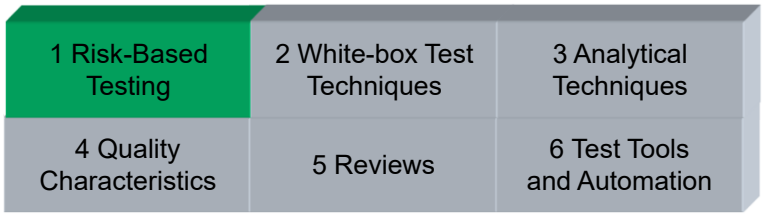
ISTQB® Advanced level Technical Test Analyst

The Technical Test Analyst's Tasks in Risk-Based Testing



1.1

Contents

1.2

1.1 What is risk?

- risk is the possibility of an undesired outcome
  - if it occurs will decrease customer, user, participant or stakeholder perceptions of product quality or project success
- two types of risk

  - project risk (planning risks)
    - ► the primary effect of the potential problem relates to the project success

  - product risk (quality risks)
    - ► the primary effect of the potential problem is on product quality
- risks can be prioritised by considering two aspects:
  - the likelihood of the problem occurring
  - the impact of the problem should it occur

} = **risk level**

Explosion risk

1.3

1.1 Examples of product and project risks

Project risks

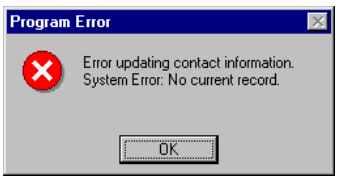
management issues

- test environment might not be ready when needed
- test staff might not be available when needed
- development might slip in handing software to testing
- testing standards, rules and techniques might not be in place when needed
- requirements might change

Product risks

testing issues

- users might not be able to pay by credit card
- overnight batch run might not finish in the time specified
- invoices might be calculated incorrectly
- system might not sustain 20 concurrent users



1.4

1.1 Risk-based testing

- Test Manager has overall responsibility
- TTA actively involved in all risk management activities
  - risk identification
  - risk assessment
  - risk mitigation

Explosion risk

- performed iteratively throughout the project
  - handle emerging product risks and changing priorities
  - regularly re-evaluate and communicate risk status

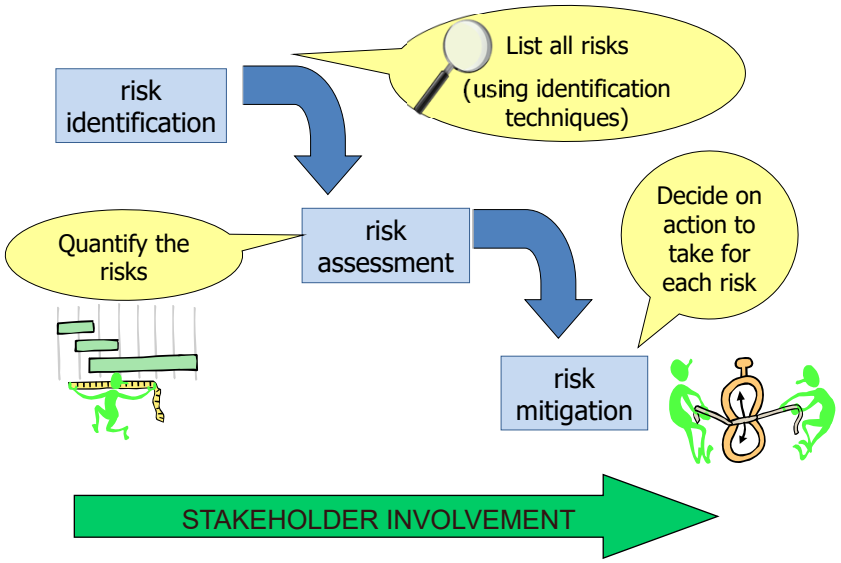
- TTAs focus on technical risks:
  - security
  - reliability
  - performance
  - maintainability
  - portability
  - compatibility

