Risk Assessment for Use of Automated Systems Supporting Manufacturing Processes
Part 2 - Risk to Records

by the ISPE GAMP Forum

Introduction
Risk Assessment is a vital component in determining the appropriate validation and data integrity for automated systems used in supporting pharmaceutical and healthcare processes. Risk is considered in this article in terms of the impact an automated system can have on public health. The underlying assumption is that validation and data integrity controls should be established to commensurate with risk. Although the philosophy is not new, it has found recent prominence in relation to the FDA’s current Good Manufacturing Practice (GMP) review in relation to electronic records/signatures.1,2

This article sets out to demonstrate how the GAMP 4 risk analysis guidance can be applied in relation to these topics in the context of the GMPs and Good Distribution Practices (GDPs).1,4 This article begins by explaining how regulatory documents can be used to identify electronic records, goes on to discuss the impact...
of records, and then proposes guidance on appropriate risk mitigation with some illustrative examples. It is acknowledged that the context of different automation systems will vary and that this may alter the outcome of the risk assessment.

The structure of this article has been specifically chosen to complement a companion article on functional risk assessments for use of automated systems supporting manufacturing processes. It is anticipated that both functional risks and risks to electronic records will be combined into a single risk management process. Guidance to industry, including just such a single risk management process is currently being developed by GAMP.

For consistency with other publications on risk management, the terminology defined in ISO 14791 ‘Application of Risk Management to Medical Devices’ is adopted throughout this article.

**Records in Automated Systems**
The now almost universal use of automated systems across all aspects of pharmaceutical manufacturing means that there are electronic instances of all the records required by the GMPs. While the GMPs might be expressed slightly differently within different legislation around the world, the record requirements that they identify are broadly the same.

The FDA have clearly steered the focus of Electronic Records and Electronic Signatures (ERES) thinking away from legalistic compliance with the technical requirements of 21 CFR Part 11, toward a more pragmatic concern for reliable and secure records that adequately support the predicate rules. Their latest draft guidance mentions the predicate rules no less than 27 times in only five pages of guidance.

The key role of predicate rules (GMP regulations) is shown in Figure 1. Once electronic records have been identified then US Part 11, EU GMPs Annex 11, the Pharmaceutical Inspection Cooperation Scheme (PIC/S) guidance, and other regulatory expectations for record controls can be considered. A risk assessment to determine necessary controls must take into account the environment and context of use of those records. Controls should be appropriate to ensure the security, integrity, and confidentiality of records.

In Part 1 of this article, the functional risks arising from different types of automated systems were discussed. The high-risk issues identified by the Canadian Health Products and Food Branch Inspectorate were mapped onto the FDA’s ‘systems approach’ to inspection. Figure 2 maps the examples of GMP records onto six main operational aspects of pharmaceutical manufacturing.

**Risk Assessment Process**
The GAMP risk assessment methodology provides a means of identifying the relative priority that needs to be assigned to...
various examples of electronic records. The risk assessment process is slightly modified to address the generic nature of potential hazards arising from electronic records.

The risk assessment process can be conducted by examining record types to see if they are GxP or non-GxP, and then applying severity checks, likelihood, and probability of detection criteria as illustrated in Figure 3. The most critical records should be linked to direct patient/consumer impact. GxP non-compliance and broken license conditions are severe in their own right, but not as critical as patient/consumer health, in this analysis. Likelihood will be influenced by the degree of human error in how the record is input and/or used. The probability of detection needs to take into account the probability of the impacted record being used and its susceptibility to corruption or loss.

Once the hazards are understood, the appropriate design controls can be introduced. Controls should be specified and validated as part of established system development practices.

**Class of Record**
The first step in the risk assessment process is to identify records and determine their class in relation to impact and probability.

**Criticality Impact of Records**
Given that the first GAMP Risk Assessment step concerns the impact of failure rather than its likelihood or visibility, then it is reasonable to assume generic severities for hazards arising from a given record, based on the use of the record, rather than its implementation. The decision making supported by the records required by the GDPs are to some extent also defined within the GMPs, and therefore, generic. Table A proposes typical severities for the hazards arising from various example records identified by the GMP and GDP regulations.

