ANALYSIS OF IT PROJECTS

RISK MANAGEMENT
TESTING

ELSA ESTEVEZ
Universidad Nacional del Sur
Universidad Nacional de La Plata
CONICET, Argentina

AIM AND AGENDA

AIM

To present main concepts about project risk management and software testing.

AGENDA

1	RISK	How can we manage project risks?
2	TESTING	What does software testing entails?
3	SUMMARY	What was covered in this section?

DEFINITIONS

Project Risk [definition]

Project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, and quality.

Project Risk Management [definition]

Project risk management refers to identifying, analyzing, and responding to risk throughout the life of a project and in the best interests of meeting project objectives.

If we do not actively attack risks, risks will definitely attack us

Tom Gilb

RISK CAUSES AND IMPACTS

A risk may have one or more causes and , if it occurs, it may have one or more impacts.

A cause may be related to a given or potential requirement, assumption , constraint or condition that creates the posibility of negative or positive outcomes.

EXAMPLE	
CAUSE	the need to hiring a foreign expert to work
RISK	the Inmigration Office may take longer than planned to issue the visa
IMPACT	the task assigned to the foreign expert is delayed

KNOWN AND UNKNOWN RISKS

Known risks (known unknowns) are those that have been identified and analyzed, making it possible to plan responses for those risks.

Known risks require a proactive management strategy.

Unknown risks (unknowns unknowns) cannot be managed proactively and therefore may be assigned a reserve.

ATTITUDES TOWARDS RISKS

Organizations perceive risk as the effect of uncertainty on projects and organizational objectives.

Organizations and stakeholders are willing to accept varying degrees of risk depending on their risk attitude.

Risk may be influenced by a number of factors, which are broadly classified into:

Risk appetite	degree of uncertainty an entity is willing to take on in anticipation of a reward
Risk tolerance	degree, amount, or volume of risk that an organization or individual will withstand
Risk threshold	refers to measures along the level of uncertainty or the level of impact at which a stakeholder may have a specific interest. Below that risk threshold, the organization will accept the risk. Above the risk threshold, the organization will not tolerate the risk.

POSITIVE AND NEGATIVE RISKS

Positive risks are commonly referred as opportunities; while negative risks as threats.

Positive risks that offer opportunities within the limits of risk tolerances may be pursued in order to generate enhanced value.

EXAMPLE	
POSITIVE	adopting an aggressive resource optimization technique is a risk taken in anticipation of a reward for using fewer resources
NEGATIVE	the new final product will not be able to satisfy user´s performance requirements

RISK MANAGEMENT

Typical risk management activities include:

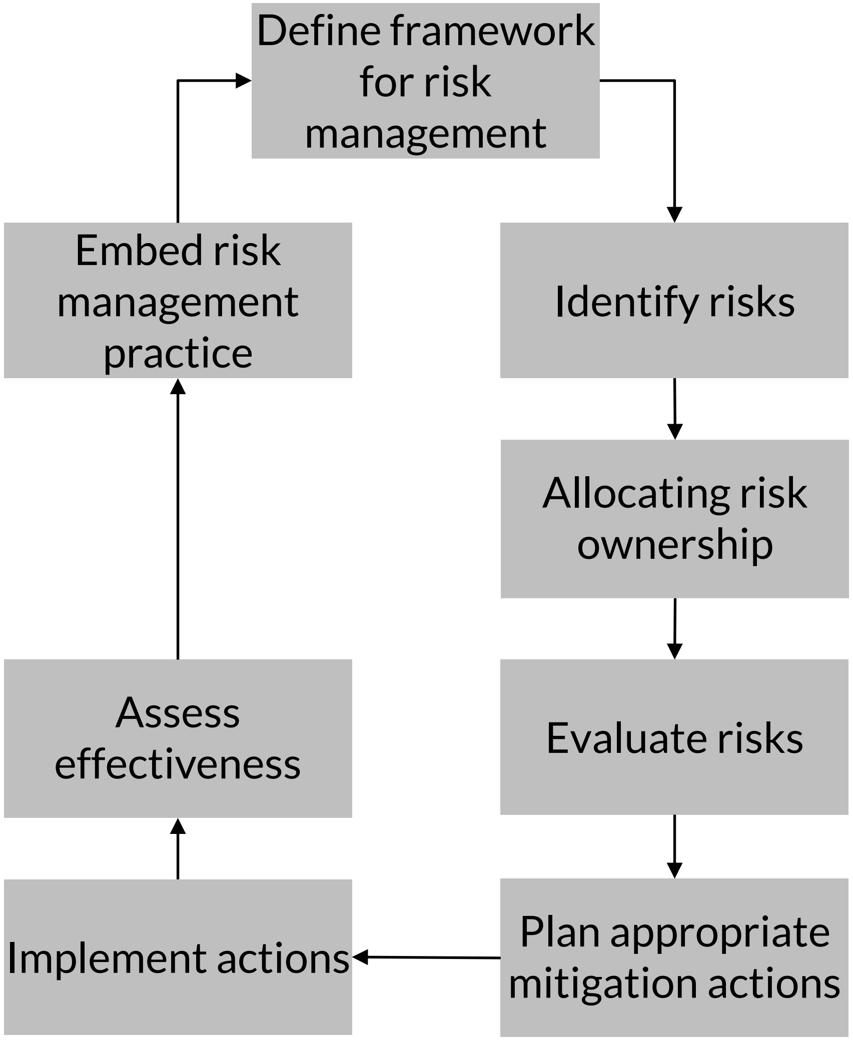
1) Establishing a Risk Management Framework/Strategy
2) Identifying risks
3) Establishing a risk register
4) Allocating risk ownership
5) Evaluating risks
6) Planning mitigation
7) Implementing mitigation actions
8) Assessing effectiveness
9) Embedding risk management

