Improving Software Risk Management in a Medical Device Company

Fergal Mc Caffery
Dundalk Institute of Technology
& Member of Lero
Fergal.McCaffery@dkit.ie

John Burton
Vitalograph Ltd.
John.Burton@vitalograph.ie

Ita Richardson
Lero – the Irish Software Engineering Research Centre
University of Limerick
Ita.Richardson@ul.ie

Abstract

Software Risk Management (RM) within Medical Device (MD) companies is a critical area. Failure of the software can have potentially catastrophic effects, leading to injury of patients or even death. Therefore regulators penalise MD manufacturers that do not devote sufficient attention to the areas of hazard analysis and RM throughout the software lifecycle.

This paper describes the experience of a MD software development organization when they engaged in a research project to improve their RM practices. We explain how this was achieved through the development of a software process improvement RM model that integrates regulatory MD RM requirements with the goals and practices of the Capability Maturity Model Integration (CMMI). This model is known as the Risk Management Capability Model (RMCM). The authors describe the complete project lifecycle and evaluate the success of the project.

1. Context

RM is a very necessary aspect of all software development projects. The absence of RM within software projects can lead to failures and loss at several levels. Barry Boehm has defined the degree to which a software project may be exposed to failure i.e. risk exposure, as the probability of an unsatisfactory outcome and the loss to the parties affected if the outcome is unsatisfactory [6]. Two key terms from this definition are "unsatisfactory outcome" and "loss". However, RM is industry-specific. Within the MD industry, RM aims to manage software risk from a safety perspective. The MD industry and its associated regulators view "unsatisfactory outcome" and "loss" in terms of loss of life, injury or damage to the operator, subject, bystander or environment. Therefore, software quality in the MD sector is defined and measured against these criteria.

MD companies are responsible for ensuring they take adequate precautions to produce safe and efficient software that does not pose a severe hazard should a software-related failure occur. An issue facing MD companies producing software is that it is not practical, even in the simplest software programs, to fully test all possible execution paths. Therefore, the quality of software cannot be determined by software testing alone. A simple change in a software component can cause unforeseen problems in other components within

the system, which could go undetected unless a robust RM, software design and implementation process exists. Safe MD software depends on solid software engineering practices [12] with RM being a core practice.

Although MDs and associated software are developed to increase the well-being of patients, the MD industry and governments are faced with the challenge that MDs fail to operate properly on occasion, or are misused in ways that are associated with injuries and death. According to the Institute of Medicine report "To Err is Human", between 44,000 to 98,000 people die throughout the world in hospital from preventative medical errors [22]. The report also says that more people die every year in the USA as a result of medical errors than from motor vehicle accidents, breast cancer or AIDS. Another challenge facing both the MD industry and global governments include the illegal sale of sub-standard devices which fail to meet minimum quality and safety standards, therefore putting further lives at risk.

To tackle the issue, governments have put in place regulatory bodies whose job it is to define regulatory systems for MDs. The goal is to protect the public from faulty software which may be placed into MDs and thus reduce the risk of potential injury [13]. MD companies wishing to market in those countries must prove compliance with the regulatory system.

Typically, before a MD company can sell their product in a country, they must follow the registration or licensing procedure of that country. This in turn establishes a contract between the device manufacturer and that country, whereby the device manufacturer is obligated to perform both pre-market and post-market duties as defined in the quality system requirements. The quality system is defined as the organisational structure, responsibilities, procedures, processes and resources required to implement quality management. It may cover the methods, facilities and controls used by the manufacturer in design, manufacturer, packaging, labelling, storage, installation, servicing and post-market handling of MDs. Applicable requirements are typically directly related to the class of the device. However hazard analysis and RM are key components that are applicable to all classes of device. The regulatory or approved body, through audits, checks conformance to the quality system requirements periodically. By conforming to the quality system requirements, the device manufacturer is being pro-active and demonstrates a tightly controlled manufacturing system, which in turn provides for greater reliability, safety and effectiveness in the device.

In the US, all MDs containing software are subject to the United States Quality Systems Regulation, 21 CFR 820 [14]. The regulations stipulate the requirement for risk analysis as part of the design validation process. Because there is little guidance in Europe on the information that should be included in a MD Technical File for CE-marking, many companies use relevant US guidance documents [11]. As such, this research integrates guidance by the US regulatory agencies.

2. What was the goal?

The aim of this project was to improve the software RM process within an Irish MD organization i.e. Vitalograph Ltd. This is a privately owned company that was established in the 1960's. The company manufacturers devices that are used in the diagnosis and monitoring of vital physiological processes. The electronic devices, which the company produces fall into several categories including: hand-held personal devices containing embedded software; larger office based devices containing embedded software which include the capability to interact with PC based software; pure electronic/mechanical devices that do not themselves contain software.

Vitalograph's primary markets include clinical trials, primary care, occupational health, sports medicine, asthma management, emergency services and hospitals. Their products are represented in 113 countries throughout the world through local distributors. Its headquarters are located in the U.K. and additional offices are located in the U.S.A. and Germany. These offices support the sales, training and service teams. The manufacturing and research and development (R&D) facilities are based in Ireland.

