. Principle

"Good documentation constitutes an essential part of the quality assurance system" – Code of GMP). Documentation is used to:

- Identify the components and operations to be used (e.g. specifications, procedures)
- Record the actions, activities, or events that occur (e.g. records, alarm logs)
- Capture the outcome of operations, testing or assessments (e.g. certificate of analysis)
- Respond to deviations or complaints (e.g. investigation reports, distribution records)
- Demonstrate authorisation by appropriate persons (e.g. batch release).

It is clear that documents that support GMP compliance must be reliable.

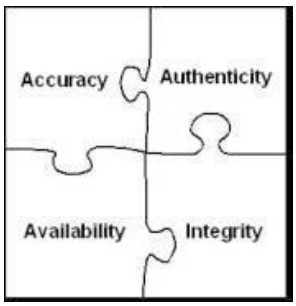

Figure 1:
The elements of Reliability

This SOP considers reliability to comprise four separate attributes:

- Accuracy: data is factually correct; free from error, defect or misrepresentation
- Authenticity: data is genuinely sourced from the reputed author, device or origin. May include the ability to uniquely trace the data to that entity.
- Availability: data is suitable or ready for timely, future, authorised use. May include restriction of access to intended purposes / users.
- Integrity: data is complete and entire; not altered in an unauthorised, unanticipated or unintentional manner.

A compromise to any of these attributes reduces the reliability of a record.

There are very many potential threats to the reliability of data. These can be split into various categories (e.g. Human-related; Computer-related and Operation-related). Table 1 provides some examples of how reliability attributes are vulnerable to potential threats.

A wide range of Control Measures can be deployed against the various threats to data reliability. Controls perform in various means - supportive (enabling other control measures to be implemented), preventive (providing initial defence against threats) and responsive (detecting and recovering from a failure of other controls). Control measures must address all three general threat sources (human, computer and operation) and may be classified as either technical or non-technical (management and operational):

- Management controls focus on the development of policies, guidelines and standards to be carried out through operational procedures (e.g. access authorisations, responsibility definitions, continuity support plans and system performance auditing).
- Technical controls are safeguards that are incorporated into computer hardware, software or firmware (e.g. access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software).
- Operational controls are procedures and systems implemented alongside technical controls to address computer system deficiencies that might result in loss of reliability (e.g. virus protection software, data backup, physical security measures and environmental controls).

2. Assessment Procedure

The process of assessing the Control Measures supporting specific records is illustrated in Figure 3. The outcomes of this assessment are to be documented **on Form 710**. The steps involved in this process are described below:

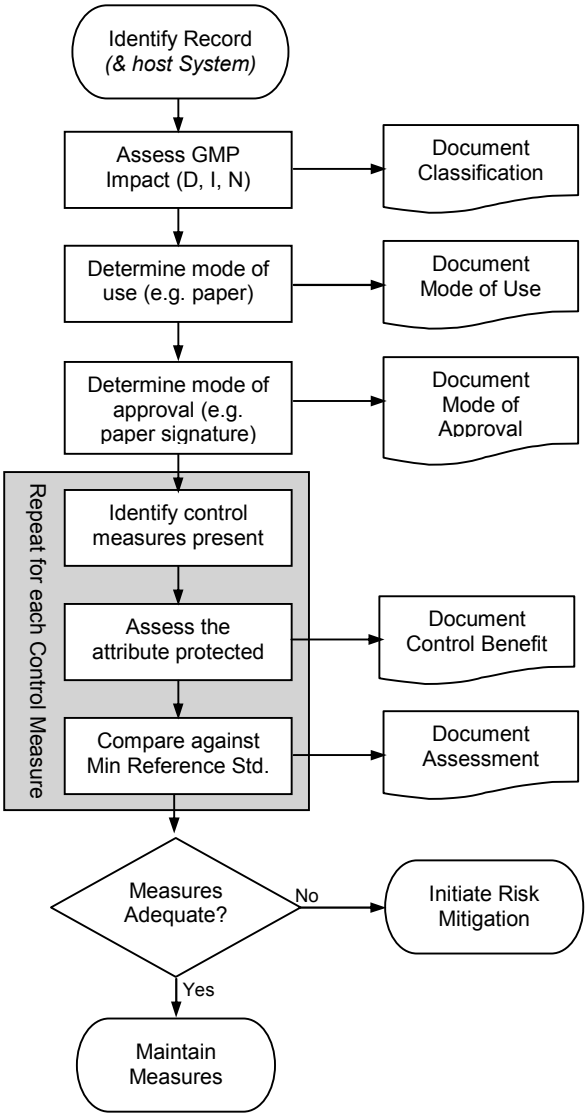

Figure 3:
Flowchart for Risk-Assessment Procedure

2.1. Identify the Record

Identify the record to be assessed and the host computer system(s) where the record is generated, processed or stored. Briefly describe the Record's role and use. Note these and the computerised system Inventory number on **Form 710**.