1) RISK MANAGEMENT STRATEGY

The program's framework for risk management is defined and documented in the Risk Management Strategy.

The Risk Management Strategy sets the context in which risks will be identified, analyzed, controlled, monitored and reviewed.

It is important that the approach to managing risk is consistent with the broader 'appetite' for risk within the organization's culture and general work practices.


Define framework for risk management
Identify risks
Allocating risk ownership
Evaluate risks
Plan appropriate mitigation actions
Implement actions
Assess effectiveness
Embed risk management practice

2) IDENTIFYING RISKS

Identifying risks means considering what exactly is at risk, like schedule, resources, delivery of new capability, or realization of benefits.

There are generic and specific risks.

Generic risks are affecting all projects.

Specific risks are those related to the project at hand.

It is unlikely that all possible risks will be identified; as a guideline, a realistic expectation should be to identify the 20% of risks that would have 80% of the potential impact.

For identifying risks, an approach is to use a classification of risks.

RISK CLASSIFICATION (1)

- Strategic level risks – e.g. adverse business decisions
- Programme-level risks – e.g. lack of interest from stakeholders
- Project-level risks – e.g. required expert not available
- Operational level risks – e.g. bad performance of the software system produced

RISK CLASSIFICATION (2)

- Project risks – e.g. threatening the project plan
- Technical risks – e.g. threatening the software quality
- Business risks – e.g. threatening the viability of the system to be produced
- Market risk – e.g. threatening the adoption of the new solution
- Strategic risk – e.g. threatening the fitness of the new product into the business strategy of the company
- Sales risk – e.g. threatening the opportunities for commercializing the new product
- Management risk – e.g. threatening loosing the support of an expert manager due to changes in focus or personnel.
- Budget risk – e.g. threatening loosing the financial resources committed

3) ESTABLISHING A RISK REGISTRY

Risks should be documented in the program's Risk Register, which is the central repository of information about the risks and provides the basis for prioritization, action, control and reporting.

The Risk Register will contain a large volume of information, and it is useful to present an overall picture of the program's risk profile showing how many risks fall into the high-probability, high-impact area.

RISK REGISTRY – CONTENT EXAMPLE

- a unique identifier for each risk
- a description of each risk and how it will affect the project
- an assessment of the likelihood it will occur
- an assessment of the possible seriousness/ impact if it does occur (low, medium, high)
- a grading of each risk
- who is responsible for managing the risk
- an outline of proposed mitigation actions
- in larger projects, costings for each mitigation strategy

RISK REGISTRY – EXAMPLE

Id	Description of Risk	Impact on Project	Likelihood	Seriousness	Grade	Change	Date of Review	Mitigation Actions	Responsibility for mitigation action(s)	Costs	Timeline for mitigation action(s)	WBS
		Describe the nature of the risk and the impact on the project if the risk is not mitigated or managed				Change in grade since the last review	Date of the last review	Specify planned mitigation strategies	Specify who is responsible for undertaking each mitigation action(s)		Specify timeframe for mitigation action(s) to be completed by	This is to indicate that the identified mitigation action has been included in the Work Breakdown Structure (WBS).

Ref: Government of Australia, http://www.egovernment.tas.gov.au/project_management/supporting_resources/templates/medium_to_large_projects/Project_risk_register_template_and_guide.docx

4) ALLOCATING RISK OWNERSHIP

Each identified risk should be allocated to an individual who is best placed (with relevant seniority, authority and responsibility) to monitor it and manage any appropriate mitigation or contingency actions.