Following initial discussions with the General Manager of Vitalograph Ireland, it was agreed that the research would focus on improving the company's software RM framework, as it was believed their existing RM framework required re-aligning with the latest regulatory standards and guidance. Our aim was to create a RM framework which when followed, would ensure that any software developed by the company, adhering to the framework, would be compliant with respect to regulatory RM requirements.

The desired future state for the organisation was to have in place a more comprehensive and reusable software hazard analysis and RM procedure with associated templates, which could be used in the production of MD software including both embedded and desktop software applications. The procedures

should be in full compliance with the RM requirements set forth by the FDA for marketing in the USA and BSI for marketing in Europe. It was expected that this would lead to safer and more efficient software design and device development. It was desirable that the resulting RM framework be comprehensive enough to satisfy regulatory requirements of other regulatory bodies in the future. Therefore, the focus and content of the resulting framework could not be restricted to just FDA and BSI guidance documents.

3. Approach used to achieve the goal

The research question we are investigating is: "Can the RMCM assist MD companies in improving their software RM practices and put them on the path to regulatory compliance?" To answer this question we trialed the RMCM in Vitalograph Ltd., an Irish MD company that produces both embedded and desktop application software for their devices. A five phase cyclical action research approach [5, 24], involving diagnosing, action planning, action taking, evaluating and specifying learning was used to perform this research. As action research normally includes multiple cycles it was ideally suited to this research project. Additionally, it was also suited to this project as one of the researchers was an employee of Vitalograph, in the role of Principal Engineer of Application Software, Quality Assurance and Customised software. This experience report discusses cycle 1 and the proposed modifications for cycle 2 of the research project.

4. Establishing the research environment *(Diagnosing)*

The research commenced with the establishment of the research environment. This was agreed to be the R&D department of Vitalograph. The boundaries of the research area were defined to be software RM.

The diagnosing stage commenced with discussions with the client on existing issues within the software development environment, focusing specifically on process and procedures. Vitalograph is bound legally by the regulatory bodies of the countries in which it markets. The two primary regulatory bodies of concern for the organization include the British Standards Institution (BSI) who regulate European sales and the FDA in the USA. The regulatory bodies regularly review the organisation's process and procedures, through audits, to ensure the organisation is compliant with the regulations set out by the bodies. To this end, the organisation has a solid base of documented process and procedures encapsulated in development handbooks, standard operating procedures and templates.

As an employee of the organization, one of the researchers was trained on existing procedures, including the hazard analysis and RM procedure. Access was also provided to all of the company's standard operating procedures and the templates used in the design and development of new software products. The researcher also had the capacity to update the organisation's software related procedures, which when modified and released back into the organisation, have a direct and immediate impact on all new software developed. This is because any new software developed must adhere to the latest procedures, which have been released into the quality system.

5. Development of the proposed solution *(Action Planning)*

In response to research problem, the researchers developed the RMCM. The RMCM was developed to assist Vitalograph in meeting the MD regulations for RM through adopting disciplined software engineering practices. The model has been designed to be flexible in that relevant elements of the model may be adopted as required to provide the most significant benefit to the business. The model is based on the CMMI® [9] and the regulations used to extend the CMMI® framework are those of the FDA [15,16,17,18], ISO 14971 [3], ANSI/AAMI/IEC 62304:2006 standard (IEC 62304) (MD software – Software life cycle processes) [4] and EN 60601-1-4 [7]. Additionally, reference was made to IEC 60812 [19], GAMP 4 [20], GAMP 5 [21], TIR 32 [2] and guidance from the AAMI (Association for the Advancement of Medical Instrumentation) on RM [1]. The RMCM contains an assessment method that provides a means of assessing the software engineering capability for the RM process area in relation to MD software (both application and embedded software).

The RMCM is a foundation upon which to promote software practices into the RM process adopted by MD companies. This is expected to improve the effectiveness and efficiency of RM within MD companies through mapping MD regulatory guidelines against the CMMI® RM process area. The mappings between the MD regulatory guidelines and the CMMI® specific practices for the RM process result in the RMCM being composed of a number of goals and practices. Goals and practices may be either generic (relating to the entire organisation) or specific (relating

directly to the RM process). The RMCM determines what parts of the CMMI® RM process area (part A of Figure 1) are required to satisfy MD regulations (part B of Figure 1).

