CONCEPT
HEIDELBERG

GMP Compliance for
Computerized Systems Validation
January 16 - 17, 2003 at Istanbul, Turkey

Risk Management

Dr.-Ing. Guenter Generlich
guenter@generlich.de

The Expert's Opinion

Peter Drucker (1975)
We must be able to chose rationally among risk-taking courses of action, rather than plunge into uncertainty on the basis of hunch, hearsay, or incomplete experience, no matter how meticulously quantified.

Tom Gilb (1988)
If you don't actively attack the risks, they will actively attack you.

Definition of Risk

- Risk is the possibility of an undesired event
- Risk is the possibility of suffering loss, injury, disadvantage, or destruction (Webster's Dictionary)
- In a development project, the loss describes the impact to the project which could be in the form of diminished quality of the end product, increased costs, delayed completion, loss of market-share, or failure
- From a regulatory point of view, there is a risk not to comply with the (regulatory, legal) requirements

A Strange Definition of Risk

Risk equals the sum, for all possible threads, of the probabilities of those threads being realized multiplied by either the replacement costs or the cost of not having the asset

$$\text{Risk} = \sum_{\text{Thread}=1}^{n} \text{Asset Value} \times \text{Probability}$$

A Risk Manager´s Prayer

” O Lord, grant me
the courage
to change things I cannot accept,
the serenity
to accept things I cannot change,
and the wisdom
to know the difference.”

Risk Management

Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to:

- assess continuously what can go wrong (risks)
- determine what risks are important to deal with
- implement strategies to deal with those risks

Definition: Risk Assessment

Risk Assessment is an examination of risk areas or events to assess the probable consequences for each event, or combination of events in the analysis, and determine possible options for avoidance.

When Do People Do Risk Management?

After they've been burned in similar situation
- Pain-avoidance
- Convincing evidence of consequences

When everybody involved is convinced that risks exist, but that it's still worth going forward
- Everyone is a winner ✝ Realistic expectations

When they've learned how to do it well
- Techniques not well-known, but can be learned

When Should Risk Management Be Performed?

- When important high-consequence decisions must be made about complex systems under uncertainty
- When information is not sufficient to comprehensively assess all important strengths and weaknesses of complex systems by other means
- When an important complex job must be performed correctly for the first time
- In all life cycle phases, including
  - design
  - operation
  - upgrade/retrofit,

  when important decisions must be made cost-effectively

Observations

- Most managers believe they are managing risk
- Risk is seldom managed systematically
- Managers tend to address only risks from technical areas with which they have expertise
- Risk management is highly dependent on individuals
- Known risks typically are not managed
- Top 3 risks are requirements, resources, and the customer-supplier interface

If Risk Management is so important, why don't people do it?

Unwillingness to admit risks exist:
- leaves impression that you don't know exactly what you're doing
- leaves impression that your bosses, customers don't know exactly what they're doing
- "success-orientation"

Tendency to postpone the hard parts:
- maybe they'll go away
- maybe they'll get easier, once we do the easy parts

Costs money and time up front

Decisions Under Uncertainty

- Most decisions, especially complex ones, are made under some degree of uncertainty
- Risk assessment and management have therefore been performed either implicitly or explicitly in all rational decisions regarding complex systems and activities that have involved many stakeholders
- Following is an interesting example from history

Example from History

"We the Athenians in our persons, take our decisions on policy and submit them to proper discussion. The worst thing is to rush into action before the consequences have been properly debated. And this is another point where we differ from other people. We are capable at the same time of taking risks and estimating them beforehand. Others are brave out of ignorance, and when they stop to think, they begin to fear. But the man who can most truly be accounted brave is he who best knows the meaning of what is sweet in life, and what is terrible,
and he then goes out undeterred to meet what is to come."

from Pericles' Funeral Oration in Thucydides' "History of the Peloponesian War"
Excerpt from Funeral Oration, a speech by Pericles, Athenian general, to his troops before a battle in the war between Athens and Sparta that started in 431 B.C.

Risk Management Affects

Compliance	conformity in fulfilling official requirements
Reliability	the extent to which a procedure yields the same results on repeated trials
Security	something given, deposited, or pledged to make certain the fulfillment of an obligation
Integrity	the quality or state of being complete or undivided

Risk vs. Opportunity

- Risk is essential to progress
- Failure can be key part of learning
- High risks justify high profits

Functions of Risk Management (1)

The Risk Management Paradigm
(Software Engineering Institute)

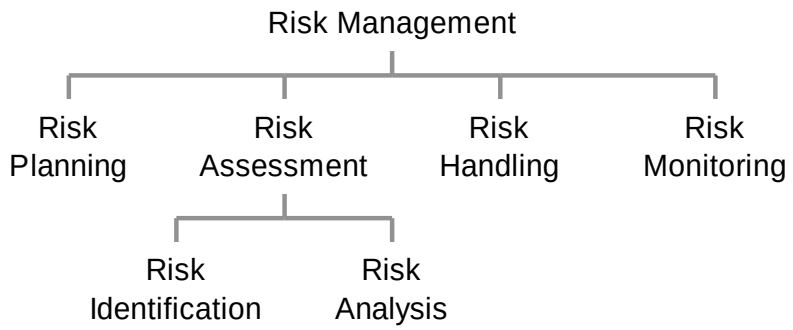
Functions of Risk Management (2)