In many instances, this ownership will fall to the Program Manager, but the Programme Director and other members of the Sponsoring Group are equally likely to be identified as the most appropriate Risk Owner.

On major or complex programmes, the responsibility for risk management may be assigned to a dedicated Risk Manager role.

5) EVALUATING RISKS

Evaluating each risk involves assessing the probability of its occurrence and the potential impact if it occurs.

It may be useful to set tolerance levels for as many risks as possible to assist with prioritization of management actions.

Actions should be defined such that, if the risk approaches its tolerance level, the risk owner reports the situation to the programme (usually the Programme Manager) and is able to take appropriate action.

EVALUATING RISKS

Id	Description of Risk	Impact on Project	Likelihood	Seriousness	Grade	Change	Date of Review	Mitigation Actions	Responsibility for mitigation action(s)	Costs	Timeline for mitigation action(s)	WBS
		Describe the nature of the risk and the impact on the project if the risk is not mitigated or managed				Change in Grade since last review	Date of last review	Specify planned mitigation strategies	Specify who is responsible for undertaking each mitigation action(s)		Specify timeframe for mitigation action(s) to be completed by	This is to indicate that the identified mitigation action has been included in the Work Breakdown Structure (WBS).

6) PLANNING MITIGATION

Each risk has a range of possible mitigation actions summarized as 'the four Ts':

Transfer	Transfer the risk to the third party best placed to manage it, e.g. by taking out an insurance policy. Some risks, such as reputational risk, cannot be transferred.
Terminate	Terminate the risk by adjusting the programme so that the risk no longer applies, e.g. by removing those activities that would lead to a particular risk.
Tolerate	Tolerate the risk - basically the 'do nothing' option, which means the programme will use existing management arrangements to handle the results of the risk happening. Typically used for 'low-impact' risks. Sometimes, it is as risky as a more proactive response, particularly in an environment of constant change.
Treat	Treat the risk by identifying and implementing mitigating actions that address either the probability or impact of the risk and so contain it at an acceptable level.

7) IMPLEMENTING MITIGATION ACTIONS

Based on the selected mitigation actions, an implementation plan should be defined and implemented.

Risk mitigation planning is the process of developing options and actions to enhance opportunities and reduce threats to project objectives.

Risk mitigation implementation is the process of executing risk mitigation actions.

8) ASSESSING EFFECTIVENESS

The evaluation of the risk management process effectiveness should be conducted throughout the project.

The defined arrangements for risk management and the implementation of mitigation actions should be assessed at appropriate points during the programme, as a minimum at the end of each stage.

The assessment includes tracking identified risks, identifying new risks, and evaluating risk process effectiveness.

8) EMBEDDING RISK MANAGEMENT

Some critical success factors for the effective management of risk	
Nominating individuals with clearly defined responsibilities to support, own and lead the risk management process.	Implementing risk management fully embedded in management processes and consistently applied.
Having a pragmatic risk management approach, and the benefits of following it clearly communicated to all personnel involved with the programme.	Managing risks closely linked to achievement of programme objectives and benefit delivery.
An organizational culture that supports well thought-through risk-taking.	Actively monitoring risks y monitor and regularly reviewing them on a constructive, 'no blame' basis.

AIM AND AGENDA

AIM

To present main concepts about project risk management and software testing.

AGENDA

1	RISK	How can we manage project risks?
2	TESTING	What does software testing entails?
3	SUMMARY	What was covered in this section?

CONCEPTS

Testing a program means running it under controlled conditions, such as to observe its output or results.

CONCEPTS	
Failure	the physical manifestation of a defect It happens when a software component produces an incorrect result or does not perform the correct action.
Fault	a manifestation of an error in software, also known as Defect or Bug.
Error	a mistake made by a software developer (human action)

TESTING – MOTIVATION

The aim of testing is:

- Uncover significant defects in the tested artefact - by causing it to behave incorrectly (e.g., to fail or enter a faulty state) so that these underlying defects can be identified and fixed and the artefact can be improved.
- Provide Evidence that the tested artefact can be used to determine:
  - ✓ Quality
  - ✓ Fitness for purpose
  - ✓ Readiness for shipping, deployment, or being placed into operation
- Support Process Improvement by helping to identify:
  - ✓ Development processes that introduce defects
  - ✓ Testing processes that fail to uncover defects
- Prevent Defects by:
  - ✓ Testing executable requirements, architecture, and design models so that defects in the models are fixed before they can result in defects in the system/software.

