

A Case for Software Quality Risk Management Principles and Industry Case Study Return on Investment (ROI)

Anthony Wilson

*Sigma Global Solutions 55 York Street, Suite 1100, Toronto M5J 1R7
(B) 416-368-2000 ext. 2349 (F) 416-362-8131
website: www.sigmaglobal.ca*

 **Sigma Global Solutions**



On Site. Near Shore. Off Shore.

About Sigma Global Solutions

- Sigma defines, designs and delivers technology-enabled business solutions for many of the Fortune 1000 companies in the financial, healthcare, insurance, retail, loyalty, airline, utility and telecom industry
- A privately held Canadian company headquartered in Toronto
- We are experts in delivering complex “service oriented” project solutions
- We believe in sustained growth by being a partner to industry leaders, attracting the best and most talented professionals to offer industry-leading edge solutions to our customers.

About Anthony Wilson

- Subject Matter Expert in Quality Assurance Management Practice at Sigma Global Solutions in Toronto
- Senior IT and Pharmaceutical Quality Assurance Specialist
- Computer Systems Quality (CSQ) and Computer systems Validation (CSV) Specialist
- Quality Assurance Systems Engineering & Framework
- Food and Drug Administration (FDA) Regulatory Affairs Specialist

Agenda

1. A Discussion on “Return on Investment”
2. Introductions
3. Key Risk Indicators
4. Risk Assessment Process
 - Risk Identification
 - Risk Analysis
 - Risk Evaluation
5. Risk Control Process
 - Risk Reduction
 - Risk Acceptance
6. Risk Communication Process
7. Risk Review
8. Case Study

Introduction

- How cost effective is your organization Quality Risk management principles and process?
- To measure the Return On Investment Quality Risk Management '*indicators*' must be effectively managed.
- Risk should be identified, assessed, analyzed, reviewed and considered for further mitigation and communicated.
- Today we will learn more about the stages to an effective quality risk management process as defined by Quality Management System (QMS), Food and Drug Administration (FDA), International Conference on Harmonization (ICH) and Quality and Risk Management Standards.
- Quality Risk Management return on investment is the ratio of savings to cost that indicates the value of performing quality assurance.

Introduction

- Quality and Risk Management are complimentary and, together, are the key component for business and product success and continuous ROI
- The cost of quality assurance risk management is the total investment in resources time spent in risk management meeting, the cost of reporting risk information, and staff to develop a risk action plan, for risk assessment and risk control. The return for each managed risk is the savings. Risk management ROI is the saving for managed risk divided by the total cost of risk management activities, which expressed which is expressed in the equation.

$$\text{ROI (rm)} = \frac{\sum \text{Savings}}{\text{Cost}}$$

Cost

What is Quality Risk Management

- Quality Risk Management defines QRM as a systematic process for the assessment, control, communication and review of risk to the quality of product development across the product lifecycle.
- A Risk-Based Approach, states the using of evidence-based and scientific-based framework to find ways of mitigating risk while facilitating continuous improvement and innovation in business product development / manufacturing is a key business objective, for Return on Investment (ROI)

Quality Risk Management Principle

- The principles and tools of quality risk management can be applied in different aspects of the business and product development quality. These aspects include software product development, manufacturing, distribution, and the inspection and submission/review processes throughout the lifecycle of the business, products, and drug substances and other medicinal products.

Principles of Quality Risk Management

- The primary principles of quality risk management are and involve the following:
 - The evaluation of the risk to quality, should be based on sound evidence and scientific knowledge and ultimately be linked to the products deliverable, i.e. failure of software product, the protection of the patient using a drug product; and
 - The level of effort, the formality and documentation of the quality risk management process, should reflect the level of risk.

Understanding Risk

What is Risk?

- Risk is the chance of something happening that may have an impact on the achievement of objectives. Risk is the combination of harm and the severity of that harm. Risk is measured in terms of consequences and likelihood combined to arrive at a risk rating from Low to Very High.
- A risk is an event (i.e. what could happen) that should be distinguished from identified sources of the risk (i.e. how each risk could arise) and impacts (i.e. what the resultant effect is).

What is quality Assurance Risk Management

- Quality assurance Risk Management incorporates the culture (People), processes, technology and structures that are directed towards the effective management of potential opportunities and adverse effects within the business and/or product development and operational environment.
- Quality Assurance Risk management is an integral part of the business approach to decision-making and accountability.

