Effective and Practical Risk Management Options for Computerised System Validation

R.D.McDowall, McDowall Consulting, 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK.
Phone/Fax: +44 20 8313 0934
E-mail: r_d_mcdowall@compuserve.com

ABSTRACT

Risk management and risk assessment for computerised systems validation is a key regulatory issue following the Food and Drug Administration's (FDA) reassessment of the 21 Code of Federal Regulation (CFR) Part 11 regulations (Electronic Records and Electronic Signatures final rule). This paper reviews the GXP (i.e. Good Laboratory Practice (GLP), Good Clinical Practice (GCP) and Good Manufacturing Practice (GMP)) regulatory requirements and associated guidance documents and then focuses on the ISO 14971 risk management process and vocabulary for an overall risk management framework.

Several risk analysis methodologies are presented and assessed for their applicability for computerised system validation. The conclusion is that one methodology does not fit all situations and the prudent professional should select the best methodology applicable for the problem at hand. Finally, an overall risk management process flow for computerised system validation is presented and discussed based on two questions: "Do I need to validate the system?" and if so, "How much work do I need to do?" A single integrated document is presented as an alternative to a full V-model for the validation of lower risk computer systems.

KEYWORDS

Computerised System Validation, Risk Management, Risk Assessment, Risk Analysis, Hazard Analysis and Critical Control Points (HACCP), Hazard Analysis and Operability Analysis (HazOp), Fault Tree Analysis (FTA), Failure Mode Effect Analysis (FMEA), Functional Risk Analysis (FRA), BS7799 IT Risk Assessment, NIST SP800-30 Risk Assessment, Integrated Validation Document

INTRODUCTION

In 2002, the FDA adopted a risk based approach to regulatory compliance in pharmaceutical manufacturing when they started a review of their overall approach under the GMPs for the 21st Century programme[1]. As part of this programme, 21 CFR Part 11 was reassessed, the scope narrowed and industry was encouraged to adopt a risk based approach to interpretation of the regulation and validation of systems [2]. Under this approach, risk assessment and risk management are key, but emerging, components of computerised system validation using the approach outlined in ISO 14971 [3].

In order to understand the regulatory rationale for risk assessment and risk management, this paper reviews the current regulations and guidances for industry issued by healthcare agencies. In addition, the currently available guidances written by the industry in collaboration with regulatory agencies on the subject are reviewed. The aim is to provide a concise summary of regulatory requirement and industry guidance upon which to base a risk management approach for computerised system validation (CSV).

Next, using the topic of risk management and its associated vocabulary is introduced and discussed. It is important to state that risk management is not a one off process nor separate from CSV and the system development life cycle, but it is a continuous process and must be integrated within the overall lifecycle of system development. Under an overall risk management approach, there is the choice of risk analysis methodology. Several of the currently available methodologies are presented and discussed in the context of their suitability and applicability for CSV and IT risk assessment.

Finally, a practical approach is suggested for risk management within computerised system validation that attempts to answer the two key questions. The first question is: Does the system need validating? If yes, the second question is: How much validation is needed? A simple process flow is presented to give an overall context for the two questions. To answer the second question fully, one of two approaches is suggested: either full V-model validation (with subsequent adoption of one of the risk analysis methodologies discussed above) or a reduced validation for low risk systems using a single integrated document.

The purpose of this paper is to present and debate that different risk analysis methodologies are more appropriate to a given situation than a single one-size fits all approach.

REGULATIONS AND GUIDANCE FOR MANAGING CSV RISK

In this section, the key sections from regulations, regulatory agency guidance documents or industry guidance are highlighted and discussed. The recent driver for risk management started with FDA's adoption of risk based approaches to regulatory compliance in 2002. In 2003, the Agency started a review of 21 CFR Part 11 [4] (Electronic Records and Electronic Signatures) where the scope of the regulation was

narrowed and risk based validation was suggested. Therefore, the purpose of this part of the paper is to derive an overall approach to the risk management of validation of any computerised system operating in a regulated environment before starting any work. Failure to do this can result in over or under-engineering any validation effort.

What Do the Regulators Say?

FDA Guidance on Part 11 Scope and Application

In the section on validation is written the following statement [2]:

We recommend that you base your approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.

This one sentence has started a major change in the approaches used to validate computerised systems. However, as can be seen below, it now brings the FDA into line with the European Union (EU) GMP approach to computerised system validation.

EU GMP Annex 11

In existence since 1992, clause 2 [5] of EU GMP Annex 11 states:

The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated.

The two main factors that determine the extent of validation from this clause of the regulation are:

- What does the system do?
- Is the software commercial off-the-shelf (COTS), configurable COTS software or custom coded?

The combination of customised system and automating a high regulatory risk operation will require the most validation effort; the corollary is that a COTS application undertaking a low regulatory risk task should entail less validation effort.

ICH Q7A

The International Conference on Harmonisation (ICH) GMP regulations for Active Pharmaceutical Ingredients (APIs) [6] cover computerised systems mainly in section 5.4. Of direct interest to this debate are the following three clauses:

5.40: GMP related computerised systems should be validated. The depth and scope of validation depends on the diversity, complexity and criticality of the computerised application.

5.41: Appropriate installation qualification and operational qualification should demonstrate the suitability of the computer hardware and software to perform assigned tasks.

5.42: Commercially available software that has been qualified does not require the same level of testing. If an existing system was not validated at the time of installation, a retrospective validation could be conducted if appropriate documentation is available.

Again, a similar approach to EU GMP is advocated: the depth and scope (equivalent to "extent of validation" in EU GMP) depends on what the system automates and the nature of the software. However, Q7A goes further by saying that commercially available software that has undergone installation qualification (IQ) and operational qualification (OQ) (as outlined in 5.41) does not require the same level of end user (performance qualification) testing as a customised system.

FDA Quality System Regulation (21 CFR Part 820)

This is GMP [7] for the medical device industry and it became effective in 1997. As it is a relatively recent regulation, there are specific requirements for validation of software used in the medical device itself or computer applications used either in the production of the medical device or the organisation's quality management system (QMS).

Design Controls: Section 820.30(g)

Design validation. Each manufacturer shall establish and maintain procedures for validating the device design. … Design validation shall ensure that devices conform to defined user needs and intended uses and shall include testing of production units under actual or simulated use conditions. Design validation shall include software validation and risk analysis, where appropriate. …

Production and Process Controls: Section 820.70(i)

Automated processes. When computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol. All software changes

shall be validated before approval and issuance. These validation activities and results shall be documented.

To help interpret these regulations, the Centers for Devices and Radiological Health (CDRH) and Biological Evaluation and Research (CBER) jointly produced a 'Guidance for Industry entitled General Principles of Software Validation' [8] – see below.

FDA General Principles of Software Validation

This Guidance for Industry [8], published by the FDA in 2002, is, in the opinion of the author, currently the best document on software validation written by the Agency. The essentials of risk management are contained in two main sections:

Section 4.8:

Validation coverage should be based on the software's complexity and safety risk – not on firm size or resource constraints. The selection of validation activities, tasks, and work items should be commensurate with the complexity of the software design and the risk associated with the use of the software for the specified intended use. For lower risk devices, only baseline validation activities may be conducted. As the risk increases additional validation activities should be added to cover the additional risk.

Section 6.1: How Much Validation Is Needed?

- *The extent of validation evidence needed for such software depends on the device manufacturer's documented intended use of that software.*
- *For example, a device manufacturer who chooses not to use all the vendor-supplied capabilities of the software only needs to validate those functions that will be used and for which the device manufacturer is dependent upon the software results as part of production or the quality system.*
- *However, high-risk applications should not be running in the same operating environment with non-validated software functions, even if those software functions are not used.*
- *Risk mitigation techniques such as memory partitioning or other approaches to resource protection may need to be considered when high-risk applications and lower risk applications are to be used in the same operating environment.*
- *When software is upgraded or any changes are made to the software, the device manufacturer should consider how those changes may impact the "used portions" of the software and must reconfirm the validation of those portions of the software that are used (see 21 CFR §820.70(i)).*

Again, the extent of validation is dependent on the documented use of the software (there is a direct reference to a written specification document being available in "documented intended use of that software"). The use of commercial software is acceptable and if a function in the application is not used it need not be validated provided that the use of the

system is not high-risk (e.g. Class III medical device). For these high risk medical devices, then the software needs to be validated fully as a malfunction may be life threatening. Equally so, for low risk devices baseline validation activities need to be conducted.

PIC/S Guidance for Computerised Systems

The Pharmaceutical Inspection Cooperation Scheme (PIC/S) have published guidance on 'Good Practices for Computerised Systems in GXP Environments' [9] that provides good advice for risk management.

Section 4.3:

For GXP regulated applications it is essential for the regulated user to define a requirement specification prior to selection and to carry out a properly documented supplier assessment and risk analysis for the various system options.

Section 23.7:

GXP critical computerised systems are those that can affect product quality and patient safety, either directly (e.g. control systems) or the integrity of product related information (e.g. data/information systems relating to coding, randomisation, distribution, product recalls, clinical measures, patient records, donation sources, laboratory data, etc.). This is not intended as an exhaustive list.

PIC/S calls for a risk analysis of the documented system components and functions. The guidance also notes that systems can impact product quality or patient safety directly or indirectly via the quality of information output. This is important to note as PIC/S is more detailed than the FDA's Part 11 guidance [2] that simply states risk assessment needs to be performed on a systems impact on product quality, safety and record integrity but does not define what it means in any further detail.

Industry Guidance Documents

There are two industry guidance documents that are useful to consider in relation to risk that have been released in 2005. These are the draft ICH Q9 consensus guideline for quality risk management [10] and the GAMP Good Practice Guide for risk based compliant electronic records and signatures [11].

ICH Q9 Quality Risk Management

This document has reached the second step of the ICH process and was released for consultation in March 2005. As the contents of this document could change before full adoption, the reader is advised to read the latest version available.

The purpose of the document is to serve as a *foundational or resource document that is independent yet supports other ICH Quality documents* by providing the *principles and examples of tools of quality risk management*. It proposes a systematic and formal approach to risk management but also recognises that ad-hoc informal processes can be acceptable. However, in the context of computerised systems, the formal approach is discussed in this paper. The overall process flow for risk management is similar to that from ISO 14971 but for clarity the ISO process flow in Figure 3 will be used for consistency throughout this paper as there are some differences with ICH Q9. The great advantage of the current version of the document is its listing of the risk analysis methodologies in section 5 and the references in section 8 where it is interesting that GAMP Guide [12] is not mentioned.

GAMP Risk Based Approach to Compliant Electronic Records and Signatures

This GAMP Good Practice Guide [11] is the replacement for an older Guidance [13], issued under the original interpretation of 21 CFR Part 11, and is intended to supplement the existing GAMP Guide version 4 [12]. The Good Practice Guide aims to provide guidance about record integrity, security and availability of records throughout the records retention period. There is a relatively comprehensive interpretation of global predicate rule regulations to help interpret 21 CFR Part 11 under the FDA's guidance on Part 11 Scope and Application [2]. The risk management approach advocated in this best practice guide is the assessment of system risk and record risk.

The risk analysis approach advocated by the guide is simply a reprint of the GAMP Guide in Appendix M3 that contains the risk assessment based on failure mode effect analysis (FMEA). However, in the introduction to the Good Practice Guide, it is noted that other methodologies can be used.

Regulatory Requirements and Guidance Summary

As presented and discussed above, the regulations are very explicit about CSV risk management; the extent of validation should be based on two main factors:

1. The functions that are automated by the system.
2. The nature of the software used in the system.

Therefore, to justify your extent of validation for any specific computer system, your approach needs to have a documented risk assessment to mitigate and manage the overall risk posed by the computerised system within acceptable and documented levels.

However, with all regulations the regulators say what they want but not how to do it to avoid being prescriptive.

The industry guidance through GAMP and ICH provides a framework to carry out the risk assessment and mentions some of the risk analysis methodologies that can be used including ISO 14971.