1.5

Contents

1.6

1.2 Tasks of risk-based testing



1.7

Contents

1.8

1.2.1 Risk identification

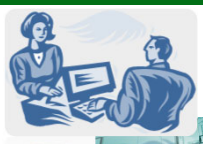
- involving broadest sample of stakeholders
  - most likely to identify largest number of significant risks
- Technical Test Analysts (TTA) well-suited for:
  - conducting expert interviews
  - brainstorming with co-workers
  - analysing current and past experiences
  - working closely with technical peers
    - ► e.g. developers, architects, operations engineers

- types of risk of particular concern to TTA
  - performance (e.g. response times may be too slow at peak loads)
  - security (e.g. system may be hacked by web user)
  - reliability (e.g. system may not meet SLA availability goals)

1.9

1.2.1 Who are the stakeholders?

- business perspective
  - users/customers, test analysts, training, support
- technical perspective
  - development, architects, DBA's
  - technical test analysts / test analysts
- financial perspective
  - senior management, sales/marketing, CEO



- what if you cannot get all the users involved
  - e.g. mass market software development?
  - use a sample of potential users
    - ► surrogate for entire customer base

1.10

1.2.1 Typical technical risk areas

- related to ISO25010 non-functional quality characteristics (see 4)
- Performance efficiency
  - slow online response, or overnight batch takes too long
- Security
  - vulnerability to malware or theft of data
- Reliability
  - inability to restore service within the required time after an outage
- Maintainability
  - the application takes too long to modify
- Portability
  - the application cannot be installed / uninstalled correctly
- Compatibility
  - resource conflicts with other systems running in the same environment

1.11

1.2.1 Typical technical risks

Generic project risks

- Conflict between stakeholders re. technical requirements
- Communication problems from geographical distribution of the development organisation
- Tools and technology
  - and skill levels of in team
- Time, resource and management pressure
- Lack of earlier QA
  - e.g., few or no design reviews
- High change rate of technical requirements

Generic product risks

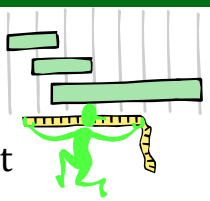
- Complexity of technology
- Complexity of code structure
- Amount of code re-use vs. newly written code
- Large number of defects found relating to technical quality characteristics in previous projects
- Technical interface and integration issues

1.12

Contents

1.13

1.2.2 Risk assessment

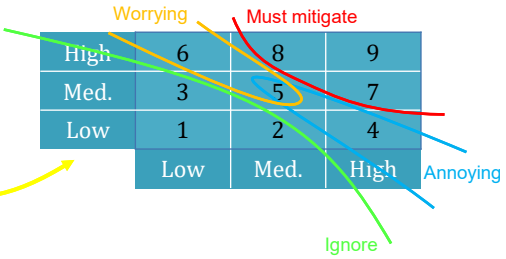


- assessing the identified risks to categorise and determine likelihood and impact
- risk level is combination of likelihood & impact
  - 'risk exposure' if can be quantified
  - used to prioritise risks
- TTA finds and understands the technical risks
  - determines their likelihood
- TA contributes knowledge of potential business impact
- TTA establishes risk levels as defined by Test Manager
  - usually qualitative values
  - scale of 1 to 9, or Critical / High / Medium / Low

1.14

1.2.2 Specifying risk levels

- qualitative way
  - very high, high, medium, low, very low
  - numbered rating (score 1-10)
  - risk level given by table
- quantitative way
  - e.g. 72% chance of happening, impact of €500,000
    - ► insurance companies use this to calculate premiums
    - ► rarely do we have such figures in testing
  - risk exposure = probability * impact = 72% * €500,000 = €360,000



Some risk-based testing approaches do not combine probability and impact. This allows technical and business risks to be addressed separately.

1.15

Contents

1.16

1.2.3 Risk mitigation

- TTAs influence how testing deals with identified risks
  - reduce risk
    - ►execute tests designed to reveal the potential problems
      - – most important (highest risk) ones first
    - ►other mitigation or contingency actions per test plan
      - – e.g. reviews and static analysis
  - evaluate risks based on additional information from testing
    - ►if uncertain about risk likelihood, run some exploratory tests to see how buggy it is
  - work with specialists in areas such security and performance





