Risk-based Testing

Erkki Pöyhönen
erkki.poyhonen@nokia.com
Nokia Research Center, SW Technology Lab

NOKIA

What is "Risk"

- "A risk is an unwanted event that has negative consequences"
  Shari Lawrence Pfleeger [PFL2000]
- *Risk Management* plans to avoid these unwanted events, or if they are inevitable, minimize their consequences
- *A Problem* is something that is a fact (happened or will happen)
- *A Risk* is something that might happen in the future
- *Risk aspects* are
  - A loss associated with the event
  - The likelihood that the event will occur
  - The degree to which we can change the outcome

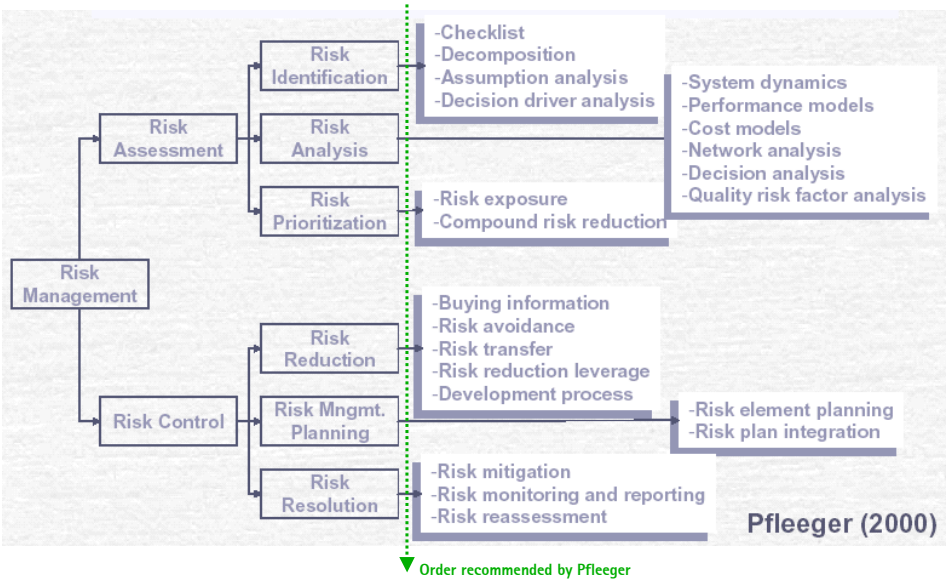
NOKIA

Project and Business risks

- *Project* or *Process risks* involve resources, planning, contracts, etc
  - About the fluency of business as usual and implementing plans
  - Most of the risk management writings deal with Process risks from the project managers point of view, as PMs are not expected to make decisions about operation **content**, but to concentrate on the **form** of operations.
  - Ultimate risk being avoided is project chaos
- *Business* or *Product risk* involves product and resulting business-time issues
  - Product stability, performance and quality at use
  - A useful point of view for testing, but not much communicated in risk management domain
  - Testing is all about business and product **content**
  - Ultimate risk being avoided is bad *quality of use* at user

NOKIA

SW Risk Management



NOKIA

Risk-Based Testing (from [KAN2001])

- Two separate meanings for one term
  - [AML99] talks about risk-based test management: risk analysis is done for focus, what to test next
    - Testing is prioritized in terms of the probability that some feature of the program will fail and the probable cost of failure, if this feature will fail.The greater the probability of an expensive failure, the more important it is to test that feature as early as possible and as carefully as possible.
    - Define all requirements
      -> Based on risk assessment, prioritize the requirements
      -> Plan and define tests according to requirement prioritization
      -> Execute test according to prioritization and acceptance criteria.
    - This is a higher-level view for System and Acceptance testing
  - [BAC99] explains doing risk analysis for the purpose of finding errors
    - A feature is being studied and asked how it could fail. Several further questions clarify this: "What would a failure look like?", "Why should this feature fail?", "What drivers of risk are likely to have affected this feature?"
    - More suitable on technical testing: Unit testing and Integration testing.
    - More about this on few next slides.

NOKIA

Testing is risk-based ("James Bach"-style)

- Risk-based testing includes the following steps:
  1. Make a prioritized list of risks
  2. Perform testing that explores each risk
  3. As risks evaporate and new ones emerge, adjust your test effort to stay focused on the current risk set
- Risk analysis is a real discipline (free tutorial available from [SEI])
- Risk analysis continues throughout the project
  - "Are we ready to release yet?" -- "Well, it depends!"
- Risk analysis for testing must always include the user/customer point of view
  - Simple stakeholder analysis and impact estimation would do wonders [Gilb99]
  - After specifying quantified quality requirements, risk assessment is a ten times easier

NOKIA

Testing is risk-based (cont.)

- Risks collected by Heuristic analysis [Bach99]:
  - Bottom-Up (Inside-Out):
    - Vulnerabilities, Threats and Victims per module
  - Top-Down (Outside-In): Assessing predefined risk categories
    - Quality criteria, like ISO 9126
      - "Functionality, Reliability, Usability, Efficiency, Maintainability, Portability"
    - Generic risk lists
      - "anything new is more risky than tried-and-true", "distribution brings its own risks"
    - Domain specific risk catalogs
      - Based on historical data and common failures,
      - "The one who does not know the history is bound to repeat it"
- Collected experiences from fault analysis on the spot
- Project post-mortem for high level findings