Computer systems will typically support a number of records and care should be taken to identify the precise record being considered (especially as each may have different control measures, modes of use and / or GMP significance). Often records may be saved as multiple, independent files generated from a standard template or computer program (e.g. on a per batch basis). In this case the analysis may be performed on the standard template or report and this should be noted. Where reports are generated from a consolidated database, the database and the report function should be considered together.

2.2. Assess the GMP Impact

Assess the GMP significance of the record being analysed. The record will be assigned one of three possible levels of Impact – Direct, Indirect or No-Impact - reflecting the role of the record in supporting product quality, patient safety or GMP compliance. **SOP VAL 045** describes the process for determining the level of Impact and includes suggested ratings for various common record types.

Note that the host computer system will also be rated according to **SOP VAL 045,** however, the record itself may have a different rating. A record might have a lower level of Impact than its associated computer system (but should never have a higher level of Impact).

In general the stringency and extent of control measures should increase with the level of Impact.

- Do a variety of control measure types protect each reliability-attribute?
- Have any limitations to the effectiveness of specific controls been identified?
- Have any potential vulnerabilities been identified?

Consider the assessment for each separate reliability attribute (i.e. accuracy, authenticity, availability and integrity) by referring to the corresponding columns. Condense the evaluation into an overall assessment of record reliability. Record each assessment on Form 710 along with a justification.

Completion of this process may highlight particular vulnerabilities. The control measures associated with these vulnerabilities will help to identify some suggested improvements to protect the record. Document these improvements on Form 710 under Management, Technical and Operation categories. The list of improvements may overlap and is not intended to exclude solutions using measures that are not identified; rather it is a reference and starting point for future remedial work.

If the System Owner is not comfortable with the residual risk associated with the assessed record the suggested (or other) control measure improvements should be implemented to mitigate this risk.

2.7. Authorise and Store the Assessment

The completed assessment form will be signed by the author and reviewed by a Technical Expert and the Computer Systems Validation Manager (or Validation Manager). The System Owner will authorise the assessment indicating that they are satisfied with the assessed status of the record and will take responsibility for any necessary remedial work.

The completed form should be updated after the implementation of any risk mitigation activity. The reason for, and nature of, the change is to be recorded in the version table at the bottom of Form 710 (along with the associated Manufacturing Change Request). Conversely, any change that reduces the level of protection is also to be documented on an updated form.

3. Further Considerations

3.1. Electronic Signatures

Regulators advise that:

> "the use of a computerised system does not reduce the requirements that would be expected for a manual system of data control and security" *(PIC/S 011 – Section 19.1)*.

When paper records are used, critical GMP actions and decisions are traced to individuals through a hand-written signature. This approach applies readily when a computer-system produces a record as a paper-copy. 'Electronic signatures' are the analogous authentication process for fully computerised, 'paperless', systems. A wide variety of technical solutions are available for implementing 'electronic signatures' (e.g. biometric, non-biometric). The key requirement of any 'electronic signature' is that it should serve the same purpose, have the same meaning and same legal significance as a hand-written signature. Assurance of the authenticity of any electronic signature will require a range of procedures and control measures to ensure security, integrity, confidentiality and non-transferability (i.e. unable to be cut-and-pasted). The electronic signature should also form an integral part of the completed record. These measures can be drawn from those used for protecting the reliability of electronic records in general (as per Appendix 1). Whatever measures are selected must be validated.

As noted already, electronic records do not necessarily imply a requirement for 'electronic signatures'. Hand-written authorisation of the paper-copy is suitable where the electronic record is not subject to further update or electronic use. If both paper and electronic versions are to be used (i.e. a Hybrid record) additional control measures are required. The electronic record and hand-written signature should be linked together in a completely unambiguous manner (eg including specific document or file name references on the signed

form within the target computer system. Changes to software require the ability to access this data and possibly also to interrupt the operating run-time environment before they can be made. The restriction of this access is a key means of ensuring software authenticity.