1.17

Summary: key points

- risk level and risk types
  - risk level is likelihood and impact; product risks, project risks
- responsibilities
  - Test Manager has overall responsibility
  - Technical Test Analyst focused on technical risks (ISO25010)
    - ► security, reliability, performance, reliability, maintainability, compatibility
- risk identification
  - TTA well-suited for expert interviews, brainstorming, analysing experiences and working with technical peers
- risk assessment
  - specifying risks qualitatively (most common) or quantitatively

- risk mitigation actions
  - dynamic testing for identified risks, choice of test techniques, static testing, regression testing, use of most experienced people
  - use of testing to evaluate risk

1.18

Session 1

The Technical Test Analyst's Tasks in Risk-Based Testing

From the ISTQB Glossary

freedom from risk: The degree to which a component or system mitigates the potential risk to economic status, living things, health, or the environment.

project risk: A risk impacting the quality of a product.

product risk: A risk that impacts product success.

quality risk: A product risk related to a quality characteristic.

risk: A factor that could result in future negative consequences.

risk analysis: The overall process of identification and assessment.

risk assessment: The process to examine identified risks and determine the risk level.

risk identification: The process of finding, recognising and describing risks.

risk level: The estimated probability that a risk will become an actual outcome or event.

risk likelihood: The qualitative or quantitative measure of a risk defined by impact and likelihood.

risk management: The process for handling risks.

risk mitigation: The process through which decisions are reached and protective measures are implemented for reducing or maintaining risks to specified levels.

risk type: A set of risks grouped by one or more common factors.

risk-based testing: Testing in which the management, selection, prioritization, and use of testing activities and resources are based on corresponding risk types and risk levels.

1.1 Introduction

What is risk?

Risk is the possibility of an undesired outcome. Risk exists whenever some problem may occur that would decrease stakeholder (customer, user, participant) perceptions of product quality or project success.

Product and project risks

Where the primary effect of the potential problem is on product quality, potential problems are called product risks. Examples are defects that could cause a system to fail during normal operation. Where the primary effect of the potential problem is on project success, that potential problem is called a project (or planning) risk. An example is a possible staffing shortage that could delay completion of a project.

Product risks vs. Quality risks

These two terms used to be synonymous but the Glossary now defines a quality risk as "A product risk related to a quality characteristic.". Presumably, this specifically refers to non-functional quality characteristics; according to ISO25010 (see later), Functionality is also a quality characteristic, but if this were included in the ISTQB's definition of quality risk then they would still be synonymous.

This loose usage of the term "quality characteristic", when it seems that specifically only the non-functional quality characteristics is meant, is common in ISTQB syllabi.

The easiest way to understand which risks are predominantly product or project is to ascertain whether testing can help reduce the risk. If testing cannot help then it is usually a project risk and these are addressed by project managers or test managers. The example of possible staffing shortage can be addressed by identifying potential external resource so should we have a shortage internally they will employ outside staff.

Not all risks are of equal concern. The level of risk is influenced by two different factors:

- the likelihood of the problem occurring; and
- the impact of the problem should it occur.

We need to quantify each of these factors in some way and then combine them to give us a single 'risk level' measure in order to determine the priority of one risk relative to another. Combining these two factors to obtain a single risk level measure is optional. (More on this later when we discuss risk assessment).

Risk management

Risk Management can be thought of as consisting of three primary tasks:

- Risk Identification
- Risk Assessment
- Risk Mitigation (also referred to as risk control)

These tasks are in some senses sequential, but the need for continuous risk management means that, during most of the project, all three of these risk management activities should be used iteratively.

Risk-based testing

Test Managers have overall responsibility for risk-based testing. They should define the testing strategy to specify the activities that are to be performed and define the responsibilities of the team members. Once implemented, the Test Managers should manage the testing to ensure that the risk management activities are carried out iteratively as necessary.

Technical Test Analysts will be involved in each of the risk management activities. They will work within the risk-based testing framework established by the Test Manager, contributing their particular expertise to identify risks of a technical nature, assess the likelihood of those

risks and suggest and implement mitigation activities. Note the distinction made in the ISTQB's model of testing between the (non-technical) Test Analyst (TA) and the Technical Test Analyst (TTA):

- the TA role is primarily business-facing; s/he is expected to understand the business, what it needs and how the users / customers expect to use their systems, and will take a (mostly) black-box and functional approach to testing.
- the TTA role is more concerned with the details of system architecture and implementation and with those aspects of quality that are more technical in nature.