INTERNATIONAL STANDARDS ORGANISATION (ISO) AND RISK MANAGEMENT

The FDA Part 11 Scope and Application [2] guidance references ISO 14971 [3] as the basis for risk assessment. Note that references in guidances for industry are informative and not mandatory in that they provide examples and relevant information rather than define the definitive approach. Alternative approaches are acceptable providing that applicable regulations are met. This ISO standard presents a framework for risk management for medical devices. Therefore, we will discuss the terms and definitions used in this standard which also further references ISO Guide 73 [14]. When we complete this section, you will realise that the FDA actually require risk management rather than just risk assessment.

Vocabulary Issues

However, before we can discuss risk management in the context of computer validation, we need to have a common vocabulary for risk management as the regulations use different terms without defining what they mean. For example, *risk assessment* is used by the FDA in the Part 11 guidance [2] and *risk analysis* in 21 CFR Part 820 [7] and *risk analysis* by the PIC/S guidance [9]. Do they want the same end result or are they different? In short, we do not know as there appears to be insufficient advice offered in these regulations and guidance documents.

Therefore, we need to discuss and agree upon a common vocabulary for risk management and here is where ISO 14971 [3] and ISO Guide 73 [14] enter the scene.

ISO Guide 73 and ISO 14971: Risk Management Definitions

The following definitions are taken from ISO 14971 [3] and these should be read in conjunction with Figure 3 adapted from ISO Guide 73 [14]:

- *Risk management:* The systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. From Figure 3, this is the overall process that is the subject of this paper.

- *Risk assessment:* The overall process of a risk analysis and risk evaluation. This is the major sub-process and comprises two elements: risk analysis and risk evaluation as shown in Figure 3. This is the stated requirement of the FDA [2].

- *Risk analysis:* The systematic use of available information to identify hazards and estimate the risk.

- *Risk evaluation:* Judgement, on the basis of risk analysis, of whether a risk that is acceptable has been achieved in a given context.

- *Risk:* combination of the probability of occurrence of harm and the severity of that harm.

- *Harm:* physical injury or damage to the health of people, or damage to property or the environment.

  Note this is for a medical device; this needs to be interpreted as the consequences of a software error or malfunction of the system.

- *Severity:* measure of the possible consequences of a hazard.

- *Hazard:* potential source of harm.

- *Risk control:* The process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, acceptable levels. Note that all risks cannot be eliminated but they are mitigated within acceptable levels. What is acceptable will be determined by the operating environment and the functions that the computerised system automates.

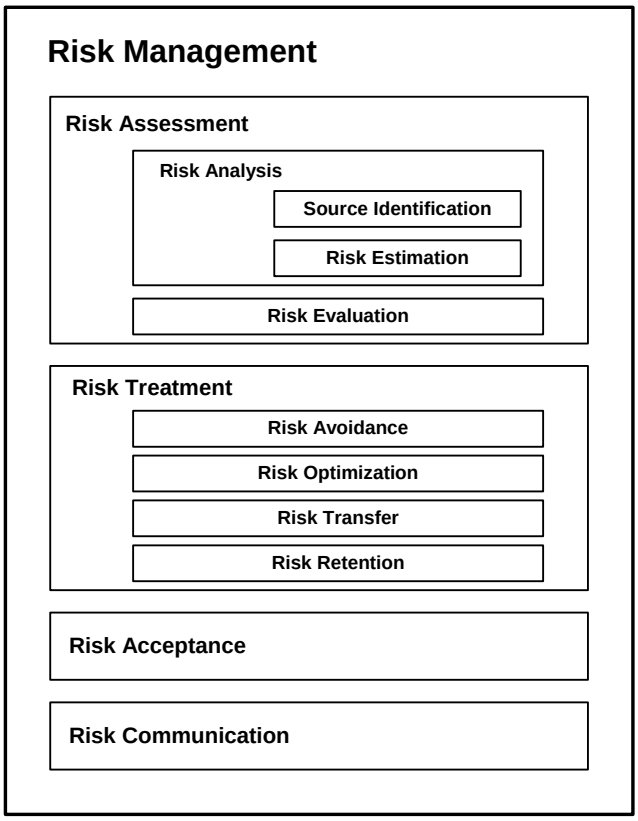

Figure 1: Risk Management Terminology and Relationships from ISO Guide 73 [15]

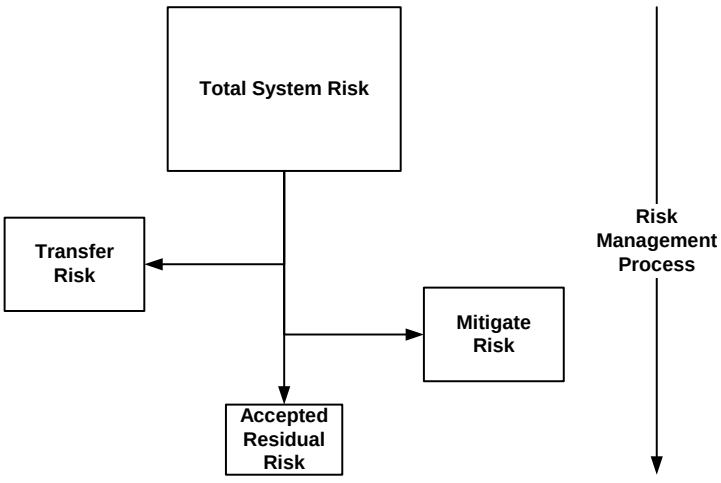

Figure 2: Outcome of a Risk Management Process

Aims of Risk Management

The aim of the overall risk management process is shown in Figure 2. It is to take all the identified risks of a computer system and reduce them by mitigation activities using different approaches or design so that the residual risk is within manageable or acceptable limits. There are a number of options that can be used:

- *Risk Assumption:* Accepting the potential risk and continue operating the IT system without any additional actions.

- *Risk Avoidance:* Avoiding the risk by eliminating the risk cause and/or consequence such as the addition of design features or procedural controls that prevent the risk from occurring.

- *Risk Limitation:* Limiting the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls) or by authorizing operation for a limited time during which additional risk mitigation by other means is being put into place.

- *Risk Transference:* Transferring the risk by using other options to compensate for the loss, for example purchasing insurance against the threat in carefully defined circumstances.

It is important to understand that not all risks are the same level. That is why the majority of risk analysis methodologies rank risk and deal with the highest priority/severity first and may often leave lower risks as they are within an acceptable level.

There is are additional definitions from IEEE Standard 1540 [16] (Software life cycle processes – Risk management) that should be included for consideration here:

- *Acceptability*: The exposure to loss (financial or otherwise) that an organisation is willing to tolerate from risk.

- *Likelihood*: A quantitative or qualitative expression of the chances that an event will occur.

It is important that acceptability be included in these definitions as it summarises succinctly the residual risk of a computerised system. Typically the downside could be misinformation or regulatory citations of a poorly validated system.

ISO 14971: Risk Management for Medical Devices

This standard provides an overall risk management framework to identify, analyse, mitigate and accept risk for medical devices. Within this framework there are further

definitions to consider; however, as will be pointed out below, there is not always a 1:1 relationship between ISO Guide 73 and ISO Standard 14971:

- *Intended use / intended purpose:* use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer.

  For a computerised system or software application, this means the user requirements specification or equivalent documents; even for a custom code system, there needs to be a specification. This is imperative and non-negotiable as it is the starting point of the whole risk management process. It is still surprising that many people working in regulated industries fail to see the need for a properly written requirements specification from either the business or regulatory perspectives.

- *Residual risk:* risk remaining after protective measures have been taken.

- *Risk management file:* set of records and other documents, not necessarily contiguous, that are produced by a risk management process.

  This is the documented evidence required by the FDA and other regulatory agencies. It is important to ensure that the risk management file is integrated within the overall process of computerised system validation.

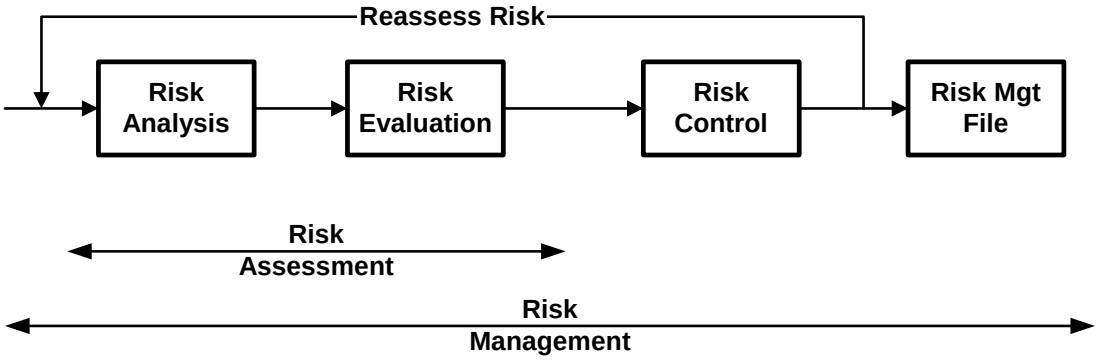

Figure 3: The Risk Management Process adapted from ISO 14971 [3]

Risk Analysis

The input to this process is a statement of intended use of the computerised system i.e. a user requirements specification or equivalent document. As requirements may change during development or are refined, this is the major reason why risk assessment needs to be reviewed and updated. From the requirements, potential hazards are identified and the probabilities of risk for each hazard are estimated.

The aim here is to ask two simple questions:

1. What can go wrong?
2. If something does go wrong:
   What is the probability of it happening and what are the consequences? [17]

The aim is to anticipate problems in the design phase to prevent them occurring in the operational system and improve the reliability of any computer system.

Risk Evaluation

Following on from the analysis phase, the evaluation process is in essence very simple: it asks the question does the risk need to be mitigated or not? If the answer is no, then the risk is accepted and nothing further is required. However, if there is a requirement for mitigation, then the risk moves into the next stage of the process: risk control. Typically only high risk factors will pass to the next stage; however, this decision depends on the criticality of the project in question.

Risk Control

Once the high-risk tasks have been highlighted, then it is possible to prepare plans and countermeasures to overcome the risk. Note that it is not always possible to eliminate a risk as this may be impossible or require too much effort. However, sufficient work needs to be done to ensure that the impact of any identified risk is managed and is acceptable. For example, modifying the user requirements specification or functional design of specific features or functions of a system may be one way of controlling a defined risk. Equally so, implementation of user training may also be a method of avoiding or transferring a risk. Ultimately, the final outcome of this process is where risk has been reduced to an acceptable level that is documented appropriately.

Note that this is risk treatment in ISO Guide 73 and covers topics such as risk avoidance, risk optimisation, risk transfer and risk retention; risk control here also includes risk acceptance. Equivalent processes occur in ISO 14971; however, the framework diagram in Figure 3 does not make this clear immediately.

Risk Management File

As the project progresses, a body of information about how the project risk has been managed and mitigated has been amassed; it is important that this information is not forgotten or ignored. Reuse and update the information: it can be used to feedback into the risk cycles as shown in Figure 3. This portion of the risk management process incorporates the element of risk communication from ISO Guide 73.

Continuous Process

Risk Management is a continuous process that needs to be conducted at least early in the validation project using outline specifications of intended purpose and later in the project when the intended purpose has been completed. The reason is a project starts with a high degree of uncertainty and hence high risk. As it progresses, uncertainty in some areas is reduced but in others it can increase, hence the need for repeating the risk assessment and plan approaches to counter any newly identified risks.

POSSIBLE RISK ANALYSIS METHODOLOGIES FOR CSV

The choice of the risk analysis methodology is left to the individual organisation to select both by the FDA and ISO. There are a number of methodologies that are listed in ICH Q9 [10] and ISO 14971 [3]. The following are potential risk analysis methodologies that could be used within the ISO 14971 risk management framework, each will be discussed and their applicability for CSV assessed and summarized at the end of this section.

- Hazard Analysis and Critical Control Points (HACCP).
- Hazard Operability Analysis (HazOp).
- Fault Tree Analysis (FTA).
- Preliminary Hazard Analysis (PHA).
- Failure Mode Effect Analysis (FMEA).
- Failure Mode, effect and Criticality Analysis (FMECA).