Identify	Search for and locate risks before they become problems. *Anticipate what can go wrong*
Analyze	Transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks. *Decide what is important*
Plan	Translate risk information into decisions and mitigating actions (both present and future) and implement those actions. *Plan to take action*

Functions of Risk Management (3)

Track	Monitor risk indicators and mitigation actions. *Track Actions*
Control	Correct for deviations from the risk mitigation plans. *Integrate activities*
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks
	***Note*:** Communication happens throughout all the functions of risk management

Risk Management Structure



Principles of Risk Management

- Core principle: open communication
- Sustaining principles:
  - integrated management
  - teamwork
  - continuous process
- Defining principles
  - forward looking view
  - global perspective
  - shared product vision

Risk: Core Principle

Open communication
- Encouraging free-flowing information at and between all project levels
- Enabling formal, informal, and impromptu communication
- Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk)

Sustaining Principles

Integrated Management
- Making risk management an integral and vital part of project management
- Adapting risk management methods and tools to a project's infrastructure and culture

Teamwork
- Working cooperatively to achieve common goal.
- Pooling talents, skills, and knowledge

Continuous Process
- Sustaining constant vigilance
- Identifying and managing risks routinely through all phases of the project's life cycle

Defining Principles

Forward-looking view
- Thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes
- Managing project resources and activities and anticipating uncertainties

Global perspective
- Viewing software development within the context of the larger systems-level definition, design, and development
- Recognizing both the potential value of opportunity and the potential impact of adverse effects

Shared product vision
- Mutual product vision based on common purpose, shared ownership, and collective communication
- Focusing on results

Risk Statement

- a short, fact-based, and actionable statement of concern
- a description of program/project conditions that may lead to the loss
- includes indications of the sources of the underlying condition(s)
- accompanied by context, that will preserve the specific original intent, i.e. a description of the loss
- elicited from the stakeholders of the program/project

“For a risk to be understandable, it must be expressed clearly”

Risks Within a System Context

… can involve **all** resources

Risk Taxonomy

- Provides a framework for organizing data and information
- Should be used as a questionnaire
- Three major classes
  - (1) **Product Engineering:** the technical aspects of the work to be accomplished
  - (2) **Development Environment:** the methods, procedures, and tools used to produce the product
  - (3) **Program Constraints:** the contractual, organizational, and operational factors; partly outside the direct control

(1) Product Engineering Class

Requirements: The definition of what the software product is to do, the needs it must meet, how it is to behave, and how it will be used. This element also addresses the feasibility of developing the product and the scale of the effort.

Design: The translation of requirements into an effective design within project and operational constraints.

Code and Unit Test: The translation of software designs into code that satisfies the requirements allocated to individual units.

Integration and Test: The integration of units into a system and the validation that the software product performs as required.

Engineering Specialties: Product requirements or development activities that may need specialized expertise such as safety, security, and reliability.

(2) Development Environment Class a

Development Process: Definition, planning, documentation, suitability, enforcement, and communication of the methods and procedures used to develop the product.

Development System: Tools and supporting equipment used in product development (e.g. CASE tools, simulators, compilers,...)

Management Process: Planning, monitoring, and controlling of budgets and schedules; controlling factors (defining, implementing, and testing the product), project manager's experience (software developm't, management, the product domain; and the manager's expertise in dealing with external organizations incl. customers, senior mgmt, matrix mgmt, other contractors.

(2) Development Environment Class b

Management Methods: methods, tools, and supporting equipment used to manage and control the product development (e.g. monitoring tools, personnel management, quality assurance, and configuration management)

Work Environment: The general environment: the attitudes of people and the levels of cooperation, communication, and morale.

(3) Program Constraints Class

Resources: The external constraints imposed on schedule, staff, budget, or facilities.

Contract: The terms and conditions of the project contract.

Program Interfaces: The external interfaces to customers, other contractors, corporate management, and vendors.

