Software Risk Management in Medical Device Systems

John Burton

ICSP, May 2008
Overview

• Research Question & Objectives
• Positioning the Research
• Research Method
• The RMCM
• Evaluation of the RMCM
• Contributions of Research
Research Question and Objectives

• Research Question
  – Can the development of a new SPI Risk Management Capability Model (RMCM) assist medical device companies in improving their software risk management practices and put them on the path to regulatory compliance?

• Research Objectives
  – Develop a Risk Management Capability Model (RMCM)
  – Evaluate the Model
Overview of Software Risk Management Evolution

Domain Specific Models

Space Industry
- SPICE for SAGE (S/4S)
- Spice for Space-Risk (R4S)
  [Cass, Voletter et al.]

Automotive Industry
- Automotive SPICE
  [Automotive SIG]

Medical Device Industry
- MedSPI
- RMC-M

Risk Metrics & Attributes
[Hackett, Rosenberg '96]

Formal SPI Models
CMMI, SPICE (ISO 15504)

General Principles and Practices
- Boehm '86, '91
- Brooks '87
- Boehm '89

Perspectives
- Risk Taxonomy
  [SEI – Carnegie Mellon]

Methodological (Process)
- Lifecycle
  (Specification, Contractor Selection, Design & Development, Systems Integration)

Human Dimension (Individual, Management, Team, Stakeholder)
## Researcher’s perspective of Risk Management by Industry Sector based on Literature Review

<table>
<thead>
<tr>
<th>Industry Domain</th>
<th>Focus of Risk Management</th>
<th>Drivers of Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Schedule</td>
<td>Budget</td>
</tr>
<tr>
<td>General</td>
<td>Primary</td>
<td>Primary</td>
</tr>
<tr>
<td>Defence</td>
<td>Primary</td>
<td>Primary</td>
</tr>
<tr>
<td>Space</td>
<td></td>
<td>Spread Evenly</td>
</tr>
<tr>
<td>Automobile</td>
<td></td>
<td>Spread Evenly</td>
</tr>
<tr>
<td>Medical</td>
<td>Secondary</td>
<td>Secondary</td>
</tr>
</tbody>
</table>
Development of the RMCM

Literature Review

RMCM Model

- FDA/CDRH Guidance
- ISO 14971
- AAMI TIR 32
- SW 68, IEC 62304
- ISPE GAMP Guide
- CMMI
Proposed Benefits of a Medical Device Specific RMCM

- Bring the disparate knowledge on Software Risk Management for Medical Devices together into one place
- Provide a method to quickly assess and improve Software Risk Management (RM) capability
- Incorporates both regulatory requirements and proven SPI RM practices
  - Promote SPI practices into medical device software
- “Offers the opportunity to get it right first time” – (Feedback on the RMCM from a Medical Device Company who is not directly involved in the research)
A- CMMI® Practices that are not mandatory for Medical Device standards.
B- CMMI® Practices that are required for Medical Device standards.
C- Non-CMMI® Practices that are required for Medical Device standards.
D- CMMI® Practices that are not mandatory for Medical Device standards – but if performed could contribute to the safety of the Medical Device software or enhance the company’s RM practice.
## RMCM Summary

**Goal: GG1: Perform the Specific Practices**

<table>
<thead>
<tr>
<th>Specific Goal</th>
<th>CMMI® based sub-practices</th>
<th>CMMI® sub-practices to meet MD regulations</th>
<th>Additional sub-practices to meet MD regulations</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG 1: Preparing for RM</td>
<td>6</td>
<td>6</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>SG 2: Identifying and Analysing Risks</td>
<td>9</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>SG 3: Mitigate Risks</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td><strong>Specific Goal Totals</strong></td>
<td><strong>23</strong></td>
<td><strong>15</strong></td>
<td><strong>20</strong></td>
<td><strong>8</strong></td>
</tr>
</tbody>
</table>