In addition there are other methodologies that have been used either for computerised system validation or for IT infrastructure risk assessment, for example:

- Functional Risk Analysis (FRA).
- BS7799 Risk assessment (Guidance Document PD 3002).
- NIST SP800-30 Risk Management Guide for IT Systems.

Currently the main emphasis for risk management in CSV is the GAMP methodology (similar to Failure Mode Effect Analysis (FMEA)) which is suitable for complex and bespoke computer systems. However, other approaches are also acceptable and we will discuss some other main methodologies that could be used.

The key point to make with these methodologies is that they should be used in a predictive mode (anticipating events) rather than reactive one (analysis after an event). As such, a methodology such as root cause analysis is not applicable to CSV risk management as it is applied after a “significant event” to analyse it, to find the fundamental causes of the event and to implement changes to prevent a reoccurrence [18]. The focus of CSV risk management is on prevention by eliminating problems, leaving risk at an acceptable level.

Risk Analysis Entry Criterion: A Complete URS

To complete a successful risk assessment you must ensure that until you have a user requirements specification (URS) or equivalent specification that reflects your intended use of any new or updated computerised system. A URS is THE key document around which all further risk management and validation work is predicated. If the URS is not complete or accurate then the risk analysis will be incomplete and will need to be updated as the definition of the system proceeds. This is also important for an upgrade of an existing system where new features need to be evaluated carefully and incorporated into the requirements documentation.

Team Approach to Risk Assessment: Performing the Assessment

It is important to realize that a single individual typically cannot conduct a risk assessment; it is a multidisciplinary team approach. The team membership will vary with the system being implemented or developed but a core team will consist of:

- Users of the system.
- Technical implementers (e.g. IT and/or engineering).
- Validation.
- Quality Assurance.
- Project Manager.

The team should be relatively small, say five, seven or nine people, so that it performs well rather than getting bogged down with detail that can happen with larger groups. The odd number is deliberate so that there is an inbuilt majority. One member of the team should be a facilitator of the group and ensure that every person can have their say, avoid the group being dominated by personalities and to facilitate a consensus on risks to be reached. The process can vary from brainstorming (FMEA/FMECA) to selection of one of two options (FRA).

Typically a room is dedicated for the risk assessment workshop and attendees should not be distracted by calls from their work colleagues to ensure that their focus is on the risk assessment. The workshop scope needs to be defined and agreed in advance of the start. It is advantageous to start the workshop in the morning when people are most alert and before issues can have impacted them. A minimum of two workshops are needed with time between them so that the workshop output can be written up and circulated for review.

Depending on the methodology used, either flip charts (alternatives are whiteboards with photocopy facilities or computer white boards) or a data projector showing the starting document templates are used to capture the workshop output. The URS or other specification document will be used as the input and to stimulate discussion and debate. Depending on the size of the group, the facilitator can collate the workshop output or another team member can act as the scribe for the workshop.

Hazard Analysis and Critical Control Points (HACCP)

HACCP is a systematic, proactive, and preventive method for assuring product quality, reliability, and safety that was developed by Pillsbury Foods to provide food for the astronauts of the NASA space programme. The FDA has adopted this methodology and has applied it to seafood (since 1995) and fruit juice (since 1998) and is expanding it to other food areas over which it has control. The US Department of Agriculture also uses HACCP for meat and poultry production. There is an FDA guidance document [19] and failure to confirm to HACCP guidelines is the source of many warning letters on the FDA website for seafood and other food processors.

The methodology is a structured approach to analyse, evaluate, prevent, and control the risk or the adverse consequences of identified hazards during the production and distribution of food products. The methodology consists of seven steps [10]:

1. Conduct a hazard analysis and identify preventive measures for each step of the process.
2. Determine the critical control points.
3. Establish critical limits for each of the control points.
4. Establish a system to monitor the critical control points.
5. Establish the corrective action(s) to be taken when monitoring indicates that the critical control points are not in a state of control.
6. Establish a system to verify that HACCP system is working effectively.
7. Establish a record-keeping system.

The ICH Q9 document identifies the potential areas of use as mainly in process manufacturing and notes that HACCP is most useful when product and process understanding is sufficiently comprehensive to support identification of critical control points [10]. The key phrase here is ‘sufficiently comprehensive’ as the applicability of this methodology for many commercial applications may be inappropriate as this information may not be available, possibly limiting its applicability to computerised systems validation.

Hazard Operability Analysis (HazOp)

A HazOp risk analysis is a bottom-up methodology that is intended to identify hazards and operability problems in the design of a process facility or plant. The key concept of HazOp is that the team investigates how a plant might deviate from the designed intent, thus identifying the hazards. The risk analysis methodology is based on the principle that several experts with different backgrounds can interact and identify more problems when working together as a team than when working separately and then combining their individual results. The methodology uses guide words to structure the analysis, such as:

- More or high, higher or greater (implying an excess).
- No, none, less or low, lower or reduced (implying insufficiency).

- These are compared with the intended design parameter such as high + flow = high flow [20].

If, in the process of identifying problems during a HazOp study, a solution becomes apparent, it is recorded as part of the HazOp result; however, care must be taken to avoid trying to find solutions which are not so apparent, because the prime objective for the HazOp is problem identification.

The success or failure of an individual HazOp analysis depends on several factors:

- The completeness and accuracy of drawings and other data used as a basis for the study (translating for CSV, these are the specification documents for the system).
- The technical skills and insights of the team.
- The ability of the team to use the HazOp approach as an aid to their imagination in visualizing deviations, causes, and consequences.
- The ability of the team to concentrate on the more serious hazards which are identified and not become side tracked with minutiae.

ICH Q9 [10] notes that HazOp can be applied to manufacturing processes, equipment and facilities for drug substances and drug (medicinal) products. It has also been used primarily in the pharmaceutical industry for evaluating process safety hazards. However, as noted above, one of the keys for success if applied to computer validation is the completeness of the system specification; therefore, it is probable that this risk analysis methodology will remain with drug manufacturing processes and not be applied widely to computerised systems.

Fault Tree Analysis (FTA)

The FTA method is a top-down risk analysis methodology that assumes failure of the functionality or an undesired consequence of a product or process. FTA identifies various combinations of faulty and possible events occurring in the system. Typically, FTA evaluates each failure one at a time and the results are displayed as a tree of faults with the corresponding failure mode. FTA relies on process understanding of the experts to identify causal factors.

At each level in the tree, combinations of fault modes are described with logical operators or gates [20]:

- AND gate (output event occurs if all input events occur simultaneously).
- OR gate (event occurs if any one of the input events occurs).

The gates are linked with events to describe the actions such as:

- Circle event (basic event with sufficient data).
- Diamond (undeveloped event).

- Rectangle (event represented by a gate).
- Triangle (Transfer symbol).

It is the combination of gate and events that allows the top-down risk analysis of a design.

ICH Q9 [10] notes that FTA can be used to establish the pathway to the root cause of the failure. The use of FTA can be applied while investigating complaints or deviations to fully understand their root cause and to ensure that intended improvements will fully resolve the issue and not lead to other issues (i.e. solving one problem leads to the causing of a different one). Fault Tree Analysis is a good method for evaluating how multiple factors affect a given issue and it is useful for both risk assessment and in developing monitoring programs.

Preliminary Hazard Analysis (PHA)

PHA is a risk analysis methodology that uses previous experience or knowledge of hazards and failures to identify future ones that might cause harm. It can also be used for estimating their probability of occurrence for a given activity, facility, product or system. The method consists of:

- Identification of the possibilities that the risk event happens.
- Qualitative evaluation of the extent of possible injury or damage to health that could result.
- Identification of any remedial measures that could be implemented.

ICH Q9 [10] notes that PHA might be useful when analysing existing systems or prioritising hazards where circumstances prevent a more extensive technique from being used. The methodology is most commonly used early in the development of a project when there is little information on design details or operating procedures; thus, it will often be a precursor to further studies. However, from the perspective of CSV it is unlikely that this methodology will be used widely as there are more established ones used with computerised systems. If the system is unique, then the PHA may be inappropriate as it relies on a baseline of previous experience.

Failure Mode Effects Analysis (FMEA)

FMEA provides for an evaluation of potential failure modes for processes and the likely effect on outcomes and / or product performance. Once failure modes are established, risk reduction can be used to eliminate, reduce or control the potential failures. It relies on product and process understanding. FMEA methodically breaks down the analysis of complex processes into manageable steps. It is a powerful tool for summarizing the important modes of failure, factors causing these failures and the likely effects of these failures.

The methodology was primarily developed for material and equipment failures, but has also been used for human error, performance and software errors [20]. The process has three main aims:

- The recognition and evaluation of potential failures and their effects.
- The identification and prioritisation of actions to eliminate the potential failures or reduce their chances of occurring.
- The documentation of these identification, evaluation and corrective activities so that product quality improves over time.

FMEA was developed in the late 1940's for the US Military and is described in US Military Standard 1629a [21]. The approach has been further developed for the US car industry as the Society of Automotive Engineers Standard J-1739 [22]; as such it is suitable for complex design and processes. This methodology is the basis of the approach described in GAMP Guide Version 4, Appendix M3 [12] and suggested for use for risk assessment in computer validation.

The broad FMEA will be described in this paper but the reader must realise that there are both quantitative and qualitative modes of this methodology that can be applied depending on what outcome is required [17], therefore the reader is encouraged to read further to gain more understanding. The following books are recommended:

- McDermott et al [23] for simple overview of FMEA.
- Stamatis [17] for the FMEA vocabulary, organising the exercise, the detail of the technique and its application to several industries including software. Chapter 11 is devoted to FMEA of software and provides a number of questions to consider. There is also a detailed appendix on CD-ROM with further information and document templates. This book is the personal choice of the author on cost-benefit grounds.
- Dyadem Engineering Corporation [20] for FMEA of medical devices including a CD-ROM containing trial copies of software for FMEA analysis.

The FMEA risk analysis methodology is shown as an overall process flow chart in Figure 4. The starting point for the process, as with other risk analysis methodologies, is the URS or equivalent specification document(s). Note that the numbers in the list below correspond to the equivalent stages in the process flow chart of Figure 4:

1. Identify potential risks in the system from both a business and a regulatory perspective. This is done by considering the functions documented in the URS. For each function identified the team should list all possible causes of failures (here is where paranoia comes into play and the process needs to be carefully facilitated). Equally so if a function poses no apparent risk, this should also be documented.

2. Next, for each failure mode identified above, the severity of the failure needs to be assessed. Here there are differences in the way that FMEA can be used, either in quantitative or qualitative mode. The qualitative mode is preferable for the nature of

the systems used in the pharmaceutical and medical device industries unless the system is life threatening and then a more rigorous approach should be considered. Qualitative FMEA is outlined in the GAMP Guide Appendix M3 [12] and is discussed in this paper. For information on quantitative mode FMEA, the book by Stamatis [16] is recommended.

The assessment of the severity of the failure is one of the following options:

- Low: system malfunctions without impact.
- Medium: system malfunctions without impacting quality issues.
- High: significant impact (health issues, regulatory issues, data integrity/quality compromised).

3. For each failure the team needs to assess the probability of occurrence and this is usually one of the following:

   - Low.
   - Medium.
   - High.

   In the early stages of a system design, there may not be enough known of how the computerised system may handle and identify failures and errors. Therefore it may be prudent to allocate a medium probability of occurrence that can be refined later in the life cycle as the designed is developed and refined.

4. Then the risk of each failure is classified by plotting the probability of occurrence (low, medium or high) versus the severity of the failure (also low, medium or high) using a 3 x 3 Boston grid as shown in Figure 5. The risk is classified into one of three levels:

   - Level 1 (high/high, medium/high or high/medium) = high impact risk.
   - Level 2 (low/high, medium/medium or high/low) = medium impact risk.
   - Level 3 (medium/low, low/low or low/medium) = low impact risk.

   Each risk is formally classified graded using this grid to identify the most important ones versus the lower impact ones in a very structured manner.

5. Now the probability of the system to detect the failure is assessed as one of the following options:

   - Low: Detection is unlikely.
   - Medium: Moderate probability of detection.
   - High: Malfunction detection highly likely.