Risk Has 2 Dimensions

Deterministic Risk Assessment answers the two questions:

1. What can go wrong ?
2. How severe are the (adverse) consequences?

Probabilistic Risk Assessment answers one more question:

3. How likely are the (adverse) consequences?

Risk Exposure: Impact

Impact the effect of the particular risk on the project which is determined on the basis of the risk's effect on the software's performance, supportability, cost, and schedule

The levels of impact are

4 - unacceptable / catastrophic
3 - undesirable / critical
2 - acceptable with review / marginal
1 - acceptable without review / negligible

Risk Exposure: Probability

Probability is the chance that a particular impact will occur

The levels of probability are

3 - very likely
2 - probable
1 - improbable

Risk Exposure

Risk exposure is the function of probability and impact rated on a 6 - point scale are computed by the simple look-up table

Probability → / Impact ↓	3 very likely	2 probable	1 improbable
4 unacceptable	6 high	5 high	4 medium
3 undesirable	5 high	4 medium	3 medium
2 acceptable with review	4 medium	3 medium	2 low
1 acceptable without review	3 medium	2 low	1 low

Risk Exposure Matrix

… just an example:

Component → / Category ↓	Performance	Compliance	Support	Cost	Schedule
unacceptable	nonachievement of technical performance	nonachievement of validation	unsupportable software	major budget overrun (>50%)	unachievable
undesirable	significant degradation of technical performance	serious gaps in regulatory compliance	major delays in software modifications	serious budget overrun (~30%)	serious delays (>30% late)
acceptable with review	some reduction in technical performance	minor gaps in regulatory compliance	minor delays in software modifications	budget overrun (~10%)	delay (>10% late)
acceptable without review	minimal to small reduction in technical performance, at detail level	some formal aspects are suboptimally considered	irritating and awkward maintenance	consumption of some budget cushion	consumption of some slack - not on critical path

Residual Exposure Acceptance

Final Exposure	Required Sign-Offs (Example)
Unacceptable	Project Manager, Sponsor, User Director, CEO
Undesirable	Project Manager, Sponsor, User Director
Acceptable with Review	Project Mgr, Project Sponsor
Acceptable without Review	Project Manager

Strategies for Risk Reduction

- Reduce probability / frequency

  frequency = events per time unit
  probability = occurence per time unit (with rare events)

- Reduce severity / impact

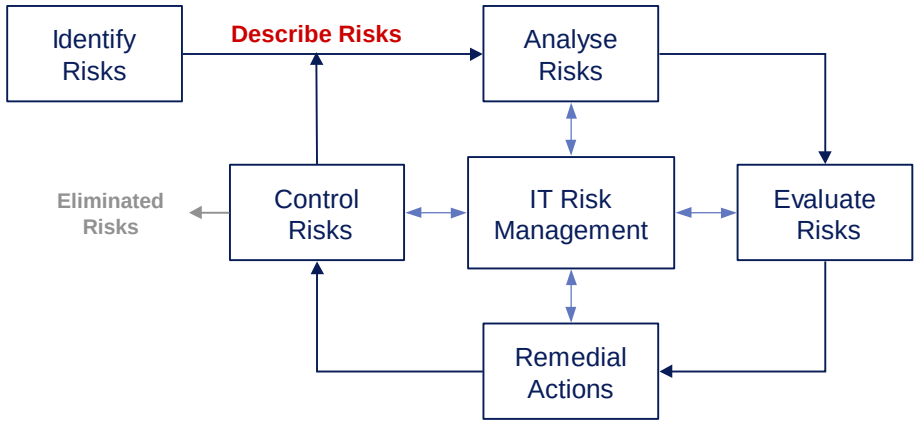
  severity = detriment per event

$$\text{Risk}\ \left[\frac{\text{detriment}}{\text{unit time}}\right] = \text{Frequency}\ \left[\frac{\text{events}}{\text{unit time}}\right] \times \text{Severity}\ \left[\frac{\text{detriment}}{\text{event}}\right]$$

Risk Assessment Summary (Risk Log)

Project Area	Risk Area	Risk Statement	Probability	Consequences	Impact	Risk Exposure	Precautions Countermeas.	Person Respons.	Rev. Date
1	2	3	4	5	6	7	8	9	10
functional geograph. organiza- tional ...	manpower money material machines minutes		3 very likely 2 pro-bable 1 inpro-bable		4 catastroph. 3 serious 2 marginal 1 neglectible	1 ... 6	✍ probability ✍ impact		

The Risko Management Cycle



Benefits of Risk Assessment (1)

- Creates a shared view of risks facing a project among the staff
- Creates a common framework for talking about and mitigating risks
- Provides a snapshot of risks
  - enables the tracking of risks systematically (changes in probability and impact)
  - enables the tracking of risk mitigation efforts systematically
  - provides an impetus to focused project-level process improvement
  - provides decision-making information to the project manager
  - accelerates the creation of a shared product vision among project staff

Benefits of Risk Assessment (2)

- Cultural shift from “fire-fighting” and “crisis management” to proactive decision making avoids problems before they arise
- Base decisions on more complete information and adequate knowledge of future consequences
- Increase probability of successful completion of the program / project
- Avoid high costs otherwise occurring with retrospective correction of problems / validation

Never Forget

- Risk prevention is more cost-effective than risk detection
- The degree of risk, and its causes, must never be hidden from decision-makers
- If you don’t ask for risk information, you are asking for trouble
- Never trust it until you can see it and feel it

Tom Gilb, 1988

Final Statement

You do not have to do it!

Survival is not compulsory.

The greatest risk of all is
to take no risk at all!