Validation and Change Control are the other main means of ensuring the reliability of software, particularly its accuracy. The practices associated with this approach are already described in **SOP VAL 040.** Other control measures, however, may be appropriate to support other aspects of software reliability, (e.g. authenticity, availability and integrity):

- Infrastructure protection – physical access restrictions and "malware" protection
- Security management – external-access checks, centralised storage and user access profiles
- Backup and restore – back-up procedure, checking of outcome and redundant copies
- Disaster recovery – response capability
- Audit trail – author identification and author authentication
- Software controls – error handling, automated generation (development aids) and independent checking (validation)
- Policies, procedures, training – developer selection & training, activity history, reviews and audits, defined responsibilities and operational procedures.

As with volatile input-data, where the system is open to external-access a very high level of control should be considered.

Note that the software development environment, (i.e. source-code tool) does not have the same level of GMP significance or impact as the system that is controlled by the code. Consequently the tools do not necessarily require the same level of assurance, or control measures, as the developed process. (For instance, software that operates an automatic audit trail function does not require its development environment to have the same functionality – a manual system of change control could be adequate).

Examples of software files that are considered to be outside the scope of this procedure include:

- Vision system models,
- Autoclave-cycle configurations,
- HPLC recipes,
- Exacta Filter-test configurations.

4. Summary of Changes

Version #	Revision History
VAL-060	New

End of Procedure

Control Category	Control Measure	Control Type	Comments and Description of Control Measure	Reliability-Attribute Supported	Suggested Min. Level for Inclusion	PIC/S Ref.s
	Automated process	Technical	Is backup implemented on a regular basis using an automated (rather than a manual) process?	Availability	Direct	
	High-availability system	Technical	Is the IT hardware designed to provide backup and 'failover' (i.e. automatic fault-based switching) capabilities? • Approaches include the use of RAID or SAN technology.	Availability	Direct	
Disaster Recovery	Response capability	Operational	Have appropriate response capabilities been established? • Measures should be known and may vary with criticality. No-Impact systems should have an identified support resource capable of a restart. Direct Impact systems (e.g. to support a product recall) should have alternative arrangements / systems identified (perhaps including hot stand-by and 24x7 support).	Availability	No-Impact	
	Agreed plan / goal	Management	Have plans for recovery of service been documented, including a defined allowable outage time? • Plan should be agreed with the Business System Owner. Recovery time should reflect the criticality of record availability for GMP. Plan should align with the Response Capability.	Availability	Indirect	19.6
	Tested process	Management	Is the recovery plan tested regularly and formally (i.e. this is documented)? • Frequency of testing the Disaster Recovery plan should reflect record and system criticality.	Accuracy, Authenticity, Availability, Integrity	Indirect	19.3, 19.6
Validation & Change Control	Specification	Management	Have requirements for the system or change been described and documented (e.g. in a User Specification)? • Level of detail should be appropriate to the GMP impact. • Stored documentation should be updated as required	Accuracy, Integrity	No-Impact	21.9, 23.12, 23.13

Control Category	Control Measure	Control Type	Comments and Description of Control Measure	Reliability-Attribute Supported	Suggested Min. Level for Inclusion	PIC/S Ref.s
	Un-editable format	Technical	Are records protected from change by retaining in a format that resists change (e.g. PDF, Encryption)? • As a minimum, data should only be editable via its native application (i.e. not available in a simple text format). If changes precede the format conversion an audit trail may be required to be attached. Conversion should only occur after all processing is complete.	Authenticity, Integrity	Indirect	
	Human readable form	Technical	Is data readily available to regulators in legible form (e.g. print-out or PDF copy)? This requires an operational print-program for each stored format. Where data is encrypted auditors may want to be given decrypting ability or to witness decryption on site. Copy should include audit trails and "electronic signatures"	Availability	Indirect	19.4, 21.1, 21.10
Software Controls	Data-validity checking	Technical	Are checks performed to ensure entered data is compatible with the application? Examples of invalid data include values: - With an unrecognisable data type (e.g. non-numeric); - Outside acceptable ranges for the proper functioning of the system, and - that contain a 'read-error' (i.e. corrupt or unrecognisable).	Accuracy, Integrity	No-Impact	23.15
	Error handling	Technical	Does the system include functionality to identify error conditions and respond appropriately? • May include alarms and user prompts to notify of failure.	Accuracy, Availability, Integrity	No-Impact	