6. Prioritise the risk by plotting the risk classification (Level 1, 2 or 3) versus the probability of detection (low, medium and high likelihood) in a second a 3 x 3 Boston grid as shown in Figure 6. Now risk is prioritised as:

    - High: low/level 1, medium/level 1 or low/level 2.
    - Medium: low/level 3, medium/level 2 or high/level 1.
    - Low: medium/level 3, high/level 3 or high/level 2.

7. Mitigation of unacceptable risks is now undertaken. The key question is what is unacceptable, which of course depends on the system and the functions it automates, but generally speaking the high priority risks need to be mitigated in some way through design modifications or procedural means. As many of the medium risks should be addressed as possible and the low risk ones are generally left if the risk is acceptable. All of these decisions should be documented in the appropriate validation documentation.

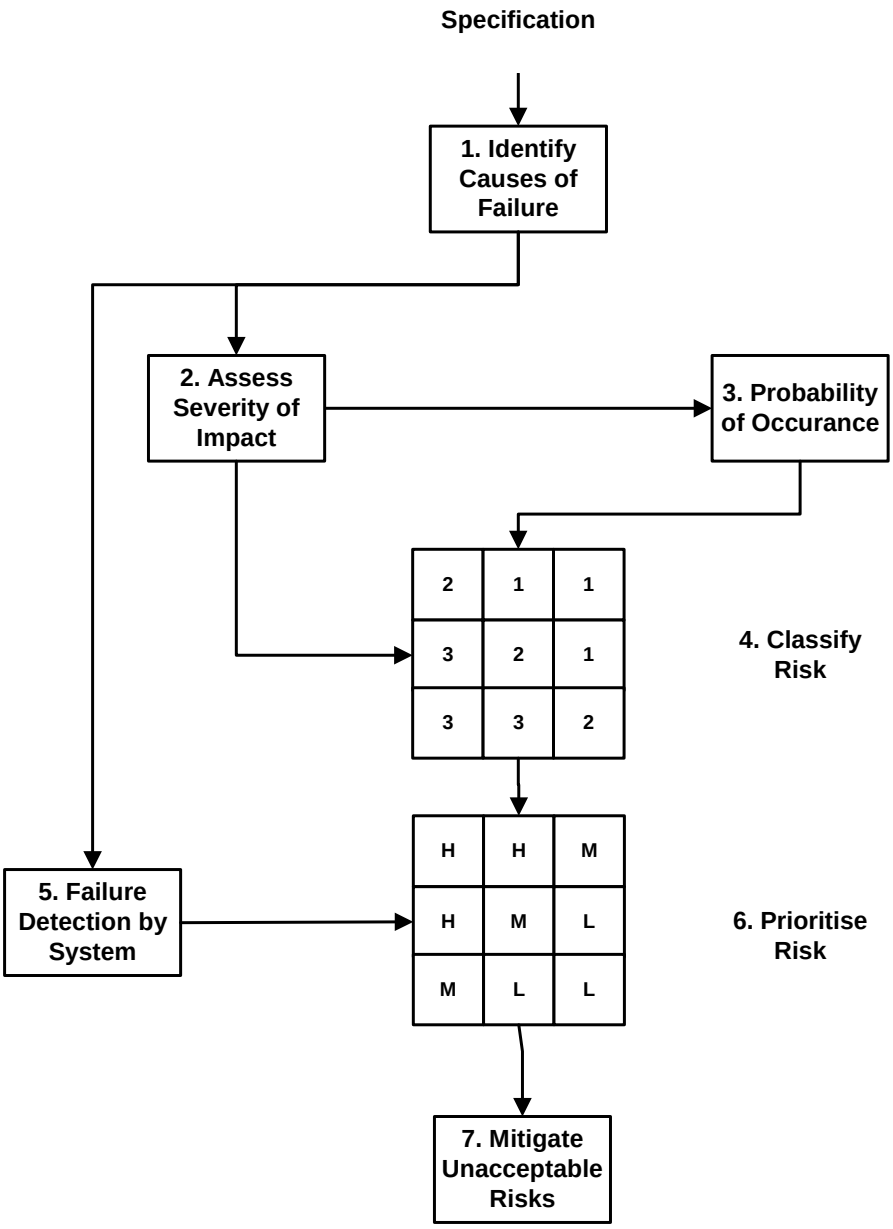

Figure 4: Process Flow for a Failure Mode and Effects Analysis

Some FMEA schemes can have an additional stage to identify if the failure is due to the system itself or an operator. This minor refinement of the approach can be used to highlight issues outside of the system such as user training and documentation of procedures.

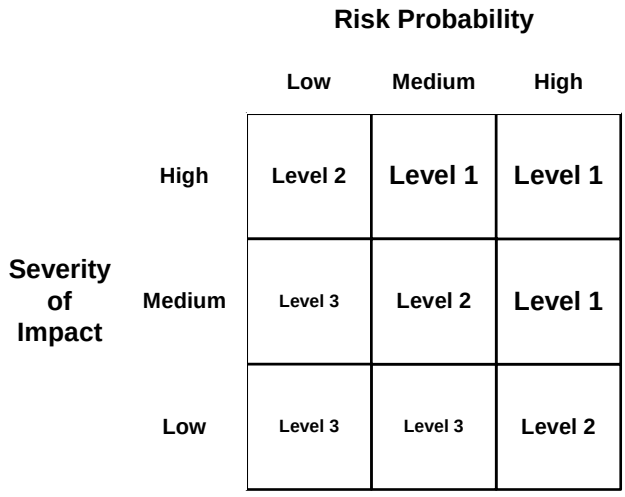

Figure 5: Boston Grid for Classifying a Risk (FMEA Step 4)

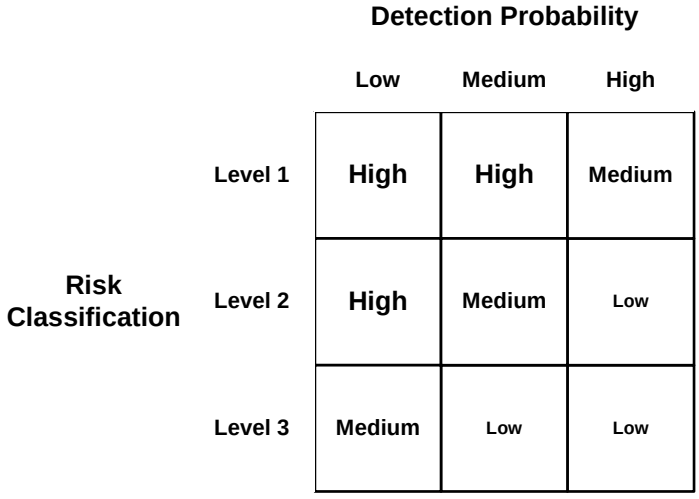

Figure 6: Boston Grid Used to Prioritise Risk (FMEA Step 6)

ICH Q9 [10] notes that FMEA can be used to prioritise risks and monitor the effectiveness of risk control activities. FMEA can be applied to equipment and facilities, and might be used to analyse a manufacturing process to identify high-risk steps or critical parameters. When used at early stages of the specification of a system it can also be used to improve the design of the system to mitigate or remove potential failure modes.

Limitations of FMEA

Limitations of FMEA can be summarised as follows [20]:

- Analysis of complex systems that have multiple functions consisting of a number of components can be tedious and difficult.
- Compound failure effects cannot be analysed.
- Can be costly and time consuming, unless carefully controlled.
- Successful completion requires expertise, experience and good team skills.
- Incorporating all possible factors influencing the system, such as human errors and environmental impacts, can make the analysis lengthy and requires a thorough knowledge of the characteristics and performance of the components of the system.
- Dealing with data redundancies can be time consuming.

In addition, the use of FMEA in the validation of commercially available or configurable software (GAMP categories 3 and 4) is, however, overkill as the design documentation for the application nor the source code are available to the validation team. As such the methodology is far more suitable for complex process equipment or category 5 software.

Failure Mode, Effects and Criticality Analysis (FMECA)

FMEA can be extended to incorporate an investigation of the degree of severity of the consequences, their respective probabilities of occurrence and their detectability, and might become a Failure Mode Effect and Criticality Analysis. Again, to perform such an analysis, the product or process specifications should be established.

ICH Q9 [10] notes that FMECA application in the pharmaceutical industry will mostly be utilized on failures and risks associated with manufacturing processes; however, it is not limited to this application. The output of an FMECA is a relative risk "score" for each failure mode that is used to rank the modes on a risk basis.

Functional Risk Assessment (FRA)

Functional Risk Analysis is a simpler risk analysis methodology that has been developed specifically for computerised system validation of commercially available software [24, 25]. The input to the process, as is the case with the other risk analysis methodologies, is a prioritised user requirements specification. The process flow in Figure 7 is described in the list below and the numbers in the figure correspond to the tasks below.

1. The URS requirements are prioritised as either mandatory (M) or desirable (D). The mandatory assignment needs the requirement must be present for the system to operate and if desirable is assigned, then the requirement need not be present for operability of the system simply a nice to have [26].

2. The next stage in the process is to carry out a risk assessment of each function to determine if the function is business and/or regulatory risk critical (C) or not (N). This risk assessment methodology uses the tables from the URS that have two additional

columns added to them as shown in Table 1. For a requirement to be assessed as critical one or both of the following criteria need to be met.

The requirement functionality poses a regulatory risk that needs to be managed. The basic question to ask here is: will there be a regulatory citation if nothing is done? For example, requirements covering security and access control, data acquisition, data storage, calculation and transformation of data, use of electronic signatures and integrity of data are areas that would come under the banner of critical regulatory risk.

A requirement can also be critical for business reasons, e.g. correctness of data output, performance of the system or system availability. A requirement for the availability of the system will adversely impact a chromatography data system supporting a continuous chemical production far more than the same system in an R&D environment.

The approach is shown in Table 1 in the fourth column from the left. Here, each requirement has been assessed as either critical or non-critical. All other requirements are assessed as non-critical in the FRA methodology.

3. The functional risk assessment approach is based on the combination of prioritised user requirements and regulatory and/or business risk assessment. Plotting the two together produces the Boston Grid shown in Figure 8. Requirements that are both mandatory and critical are the highest risk, medium are those that are mandatory and non-critical or desirable and critical with desirable and non-critical as the lowest risk.

   For most commercial systems, requirements either fall into the high and low risk categories. There will be a few requirements in the mandatory and non-critical quadrant of the grid but few, if any, in the desirable but critical quadrant. This is logical. If your requirement were only desirable why would it be critical? If many requirements fall in this last quadrant, it may be an indication that the initial prioritisation was wrong. Therefore under this classification, only the software requirements classified as “high” in the grid (mandatory and critical) will be considered for testing in the qualification of the system. No other requirement will be considered for testing [24]. Once the risk analysis has been completed, the traceability matrix can be included in the same document.

4. The purpose of a traceability matrix is to show the coverage of testing or verification against a specific requirement. For a commercial application this matrix can be undertaken using the risk assessment by adding an additional column on the right of the table as shown in Table 1 (the column labelled Test). As outlined in the FRA, only those functions that are classified as both mandatory and critical are considered for testing in the qualification phase of the validation. Therefore functions 3.3.03 and 3.3.06 are not considered for testing, as they do not meet the inclusion criteria. Of the remaining four requirements these all constitute capacity requirements that can be combined together and tested under a single capacity test script, which in this example is called Test Script 05 (TS05). In this way, requirements are prioritised and classified for risk and the most critical one can be traced to the PQ test script.

As well as linking specific requirements to individual test scripts, a traceability matrix can also be used to link requirements to other deliverables such as Standard Operating Procedures (SOPs), IQ or OQ documents and the vendor audit report. Other requirements can be verified by linking to the system configuration log such as server requirements or writing procedures.

Limitations of Functional Risk Assessment

The FRA methodology is intended for use with commercial off-the-shelf (COTS) software (GAMP Category 3) and configurable COTS software (GAMP category 4). It has not been applied to bespoke or custom coded systems (GAMP category 5).

The methodology is relatively simple which allows it to sit on top vendor testing of commercial software as this is usually more extensive than an end user or a validation team can perform. However, this assumption should be verified by a vendor audit for critical systems.