Risk Classification

- **Severity** = Impact on Product Quality, Patient Safety, and Data Integrity (or other harm) – Low, Medium, High
- **Probability** = Likelihood of the fault occurring
- **Risk Class** = Severity \times Probability
- **Detectability** = Likelihood the fault will be noted before harm occur
- **Risk Priority** = Risk Class \times Detectability
- **Low Risk Priority** – the can business apply the use of Good/Best Practices
- **Medium Risk Priority** – the can business can apply the use of a generic checklist control
- **High Risk Priority** – the business should use a risk assessment approach to identify specific control and rigors

Quality Risk Management - Key Risk Indicators (KRIs)

- KRIs are measurable metrics or indicators that track exposure or loss, or, as one person puts it, “trouble”.
- Activities or Tools that can perform this function may be considered a risk indicator.
- The indicator becomes key when it tracks an especially important risk exposure
- Operational risk can be defined as the risk of loss resulting from inadequate or failed processes, systems, human performance or external events.
- The number of customer complaints is an example of a risk indicator. As customer complaints increase, the greater probability that there are some underlying and potentially systemic mistakes and / or errors of judgment being made is likely to increase.

Key Risk Indicators – Their Role in Quality Risk Management and measurement

Uses for KRIs

- KRIs support the tactical management of routine risks
- Anticipate emergence of major risks to help achieve “no surprises”
- Is used to set tolerance levels for risk acceptance for different risk
- Contribute to effective integration of risk management measurement
- Report risk profiles to senior management
- Meet base requirements
- Calculate qualitative adjustment to capital
- Meet regulatory requirements

Properties of a good indicator

- Key to the effectiveness of any KRI program is the quality of the KRIs themselves.
- An assessment of KRI effectiveness largely depends on expert opinion, which is based, in turn, on knowledge of how specific business functions and processes work, where they are vulnerable, and what can affect that vulnerability.
- Given the inherent subjectivity implicit in most KRI programs, there is a strong case for establishing a framework for assessing effectiveness.

Criteria for Good Key Risk Indicators

Effectiveness	Comparability	Ease of use
Indicators should:	Indicators should	Indicators should:
<input type="checkbox"/> Apply to at least one specific risk and one business function or activity;	<input type="checkbox"/> Be quantified as an amount, a percentage, or ratio;	<input type="checkbox"/> Be available reliably on a timely basis
<input type="checkbox"/> Be measurable at specific points in time;	<input type="checkbox"/> Be a reasonably precise and definite quantity;	<input type="checkbox"/> Be cost-effective to collect; and
<input type="checkbox"/> Reflect objective measurement rather than subjective judgment;	<input type="checkbox"/> Have values that are comparable over time;	<input type="checkbox"/> Be readily understood and communicated
<input type="checkbox"/> Track at least one aspect of the loss profile or event history, such as frequency, average severity, cumulative loss or near-miss rates; and provide useful management information	<input type="checkbox"/> Be reported with primary values and be meaningful without interpretation to some more subjective measure, <input type="checkbox"/> Be identified as comparable across organizations	

Quality Risk Management Responsibility

- Quality risk management activities are usually, but not always, undertaken by interdisciplinary teams.
- Quality Risk Management Teams should be developed with the inclusion of experts from the appropriate areas, i.e. quality unit, business development, project areas, engineering, regulatory affairs, production operations, sales, and marketing, legal, quality assurance risk management experts and consumers and patients.

Decision Makers are:

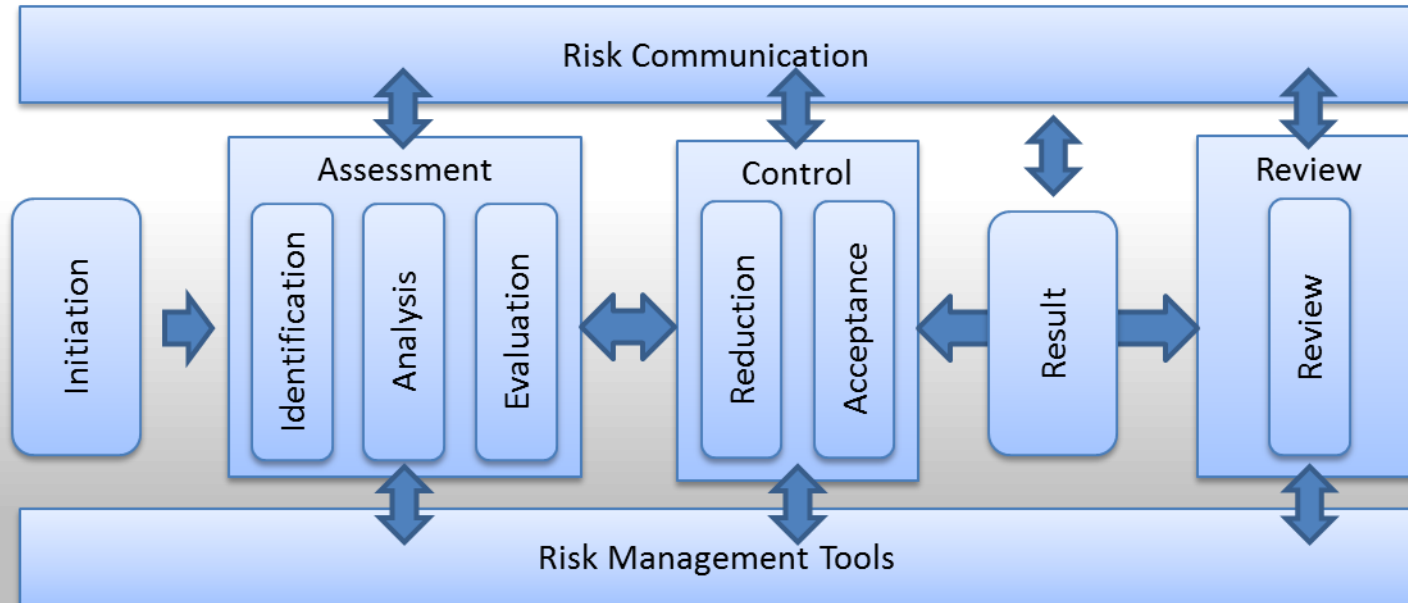
- Responsible for coordinating risk management across functional areas, projects, and department of the business.
- Ensure and assure that the quality assurance risk management program and processes are defined, deployed and reviewed and that adequate resources are available for program execution.

Quality Risk Management Process

- The Quality Risk Management approach must include systematic processes designed to coordinate, facilitate and improve sound evidence-based and science-based business decision making with respect to risk. The quality assurance risk management process must be planned and should include the following:
 - Definition of the problem and/or risk question, must include pertinent assumptions identifying the potential for risk.
 - Gather source information and/or data on the potential problem, such as harm to human health, and/or product defect that may result in failure impact relevant to the risk assessment.
 - Identified leader and resources.
 - Schedule timeline, deliverables and appropriate level of decision, making for the risk management process.

Quality Risk Management Process Overview

- Quality risk management is a systematic process for the assessment, control, communication and review of the risks to the quality of the product across the product lifecycle.



Note: Decisions are not shown in the **diagram below** because decisions can occur at any point in the process.

Quality Risk Management Identification

Risk Identification

- Risk identification applies a systematic use of information and / or data to identify problems and / or hazards as it relates to the risk question of problem description.
- Information may include current data and / or historical data, system analysis, informed decision, and concerns of stakeholders.
- Risk identification is concern with and addresses “What might go wrong” question, and identifying the possible consequences

Notes: the statement above provides the basis for further steps in the quality assurance risk management process

Quality Risk Management Analysis

Risk Analysis

- Risk Analysis is the estimation of risk linked with the identified problems/hazards.
- It is the qualitative or quantitative process of linking the likelihood of occurrence to the severity of failure and/or harm.

Risk Evaluation

- Risk evaluation compares the identified and analyzed risk against given risk criteria.
- Risk evaluation consider the strength of evidence for all there of the fundamental questions.

Risk Evaluation Output

- The output of risk assessment is either quantitative or an estimate of qualitative risk descriptors (as “High” “Medium” or “Low”).
- In quantitative risk assessments a risk estimate provides the likelihood of specific consequence given a set of risk-generating circumstances.
- Most risk management tools use relative risk measurement to combine multiple levels of severity and probability into an overall estimate of relative risk.

