

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

Department	Validation/Technical Services	Document no	VAL-060
Prepared by:		Date:	Supersedes:
Checked by:		Date:	Date Issued:
Approved by:		Date:	Review Date:

Document Owner

Validation Manager

Affected Parties

All Validation, Technical Service, Operations, Quality Assurance, Engineering and Project staffs involved in computer validation projects.

Purpose

This SOP describes a process for assessing the adequacy of measures that have been implemented to assure the reliability of GxP records created, processed, used or stored electronically.

Scope

This SOP applies to records created, processed, used or stored by (or for) the GMP Manufacturing site, that are the output of a computerised system. It is of particular relevance to records that have a GMP role, i.e. supporting product quality, patient safety or regulatory compliance. The guideline may also be used for other computerised systems that are classified as business critical.

The procedure is intended for use primarily with records that have Direct Impact (see **SOP VAL 045**). Members of the Computer Validation Department will normally execute the procedure.

Definition

Accuracy	The attribute of record reliability indicating that the data is factually correct; free from error, defect or misrepresentation
Audit Trail	Data in the form of a logical path linking a sequence of events, used to trace the transactions that have affected the contents of a record. Will usually contain all original data, the author of the changes, the time and date of the change and the reason for that change. The audit trail is not the same as an operating system activity log; it is generated at the application level and logs actions performed to a specific electronic record. The audit trail should also be immutably integrated with the actual record.
Authenticity	The attribute of record reliability indicating that the data (or record) is genuinely sourced from the reputed author, device or origin. May include the ability to uniquely trace the data to that entity.
Availability	The attribute of record reliability indicating that the data is suitable or ready for timely, future, authorised use. Availability may include the restriction of access to only intended purposes and users.
Biometric Electronic Signature	An electronic signature that uses the automatic checking of an individual's distinct and measurable physical characteristics (e.g. finger-print, retina pattern).
Control Measure	Control Measures are safeguards that protect the reliability of records from threats. Control Measures may be technical or non-technical (management or operational) and perform at various levels (supportive, preventive, responsive).
Data	Distinct pieces of information usually formatted in a special way (e.g. bits and bytes).

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

3.2.1. Volatile Data and Temporary Files.....	13
3.2.2. Programs.....	13
4. Appendix 1 – Checklist / Explanation of Control Measures.....	15

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.

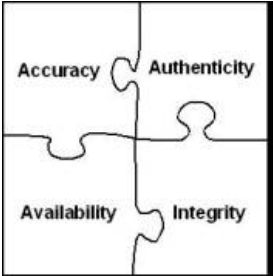
	<p>This SOP considers reliability to comprise four separate attributes:</p> <ul style="list-style-type: none">• Accuracy: data is factually correct; free from error, defect or misrepresentation• Authenticity: data is genuinely sourced from the reputed author, device or origin. May include the ability 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. <p>A compromise to any of these attributes reduces the reliability of a record.</p>
--	--

Figure 1:
The elements of Reliability

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).

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

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:

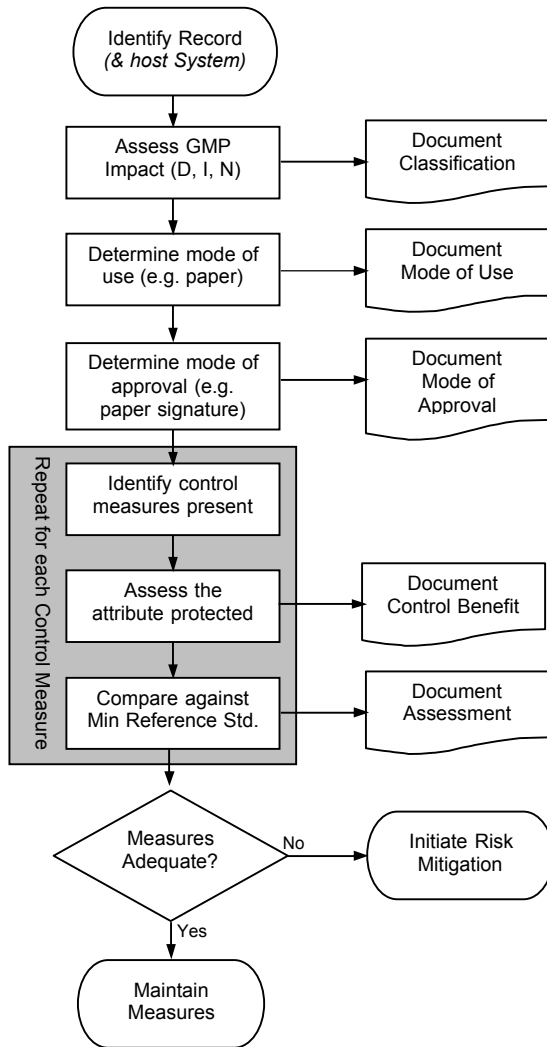


Figure 3:
Flowchart for Risk-Assessment Procedure

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.

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

Conversely mark 'N' (No) where the attribute is not protected.