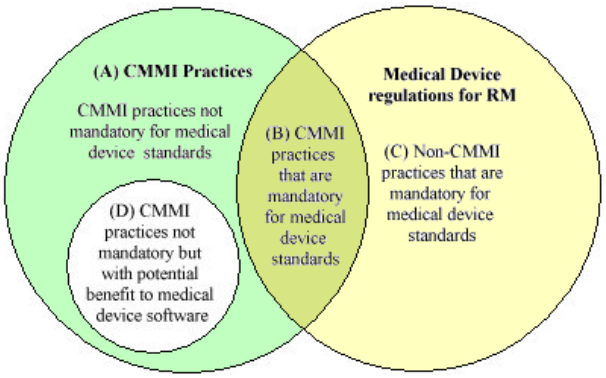

Figure 1. Composition of the RMCM

The RMCM also investigates the possibility of extending the CMMI® process areas with additional practices that are outside the remit of CMMI®, but are required in order to satisfy MD regulatory guidelines (part C of Figure 1). Additionally, the RMCM provides MD companies with the opportunity to incorporate practices from the CMMI® that are not required in order to achieve regulatory compliance but that would greatly enhance their RM process if they were included (part D of Figure 1). The RMCM will help companies to measure their organisational RM capability and to track their progression against the following software process capability levels (see Table 1):

RMCM Level Med – Companies must demonstrate that they satisfy the goals and perform the practices required to meet the requirements of the various MD regulatory guidelines and standards associated with RM. This will involve performing some practices which the CMMI® views as generic, although not to the extent of fulfilling any generic goals.

RMCM Level 0 – Insufficient practices have been performed to satisfy the requirements of Level Med.

RMCM Level 1 - Companies must demonstrate that they satisfy RMCM level Med and the CMMI® capability level 1 goal of performing the CMMI® RM base practices.

RMCM Level 2 – Companies must demonstrate that they satisfy RMCM level 1 and additionally perform CMMI® RM Advanced Practices, as well as the CMMI® capability level 2 generic goal of institutionalising a Managed Process.

RMCM Level 3 - Companies must demonstrate that they satisfy RMCM level 2 and additionally the CMMI® Generic Goal to Institutionalise a Defined Process (CMMI® Generic Goal 3) for the RM process area.

RMCM Level 4 – Companies must demonstrate that they satisfy RMCM level 3 and additionally the CMMI® Generic Goal to Institutionalise a Quantitatively Managed Process (CMMI® Generic Goal 4) for the RM process area.

RMCM Level 5 - **Companies must demonstrate that a process area satisfies RMCM level 4 and additionally the CMMI® Generic Goal to Institutionalise an Optimising Process (CMMI® Generic Goal 5) for the RM process area.**

The RMCM is composed of 5 Generic Goals (GGs). The first of these GGs requests that three specific goals (SG): (**SG1: Preparing for RM**, **SG2: Identify and Analyse Risks** & **SG3: Mitigate Risks**) are satisfied. Each specific goal is composed of a number of practices and sub-practices, with each practice consisting of a number of sub-practices. For example, **SG1. Preparing for RM** consists of 3 practices: *Determine risk sources and categories*, *Determine risk parameters*, and *Establish a RM strategy*.

Table 1, illustrates how the *Determine risk sources and categories* sub-practice consists of 5 sub-practices and each sub-practice is assigned an RMCM capability level. Practices that are indicated in ***bold italics*** were not included in the CMMI RM process area and had to be added to provide coverage of the MD regulations.

Table 1: RMCM Sub-practices for determining risk sources and categories

Practice: Determine Risk Sources and Categories		
Sub-Practice Number	**Sub-Practice**	**RMCM Level**
1	Determine risk sources	Med
2	Determine risk categories	Med
3	***Determine software hazards***	***Med***
4	***Include failure in the OTS software as a potential hazard***	***Med***
5	***Include hardware failures as a potential hazard***	***Med***

Table 2 summarises the RMCM, illustrating the RMCM capability levels for sub-practices belonging to a particular practice. To achieve a determined capability level for any of the RMCM goals, it is necessary for the associated practices and sub-practices

(with an assigned capability level less than or equal to the desired capability level) to be performed (Detailed in [8, 23]). The generic goals GG2-GG5 are not broken down to the sub-practice level. Therefore, the capability level is assigned at the practice level within these goals.

The RMCM contains 59 sub-practices, with level Med containing 41 of these sub-practices. Only 21 of the 39 CMMI® RM sub-practices are included in the RMCM level Med. Therefore, following the MD regulations will only partially meet the goals of this CMMI® process area, with only specific goal 1 being fully satisfied. The RMCM also shows that 35 specific sub-practices have to be performed in order to satisfy MD regulations and that only an additional 8 sub-practices are required to satisfy all the CMMI® level 1 (or RMCM level 1) requirements.

Meeting the goals of the RM process area by performing the CMMI® specific practices would not meet the requirements of the MD software regulations as an additional 20 MD specific sub-practices had to be added to meet the objectives of RMCM.