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Severity</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment cleaning and maintenance records</td>
<td></td>
<td>While the cleanliness of product contact equipment has immediate potential to create harmful product, GMPs require Quality Control (QC) checks before product release.</td>
</tr>
<tr>
<td>Master production and control records</td>
<td></td>
<td>These contain all the critical instruction and control points supporting product release decisions.</td>
</tr>
<tr>
<td>Batch production and control records</td>
<td></td>
<td>These contain the final record documenting decision to release potentially harmful product.</td>
</tr>
<tr>
<td>Out of specification (OOS) investigations</td>
<td></td>
<td>Often OOS investigations provide feedback prompting improvement in the Quality Management System (QMS).</td>
</tr>
<tr>
<td>Customer complaint records</td>
<td></td>
<td>As customer complaints are used to prompt OOS investigations, similar arguments on their impact will apply.</td>
</tr>
<tr>
<td>Distribution and shipment records</td>
<td></td>
<td>Records that support product return and recall processes are HIGH severity. Others, like intervening logistics are LOW severity with the exception of distribution of controlled drugs.</td>
</tr>
<tr>
<td>Adverse event reports</td>
<td></td>
<td>Adverse events management is clearly to do with control of potentially harmful product, implying HIGH severity for associated records.</td>
</tr>
<tr>
<td>Validation Reports</td>
<td></td>
<td>While the correct function of equipment and systems has immediate potential to create harmful product, GMPs require QC checks before product release.</td>
</tr>
<tr>
<td>Training records, Job descriptions and Organogram</td>
<td></td>
<td>Critical decision points are governed by SOPs, and typically involve more than 1 responsible person.</td>
</tr>
<tr>
<td>Self-Inspection Records</td>
<td></td>
<td>No immediate potential to compromise individual decisions on product quality, but self-inspection has broad impact on an organization’s QMS.</td>
</tr>
</tbody>
</table>

Table A. Typical severity for generic record types.
In some business processes, there may be a call for high volumes of data entry, or multiple data entry, or very infrequent use of complex user interfaces, all of which can lend themselves to an increased human inaccuracy in data entry into electronic records.

With all systems, the frequency of failure is linked to the frequency of demand. Therefore, it is not possible to make generic statements about the probability of failure for specific classes of record. Instead, when assessing a specific system and its associated records, the risk assessment must include context-specific estimation of the likelihood of all identifiable potential failure modes.

**Level of Susceptibility**
The second step in the risk assessment process is to determine the level of records in relation to their exposure to loss or corruption and likelihood of detection.

**Likelihood of Detection**
As with the probability of failure, the likelihood of detection of any given potential failure mode is very dependent on its context. For example:

- Some data file structures such as Relational Database Management System (RDBMS) files include a checksum that proves the integrity of electronic records, and allows immediate detection of any corruption to the data files. Such data file structures can only be successfully manipulated through the proper application software, whereas simple ASCII file structures may be easily edited with basic editing tools without the application detecting the record corruption.

- Many user interfaces for data entry include some form of data verification to ensure that manually entered data fall within sensible ranges, or that related data is sensible (for example, day of the month field should fall inside a range...
Exposure Probability of detection is a bit more complex than in the GAMP 4 model, which is geared toward system failure instead of record integrity. This is because of the additional mode of loss of record integrity which involves alteration or deletion of the record through knowledgeable human actions. These will inevitably be harder to detect through electronic means; indeed, this is the major principle by which the need for an audit trail should be judged. Hence, the GAMP 4 risk assessment model is modified slightly by adding a second “first tier” risk assessment that gauges exposure (the likelihood of unauthorized human changes) versus detectability. Clearly, if a system has an audit trail or a checksum verification built in, detectability will be high; whereas if detectability is dependent upon human observation, it will be low.

When critical data is manually entered, sometimes it is very difficult to spot erroneous information (analogous to your own spelling mistakes that you just cannot see), whereas other manually entered data may be presented in such a way as to make errors very easy to spot.

Risk Priority The risk priority can be determined by assessing the relationship between the class of record and the level of susceptibility. A risk mitigation strategy is then developed to reduce risks to an acceptable level. Technical controls are discussed later in this article. The Medicines and Healthcare products Regulatory Agency’s (MHRA) definition of critical deficiencies9 provides valuable guidance (Table B) when prioritizing risk controls.

Illustrative Examples In order to illustrate the full risk assessment and risk management process in practice, seven example electronic record classes have been selected for further discussion as follows:

- Computer Aided Design (CAD) drawing files, generated using a standard CAD tool on a LAN, used to generate, maintain, and print equipment design drawings. The paper drawings are subject to manual review and approval with hand-written signatures. Only paper copies of the CAD drawings are used in plant construction and maintenance activities.

- SOPs stored and accessed over a corporate intranet. Standard software products (Microsoft® Word, Adobe® Acrobat® PDFWriter) are used to publish and electronically sign each SOP. They are made available on the intranet using only standard network operating system file services. This specific set of SOPs govern IT development and maintenance.

- Automatic Test Tool (ATT) records from a GxP significant computer applications (such as SAP). The ATT is used to define test procedures with associated test criteria, and then to execute and capture test results. In this example, there is no further testing after the ATT. The ATT records are not signed.