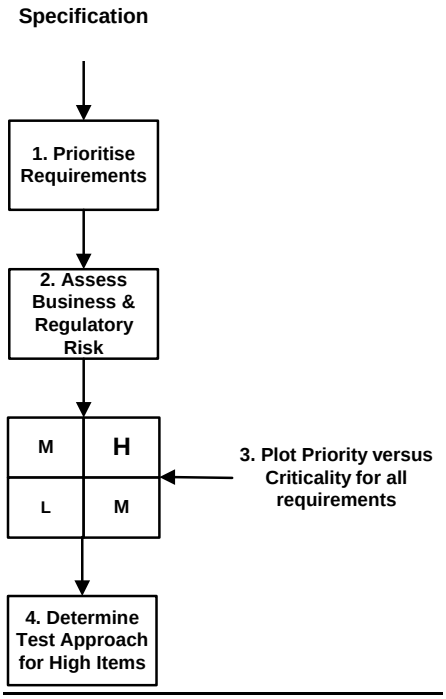

Figure 7: Functional Risk Assessment Process Flow Chart

Table 1: Part of a Combined Risk and Analysis and Traceability Matrix for a Chromatography Data System (CDS)

Req. No.	Data System Feature Specification	Priority M/D	Risk N/C	Test
3.3.01	The CDS has the capacity to support 10 concurrent users from an expected user base of 40 users.	M	C	TS05
3.3.02	The CDS has the capacity to support concurrently 10 data A/D data acquisition channels from an expected 25 total number of channels.	M	C	TS05
3.3.03	The CDS has the capacity to support concurrently 10 digital data acquisition channels from an expected 25 total number of channels.	D	N	-
3.3.04	The CDS has the capacity to control concurrently 10 instruments from an expected 20 total number of connected instruments.	M	C	TS05
3.3.05	The CDS has the capacity to simultaneously support all concurrent users, data acquisition and instrument connects whilst performing operations such as data reprocessing and reporting without loss of performance (maximum response time is < 10 seconds from sending the request) under peak load conditions.	M	C	TS05
3.3.06	The CDS has the capacity to hold 70 GB of live data on the system.	D	N	-

Table Legend:
Priority: M/D = prioritisation of the requirement as either Mandatory (M) or Desirable (D)
Critical: N/C = assessment of regulatory and / or business risk as either Critical (C) or Not Critical (N)
Test: Traceability matrix these requirements are tested under Test Script 5 (TS05), other requirements can be traced to installation of components or to an SOP

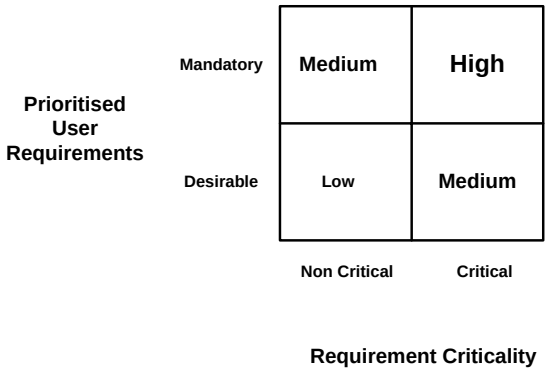

Figure 8: Plot of Prioritised Functions versus Risk Assessment

IT Risk Assessment Methodologies

There are two risk assessment methodologies that have been developed specifically for information technology, the first within the BS 7799 (Information Management Security) [27] and the second from the National Institute of Standards and Technology (NIST) [28]. Each methodology will be presented and discussed in the following sections; however, before we start it is important that a few concepts are presented and discussed.

In the context of IT risk assessment vulnerability is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy [28].

In addition, the status of the system being analysed for risk is important as it modifies the approach that should be taken in the analysis.

- If the system is being designed, the search for vulnerabilities should be driven from an organisation's security policies and procedures together with the specification for the system and the vendors' or developers' security product analyses. This is the best and most cost-effective way to conduct the analysis as controls can be designed into the system rather than added on to an existing system as an afterthought.

- If the system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features inherent within the system and how they are being implemented. Equally so, a second risk analysis can be conducted at this stage of a system being developed to build on the first risk analysis performed above.

- However, if the system is operational, then the process of identifying vulnerabilities should include an analysis of the system security features and the security controls, both technical and procedural, already used to protect the system in addition to any

intelligence from suppliers about the level of threats to components, e.g. operating system.

Both technical and non-technical controls can be classified as either preventive or detective [28], which are described as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

BS 7799 IT Risk Assessment Methodology

The flow chart in Figure 9 depicts the BS 7799 risk assessment methodology described in PD 3002 [27], this is a simpler and IT specific risk assessment methodology than that suggested by GAMP in their Good Practice Guide for IT Infrastructure [29].

1. *Define Scope and Boundaries of System:* The starting point of the BS 7799 risk assessment methodology is to define what is in scope and what is out of scope. In this way the part of the system covered by the individual risk assessment is identified and localised. For example, if a risk assessment needs to be conducted before a new wireless Local Area Network (W-LAN) is implemented, then the site or specific buildings where the next W-LAN will be installed are specifically documented. Equally so, if a global Wide Area Network (WAN) is being upgraded then the WAN elements can be identified up to the site routers but the individual site LANs can be explicitly excluded.

   This phase of the work is important as the definition of what is in and what is out of the scope of the risk assessment is the basis on which all other parts of this methodology are based. Equally so, it is also important to document what has been excluded from the scope of the risk assessment.

2. *Asset Identification and Valuation:* Once the scope and boundaries of the risk assessment have been established, the information assets contained within need to be identified and listed. This is typically done by listing the applications and data contained within the boundaries identified in the previous stage.

   The list should not just be limited to regulatory systems but should also include business systems, e.g. manufacturing and distribution systems, laboratory systems, R&D systems, financial systems, and business systems and all the associated records and data. Once the list has been generated, the value of the records needs to be quantified in approximately terms. For example, if there is a problem and records or data are lost what would the loss to the organisation be? What is the value of a

production batch or the cost of repeating a clinical or non-clinical study?

3. *Threat Identification:* see step 4, as in practice this stage can be merged into a single task.

4. *Treat Identification and Vulnerability Assessment:* This is shown as two stages in Figure 9 but is considered here as a single process as it can be combined in a risk assessment workshop. The first stage is to identify the possible threats to the network and the information assets contained within the defined boundary. Then the impact of each threat needs to be identified and documented. For example, if an unauthorised user were able to access a regulated network what could that individual be able to do? Once identified, the probability or likelihood of each threat occurring should be assessed as high, medium or low.

5. *Identification of Security Controls:* Each of the threats needs to be assessed against the existing or planned controls for the network. This is a key stage and should be performed as a facilitated workshop where the threats and controls are discussed interactively. Here ideas and views can be harnessed effectively to debate the issues posed by each threat.

   The output of this phase of the assessment is a considered opinion that the controls are adequate or that further controls are required. This phase needs to be documented carefully as it is the core of the risk assessment.

6. *Risk Assessment:* Are Controls Adequate? If the controls for each threat are considered adequate then this is documented and no further work is required. However, where there is still a risk the threat moved to the next stage as further controls are required.

7. *Select Controls to Mitigate Risk:* Where the risk is unacceptable, then further technical or procedural controls are implemented.

8. *Risk Acceptance:* If the residual risk for each of the identified risks and vulnerabilities is acceptable after appropriate controls have been devised, then this is documented and the process stops here. However, if the residual risk is unacceptable then the process loops back to the identification of further controls and assesses what further ones are required.

In essence, this is the simplified BS 7799 risk management process, there is a more detailed risk assessment process described in PD 3002 [27] but there is not sufficient space to discuss this and the reader is recommended to look at this publication for more information.

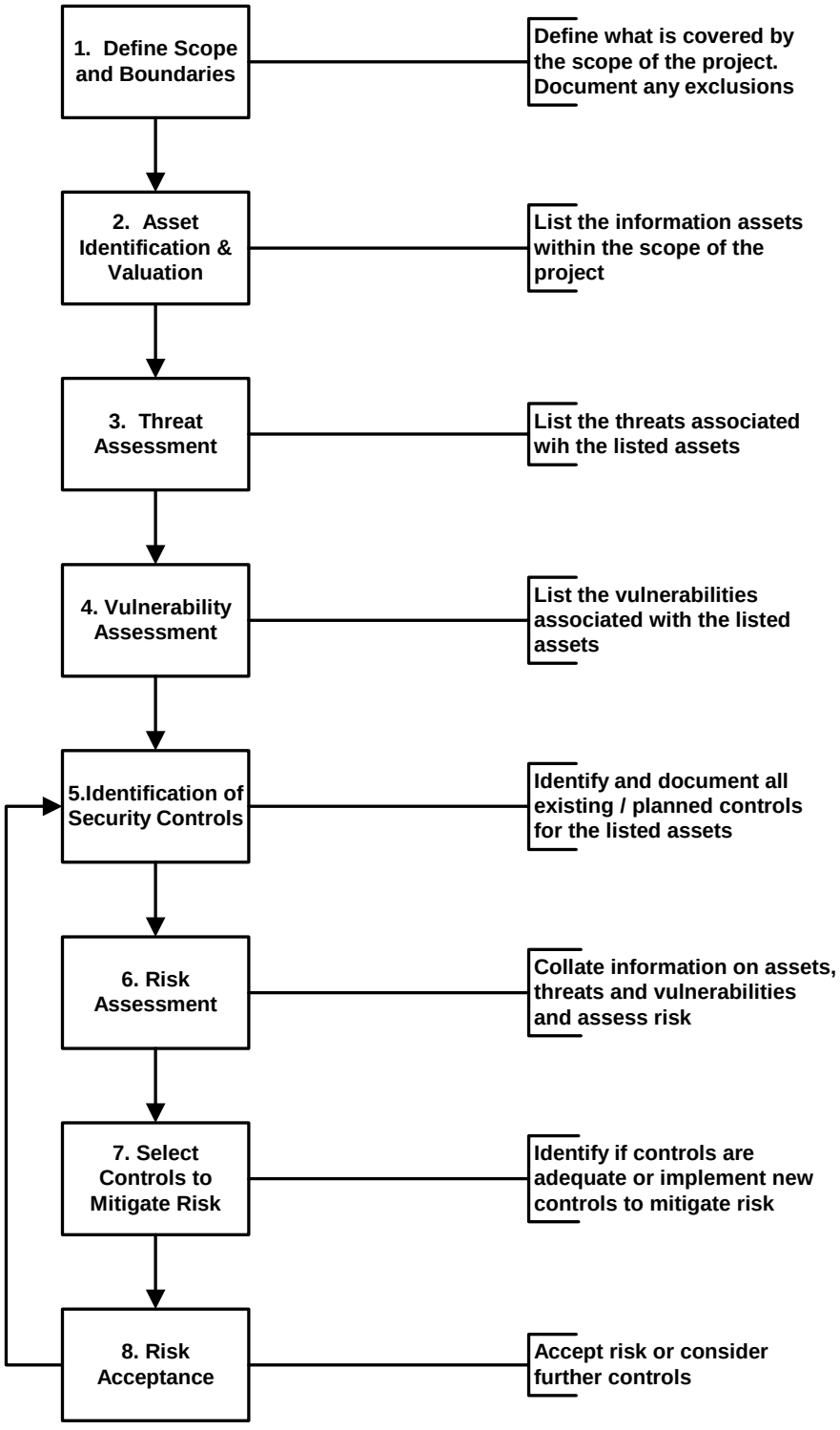

Figure 9: BS 7799 IT Risk Assessment Methodology

NIST SP800-30 Risk Management Guide for IT Systems

The NIST SP800-30 [28] risk assessment methodology is shown diagrammatically in Figure 10 and describes the process in more detail. The numbers in the text below refer to the corresponding steps in the flow chart in Figure 10.

1. *Characterise the System:* Similar to the BS7799 risk assessment methodology, the NIST approach starts by defining the scope and boundaries of an IT system including with the resources and the information that constitute the system:

   - System functions.
   - Definition of the operational boundaries.
   - Definition of the system components such as hardware, software, system connectivity etc.
   - System and data criticality (e.g. the system's value or importance to an organisation).
   - Identification of the system owner and support personnel.
   - Physical and logical security for the system.
   - Other operational controls for the system and any monitoring utilities used.