Table 2: Summary of the RMCM

Goal: GG1: Perform the Specific Practices					
GP 1.1 Perform Base Practices					
			RMCM Level s Med, 1, 2, 3, 4, 5		
				RMCM Level Med	
Specific Goal	**Specific Practice**	**RMCM Sub-Practice Numbers**	**CMMI® based Sub-practices**	**CMMI® Sub-practices required to meet regulatory requirements**	**Additional Sub-practices required for regulatory req's**
SG 1: Preparing for RM	Determine Risk Sources and Categories	1 to 5	2	2	3
	Define Risk Parameters	6 to 8	3	3	0
	Establish a RM Strategy	9 to 16	1	1	7
SG 2: Identifying and Analysing Risks	Identify risks	17 to 25	6	1	3
	Evaluate, categorise, and prioritise risks	26 to 29	3	3	1
SG 3: Mitigate Risks	Develop Risk Mitigation Plans	30 to 38	3	1	6
	Implement Risk Mitigation Plans	39 to 43	5	4	0
Specific Goal Totals			**23**	**15**	**20**
Goal: GG2: Institutionalise a Managed Process					
GP 2.1 Establish Policy		44	1	1	0
GP 2.2 Plan the process		45	1	1	0
GP 2.3 Provide Resources		46	1	1	0
GP 2.4 Assign Responsibility		47	1	1	0
GP 2.5 Train People		48	1	1	0
GP 2.6 Manage Configurations		49	1	0 (Level 2)	0
GP 2.7 Identify stakeholders		50	1	1	0
GP 2.8 Monitor& Control the Process		51	1	0 (Level 2)	0
GP 2.9 Evaluate Adherence		52	1	0 (Level 2)	0
GP 2.10 Review		53	1	0 (Level 2)	0
Goal: GG3: Institutionalise a Defined Process					
GP 3.1 Establish a defined Process		54	1	0 (Level 3)	0
GP 3.2 Collect Improvement Information		55	1	0 (Level 3)	0
Goal: GG4: Institutionalise a Quantitatively Managed Process					
GP 4.1 Establish Quantitative Objectives for the Process		56	1	0 (Level 4)	0
GP 4.2 Stabilise Sub-process Performance		57	1	0 (Level 4)	0
Goal: GG5: Institutionalise an Optimising Process					
GP 5.1 Ensure Continuous Process Improvement		58	1	0 (Level 5)	0
GP 5.2 Correct Root Causes of Problems		59	1	0 (Level 5)	0
Totals			**39**	**21**	**20**
Total Number of RMCM Level MED Sub-practices				**41**	
Total Number of RMCM Sub-practices				**59**	

6. Gap Analysis using the proposed solution *(Action Taking - Part I)*

The RMCM was used to perform a gap analysis in determining which practices were missing or not adequately addressed in the MD company's software RM procedure. The RMCM provided the researcher with a solid tool for examining the MD company's existing RM framework. Using the RMCM, the researcher could perform a gap analysis on what already existed in the MD company versus what was required to satisfy regulatory requirements. Each specific goal and its associated sub-practices within the RMCM were examined and compared against the

organisations existing practices. Specific goals and sub-practices, which were required but not addressed in the organisation's standard operating procedures and templates, were noted so that they could be addressed. Note that the researcher's focus was solely on those goals and practices at level Med. This was the level of maturity required by the Vitalograph. Therefore, the remaining tables listed in this paper show only those practices related to level Med.

In evaluating the RMCM and its impact upon the company's RM practices, the authors initially analysed the company's standard operating procedures and associated design templates (DTs) for performing software RM. Analysis was performed to determine the state of the company's software RM procedures prior to the implementation of the RMCM. The analysis involved examining each goal and associated practices within the RMCM, identifying what was required to meet the goals of the RMCM and then determining if that goal had been satisfied through the company's existing standard operating procedures and DTs or other records such as training logs.

The analysis showed that prior to the introduction of the RMCM, 9 out of the 35 required base practices (i.e. level Med practices for SG1 to SG3) were adequately addressed by the company's standard operating procedures and DTs. Twenty-six were found to be missing and 1 was insufficient as it only partially met the requirement laid out by the RMCM for the practice. The findings are summarised in table 3.

Table 3. Gap analysis findings

Goal	Activities required by regulation	Activities satisfied by company procedures
SG 1: Prepare for RM	16	3
SG 2: Identify and Analyse Risks	8	3 (plus an additional 1 incomplete)
SG 3: Mitigate Risks	11	3
GG2: Institutionalise a Managed Process	6	6
GG3: Institutionalise a Defined Process	0	0
GG4: Institutionalise a Quantitatively Managed Process	0	0
GG5: Institutionalise an Optimising Process	0	0
Total	**41**	**15**

What is interesting about the initial analysis is that all 6 of the practices required to satisfy level Med for Generic Goal 2 of the RMCM had been met by the MD company. However, establishing the policy, planning the process, providing resources, assigning responsibility, training people and identifying stakeholders can be seen to be ineffective if the base practices (i.e. SG1 –SG3) themselves are insufficient in terms of the practices it addresses.

7. How the company's RM practices were changed *(Action Taking - Part II)*

With the gap analysis findings at hand, the researchers commenced the development of a new RM framework for Vitalograph. This entailed a significant re-write of the client's RM standard operating procedure and template, as well as integration of the RM process into the top-level software development procedure.