- Production Record (PxR) generated by a stand-alone PLC/SCADA combination that controls a discrete item of process equipment. The PxR is not electronically signed, but when printed forms part of a full batch record that is approved with handwritten signatures. It is, therefore, a hybrid record. The batch parameters captured in this partial batch record are subsequently verified through QC controls.
Risk Assessment

<table>
<thead>
<tr>
<th>Impact</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Critical | - A critical GMP failure occurs when a practice could give rise, or has given rise, to a product that is harmful to the patient.  
- A critical GDP failure occurs when a practice or omission could result, or has resulted, in the supply to a patient of a harmful product.  
- A combination of major deficiencies that collectively indicate a serious systems failure may also be classified as a critical deficiency. |
| Major | - A non-critical deficiency which could or would produce a product which is not in compliance with its marketing authorization  
- A non-critical deficiency which contravenes significant provisions of the manufacturer’s license  
- Repeatedly failing, or significant failure, to fulfill legal responsibilities  
- Any non-critical deficiency which indicates a significant and unjustifiable deviation from GxP regulatory requirements |
| Other | - Deficiencies that cannot be classified as critical or major, possibly because of lack of information, but which nevertheless indicate departures from good practices. |

Table B. MHRA’s definitions of criticality.

- Certificate of Analysis (CoA) generated from automatically collated and analyzed QC samples by a LIMS system. The LIMS system prints the CoA to paper, where it becomes part of the Batch Release documentation, and is approved with handwritten signature.

- Training Records (TrR), created using a word processor, printed and stored in an employee’s personal training dossier.

- Adverse Event Reporting Records managed using a database to capture call information from multiple users.

**Class**

Taking the generic records’ typical severities from above, we can deduce the following relative severities:

- CAD documents form part of the design and validation evidence of manufacturing equipment, and therefore, inevitably have potential to impact the eventual product quality produced through that equipment. However, the equipment is always subject to equipment validation, the production process manufactured through that equipment is always subject to process validation, and then all product manufactured through that equipment is always subject to rigorous QC controls prior to release to the public. Given these three levels of subsequent controls, it is safe to classify any failure arising from CAD records as Low severity.

- The IT SOPs have no direct impact on manufacturing processes or manufactured product. Their accuracy is important to the security and availability of electronic systems; however, production using systems controlled by the computers developed and managed under these SOPs is subjected to process validation, and then manufactured product is subjected to QC controls prior to release. These SOPs are, therefore, classified as Medium/Low severity.

- The ATT records form part of the Validation Records of a GMP significant system, and would, therefore, be classified as Medium severity (Table A).

- Production Records (PxR) provide information used to decide whether to release the batch. As in this case, there is independent QC of the quality significant parameters, these PxRs may be considered as Medium severity.

- The CoA is the record used as part of the decision on batch release, and has no additional verification. Errors arising within a CoA should, therefore, be considered as High severity.

- As discussed in Table A, the training records should be considered as Low severity.

- As Adverse Event (ADE) records are required to manage potentially harmful product, they must be considered a High severity.

As discussed above, the likelihood of failure of each of these illustrative examples is context dependant, as follows:

- The CAD records have a closed file structure and are manipulated using industry standard CAD software with almost no scope for application specific configuration. The software is, therefore, extremely unlikely to introduce errors. The CAD tool has a graphical data entry mechanism, and strong drawing identification and versioning functions, minimizing the possibility of erroneous data entry, so that it is reasonable to consider CAD records as having a Low likelihood of failure.

- Like the CAD records, the IT SOPs are created using industry standard software. However, the likelihood of human error within the IT SOPs is slightly higher than the CAD records as typical word processing tools have no document identity and versioning functions, making the likelihood of failure Low/Medium.

- While an ATT tool is typically a COTS product delivering standard functionality, the test scripts themselves entail high volumes of data entry that are relatively meaningless to those entering the data. This gives rise to the potential for a High likelihood of errors.

- The final PxR is all automatically generated data, and has no dependency on manual entry; however, it is dependant on the correct configuration of the PLC and SCADA, both of which offer opportunity for error. It is, therefore, reasonable to assume that the likelihood of error is Medium/Low.

- Like the partial PxR, the main data content of the CoA is
automatically collected, which like the PLC/SCADA system, is subject to potential configuration problems. This likelihood of failure is slightly increased by the fact that some manual data is also entered, so the potential for human error is introduced. This leads to a classification for the CoA as having a Medium likelihood of error.

- As the training records in this example were generated using the same technologies as the SOPs, they also should be considered as having a Medium/Low likelihood of error.

- The ADE records in this example are entered by several different users, each using the system infrequently to capture complex information. Even with data entry validation select lists, etc., the likelihood of inaccurate data entry due to operator error must be treated as High/Medium.