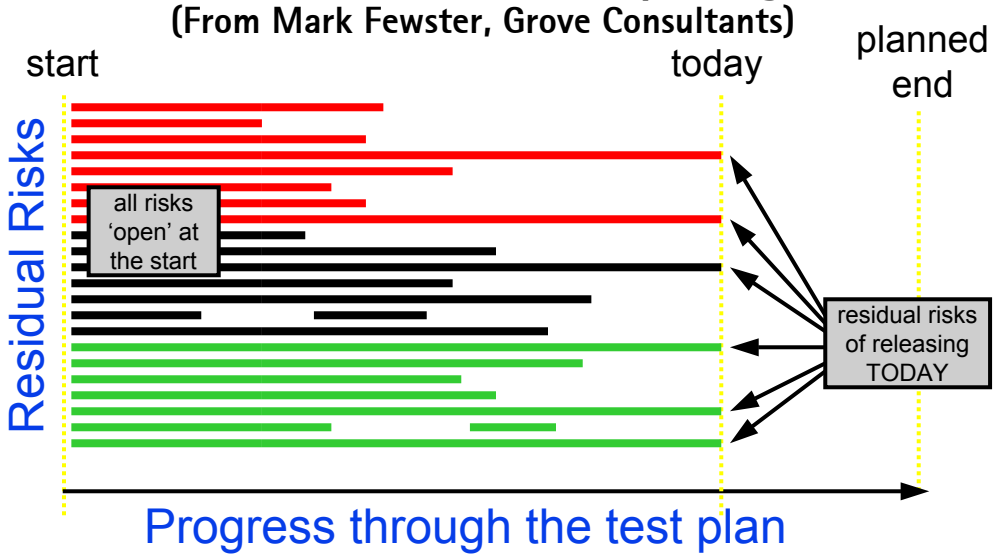
NOKIA

4. ... Two more considerations
(From Mark Fewster, Grove Consultants)

- Business managers understand 'risks' and 'benefits'
  - They are terms that describe the future
- Business managers are interested in the future
  - They are not interested in the past
  - Faults that have been found and fixed are history

NOKIA

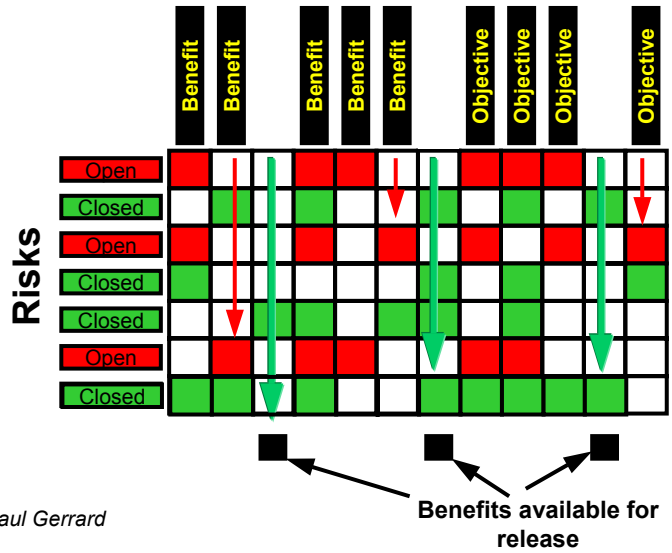
4. ... Risk-based test reporting
(From Mark Fewster, Grove Consultants)



Source: Paul Gerrard, Risk - the new language of e-business testing, BCS SIGIST 29 Sept 2000

NOKIA

4. ... Benefit based test reporting
(From Mark Fewster, Grove Consultants)



Source: Paul Gerrard

NOKIA

Risk-based test reporting

- Why not use them also for test planning and reporting
  - Think you're a project manager and you ask for testing manager if the SW is ready next week as planned. What if you get the response in the test report
    - *"We are not ready, because we still have 600 test cases to run, we have found 120 new faults during this test campaign, and there are many more to be found"*
  - Or even worse:
    - *"sure, it works OK"*
  - At least I would be very inclined to ask for clarification "So what?"
  - Wouldn't it be better for test manager to tell something, like
    - *"The platform seems stable, features A to C functionality OK (except scenarios for remote customer) and we are not yet sure about the scalability to the smallest configuration; feature D testing just started, but the initial estimate is for problems in performance with parallel access scenarios and security."*
- Which gives better basis for decision making?

NOKIA

References

- [AML99]
  Ståhle Amland: *Risk-Based Testing and Metrics*
  EuroSTAR99 Proceedings, 1999.
  http://www.amland.no/articles
- [Bach99]
  James Bach:
  James Bach on Risk-Based Testing
  Software Testing and Quality Engineering, Nov/Dec 1999.
- [Gilb00]
  Tom Gilb: *Competitive Engineering*
  Unpublished book manuscript, available free at http://www.result-planning.com
- [Hetzel88]
  Bill Hetzel:
  The Complete Guide to Software Testing
  John Wiley & Sons, 1988.
- [KAN2001]
  Cem Kaner, James Bach, Bret Pettichord:
  Lessons learned in Software Testing
  Wiley, 2001.
- [PFL2000]
  Shari Lawrence Pfleeger: *Risky Business: What we have yet to learn about SW risk management*
  Journal of Systems and Software, 11/2000.
- [SWEBOK]
  Guide to the SW Engineering Book Of Knowledge, version 0.95
  http://www.swebok.org/
- [TMAP01]
  Martin Pol, Ruud Teunissen, Erik van Veenendaal: *Software Testing – A Guide to the TMAP Approach*
  Addison-Wesley, 2001.
- [TPI99]
  Tim Koomen & Martin Pol:
  Test Process Improvement
  Addison-Wesley, 1999.
  (http://www.iquip.nl/tpi)

NOKIA