A new software RM procedure was created to address missing and inadequate practices as identified through the RMCM gap analysis. The procedure was released into the company's quality management system and implemented in MD software projects. This is referred to as cycle 1 of the action research cycle.

The RMCM was implemented within a MD company over a period of two years covering 5 software projects consisting of 2 embedded software projects and 3 desktop software projects. The next section reports the evaluation of the RMCM for cycle 1 of the action research project and the effect it has had thus far on the company's software RM activities. Suggestions are made for modifications to both the RMCM and the company's implementation of the RMCM practices for a further cycle in this research.

8. What happened when the new solution was implemented *(Evaluation)*

The updated revision of the company's software RM procedure was analysed with respect to the required RMCM level Med practices by repeating the gap analysis process described above. We found that all required level Med practices listed in the RMCM were addressed by the latest revision of the company's software RM procedure. This was no surprise given that the RMCM was central in determining what practices were missing or inadequate and should be addressed within the subsequent revision.

The RMCM has had a positive effect on the MD company (e.g. Table 4, illustrates the effect of the changes that were made in relation to the practice of *Determining risk sources and categories*). It has provided them with a single reference point for determining their capability with respect to the required RM practices, enabling them to quickly

identify what practices were missing or inadequate with respect to MD regulations. It has provided them with a source to refer to when addressing the missing practices deemed essential by the MD regulators in achieving safe and efficient software.

Table 4. Post-RMCM implementation findings

RMCM Sub-Practice	Change	Effect of Change
1	Updated software RM procedure and template with a requirement to identify risk sources.	More comprehensive analysis of potential risk sources. Sources are identified and tabulated within client's RM documents.
2	Updated software RM procedure and template with requirement to categorise risk sources.	Better categorisation of risks. Risks can now be found, reviewed and analysed by category.
3	The client's RM template was updated with a revised list of potential hazards and hazard categories.	The client's software RM template complies with the latest ISO 14971 standard.
4	Requirement to analyse OTS failure as a potential hazard has been added to client's procedure and template	Off-the-shelf (OTS) is now considered during hazard and risk analysis in the project files examined.
5	Requirement to analyse hardware failures as a potential hazard added to client's procedure and template	Hardware failures now considered during hazard and risk analysis in project files examined.

The following sections evaluate the impact the RMCM based software RM procedure had upon the MD company since its formal release. The findings are based upon employee interviews and where possible are supported by other available document sources.

The interview participants were categorised as Project Management, Software QA (Senior and Junior) and Software Development (Senior and Junior). The participants spanned both PC software and embedded software, with the software developers seeing their roles as being distinctly related to either embedded or PC software but not both. The software QA team on the other hand saw their role as involving interaction with both embedded and PC software, and both software development teams. Inspection of the teams training records supported the roles and responsibilities the interviewees assigned themselves. The participants had been employed in the company for varying lengths of time ranging from zero (new employees) to two years, two to five years and more than five years. Those participants with greater than two and a half years experience in the company had exposure to what processes existed in the company prior to the implementation of the RMCM model in the company.

8.1. Safety

The interview participants recognised that the software hazard analysis and risk management procedure is one method of ensuring safety pre-production. All team members demonstrated an awareness of the new procedure. However, the project manager also discussed user trials, not mentioned in the RMCM, as a method for ensuring safer software pre-production. Sub-practice 16 of the RMCM [8,23] mentions the analysis of post-production queries and issues to safeguard against a risk scenario arising post-production that were not originally considered during development. User trials could also be used for similar analysis but before the software actually goes into production. Therefore the practice of performing user trials pre-production shall be added to the RMCM, but not as a level Med requirement because it's not a regulatory requirement.

The team members discussed dealing with non-conformance requests through the completion of corrective actions/preventative actions (CAPAs) and both fixing and testing any software related bugs/issues through unit testing and system testing. This is in keeping with the company's procedures, which states "all post-production RM activities are covered by (the company's) CAPA system." Only one team member, a software QA engineer, alluded to updating the software RM report when dealing with post production queries and issues. Sub-practice 16 of the RMCM references how three of the major MD related standards point to this as a very important practice. Therefore it is surprising that only one team member discussed this practice in relation to safety post-production. The RMCM addresses the need for this practice. However, both the way in which this practice has been integrated into the MD company's procedures and the training that individuals have received in this respect does not appear to be sufficient. On inspection of the company's procedure it states that changes must be analysed "to determine if any changes have taken place that adversely affect the risk analysis and mitigation". This is mentioned under the life-cycle phases section of the procedure but does not appear under the post-production information section.

In the past couple of years, since the RMCM was introduced to the company, the team has recognised an improvement in both software quality and safety. Although there have been several projects implemented since the introduction of the RMCM, the projects were long-term design developments and a short term evaluation of their effectiveness is not possible within the scope of this work. The devices and associated software are relatively new with respect to the time they have been in production, i.e. they have all been released within the last six months. It is important to state that there have not been any post-production complaints raised in relation to software quality or safety since the product releases. However it cannot be said definitively whether this is due to effective and efficient software risk management or whether it is due to product immaturity in the market.