1.2 Risk-based Testing Tasks

Learning Objectives

TTA-1.2.1 (K2) Summarize the generic risk factors that the Technical Test Analyst typically needs to consider

TTA-1.2.2 (K2) Summarize the activities of the Technical Test Analyst within a risk-based approach for testing activities

1.2.1 Risk Identification

To be most effective, risk management should involve all stakeholders of the project. Often this will not be possible, so a pragmatic compromise has to be achieved. The goal must be to involve the broadest possible sample of stakeholders, as this will most likely help achieve the identification of the largest number of significant risks.

Sometimes project realities result in some stakeholders acting as surrogates for others. For example, a developer of mass market software (such as Microsoft) may ask a small sample of potential customers to help identify potential defects that would impact their use of software most heavily. In this case the sample of potential customers serves as a surrogate for the entire eventual customer base.

Who are the stakeholders?

The stakeholders of a project are typically many and varied. Anyone who has an interest in the outcome of a project is a stakeholder. We can list some groups of stakeholders based on their perspective on the project.

- business – users / customers, test analysts, training staff, support staff
- technical – developers, architects, designers, technical test analysts
- financial – senior management, sales and marketing, CEO

Risk identification techniques

There are many risk identification techniques and which ones are used will usually be governed by the test strategy. However, because of their technical skills, Technical Test Analysts are well suited for the following risk identification techniques:

- conducting expert interviews
- brainstorming with co-workers
- analysing current and past experiences
- working closely with technical peers

Typical technical risks

Risks that might be identified by the Technical Test Analyst are typically related to the ISO25010 non-functional quality characteristics listed in Chapter 4:

- Performance efficiency (e.g. inadequate online response or batch throughput)
- Security (e.g. denial of service attacks)
- Reliability (e.g. inability to restore service within the required time after an outage)
- Maintainability (e.g. the application takes too long to modify)

- Portability (e.g. the application cannot be installed correctly)
- Compatibility (e.g. resource conflicts with other systems running in the same environment)

1.2.2 Risk Assessment

Risk assessment is the activity in which we consider each risk individually to determine the likelihood of the risk maturing (i.e. the potential problem occurring) and the impact of the problem should it occur. In making this assessment we assign one value to the likelihood and another value to the impact.

Technical Test Analysts are expected to use their particular skills to identifying the technical risks and helping to determine their likelihood. Test Analysts can contribute by determining the potential business impact of these risks.

Technical project risks

Typically, the following generic project risks should be considered; these may affect the project's ability to deliver according to expectations.

- Conflict between stakeholders regarding technical requirements.
- Communication problems resulting from the geographical distribution of the development organisation.
- Tools and technology, and the skill levels of those who will use them.
- Time, resource and management pressure.
- Lack of earlier quality assurance (e.g., few or no design reviews).
- High change rate of technical requirements.

Technical product risks

The following generic product risks should be also considered, because they may lead to defects.

- Complexity of technology.
- Complexity of code structure.
- Amount of code re-use compared to newly written code.
- Large number of defects found relating to technical quality characteristics in previous projects.
- Technical interface and integration issues.

These lists are not exhaustive.

Determining the risk level

The values assigned may be either quantitative or qualitative. Quantitative measures assign specific values such as 80% likelihood and €5,000 for impact. Such values are usually not available and are impossible to estimate with any degree of (justified) confidence.

Qualitative values are most common because these are not precise measures but broad categories such as high, medium and low. It is often easier to gain a consensus amongst a group of people that a given risk is, for example, high rather than medium than it is to gain agreement about a more specific quantifiable measure.

Having two measures for each risk makes it more difficult to prioritise them, so we combine them into one measure called the risk level (known as risk exposure if quantitative values are being used). We can then use this risk level to prioritise the risks so we know which ones we have to do something about (the highest level risks) and which ones we can safely ignore (the lowest level risks). The action to take on the risks in the middle of the risk level range may not be so easily decided!

For quantified measures of likelihood and impact, the risk level is given by the product of the two figures. For example, a likelihood of 30% and an impact of €10,000 gives a risk level of 30% * €10,000 = €3,000.

