

# Risk and Testing

- It is not possible to talk about test management without first looking at risk and how it affects the fundamental test process.
- If there were no risk of ***adverse*** future events in software or hardware development then there would be no need for testing. In other words, if defects did not exist then neither would testing.

# Risk and Testing

- Risk can be defined as the chance of an event, hazard, threat or situation occurring and its undesirable consequences:

***Risk*** – a factor that could result in future negative consequences, usually expressed as impact and likelihood.

In a project a test leader will use risk in two different ways: project risks and product risks.

In both instances the calculation of the risk will be:

**Level of risk** = probability of the risk occurring × impact if it did happen

# Risk-based testing

- One metaphor sometimes used to help people understand **risk-based testing** is that **testing is a form of insurance**. In your daily life, you buy insurance when you are **worried about some potential risk**. You **don't buy insurance for risks that you are not worried about**. So, we should test the areas and test for bugs that are worrisome and ignore the ones that aren't.

# Risk Management

Risk management includes three primary activities:

- **Risk identification**, figuring out what the different project and quality risks are for the project
- **Risk analysis**, assessing the level of risk—typically based on likelihood (Çì ∞ Ò) °ì ®™~™®) and impact—for each identified risk item
- **Risk mitigation** (®∞ òó≥™™), which is really more properly called “risk control”

# Two Main Types of Risks

- Product Risks
- Project Risks



# Project Risks

- Whilst managing the testing project a test leader will use project risks to manage the capability to deliver.
- Project risks include:
  - Supplier issues:
    - Failure of third party to deliver on time or at all.
    - Contractual issues, such as meeting acceptance criteria.

# Project Risks

- Organizational factors:
  - Skills, training and staff shortages.
  - Personal issues.
  - Political issues, such as problems that stop testers communicating their needs and test results.
  - Failure by the team to follow up on information found in testing and reviews (e.g. not improving development and testing practices).
  - Improper attitude toward or expectations of testing (e.g. not appreciating the value of finding defects during testing).



# Project Risks

- Technical issues:
  - Problems in defining the right requirements.
  - The extent that requirements can be met given existing project constraints.
  - Test environment not ready on time.
  - Late data conversion, migration planning and development and testing data conversion/migration tools.
  - Low quality of the design, code, configuration data, test data and tests.

For each risk identified a probability (chance of the risk being realised) and impact (what will happen if the risk is realised) should be identified as well as the identification and management of any mitigating actions (actions aimed at reducing the probability of a risk occurring, or reducing the impact of the risk if it did occur) should be identified.

# Project Risk Example

So, for example if there was a risk identified **that the third-party supplier may be made bankrupt during the development**, the test manager would review the supplier's accounts and might decide that the **probability of this is medium** (3 on a scale of 1 to 5, 1 being a high risk and 5 a low one). **The impact on the project**

if this did happen would be very high (1 using the same scale). The level of risk is therefore  $3 \times 1 = 3$ . Thus, the lower the number, the more the risk. With 3 being in the medium risk area the test leader would now have to consider what mitigating actions to take to try to stop the risk becoming a reality.

# Product Risks

- When planning and defining tests a test leader or tester using a risk-based testing approach will be managing product risks.
- Potential failure areas (adverse future events or hazards) in software are known as product risks, as they are a risk to the quality of the product. In other words, the potential of a defect occurring in the live environment is a product risk.

# Product Risks

- Examples of product risks are:
  - The potential that a defect in the software/hardware could cause harm to an individual or company.
  - Poor software characteristics (e.g. functionality, security, reliability, usability, performance).
  - Poor data integrity and quality (e.g. data migration issues, data conversion problems, data transport problems, violation of data standards).
  - Software that does not perform its intended functions.

# Product Risks

- Risks are used to decide where to start testing in software development life cycle, e.g. the risk of poor requirements could be mitigated by the use of formal reviews as soon as the requirements have been documented and the start of the project.
- Product risks also provide information enabling decisions regarding how much testing should be carried out on specific component or systems, e.g. the more risk there is, the more detailed and comprehensive the testing may be.



# Product Risks

- Mitigating product risks may also involve non-test activities.

For example, in the poor requirements situation, a better and more efficient solution may be simply to replace the analyst who is writing the poor requirements in the first place. Or, provide trainings to the team.



# Product Risks

- In a risk-based approach the risks identified:
  - Will determine the test techniques to be employed, and/or the extent of testing to be carried out.
  - Prioritize testing in an attempt to find the critical defects as early as possible.
  - Will determine any non-test activities that could be employed to reduce risk.
- Risk-based testing draws on the collective knowledge and insights of the project stakeholders, testers, designers, technical architects, business reps and anyone with knowledge of the solution to determine the risks and the levels of testing to address those risks.

# Risk Identification

- Expert interviews
- Independent assessments
- Use of risk templates
- Project retrospectives
- Risk workshops and brainstorming
- Checklists
- Calling on past experience

## RISK BASED TESTING A STEP BY STEP GUIDE

- 1 IDENTIFY THE S/W  
YOU WANT TESTED

I WANT  
THAT ONE



- 2 IMAGINE SITUATIONS  
WHERE THERE MIGHT  
BE DAMAGE TO THE S/W



- 3 ANALYSE THE IMPACT  
OF THE RISK OCCURING



- 4 ANALYSE THE LIKELYHOOD  
OF THE RISK OCCURING



- 5 EXECUTE A TEST TO CONFIRM  
THE RISK IS CREDIBLE



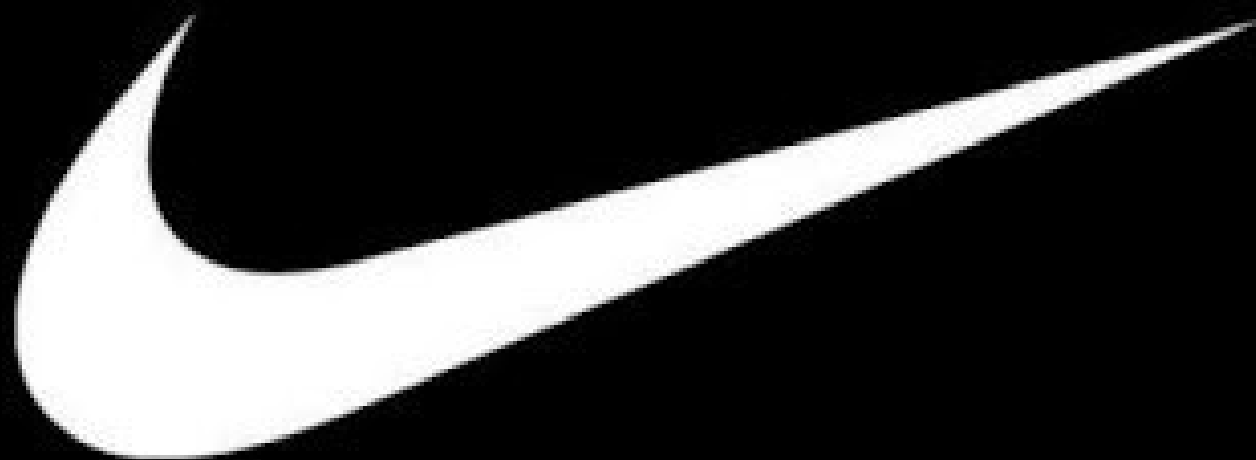
- 6 MITIGATE THE RISK



NOTE: NO ANIMALS WERE HARMED IN THE MAKING OF THIS CARTOON

Andy Glover [cartoontester.blogspot.com](http://cartoontester.blogspot.com) Copyright 2010

AG



**JUST TEST IT.**