From a positive perspective, one of the new software devices has been released for a clinical trial with a major pharmaceutical client. Prior to commencing the trial the client performed user trials on the software. There were no major issues raised during the user trial with respect to software safety or quality. Furthermore, the pharmaceutical client commented how this was a rare finding based on their experience on performing user trials on other third party software.

8.2. Change control

The Centre for Devices and Radiological Health reviewed MD recalls due to software failures between 1983 to 1991 and estimated that 90% were due to inadequate design and 19% were caused by inadequate change control [10]. This highlights the importance of both adequate change control and proper impact analysis of requirements changes. In this respect, the RMCM addresses change control in sub-practices 1 and 2 for determining risk sources and risk categories. It states that as per FDA requirements "it is important to define risk-related functions when analysing requirements and to monitor this ongoing source of risk throughout the lifecycle process as requirements change".

Upon initial analysis of the interview transcripts it appeared that the team recognised the need to perform software risk analysis following changes to requirements. However, further investigation revealed that it was QA who updated the software RM document at the end of the life-cycle because "the software hazard analysis document was not kept in line with the changes to the software requirements". As no updated requirements specification or updated software risk analysis was received there could be no way of providing traceability from the changes, to risk analysis, to mitigation/control and to verification. Additional testing was implemented by QA to ensure there were no adverse side effects. The evaluation has highlighted inadequate software risk analysis being performed in the company with respect to change control. A follow-up discussion was held to determine why the new process was not being followed. This highlighted a number of short-comings in the company's procedures. Within the company, all changes to the software are detailed in a software changes specification. However a few issues were highlighted. The first issue discussed the fact that no traceability is provided between the software changes specification and the original requirements in the software requirements specification (SRS). This was confirmed through a review of the company's procedures. This presented a difficulty for the QA team in determining what regression tests must be performed to ensure original requirements have not be compromised in terms of quality and safety. It also emerged that the software changes specification only contains a header called "hazard analysis". The procedure does not state what this section should contain. This has also been confirmed through the inspection of software change specifications for several different projects within the company. The inspection showed some projects provided a reference to the software hazard analysis document, whereas others simply used the terms major, moderate or minor with a text description as to why the chosen category was assigned. This has led to inconsistencies and insufficiencies in terms of software hazard and risk analysis for software changes within the company.

8.3. Lifecycle phases for software RM

The RMCM model states that software risk analysis "should begin at the requirements phase and continue through to product retirement". There was awareness amongst the team of the safety benefits for performing the software risk analysis at every lifecycle phase as per the RMCM. However the team did not always follow the procedure and this was even acknowledged, "the problem is we don't follow our procedure". When questioned as to what stage of the software lifecycle the software risk based activities were actually performed and when they were most beneficial, the responses varied. There was a general consensus that the software risk analysis document was drafted at the requirements stage and then re-visited at the very end of the lifecycle (prior to product launch) but that

"sometimes is not properly looked at in between". It was even acknowledged by interviewees that this was not sufficient because "if we find out at the end that something is missing such as a unit test or code review (mitigations), it can be too late because the development is already done", it can be "more costly" and "the project is practically completed and you're basically doing the RM document for the sake of it".

To confirm software hazard and risk analysis was only being performed at the start and end of the lifecycle, the project files were inspected to see when they were created and updated. This method of triangulation involved inspecting the issue control sheets and comparing the dates of issue with the corresponding project phase dates. The projects chosen were two major software development projects discussed in the interview transcripts. Inspection of the issue control sheets showed that both documents had only two issues, the original issue drafted at phase 1 which is the technical requirements/design phase and the final phase pre-release.

The primary reasons that the RM was left until the very end of the lifecycle was due to "time constraints" and the company's implementation of the RMCM practices for analysing and categorising risks were cumbersome. The company generated procedure and associated template which were based on the RMCM were recognised as being sufficient in terms of the practices but at the same time were seen as being "quite a big document", "another task to be done" and it "adds more work for us". This analysis highlights the need to revisit how the RMCM has been implemented within the company's procedures, to simplify the process without removing compliance in terms of implementing the RMCM practices and to train all team members on the new process. The use of the term "time constraints" also points to the need for management within the company to ensure adequate time is allocated to the software RM activities for all software projects. Finally, it was acknowledged that software risk based activities should commence at the requirements stage, but an important clarification arose during the interviews. The term "Requirements" is used within the company to encompass both user requirements and the software/technical requirements. It's important that software risk analysis commences as early as possible during the user requirements stage, once the URS has been completed. The URS may highlight specific requirements that require corresponding software requirements or design items to mitigate potential risks, and these "should be fed into and be addressed in the SRS"

8.4. Employee knowledge

Analysis of the training records alone suggested that those individuals doing the analysis, mitigations and verification were trained appropriately. However, analysis of interview transcripts pointed to a deviant case for this finding.