Risk management is very important for the insurance industry because insurance companies take over risks from customers. Insurers consider every available quantifiable factor to develop profiles of high and low insurance risk. The level of risk determines insurance premiums. Generally, insurance policies involving factors with greater risk of claims are charged at a higher rate. With much information at hand, insurers can evaluate the risk level of insurance policies at much higher accuracy. To this end, insurers collect a vast amount of information about policy holders and insured objects. Statistical methods and tools based on data mining techniques can be used to analyse and determine insurance policy risk levels.

Quantitative analysis is used in Insurance because they have a lot of historic data. Typically risk-based testing relies on qualitative analyses because it is very difficult to accurately measure probability and impact for new software systems.

For qualitative measures of likelihood and impact we typically use terms such as high, medium and low. To combine the likelihood and impact, so that we end up with a single risk level measure for each risk, we may use a table like the one below.

Impact	Severe	**6**	**8**	**9**
	Moderate	**3**	**5**	**7**
	Minor	**1**	**2**	**4**
		Low	Medium	High
		Probability		

For example, a risk of medium probability with severe impact has a risk level of 8. A risk with low probability and moderate impact has a risk level of 3, and so on. Of course the table can be extended to allow for more impact and/or probability values. Note that this table assigns unique values for risk level to each combination of impact and probability. Minor/low scores the lowest risk level of 1 and severe/high scores the highest risk level of 9. The other values are arranged such that the value of impact takes precedence over the value for probability (i.e. a moderate impact and low probability scores 3, whereas a minor impact and medium probability scores 2).

Different schemes can be used, for example:

Impact	Severe = 4	**4**	**8**	**12**
	Moderate = 2	**2**	**4**	**6**
	Minor = 1	**1**	**2**	**3**
		Low = 1	Medium = 2	High = 3
		Probability		

This gives us the same risk level value for moderate/medium and severe/low and the higher level risks. There is no right or wrong approach. The purpose is to help us prioritise the risks so providing the stakeholders are comfortable with end results (priorities of risks) then how we arrive at them is perhaps not particularly important.

Qualitative measures may also be expressed using numbers. For example, we can assign a number in the range 1 to 5 for impact and probability where 5 represents the highest impact or probability. These numbers can then be multiplied together to give us a value in the range 1 to 25 for the level of risk. Using numbers in this way does not make it a quantitative measure as the values chosen are still subjective.

Some risk-based testing approaches do not combine the risk values. This allows the test approach to address the technical and business risks separately. PRISMA® is one such approach [vanVeenendaal12].

The approach to measurement should be decided by the Test Manager (TM). Whatever it is, the TTA is expected to propose an initial risk level in accordance with it. This initial value may be modified by the TM when all stakeholder views have been considered.

1.2.3 Risk Mitigation

During a project, TTAs influence how testing helps to deal with identified risks in two ways.

1. Reducing risk ...

   a. by running tests and by running the most important ones (those that address the highest-level risks) first. To reduce the likelihood of performance problems we may undertake more thorough performance testing. To reduce the likelihood of incorrect calculations we may focus more thorough testing on those code modules that implement the calculations, perhaps specifying higher levels of structural coverage for them.

   b. by putting into action other mitigation and contingency measures as stated in the test plan. For example, to reduce the likelihood of requirement and design defects being implemented into the system we may put more emphasis on reviews of the requirement and design specifications by performing them (if they would not have been done otherwise) or improving the review process by allowing more time, involving more people and/or adopting a more rigorous approach.

2. Evaluating risk ...

   a. by dynamic testing. If we are uncertain of the likelihood of product risks, running some tests will help give us a better idea of the likelihood of the frequency of potential failures.

Reducing the impact of an identified risk is not so easily achieved through testing actions but may in some cases be achieved by identifying suitable workarounds for potential failures of the system.

The TTA will often need to work with specialists in areas such security and performance in order to identify risks, assess and mitigate them, and even to define associated elements of the organisation's test strategy.

On a recurring basis throughout the project, testers should re-evaluate outstanding risks based on the new information obtained from the testing done so far. They should use this information and their experience of the software during the testing to identify and assess new risks. Agile teams can do this during each end-of-iteration retrospective; traditional projects should do it at major lifecycle and test level milestones, and whenever significant new information (e.g., a change request) is received.