   If required, the list can be extended to include environmental controls, e.g. for computer hardware and communications equipment. However, if this is a known entity or has been the subject of a separate risk assessment, then this may be excluded but the fact is documented along with the rationale for the exclusion.

2. *Vulnerability Identification:* Next, the vulnerabilities of the defined system are identified. The goal of this step is to develop a list of these issues that could result in a security breach or a violation of the system's security.

   It is important to understand the status of the system at this stage (being designed, being implemented or operational) and apply the appropriate approach to the assessment of threats and controls as described earlier.

   Some of the recommended ways of identifying system vulnerabilities are the use of vulnerability sources (from application vendors, security sources etc.), the performance of system security testing or using a security requirements checklist that can be based on internal policies or available publicly. In addition, there may be software utilities that can be used to analyse for example the use of poor passwords for operational systems; a password cracker can be used to assess how many accounts could be compromised through the use of poor password selection.

3. *Threat Identification:* Threats can be divided into the main sources: natural, human and environmental as listed below [28].

   Natural: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

Human: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information). Some of the more common human sources are:

- Employees who are poorly trained or motivated.
- Poor internal security procedures.
- Disaffected employees.
- Criminal or industrial espionage attack.
- Hacker.

Environmental: Long-term power failure, pollution, chemicals, liquid leakage.

Note that a threat does not present a risk when there is no vulnerability of an IT system or network that can be exploited. For example, if a facility was sited in an earthquake zone such as the San Francisco bay area, then an earthquake poses a serious risk to the IT system. However, an earthquake poses no risk if a similar system was sited in a geologically stable location. Equally so, a San Francisco bay area facility has little vulnerability from avalanches.

4. *Control Analysis:* Next, the system controls that have been or will be implemented are analysed to assess how effective they are likely to be. During this step, the personnel involved in the risk assessment determine whether the security requirements designed, implemented or are operational for the IT system are being met by existing or planned security controls. Similar to 21 CFR Part 11, there are technical and procedural controls that can be implemented; and it is the combination of the two that provide the effectiveness of any system to minimise or eliminate a threat to exploit any vulnerability. The NIST risk assessment describes three levels of security controls, namely management, operational and technical security [28].

   Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement. The outcome of this process is a security requirements checklist for the system.

5. *Likelihood Determination:* To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

   - The motivation and capability of the source of the threat.
   - Nature of the vulnerability of the system.
   - Existence and effectiveness of current controls.

   Using this information the likelihood of a threat can be determined as one of three categories:

- High: The threat is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
- Medium: The threat is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- Low: The threat lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

6. *Impact Analysis:* Before starting this stage, review the information from stage 1 of the process such as system and data criticality, this puts the impact analysis into context e.g. for a low criticality and risk system versus a high one. The impact of an adverse security event can be described in terms of loss or degradation of any, or a combination of any, of the following three areas:

   - Loss of system or data integrity.
   - Loss of system availability, functionality or operational effectiveness.
   - Loss of system or data confidentiality.

7. *Risk Determination:* The impact of the risk is assessed in qualitative terms of one of the following terms:

   - Low: Limited adverse effect on organisational operations, organizational assets, or individuals. The organisation should decide if corrective actions are required or the organisation accepts the risk.
   - Medium: Serious adverse effect on organisational operations, organizational assets, or individuals. Corrective actions are needed and implemented over a reasonable period of time.
   - High: Severe or catastrophic adverse effect on organisational operations, organizational assets, or individuals. Therefore there is an imperative need for corrective actions to resolve the issue rapidly, especially if the system is operational.

8. *Control Recommendations:* Here controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

   - Effectiveness of recommended options (e.g. system compatibility).
   - Legislation and regulation.
   - Organisational policy.
   - Operational impact.
   - Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritised, and implemented. It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in section 4.6 of the NIST guide, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g. effect on system performance) and feasibility (e.g. technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

9. *Document Results:* When the risk assessment process has been completed, the results should be formally reported and approved by management, as typically there will be corrective actions.

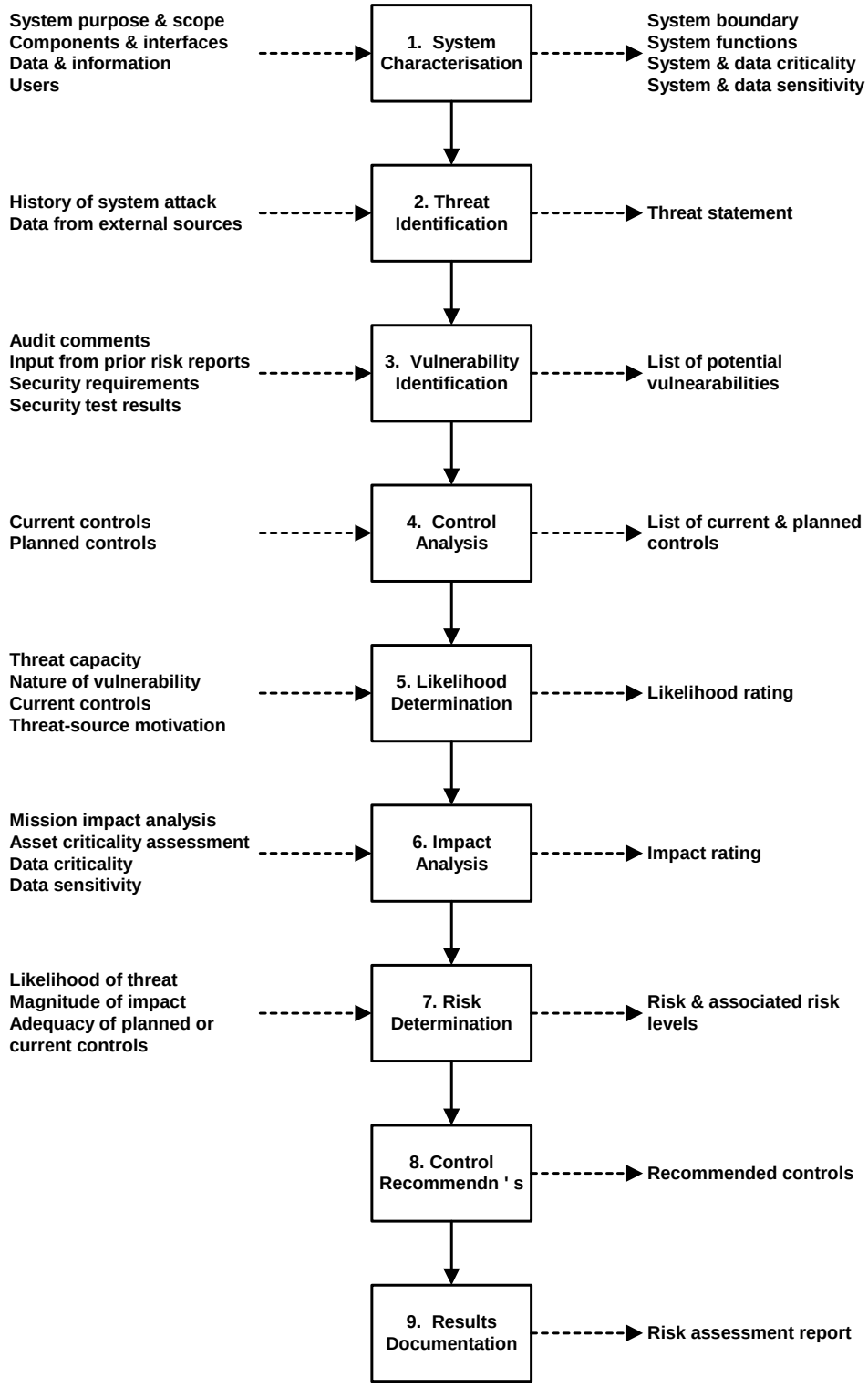

Figure 10: NIST SP800 30 Risk Assessment Flowchart
(process inputs to each stage are shown on the left and outputs on the right)

Summary of Risk Analysis Methodologies

There is no universally applicable risk analysis methodology for computer system validation as Table 2 demonstrates. Therefore, the onus is on a validation team to select the right tool for the job, using FMEA or FRA for applications and either the BS7799 or NIST SP800-30 risk assessment approaches for infrastructure or the IT elements of a specific system. Furthermore, risk assessment methodologies could be combined if required, one for the application and an IT risk assessment.

Table 2: Applicability of Different Risk Analysis Methodologies to Computer System Validation

Risk Analysis Methodology	Applicability to Computerised System Validation
HACCP	• Process based methodology for the food industry • Limited use for CSV except where there is *sufficiently comprehensive* understanding to determine the critical control points of the system
HazOp	• Developed for evaluating manufacturing process safety hazards, equipment and facilities • Limited applicability to CSV
FTA	• Structured top-down approach using gates and events • Little application to software
PHA	• Conducted at start of a project when information from similar projects available • Little application for computer system validation
FMEA & FMECA	• Well established risk analysis methodology for design or process risk analysis • Works well with complex computer systems and process equipment (Category 5) • Over complex methodology for commercially available software (Category 3 and more complex Category 4 systems)
FRA	• Developed specifically for CSV of commercially available systems (Category 3 and 4 software) • Easy to understand and apply and quick to perform • Not used for bespoke (custom) systems (Category 5)

BS 7799 (PD 3002)	• Useful for infrastructure risk analysis such as implementation of new technologies e.g. wireless LAN to mitigate potential risks • Information security management of existing or planned systems
NIST SP800-30	• Useful for infrastructure risk analysis such as implementation of new technologies e.g. wireless LAN to mitigate potential risks • Information security management of existing or planned systems

PRACTICAL APPROACHES TO RISK MANAGEMENT OF COMPUTER VALIDATION OF APPLICATIONS

After reviewing the regulatory requirements and risk management and risk analysis methodologies have been discussed and presented, we will consider a practical approach for computerised system validation in this section of the paper.

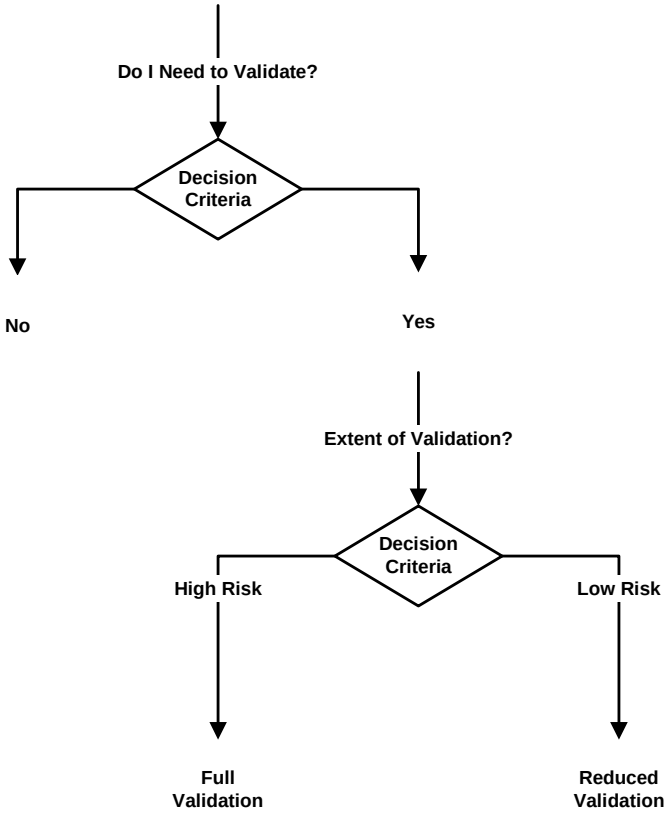

Figure 11: Process Flow to Decide if Validation is Required and What is the Extent of Work

The areas that that will be discussed in this section are discussed below and shown diagrammatically in Figure 11:

- *Do I Need to Validate My System?* This will be a discussion of the Society of Quality Assurance risk analysis questionnaire [30] from the mid 1990s. The aim is to produce a simple YES (must validate) or NO (no need to validate) response.