Quality Risk Management Control

- Risk control involves decisions to reduce risk and / or accept risk.
- Risk Control effort invested in risk control should be proportional to the significance of the risk.
- Risk control should be performed on a cost-benefit analysis, to understand the optimal level of risk control and the measure of success and ROI
- Risk control should focus on the following questions:
 - Is the risk above an acceptable level?
 - What can be done to reduce or eliminate risks?
 - What is the appropriate balance among benefits, risks and resources?
 - Are new risk introduced as a result of the identified risks being controlled?

Quality Risk Management Reduction

Risk Reduction

- Risk reduction focuses on processes for mitigation or avoidance of quality risk when it exceed a specified (acceptable) level
- Risk reduction includes actions taken to mitigate the severity and probability of harm and / or failure

Note

- Processes that improve the detectability of hazards, and problems and quality risks might be used as part of a risk control strategy
- The implementation of risk reduction measures can introduce new risks into the system or increase the significance of other existing risks.
- Hence it might be appropriate to revisit the risk assessment to identify and evaluate any possible change in the risk after implementing a risk reduction process

Quality Risk Management Acceptance

Risk Acceptance

- For some type failure(s)/hazard(s), even the best quality risk management practice might not entirely eliminate the risk.
- Risk acceptance is the decision to accept risk. Risk is usually a two way decision (i.e. Provider and patient acceptance)
- Risk acceptance can a formal decision to accept the residual risk or it could be a passive decision in which the residual risks are not specified

Note

- *In these circumstances, it might be agreed that an appropriate quality risk management strategy has been applied and that quality risk is reduced to a specified (acceptable) level.*
- *Usually the specified acceptable level will depend on many parameters and should be decided on a case-by case basis*

Quality Risk Management Communication

- Risk Communication is the sharing of information about risks between the decision makers and other stakeholders
- The sharing of risk information should be immediate and can be communicated at any stage of the quality risk management process
- The output and result of the quality assurance risk management process should be appropriately communicated and documented
- Communication should include stakeholders and affected groups, i.e. business executives, upper management, appropriate regulatory bodies and industry, client/customers, patients, etc.
- Information communicated might include the following:
 - Existence of an identified risk(s)
 - Nature of the identified risk(s)
 - From what sources did the risk(s) occurred
 - Probability of failure associated with the risk(s)
 - Severity level of the risk(s) – (Low, Medium, or High)
 - Acceptability – (Is the risk(s) above define acceptance levels)
 - Control – Can we manage the risk(s) within defined cost
 - Detectability or other aspects of risk(s) to quality