Following self-training, where individuals read the internal software RM procedure, individuals were not proficient in performing a risk analysis of the software. Frustrations in implementing the new RMCM based procedure were attributed to this and it was suggested that the company should "introduce better training".

Given this finding, there is a need for the client to provide relevant personnel with a detailed training session using practical examples and sample projects. Individuals should be coached interactively during the process. Reviews of the output from the software RM process should be performed at the various stage gates of the design process.

9. Solution Impact *(Specifying Learning)*

The evaluation of the RMCM has demonstrated a significant improvement in the company's software RM procedure and required practices in terms of meeting regulatory compliance. For example, Table 5, illustrates the impact of the changes that were made in relation to the practice of Determining risk sources and categories).

Prior to RMCM implementation, the software risk process satisfied 15 of the 41 required regulatory practices. Following its implementation the RM procedure satisfies all required practices. However, the evaluation of the RMCM within the MD company identified two distinct but inter-related set of findings and changes required for cycle 2 of the action research cycle - (a) modifications to the RMCM and (b) modifications to the company's procedures.

Table 5. Post-RMCM implementation findings

Determine Risk Sources and Categories		
RMCM Sub-Practice	**Change**	**Conclusions from Research**
1	Updated software RM procedure and template with a requirement to identify risk sources.	RMCM has had a direct impact. Client is now addressing the regulatory requirement to identify risk sources.
2	Updated software	RMCM has had a direct

Determine Risk Sources and Categories		
	RM procedure and template with requirement to categorise risk sources.	impact. The client is now addressing the requirement to categorise risk sources.
3	The client's RM template was updated with a revised list of potential hazards and hazard categories.	The practice of determining software hazards has not changed for the client. However, they now start their analysis with a more up to date list of hazards.
4	Requirement to analyse OTS failure as a potential hazard has been added to client's procedure and template	Updating the client's procedures to include OTS in the hazard analysis has had a direct impact on final project design files.
5	Requirement to analyse hardware failures as a potential hazard added to client's procedure and template	Updating the client's procedures to include hardware failures in the hazard analysis has had a direct impact on final project design files.

9.1. Modifications to the RMCM

The quality of the User Requirements Specification (URS) and the SRS have a direct impact on the quality of the RM report. Missing requirements in the URS or SRS may lead to missing analysis on associated risks. This stresses the need for documentation reviews to be implemented as a core risk mitigation. Therefore, the RMCM will be updated to include a sub-practice "Formally Review all Software Lifecycle Design Documentation", within specific goal 3 (Mitigate Risks).

Presently, the term "Requirements" is used within the company to encompass both user requirements and the software/technical requirements. The software RM procedure states that risk analysis must be performed at the requirements stage - however this should be more specific. It is important that software risk analysis commences as early as possible during the user requirements stage, once the URS has been completed. The URS may highlight specific requirements that require corresponding software requirements or design items to mitigate potential risks, and these "should be fed into and be addressed in the SRS"

User trials, which were not originally considered, shall be added to the RMCM as a method for detecting user related queries, issues and associated risk scenarios pre-production.

The description for sub-practice 23 (defining traceability) of the RMCM shall be amended to include provision of traceability between the user requirements, the technical specification, the associated hazard analysis and the software verification.

9.2. Modifying the company's procedures

All team members are aware of the RM procedure for satisfying the requirement of performing software RM when producing safe MD software. However training provided to date has been inadequate.

Additionally, performing the base practices of the RMCM (i.e. GG1 practices) alone is not sufficient. Consideration must also be given to performing the level Med practices in GG2 (Institutionalise a Managed Process). If no consideration is given to GG2, the base practices of GG1 may not be performed sufficiently or by the correct person. This could have a significant negative impact on the software risk-analysis and control. Training (GP 2.5) is a practice of GG2 and the first step must be to improve the training process and provide adequate training to all relevant personnel within the company. All team members have already received business knowledge training through a number of internal workshops and practical hands-on exercises.

The post-production section of the software RM procedure will be updated. It will specify that changes requested post-production must be analysed to determine if the changes could adversely affect the safety of the software or any of the previously controlled risks.

Procedures will be updated to ensure traceability between the software changes specification and the original requirements in the software requirements specification. This will allow the QA team to determine what regression tests must be done to ensure original requirements have not been compromised in terms of quality and safety.

The software changes specification procedure will be updated to state that software hazard and risk analyses must be performed for all changes listed and added to the software RM file. Thus, traceability will be provided from the changes specification to the corresponding analysis in the software RM file. This will ensure a consistent method of performing risk analysis for software changes.

10. What contributed to the success?

The researchers felt that the following factors contributed to the initial success of the chosen method:

the researchers' direct access to the company's employees and their cooperation at all levels (management and development teams); access to the company's existing processes and procedures; access to the regulatory affairs department as well as their library of regulation literature, guidelines and standards; the researchers' ability to directly influence how software is designed and developed through the controlled release of updated RM procedures and templates; support from management to support the research effort and its findings.