- *If I need to Validate the System: How Much Work is Necessary?* This needs to evaluate the use of the system and the nature of the software that is used to automate the process as the main factors in making a decision of the extent of validation based on the discussion of the regulations presented earlier in this paper. The outcome of this decision matrix is either a high risk system (full V-model validation approach) or a low risk system. The low risk system is suggested to be validated using a single integrated validation document, the rationale for which is based on the FDA's comment of *baseline validation* [8] provided it can be justified after an analysis of risk and complexity.

Balancing the Costs of Compliance and Non-Compliance

There is always a question of either 'how much must I do' or 'what is the minimum I can get away with' when it comes to validation of computer systems in a regulated environment. This can be summarised as balancing the cost of non-compliance (doing nothing and/or carrying the risk) versus the cost of compliance (doing the job right in the first place). It is important to understand the context of this in the validation of computerised systems.

Note well the cost of compliance is always cheaper than the cost of non-compliance. If any reader is in doubt I suggest that they read any of the recent consent decrees (e.g. Abbott [31] and Schering-Plough [32]). The cost of non-compliance can now be quantified in terms of hundreds of millions of US dollars for some companies.

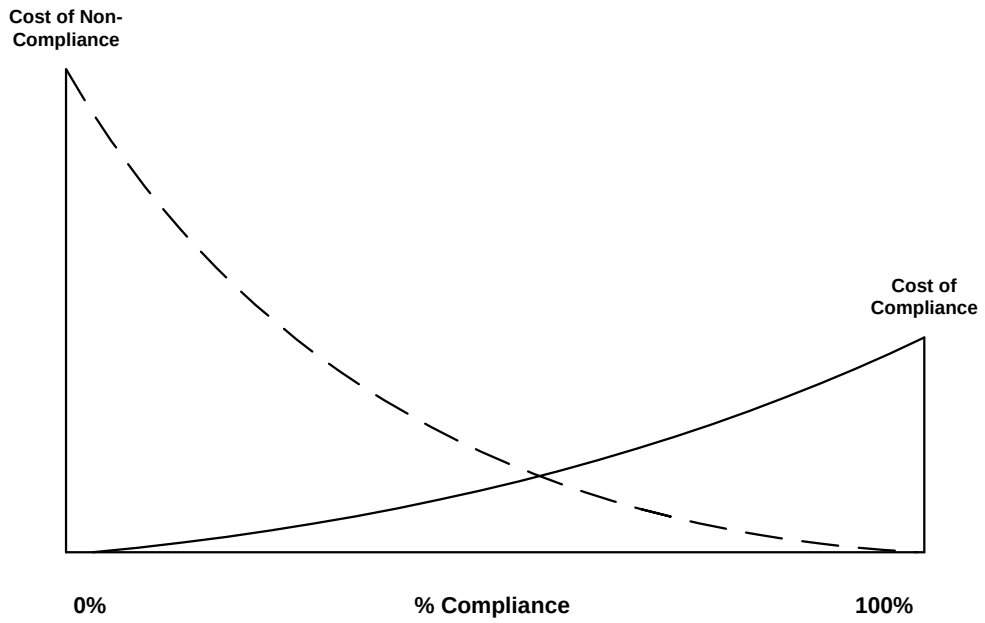

Figure 12: Balancing the Costs of Compliance and Non-Compliance [25]

Figure 12 shows the situation graphically. The vertical axes represent the cost of compliance and non-compliance respectively. Note that the cost of compliance axis is smaller than the cost of non-compliance axis this is deliberate as doing the job right first time is the best way to work. On the bottom is the extent of compliance expressed as a percentage.

If all risk is to be removed from a system then you validate as much as possible, but this would take a lot of time and resource to achieve but would for the majority of systems be difficult to justify unless there were specific reasons for this such as a critical medical device. However, if the main validation points are covered plus a commercial system is implemented then a more cost-effective validation can be accomplished in a shorter timeframe with less resource. Some risk may still exist but it is managed risk rather than regulatory exposure. This is where the term “acceptability” should be visible, the remaining risk is planned and managed and not randomly generated.

Do I Need to Validate a System?

The first question, shown in Figure 11, considers should I validate my computerised system? The key is what decision criteria should be used? To answer these questions, the Computer Validation Initiative Committee (CVIC) of the Society of Quality Assurance (SQA) developed a questionnaire to determine if a computer system should be validated or not [30]. This consists of 15 closed questions (the only answers is to the question are either YES or NO). If you answer YES to any question, then you need to validate the

system. The questions cover the whole of the regulated area of healthcare from development, submission, manufacturing and distribution.

As an example, the following questions from the CVIC document presented below are considered to a Chromatography Data System (CDS) operating in either a regulated R&D or production environment [25]:

- Does the application or system directly control, record for use, or monitor laboratory testing or clinical data?
- Does the application or system affect regulatory submission/registration?
- Does the application or system perform calculations/algorithms that will support a regulatory submission/registration?
- Is the application or system an integral part of the equipment/instrumentation/ identification used in testing, release and/or distribution of the product/samples?
- Will data from the application or system be used to support QC product release?
- Does the application or system handle data that could impact product purity, strength, efficacy, identity, status, or location?
- Does the application or system employ electronic signature capabilities and/or provide the sole record of the signature on a document subject to review by a regulatory agency?
- Is the application or system used to automate a manual QC check of data subject to review by a regulatory agency?
- Does the application or system create, update, or store data prior to transferring to an existing validated system?

If you answer YES to any question in this list, this triggers validation of the application, in this case a chromatography data system. You should undertake this assessment in an authorised document so that it is defendable in an inspection. Equally as important is documenting the NO answers that justify why you have not validated a system.

The questionnaire was written in the mid 1990's and therefore needs updating the world of the "new" 21 CFR Part 11, therefore a question that could be added to this list might be:

- Do(es) the predicate rule(s) require a record?

This allows the validation team to decide if Part 11 applies to the system as well.

For those systems where the answers to the questions are NO, the work stops with the approval of the questionnaire stating that no validation is required. However, for the systems where validation needs to be performed, a more intriguing question arises: how much validation work is necessary to manage the risk posed by the system and the records it generates?

Risk Classification: Only High and Low Risk Systems

In Figure 11 only two routes from the decision criteria are used to determine the extent of the validation work required: high and low risk systems. This is a deliberate approach based on practical issues. For example, in any classification, high and low risk systems are relatively easy to define and validate by either a V-model (full life cycle) or an integrated validation document approach respectively.

However, the practical problem lies in defining a medium risk system. Is this a low rated high risk system or a high rated low risk system? Moreover, how should a medium risk system be validated? Should a simplified V-model approach or a more detailed integration validation document approach be used for these systems? Therefore, from practical reasons, there are only two categories in this workflow.

If a system is evaluated as a high risk, the validation plan can be tailored to define exactly the tasks that will be undertaken and therefore this document provides a further mechanism to manage risk. The appropriate life cycle tasks and corresponding documented evidence to be generated can be detailed in the validation plan e.g. for an Enterprise Resource Planning (ERP) system there will be far more detail in terms of mapping the current business flows and deciding which ones are GXP relevant versus a standalone laboratory system. Both systems are high risk but the amount of work for the ERP application is far greater than for the laboratory system.

Decision Criteria for the Extent of Validation

The extent of validation required now depends on two major factors, as defined by the EU GMP Annex 11 clause 2 [5]:

1. The use of the system.
2. The nature of the software.

It is the combination of these two criteria that determines the extent of validation needed for a system as will be discussed now.

Use of the System

A system can be classified as either a high and a low risk category based on its use. Some examples of high and low risk system use are shown in Table 3, the GAMP Part 11 Good Practice Guide also lists more examples [11]. Where there are several uses of the system, the highest category ones are used for determining the risk evaluation, even if this high risk use is a minor proportion of the work performed by the system.

Table 3: Risk Assessment based on System Use

Assessment	**Potential System Uses**
High	• Data that are submitted directly to regulatory agencies or are included in regulatory submissions • Data supporting batch release (e.g. Certificate of Analysis) of drug product, clinical trial material or Active Pharmaceutical Ingredient (API) • Stability data for drug products • Data from or support to non-clinical laboratory studies • Clinical trial study data • Laboratory support to clinical studies
Low	• In- process monitoring of drug product and APIs • Supportive data not directly submitted to regulatory agencies • Pharmacology data • In vitro data • Research data • Data generated in development of analytical methods

Nature of the Software: GAMP Software Categories

The nature of the software can be defined using the software categories as defined in the GAMP guidelines [12] in Appendix M4 provide a validation strategy for different classes of software and hardware. This concept is very important as it provides a key understanding about one of the major risk factors involved in the validation of any computerised system. There are five GAMP software categories:

- **Category 1: Operating Systems (OS)**
  The strategy for the OS is to ensure that it is correctly installed and configured during the installation phase of the life cycle and then to implicitly test the OS during the Operational Qualification (OQ) and Performance Qualification (PQ) phases of the qualification. The assumption being that the correct functioning of the application infers that the OS works acceptably.

- **Category 2: Firmware**
  This class of software consists of Read Only Memory (ROM) chips that are present in the system; typically this is qualified and calibrated where appropriate and not validated. The sole exception is where the firmware is custom built and then this must be treated as Category 5.

- **Category 3: Commercial off-the-Shelf (COTS) Software**
  This is software that is commercially available and used as is from installation. The changes that are made are defining the security levels in the application, linking to printers if used on a network and any other parameters to make it work in the operating environment.

- **Category 4: Configurable COTS Software**
  This is configurable software that is commercially available and changes to the operation of the application are made with a variety of means. At its simplest the configuration is via hot buttons or switches provided by the vendor of the application (configuration or parameterisation). More complex ways of configuring the application are either to use a proprietary language that modulates the execution of the code or to configure and/or link workflows within the system.

- **Category 5: Custom or Bespoke Software**
  This is the essence of "novel elements" being software that is unique. This can range from larger systems that can be programmed in-house or outsourced to a software company to an Excel macro that uses the software package as a basis in combination with visual basic programming to generate a specific application.

Nature of the application software is defined as either high or low, in essence, the higher the GAMP category, the higher the risk to records (record vulnerability) contained within the system. The rationale is that the more unique is the software the less it is tested overall, including the experiences at customer sites.

High:
- Custom software application, or includes a custom extension, (e.g. macro) to an existing application. (GAMP category 5)
- Commercially available software package that involves configuring predefined software modules and possible developing customized modules (GAMP category 4).

Low:
- Commercially available standard non-configurable software package providing an off-the-shelf solution to a business or manufacturing process (GAMP category 3).

System Criticality Assessment

In answering the two regulatory questions of what does the system automate and the nature of the software, the overall system risk can be assessed and hence the extent of validation required can be determined. Similarly, to the Functional Risk Assessment, the answers from the two questions are plotted in a 2 x 2 Boston Grid shown in Figure 13. Only systems with the combination of high regulatory risk and high record vulnerability (top right quadrant of the grid) that results in the highest assessment will require full validation. Systems falling in the other three quadrants will require low risk validation.

The combination of these two assessments can result in different approaches to validation for the same system, the only difference being the system use. A chromatography data system used for low risk analysis such as in process analysis only could be validated using the reduced approach whilst the same system used for release testing of APIs and final product undergo full validation.

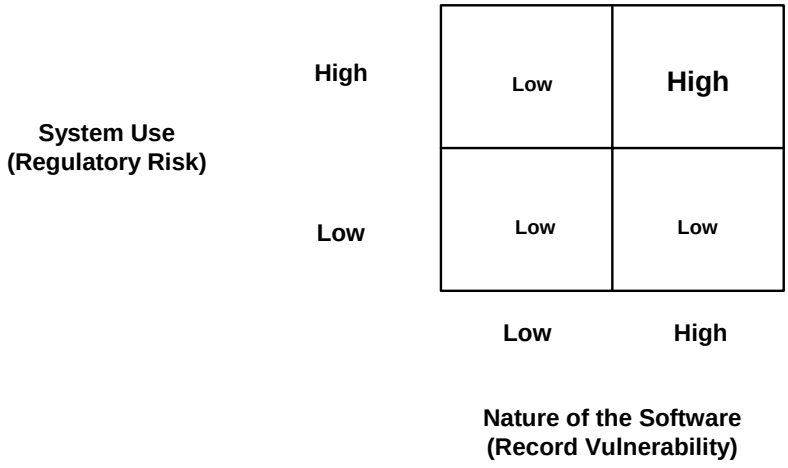

Figure 13: Boston Grid of System Use and Nature of the Software

High Risk Systems

Systems falling in the high risk category, should use a V-model validation that requires the use of a risk analysis methodology within the ISO 14971 risk management framework. Rather than a single risk assessment methodology to fit all situations as suggested by the GAMP Forum [12, 29, 33], a more practical approach of selecting the right methodology for the right system is advocated by the author. Although the GAMP documents suggest this approach and state that other approaches are acceptable, many organisations implement a GAMP risk assessment “one size fits all” approach.