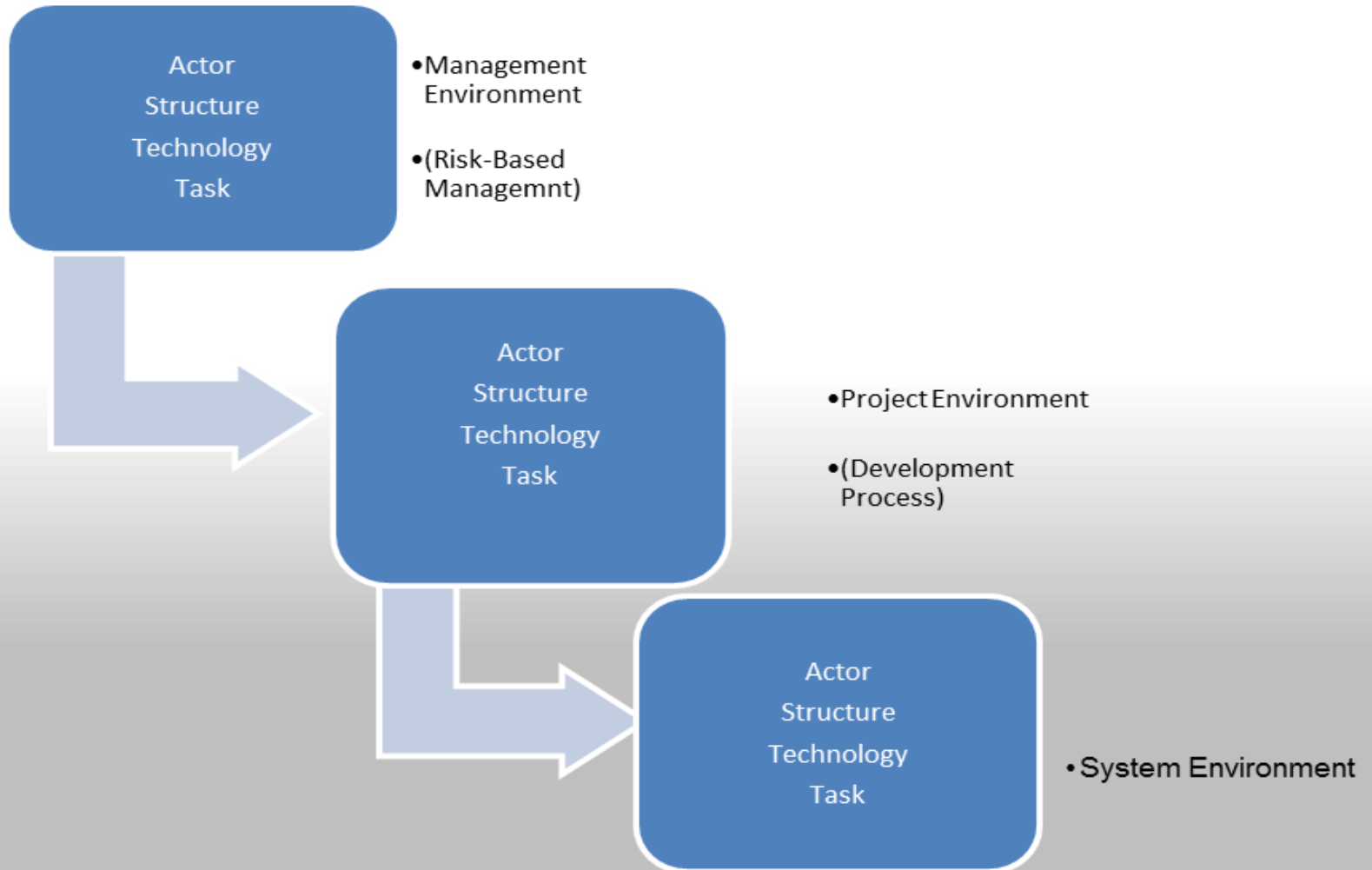
Quality Risk Process Summary

- Quality Risk Management supports an evidence-based, and scientific-based practical approach to decision-making.
- QRM is developed on the basis of documented, transparent, and reproducible methods to accomplish the process steps of the quality assurance risk management process, based on current knowledge about assessing the probability, severity and detectability of the risk.
- A framework for business and product quality assurance risk management can be created by marrying the model of behavior (process view) with the model of an organization (structural view) in the context of the quality development model
- Risk(s) must be:
 - Assessed (to include risk identification, analysis, evaluation, and documentation)
 - Controlled (to include risk reduction and acceptance)
 - Communicated to all Stakeholders
 - Reviewed by Subject Matter Experts

Case Study

- Some industries, such as pharmaceutical and medical, use several different industry recognized risk management tools and internal procedures to assess and manage risks.
- Such tools includes but not limited to the following:
 - Basic Risk Management facilitation methods (flowcharts, checklist, etc.)
 - Failure Mode Effects Analysis (FEMA)
 - Fault Tree Analysis (FTA)
 - Hazard Analysis and Critical Control Point
 - Hazard Operability Analysis (HAZOP)
 - Preliminary Hazard Analysis (PHA)
 - Risk Ranking and Filtering
 - Supporting Statistical Tools
- Quality risk management methods and the supporting statistical tools can be used in combination, (i.e. Probabilistic Risk Assessment).
- Combined use provides flexibility that can facilitate the application of quality risk management principles.