Some control measures can support more than one reliability-attribute, in such cases mark all columns affected. Some control measures cannot be implemented for the type of record that is generated (e.g. electronic backups of paper records) – in this case mark the cell as 'N/R' (Not Required).

To assist this assessment, certain cells on Form 710 have been shaded where it is considered unlikely that a control measure will provide any benefit. Shaded cells may be left blank where the answer would otherwise be 'No' or 'N/R'.

2.5.3. Compare against Minimum Reference Standard

Each control measure on Form 710 has been assigned a Minimum Reference Standard, suggesting the lowest level of Impact at which it might be considered appropriate. This determination was based on the nature of the measure (how complex, costly and common it is to implement) and any specific GMP requirements. Appendix 1 includes references to cGMP and PIC/S documents suggesting each measure. The most basic and fundamental measures have been labelled “*No-Impact*”, while the more rigorous as “*Direct*” Impact.

Compare the Minimum Reference Standard label for each control measure with the GMP Impact rating for the record, determined in Step 2.2 (above). Control measures that are labelled “*Direct*”, “*Indirect*” or “*No-Impact*” should be considered for records with Direct Impact. Records with No-Impact may be adequately protected by “*No-Impact*” measures alone.

2.5.4. Comment on any Variations

Assess and document on Form 710 the outcome of the comparison (step 2.4.3) for each control measure. Table 2 illustrates some suggested comments for various conditions of implementation:

Outcome of Control Measure Assessment	Suggested Assessment
The control measure has been implemented effectively	“Adequate”
The control measure has been implemented, but its effectiveness is restricted by certain factors or circumstances	“Limited by ...”
The control measure has not been implemented and the Impact rating of the record is less than the Reference Standard for the measure.	“Appropriate omission”
The control measure has not been implemented and the Impact rating of the record is not less than the Reference Standard for the measure.	“Potential Vulnerability” OR “Not Required because .. (<i>usage mode, presence of other controls, other factors</i>)”

The comment field may also be used to document any additional information relevant to the Control Measure (e.g. names of SOPs, implemented features).

Note that control measures corresponding to Impact ratings greater than that of the record might be implemented for reasons other than GMP compliance (e.g. to comply with IT security standards or to protect other business risks). The presence of these measures should be documented.

2.6. Assess the Total Control Strategy

After assessing all of the control measures separately, the adequacy of the total control strategy should be assessed. The following factors are relevant to this consideration:

- Are all reliability-attributes covered by the strategy?

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

purpose, it may be acceptable to use other system security controls to prove authenticity of the person. Table 4 illustrates examples from the code of GMP where persons require authorisation and/or identification.

Table 4 – Examples of Persons requiring Authorisation / Identification

Description of Person	To be Authorised	To be Recorded
Person accessing packaging materials	Yes	
Person accessing production premises	Yes	
Person accessing quarantined goods	Yes	
Person amending data	Yes	Yes
Person carrying out in-process controls		Yes
Person checking critical data		Yes
Person checking different steps of production		Yes
Person conducting internal audits	Yes	
Person conducting validation, calibrations, maintenance, cleaning or repair operations on major or critical equipment.		Yes
Person dealing with reject materials	Yes	
Person deputizing for responsible people	Yes	
Person dispensing starting materials	Yes	
Person entering data	Yes	Yes
Person investigating events	Yes	Yes
Person issuing packaging materials	Yes	
Person performing analytical tests		Yes
Person performing different steps of production / packaging.		Yes
Person responsible for each stage of production / packaging		Yes
Person responsible to execute recalls	Yes	
Person responsible to handle complaints and deciding response	Yes	
Person releasing batch	Yes	Yes
Person taking samples	Yes	
Person verifying analytical tests		Yes

In summary, cGMP (and company procedures) identify where 'signatures' are required. The way that a system is implemented or operated determines whether the 'signature' is to be electronic or hand-written. This is at the discretion of the company. If an electronic 'signature' is used it must be supported with appropriate control measures to ensure that it is a reliable component of the completed record. The measures identified in Appendix 1 should be considered for this role.

3.2. Approach for data that is not a Record

This procedure is only concerned with data that is output as a record. The following guidance, based on the principles in this SOP, may be useful when dealing with other data types.