If the company's procedure for implementing the RMCM activities is too cumbersome or hard to follow, it runs the risk of being ineffective or not being implemented in the software projects. It was suggested to management within the company that they must ensure adequate time was allocated to the software RM activities for all software projects.

The company involved in the research required a CMMI based implementation. Therefore, the focus of the research was on implementing FDA requirements with this particular model. We have no reason to believe that other models would not be successful if they were similarly modified.

11. Additional validation & generalisation

Although the RMCM has only been trialled in one MD company, the model is equally applicable to all MD companies building software under the regulatory constraints of the BSI and FDA. To support this assertion, a dedicated steering group of MD companies who develop software was arranged. The participants were based in Ireland but their organisations were global organisations that were constrained by both the BSI and FDA regulations. The RMCM was presented to the companies with time allocated for feedback on the model. The overall response to the model was very positive as it was seen that the RMCM "offers the opportunity to get it right first time" for MD software RM. There were no modifications suggested for the model.

The client's implementation of the RMCM was subjected to both a formal BSI audit and a pre-FDA audit. Following inspection there were no major findings suggested to the client with respect to their software RM practices.

12. Acknowledgements

This research is supported by the Science Foundation Ireland funded project, Global Software Development in Small to Medium Sized Enterprises (GSD for SMEs) within Lero -(http://www.lero.ie) and the SFI Stokes Lectureship Programme, grant number 07/SK/I1299.

13. References

AAMI, New Guidance Offered on Software Risk Management, Vol. 40, No. 2. February 2005

AAMI TIR32, Medical device software risk management, 2005

ANSI/AAMI/ISO 14971, Medical devices – Application of risk management to medical devices. 2007

ANSI/AAMI/IEC 62304:2006, Medical device software - Software life cycle processes Association for the Advancement of Medical Instrumentation, 19-Jul-2006 (replacement for SW68) http://www.techstreet.com/cgi-bin/detail?product_id=1277045, ISBN 1-57020-258-3

Baskerville Richard L., *Investigating Information Systems with Action Research*, Communications of the Association of Information Systems, Volume 2, Article 19, Oct 1999

Boehm, Barry W. (1991), Software Risk Management: Principles and Practices, IEEE Software, 8, 1 (January 1991): 32-41.

BS EN 60601-1-4:2000, Medical Electrical Equipment, Part 1. General requirements for safety

Burton J., Mc Caffery F., & Richardson I., "A Risk Management Capability Model for use in Medical Device Companies", 4th Workshop on Software Quality, ICSE 2006 Shanghai, China, May 2006, pp 3-8

Capability Maturity Model® Integration for Development, Version 1.2 (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html, Technical Report CMU/SEI-2006-TR-008

CDRH, FDA, "Software related recalls for fiscal years 1983-91", US Department of Health and Human Services, 1992

Donawa, M. (2005), *Useful US Guidance on Device Software*, Medical Device Technology, Dec 2005, www.medicaldevicesonline.com

Eagles S., Murray J (2001), Medical Device Software Standards: Vision and Status, http://www.devicelink.com/medical devicedi/archive/01/05/002.html

FDA Mission Statement, http://www.fda.gov/opacom/morechoices/mission.html

FDA (2005), Quality Systems for Medical Device & Equipment/Software Manufaturers (QSR), Code of Federal Regulations, April, 2005

FDA/CDRH Guidance Document. "Guidance for the Content of Premarket Submissions for Software Contained in

Medical Devices." May 2005, http://www.fda.gov/cdrh/ode/guidance/337.pdf

FDA/CDRH Guidance Document. "Guidance for Off-the-Shelf Software Use in Medical Devices." September 1999. http://www.fda.gov/cdrh/ode/guidance/585.pdf

FDA/CDRH Guidance Document. "General Principles of Software Validation; Final Guidance for Industry and FDA Staff", January 2002.

FDA Regulations. "Code of Federal Regulations 21 CFR Part 820." April 2006. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1

IEC 60812, Analysis technique for system reliability-procedure for failure modes and effects analysis (FMEA), 1985.

ISPE, GAMP Guide for Validation of Automated Systems. GAMP 4, Dec 2001. http://www2.ispe.org/eseries/scriptcontent/orders/ProductDetail.cfm?pc=4BOUNDFUS

ISPE. GAMP 5: International Society for Pharmaceutical Engineering (ISPE): A Risk-Based Approach to Compliant GxP Computerized Systemsan-2008. http://www.techstreet.com/cgi-bin/detail?product_id=1559506

Kohn, L., Corrigan, J., Donaldson, M., (2000), To Err is Human: Building a Safer Health System, National Academy Press.

Mc Caffery F., Burton J., Richardson I., "Risk Management Capability Model (RMCM) for the Development of Medical Device Software" , Software Quality Journal, 2009. (In Press)

Susman, G. and R. Evered. (1978) An Assessment of The Scientific Merits of Action Research, Administrative Science Quarterly, (23) 4, pp. 582-603