Software Quality Risk Management Process



Quality Risk Management – Risk Quantification

- When an organization has a good understanding of quality risk management they must make choices on the quantification method for assessing failure and / or hazard. The methodology should include an assessment to determine the following:
 - How bad is its impact? (Severity)
 - How often does it happen? (Frequency)
 - How much effort is required to fix it? (Cost)
 - What is the risk of fixing it? (Risk)
- The first two items can also be formulated as the classic rule for the risk that a certain failure and / or hazard carries: **Risk = Impact x Frequency**

Quantifiable Risk	Qualifiable Risk
Cost of Insurance	Organization reputation
Cost of Payout	Employee skill sets
Resource Cost	
Risk Identification timeframe	

Risk Management Return on Investment

- Cost reduction is a technique for saving that decreases the estimated planned cost. It is the difference between planned and actual cost.
- Risk management practices can lead to opportunities for a program to do better than their baseline plan
- RIO(rm) metric grows as risks are resolved
- RIO(rm) metric has a number of uses:
 - The planning of benchmark for risk leverage – when planning a risk resolution strategy, ROI(rm) is useful as a benchmark for expected risk leverage
 - Planning benchmark for management reserve. An understanding of a typical ROI(rm) can be coupled with good estimates of total program risk exposure to set realistic program reserve level.
 - Program indicator of risk management effectiveness. For a specific program ROI(rm) is an indicator of risk management effectiveness. When the ROI(rm) varies significantly from an organization metric, practices should be investigated for either improvement or lessons learned
 - Organizational measure of risk management utility. At the organizational level, ROI(rm) is a measure of the value of the risk management practice

Case Study – Software Engineering

- Over time, the cost and savings from risk management yield an RIO(rm) metric that can be used as a performance standards. The following case study of a large software systems development programs show that the benchmark for ROI(rm) is over 20 to 1.
- Each month, management reviewed the engineering team's cost saving in terms of cost avoidance and cost reduction. The team had to quantify either negative or positive cost and schedule impacts, as well as the solution cost. They had an objective of increasing productivity by 10-20%.
- One way the tem improved productivity was midcourse correction of coding standards. They quantified the inefficiency of a coding standards in the following manner:
 - If it is aggravation for 20 engineers and it slows them down by 10 min/day, that is 200 min/day – $20 \times 10 = 200$, or 867 hour/year. This calculation is based on a nominal 40 hour week, the coding phase on the program lasted 1 year, at a labor rate of \$100/hour, calculated is \$87000.
 - The cost of changing a few lines of coding standards was zero. Given that the coding standard were online, it was easily done. The team saved \$87,000 by changing a few coding standards.

Case Study – Software Engineering

- The engineering team estimated their cost saving as well as their cost of performing risk management activities. The process required the estimates for risk probability and consequence to be most likely (not worse case) estimates.
- The estimate were updated whenever significant changes occurred in the estimates or when a change in resolution strategy occurred. The reported result on return on investment as an indicator of the team's risk management effectiveness.

The calculations show the ROI(rm) was 22 to 1:

Risk Expenditures

\$150,000 program wide risk management,

\$100,000 software risk management,

\$120,000 risk resolution cost,

ROI (rm) = \$8 million/\$370,000.

ROI(rm) = 22 to 1.

Total Cost : \$370,000

Saving \$8 million (\$6 million cost avoidance and %2 million cost reduction)

Discussion

- Risk management should be an ongoing part of the quality risk management process
- There should be an implemented mechanism to review and monitoring event for capturing adverse effects in the product and business life cycle
- The output and results of the risk management process should be reviewed to account for knowledge and experience
- Once a quality risk management has been initiated, that process should continue to be utilized for events that might impact the original quality risk management decision, whether these events are planned, i.e. results of product review, inspections, audits, change control or unplanned, i.e. root cause from failure investigations, or recall

Conclusion

1. A good Quality Risk Management program must be well planned, implemented, executed, and monitored for the organization to realized ROI
2. Quality Risk Management program must have a developed Risk Mitigation Plan that allows for the appropriate assessment and control of risk
3. QRM must have tools and mechanisms that are capable of reporting “Key Risk Indicators”, risk scenario analysis, and risk mapping at the earliest stages and throughout the business and product lifecycle
4. QRM must have a risk quantification process to measure and address expected and unexpected losses – loss provision mechanism
5. The QRM framework should be flexible and scalable to assist with the identification and application of appropriate risks control where they are needed for the for the business

Thank you

References

1. E. Hall, Managing risk: Methods for software systems development, Addison Wesley, Reading, MA, 1998.
2. Charette, R. N. (1989): Software Engineering Risk Analysis and Management.
3. New York: Intertext Publications, McGraw-Hill.
4. Risk Management Association, 2005, "Report on a Survey of KRI Programmes" (Webbased survey conducted with 38 respondents comprising banks with a North American, European or global focus), Summer.