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

4. Appendix 1 Checklist / Explanation of Control Measures

Control Category	Control Measure	Control Type	Comments and Description of Control Measure	Reliability-Attribute Supported	Suggested Min. Level for Inclusion	PIC/S Ref.s
Infrastructure Protection	Physical security	Operational	Is physical access to system and operating software limited? <ul style="list-style-type: none"> Measures include system-based hardware features (such as keys) or environment-based controls (such as site / room security / physical restraints or attachments). 	Authenticity, Availability	Indirect	19.3, 19.7, 23.15
	Environmental controls	Operational	Is a suitable environment for system operation maintained? <ul style="list-style-type: none"> Measures include controls over humidity, temperature, and electrical supply; monitoring and alarms for fire, smoke and power failure. 	Availability	Indirect	23.12,
	"Malware" protection	Technical	Is the system protected against "Malware" (i.e. viruses, Trojan-horses and worms) that can cause interference with system operation and damage to stored data? <ul style="list-style-type: none"> Measures include firewalls, scanning software, hardware configuration and operating system patches. 	Accuracy, Authenticity, Availability, Integrity	Indirect	
Security Management	Access control	Technical	Does the software restrict access to the system and confirm presence of an authentic user? <ul style="list-style-type: none"> Measures may range according to level of Impact from 'group-access' (No Impact), through to 'individuated-access' and 'automated-log out' (Direct Impact). Physical measures (e.g. keys) are part of Infrastructure Protection 	Authenticity	No-Impact	19.3, 21.2, 21.8
	Password management	Management	Are there procedures for the management of password effectiveness and confidentiality? <ul style="list-style-type: none"> Measures include enforced password changing; guidelines for formatting; periodic checking; controls over temporary ids; and management of lost or compromised passwords. Includes passwords supporting 'electronic-signatures'. 	Authenticity	Indirect	19.3, 21.2, 23.15

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

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? <ul style="list-style-type: none"> Approaches include the use of RAID or SAN technology. 	Availability	Direct	
Disaster Recovery	Response capability	Operational	Have appropriate response capabilities been established? <ul style="list-style-type: none"> 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? <ul style="list-style-type: none"> 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)? <ul style="list-style-type: none"> 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)? <ul style="list-style-type: none"> 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
	Authorisation process	Management	Does an authorization process control the implementation of changes? <ul style="list-style-type: none"> Includes the review and approval of requirements; go-live / implementation. Includes QA involvement where GMP impact exists. 	Authenticity, Integrity	No-Impact	

This is not an approved copy unless stamped in red

File Location:

Date Printed:

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

Control Category	Control Measure	Control Type	Comments and Description of Control Measure	Reliability-Attribute Supported	Suggested Min. Level for Inclusion	PIC/S Ref.s
	Automatic creation	Technical	Is an audit trail record generated automatically by the system, including a time/date stamp? <ul style="list-style-type: none"> Manual generation may be suitable for simple user-identification records, where GMP impact is Indirect. The system may require a consistent time / date clock 	Accuracy, Authenticity	Direct	20.1, 21.6, 21.8, 21.10
	Secure trail storage	Technical	Is the audit trail record kept in a secure format? <ul style="list-style-type: none"> Preferably this means that the audit trail is integral with the actual record; is included in the same Backup and Security Management processes. 	Authenticity, Availability, Integrity	Direct	20.1, 21.2, 21.6, 21.10
	Alteration Approval	Management	Are changes to data-entries reviewed and approved? <ul style="list-style-type: none"> Any critical data-entry that is altered should be authorised 	Accuracy, Authenticity, Integrity	Direct	
Electronic Signatures	Signature Capture	Technical	Are "electronic signatures" applied where key decisions / actions are undertaken electronically?	Authenticity	Direct	21.5, 21.13
	Signature Responsibility	Management	Are users aware of the meaning, responsibility and accountability implied when they 'sign' <ul style="list-style-type: none"> This should be specifically covered by training and procedures. System prompts may reinforce this. 	Accuracy, Authenticity	Direct	21.9, 22.3, 22.6
	Signature Content	Technical	Does the "electronic signature" provide complete and unique identification <ul style="list-style-type: none"> Should include user name, time and date, meaning (Requirements are similar to those for audit trails) 	Authenticity	Direct	21.9
	Signature Authorisation	Technical	Does the system limit the ability of users to execute a critical "electronic signature"? <ul style="list-style-type: none"> For instance the system should only permit Authorised Persons to release batches - no User should have this authority who is not qualified or intended to exercise it. Maintenance of the signatories requires procedures and reviews (as noted for Authorisation Process) 	Authenticity	Direct	21.7

Standard Operating Procedure

Title: Protecting the Reliability of Electronic GMP Records

Control Category	Control Measure	Control Type	Comments and Description of Control Measure	Reliability-Attribute Supported	Suggested Min. Level for Inclusion	PIC/S Ref.s
	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? <ul style="list-style-type: none"> May include alarms and user prompts to notify of failure. 	Accuracy, Availability, Integrity	No-Impact	
	Data transfer protocols	Technical	Where data is transmitted to other systems, are measures used to ensure accurate and complete transmittal? <ul style="list-style-type: none"> Various approaches may be adopted depending on criticality (e.g. standard protocols for No-Impact records; receipt-confirmation, checksum and perhaps encryption for Direct Impact). The system may even keep copies of data, until the receiving system confirms it as processed, so that loss or corruption at a later stage can be addressed. Measures should be validated. 	Accuracy, Integrity	No-Impact	19.3, 20.5, 21.12
	Confirmation prompting	Technical	Is the operator requested to confirm data entry or activity prior to final committal? <ul style="list-style-type: none"> Should be used for important entries or activities. 	Accuracy	Indirect	