**Goal: GG2: Institutionalise a Managed Process**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 2</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Goal: GG3: Institutionalise a Defined Process**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 3</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Goal: GG4: Institutionalise a Quantitatively Managed Process**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 4</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Goal: GG5: Institutionalise an Optimising Process**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 5</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Totals</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Totals</strong></td>
<td><strong>39</strong></td>
<td><strong>21</strong></td>
<td><strong>41</strong></td>
<td></td>
</tr>
<tr>
<td>RMCM Level Med Sub-practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMCM Sub-practices</td>
<td></td>
<td></td>
<td></td>
<td><strong>59</strong></td>
</tr>
</tbody>
</table>
### GAP Analysis at Client’s site using the RMCM

<table>
<thead>
<tr>
<th>Goal</th>
<th>Practices to satisfy MD regulations</th>
<th>Practices satisfied by Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG 1: Prepare for RM</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>SG 2: Identify and Analyse Risks</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>SG 3: Mitigate Risks</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>GG2: Institutionalise a Managed Process</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>GG3: Institutionalise a Defined Process</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GG4: Institutionalise a Quantitatively Managed Process</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GG5: Institutionalise an Optimising Process</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>41</strong></td>
<td><strong>15</strong></td>
</tr>
</tbody>
</table>
Implementation of RMCM Practices at Client Site

• Update made to client’s software risk management process
  – Re-review of updated process against the RMCM
  – Updated process released into client’s Quality Management System (Controlled Environment)

• RMCM Implemented in the R&D department of a Medical Device company.
  – Embedded and Desktop application software
Evaluation of the RMCM

• Evaluation methods:
  – Documentation Analysis
  – Case Dynamics Matrices
  – Interviews
  – Content Analysis using Coding (Open and Axial)

• Evaluation Findings
  – Clients Software RM Strategy:
    • More robust - Incorporates previous missing RM practices
    • More consistent - Constant criteria used in the evaluation of severity and likelihood and overall classifications
    • More up to date/in line with the latest standards
Evaluation of the RMCM

- Evaluation Findings Continued
  - Lifecycle Phases for RM Strategy
    - Although the client’s RM strategy identifies the Lifecycle Phases to which the strategy applies (sub practice 10) the risks had not been monitored throughout the lifecycle (sub practice 39)
    - This finding was also supported by interview findings
  - Training
    - The requirement to provide adequate training (RMCM Sub Practice 25) was not adequately satisfied by the client
      - Client’s updated Software RM procedures identified the requirement to provide adequate training
      - Documentation Analysis and training records suggested adequate training had been carried out at client site
      - Interviews contradicted this finding – Self Training was used
Evaluation of the RMCM

• Evaluation Findings Continued
  – Prioritisation of Risks
    • Requirement to prioritise risks (RMCM sub practice 28) has had little impact, because all risks classified as unacceptable were seen equal in terms of priority by the client
    • Reason – No software could be released with unacceptable risks (irrespective of the formal priority assigned to the risks)
  – Addition of Risk Control Measures to the Software Requirements Specification Document
    • Client was following this sub practice (RMCM practice 35)
    • However…Client’s procedure for software risk management did not explicitly drive compliance with this practice
    • Sub-practice 23 to provide traceability from the risks and associated mitigations to the impacted software requirement(s) drove compliance
Evaluation of the RMCM

• Evaluation Findings Continued
  – Safety Pre-Production
    • Introduce User Trials as formal practices to the RMCM
  – Safety Post-Production
    • Must be explicit in procedures about the requirement to continue to perform software RM post-production
  – Requirements Changes
    • Changes tested by QA after implementation and then updated the Software Risk Management Document
    • No traceability provision from changes through to RM and verification of the change and any RM mitigations
    • Operating Procedure for performing changes required updating to refer back to procedure for software RM as part of the change process
Contributions of Research

– The benefits of a medical device specific software risk management capability model identified
  • Strengthening of medical device risk management through adoption of formal SPI model practices
  • Identification of weaknesses in CMMI risk management practices with respect to medical device regulations

– RMCM developed and validated
  • Brings the disparate medical device practices together
  • Provides a path for CMMI certified companies to achieve medical device compliance in risk management
  • Identifies practices that medical device companies must adopt to satisfy risk management in the CMMI model

– Knowledge contributions to the client, the medical device industry and to the software engineering community
Related Publications


Thank You