The following approach is suggested:

- Complex and custom built systems should use Failure Mode Effect Analysis (FMEA) [12].
- Commercial off-the-Shelf (COTS) and Configurable COTS software should use Functional Risk Assessment [25, 26].
- If required, both of the above risk assessments could use either of the IT risk assessments to evaluate exposure to IT vulnerabilities.

The overall approach to be used for risk assessment should be documented in the validation plan for the system along with the defined life cycle elements and anticipated documented evidence.

Low Risk Systems

The approach for low risk systems is a validation that uses a single integrated document that defines the intended purpose of the system along with any applicable predicate rule and 21 CFR Part 11 requirements. It also tests these requirements in test procedures within the same document.

Control of low risk validation is documented either in a specific SOP or in a Validation Master Plan (VMP) as defined by European Union GMP Annex 15 [5]; although the latter is the personal preference of the author.

Integrated Validation Document

The integrated validation document (Validation Lite approach) takes the key elements of the system development life cycle and condenses them into a single document. The specification of the intended use and testing sections are clearly separated within this document and pre-approved before use. As stated above, the overall control for the validation is covered in a VMP or SOP.

The main sections of the integrated validation document are:

- Introduction including and system use.
- System description.
- Referenced documents: included here are the system specific documents including approaches such as calibration, maintenance and daily control measures to ensure that the system works as intended. Where there are vendor IQ and OQ documents these are included to demonstrate that the system has been
- Definition of user requirements: only requirements that define the intended purpose of system are documented here. Each requirement must be written so that it can be tested or verified. Typically the requirements are grouped e.g. system functions, security and access control, definition and protection of electronic records, audit trail etc.
- Test preparation.
- Procedures to test user requirements, to collate documented evidence and to compare results versus acceptance criteria; there is also a section on the assumptions, exclusions and limitations of the testing approach.

- Test execution notes.
- Test summary report.
- System sign off and release for use.

The intended use and test procedures are written, reviewed and updated and then the whole document is approved before execution of testing. Requirements traceability is also included in the document as instead of a prioritisation, there is a pointer to the test procedure where it is tested. After testing and collation of the documented evidence, the document's final section is a summary report and release section for operational use.

Example of a Low Risk System Validation

As an example of this approach, a time of flight (TOF) mass spectrometer (MS) is used as a standalone system in an analytical laboratory. The instrument is used for elemental analysis to support:

- Impurity identification for process chemistry for active pharmaceutical ingredients.
- Identification of unknown and known compounds.
- The system creates and stores electronic records.

Therefore, the answer to the first question 'do I need to validate the system' is YES. Now the question is 'how much should be done?'

From the regulatory risk perspective, the data from the instrument are used in Investigational New Drug (IND) and New Drug Application (NDA) submissions, thus the assessment is high. However, the software is used for the instrument is GAMP category 3 which is low. Plotting both criteria in the Boston Grid in Figure 13, the system risk rating is low and hence a reduced validation is performed.

When collecting information about the system to prepare the integrated validation document, do not forget to assess what regular maintenance and calibration is performed. Often laboratory systems can be calibrated or checked (e.g. by performing a system suitability test) on a daily basis before any analysis is performed and this can be used to justify and support some of the approaches to testing. The key aim is to ensure integrity of data generated and maintained by the system and backup of records should always be included in the requirements and test suite.

CONCLUSIONS

This paper reviews the regulations for computerised systems and discusses some of the practical options available for risk management and risk assessment for computerised system validation (CSV). There is not a single risk assessment methodology for computerised system validation that is applicable to all systems in all situations.

Therefore the best, most prudent and cost-effective approach is to select the appropriate methodology for the computerised system rather than adopt a one size fits all approach.

In advocating this approach, the philosophy of Albert Einstein is adopted: keep it as simple as possible – but no simpler. In essence, use the right tool for the right job. Therefore the following approach to risk assessment and risk management is advocated:

- Highly configured and customised (bespoke) systems should use Failure Mode Effect Analysis (FMEA) as the best risk analysis methodology for CSV.

- Commercial off-the-shelf (COTS) or configurable COTS applications should use a simplified risk analysis methodology, Functional Risk Analysis (FRA) to build on the testing that the vendor has performed.

- IT security and infrastructure should use either the BS 7799 or NIST SP800-30 risk assessment methodologies. Either of these methodologies can be used either in isolation or in combination with risk assessment of the application itself.

ACKNOWLEDGEMENT

The author would like to thank Sion Wyn for his comments on the draft manuscript.

REFERENCES

[1] U.S.Food and Drug Administration, *Pharmaceutical cGMPs for the 21st Century: A Risk-Based Approach*, **2002**.

[2] U.S.Food and Drug Administration, *Guidance for Industry: 21 CFR Part 11; Electronic Records; Electronic Signatures Part 11 Scope and Application*, **2003**.

[3] International Standards Organisation, *ISO Standard 14971 - Medical Devices - Application of Risk Management to Medical Devices*, International Standards Organisation, Geneva, **2000**.

[4] U.S.Food and Drug Administration, *Federal Register* **1997**, *62*, 13430.

[5] Medicines Control Agency, *Rules and Guidance for Pharmaceutical Manufacturers and Distributors 2002*, 6th ed., The Stationary Office, London, **2002**.

[6] International Conference on Harmonisation (ICH), *ICH Q7A - Good Manufacturing Practice for Active Pharmaceutical Ingredients (CPMP/ICH/4106/00)*, **2000**.

[7] U.S.Food and Drug Administration, *Federal Register* **1996**, *61*, 52601.

[8] U.S.Food and Drug Administration, *Guidance for Industry: General Principles of Software Validation*, **2002**.

[9] Pharmaceutical Inspection Convention / Scheme (PIC/S), *Good Practices for Computerised Systems in "GXP" Environments*, PIC/S, Geneva, **2003**.

[10] International Conference on Harmonisation (ICH), *ICH Q9 (Step 2) Quality Risk Management*, Geneva, **2005**.

[11] GAMP Forum, *A Risk-Based Approach to Compliant Electronic Records and Signatures*, International Society for Pharmaceutical Engineering, Tampa, FL, **2005**.

[12] GAMP Forum, *Good Automated Manufacturing Practice (GAMP) Guide Version 4*, International Society for Pharmaceutical Engineering, Tampa, FL, **2001**.

[13] GAMP Forum, *Good Practice and Compliance for Electronic Records and Signatures, Part 2 - Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures*, International Society of Pharmaceutical Engineering, Tampa, FL, **2001**.

[14] International Standards Organisation, *Risk Management - Vocabulary - Guidelines for use in standards*, International Standards Organisation, Geneva, **2002**.

[15] International Standards Organisation, *Risk Management - Vocabulary - Guidelines for use in standards (ISO/IEC Guide 72: 2002)*, **2002**.

[16] Institute of Electronic and Electrical Engineers, in *Software Engineering Standards*, IEEE, Piscataway, NJ, **2001**.

[17] D. H. Stamatis, *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, Second Edition ed., ASQ Press, Milwaukee, WI, **2003**.

[18] M. Ammerman, *The Root Cause Analysis Handbook - A Simplified Approach to Identifying, Correcting and Reporting Workplace Errors*, Productivity Press, New York, NY, **1998**.

[19] U.S. Food and Drug Administration, *Hazard Analysis and Critical Control Point Principles and Application Guidelines*, **1997**.

[20] Dyadem Engineering Corporation, *Guidelines for Failure Modes & Effects Analysis for Medical devices*, CRC Press, Boca Raton, FL, **2003**.

[21] U.S. Department of Defense, *Military Standard (MIL-STD-1629a) Procedures for performing a failure mode, effects and criticality analysis*, U.S. Department of Defense, Washington, DC, **1980**.

[22] Society of Automotive Engineers, *Failure Mode Effect Analysis*, Society of Automotive Engineers, **1993**.

[23] R. E. M. McDermott, R J and Beauregard, M R, *The Basics of FMEA*, Productivity Press, New York, NY, **1996**.

[24] R. D. McDowall, in *Computer Systems Validation: Quality Assurance, Risk Management and Regulatory Compliance for Pharmaceutical and Healthcase Companies* (Ed.: G. Wingate), Interpharm / CRC, Boca Raton, FL, **2004**, pp. 465.

[25] R. D. McDowall, *Validation of Chromatography Data Systems*, Royal Society of Chemistry, Cambridge, **2005**.

[26] R. D. McDowall, in *Computer Systems Validation: Quality Assurance, Risk Management and Regulatory Compliance for Pharmaceutical and Healthcare*

Companies (Ed.: Guy Wingate), Interpharm / CRC, Boca Raton, FL, **2004**, pp. 465.

[27] British Standards Institute, *Guide to BS 7799 Risk Assessment (PD 3002 - 2002)*, British Standards Institute, London, **2002**.

[28] National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems (Special Publication 800-30)*, NIST, Gaithersburg, MD, **2002**.

[29] GAMP Forum, *Good Practice Guide - IT Infrastructure Control and Compliance*, International Society for Pharmaceutical Engineering, Tampa, FL, **2005**.

[30] Society of Quality Assurance, *Computer Validation Initiative Committee (CVIC), Risk Assessment/Validation Priority Setting*.

[31] US District Court for Illinois, *Abbott Consent Decree of Permanent Injunction*, Chicago, Illinois, **1999**.

[32] US District Court of New Jersey, *Schering Plough Consent Decree of Permanent Injunction*, **2002**.

[33] GAMP Forum, *Best Practice Guide - Laboratory Systems*, International Society for Pharmaceutical Engineering, Tampa, FL, **2005**.

USEFUL WEB SITES FOR RISK MANAGEMENT

General Sites for Risk Management

- FDA: http://www.fda.gov
- 21 CFR Part 11 web site dealing with all aspects of Part 11 including risk management specifically there is a good library and a list server for questions: http://www.21cfrpart11.com
- International Conference on Harmonisation (ICH), Q9 quality risk management document: http://www.ich.org

HACCP

- FDA site for HACCP covering resources and information for food: http://www.cfsan.fda.gov/~lrd/haccp.html
- US Department of Agriculture and FDA resource and training site with links to other HACCP resources: http://www.nal.usda.gov/fnic/foodborne/haccp/index.shtml

Fault Tree Analysis (FTA)

- Institute of Electrical Engineers overview of FTA and also FMEA: http://www.iee.org/Policy/Areas/Health/hsb26c.cfm
- Sandia National Laboratories, Centre for System Reliability: http://reliability.sandia.gov/Reliability/Fault_Tree_Analysis/fault_tree_analysis.html

Failure Mode Effect Analysis (FMEA)

- GAMP Forum for availability of advice documents and Good Practice Guides: http://www.ispe.org/gamp/
- FDA, CDRH, Design Guidance for Medical Devices – guidance from 1997: http://www.fda.gov/cdrh/comp/designgd.pdf

Functional Risk Analysis

- Bob McDowall's web site for general CSV education and articles can be downloaded from the library: http://www.rdmcdowall.com

BS 7799 Risk Assessment

- British Standards Institute (BSI) web pages for purchase of PD3002: http://www.bsi-global.com/ICT/Security/pd3002.xalter

NIST SP 800-30 Risk Assessment

- National Institute of Science and Technology (NIST) Computer Security Resource Centre for download of SP 800 series publications: http://csrc.nist.gov/publications/nistpubs/index.html