These criticalities and likelihoods are plotted on the GAMP ‘risk classifications’ grid depicted in Figure 4.

**Level of Susceptibility**

As with likelihood of failure, the probability of detection for each example record type within its context is considered, as follows:

- Errors in CAD records have a Medium/High probability of detections. Technically, the CAD file structure is binary and complex, so it is extremely unlikely to be able to corrupt or change the file structure without the CAD application software detecting the change. The possibility of human error is largely (although never completely) mitigated by the manual review and approval process.

- Like CAD records, the main potential for undetected errors in IT SOPs lies in human error. Given that it is arguably less easy to spot errors in written text than in drawings, it is reasonable to assign a Medium probability of detection to the IT SOPs.

- Following this same theme, the probability of detection of errors within ATT records centers on the likelihood of spotting human errors. This time, the records tend only to be reviewed locally (subjected to peer review for example, not full QA approval), and are less intelligible, so the probability of detection is reduced to Low/Medium.

- The final PxR is generated from automatically collected data (from the PLC), so the QA inspection has no easy reference for these data. It is, therefore, potentially difficult to detect corruption of batch record values so the probability of detection must be ranked as Low.

- Like the partial PxR, the main data content of the CoA is automatically collected with no easy reference against which to check for errors. The probability of detection, therefore, for the CoA also must be ranked Low.

- Like the IT SOPs, the training records can easily be manually inspected for errors. However, training records have very little information content, so error detection would be easier, rendering a probability of detection of Medium/High.

- As the ADE records in this example are the sole or primary source of information about an adverse event, there is no obvious means of identifying entry error, so the probability of detection should be considered Low.

As discussed in the Exposure section, the probability of detection is not the only factor that contributes to a record’s
overall susceptibility to corruption. In the examples discussed in this article, relative exposures to adulteration are proposed as depicted in Figure 5. For example, the information contained in ADE records or CAD records would be seen as highly important to an organization, giving possible motive for falsification and would be very easy to change without 'hacker' type skills, whereas PxR records are largely automatically generated and do not represent an easy opportunity for changing. ADE and CAD are, therefore, ranked as having High exposure to adulteration, whereas PxR is ranked Low/Medium. In cases where a high exposure to adulteration is identified, this could be treated as a specific hazard, and separately ranked, leading to controls designed specifically to defeat that risk.

Risk Priority

Therefore, building on the GAMP risk classifications depicted in Figure 4, and the Level of Susceptibility in Figure 5, Figure 6 presents the relative priority of the risks presented by each of our seven example record types.

A scoring system could be used to complement the approach outlined in this article. Threshold scores would need to be determined to set relative risk priorities. Rationales supporting these threshold scores would need to be documented. In general, scoring systems work better with system assessments. Scoring can become burdensome when dealing with numerous records within systems.

Appropriate Controls

The illustration of the seven example record types demonstrates that simple risk assessment techniques can be used to differentiate different electronic record types by their relative threat to public health from drug safety, quality, and efficacy. As with the demand for increasing validation rigor discussed in Part 1 of this article, increased record vulnerability demands increasingly rigorous electronic record controls. Building on the FDA's proposed areas of risk appropriate controls, Table C outlines some typical technical responses to the general requirement for secure, reliable, and confidential records.

All controls should be clearly specified, giving clear evidence of what was decided against each hazard. For the highest priority risks, a rigorous process for designing controls should be used, covering option analysis, residual risk evaluation, risk/benefits analysis and other generated hazards. Such a process is described in ISO 14971. In all cases, where a technical control, such as an audit trail, is selected, it should be validated.

Conclusion

This article has illustrated how the GAMP 4 Risk Assessment process can be used for electronic records and electronic signatures. The principles applied are consistent with those previously published by the GAMP Forum in *Pharmaceutical Engineering* for dealing with functional risk in automated systems. Although the US regulation 21 CFR Part 11 was taken as the prime example of electronic records/signature requirements, the concepts suggested are equally applicable to other GxP record-keeping requirements.

The GAMP Forum is currently preparing further detailed guidance on risk management for electronic records and electronic signatures. This work will shortly be available and discussed at forthcoming ISPE events before final publication as a GAMP Good Practice Guide.

References


Acknowledgements
The GAMP Forum would like to acknowledge the contributions of the GAMP Forum Europe and GAMP Americas Forum Steering Committees in the preparation of this article. In particular, Guy Wingate and Sam Brooks are thanked for developing the founding draft of this work.

Dr. Guy Wingate is currently the Director, Global Computer Validation, for GlaxoSmithKline in the UK.

Sam Brooks is a Validation Consultant for ABB Schweiz AG in Switzerland.