Ref: https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_447300.pdf

TESTING – LIMITATIONS

- Cannot be exhaustive

- Cannot uncover all defects because different types of testing:
  - ✓ Have different defect removal efficiencies
  - ✓ Uncover different types of defects

- May provide false positive and false negative results due to:
  - ✓ Defects in the test case
  - ✓ Defects in the test environment
  - ✓ Poor configuration management of the tested artefact, the test environment, and the test case

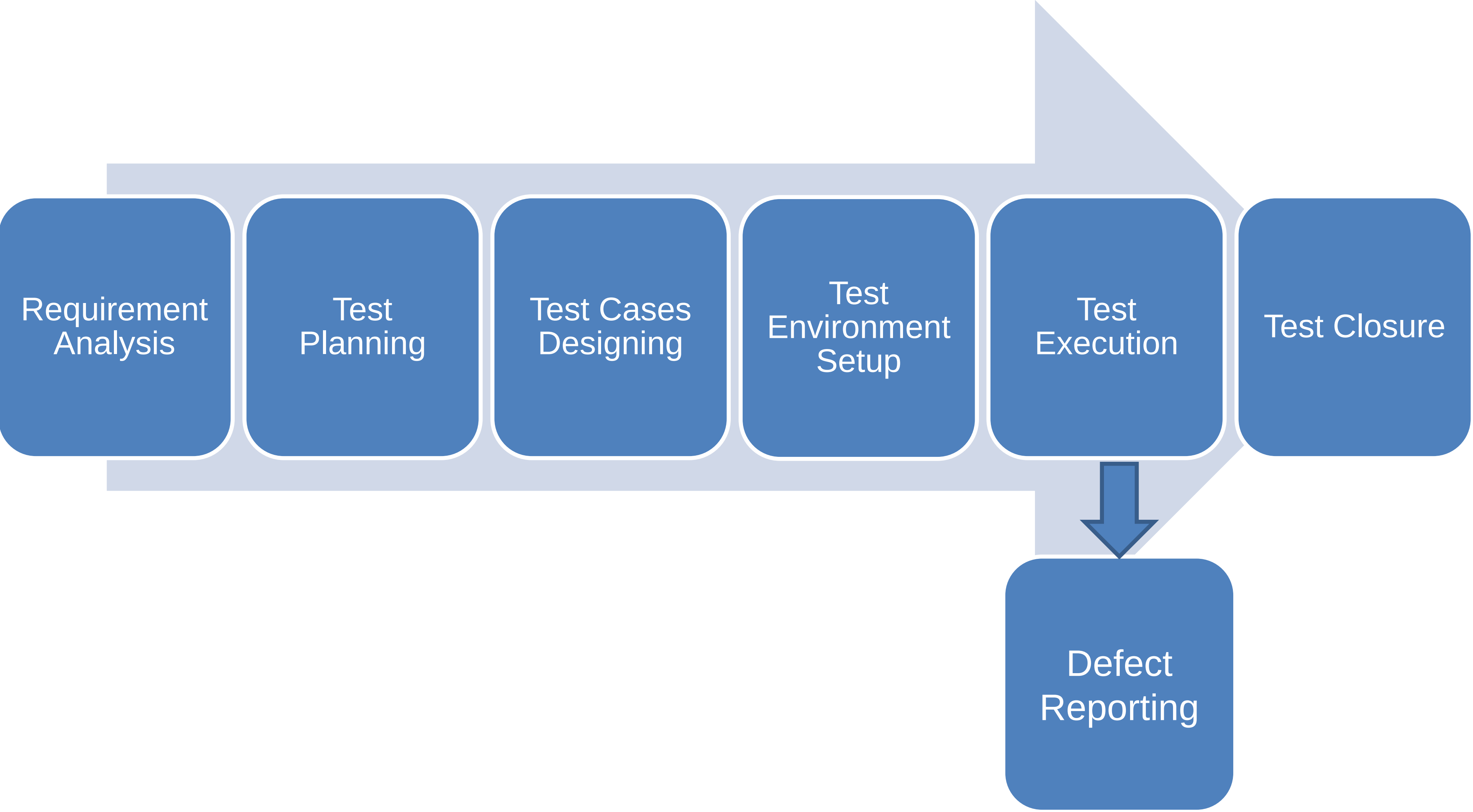
- Cannot prove that the tested artefact works properly under all inputs and conditions

Ref: https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_447300.pdf

TYPES OF TESTING

Unit Testing	Testing individual units/ components of a software The aim is to validate that each unit of the software performs as designed
Integration Testing	Testing as a group individual units that have been combined The aim is to expose faults in the interaction between integrated units.
System Testing	Testing a complete and integrated software The aim is to evaluate the system's compliance with the specified requirements.
Acceptance Testing	Testing a system for acceptability. The aim is to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.

TESTING PROCESS


Requirement Analysis

Test Planning

Test Cases Designing

Test Environment Setup

Test Execution

Test Closure

Defect Reporting

AIM AND AGENDA

AIM

To present main concepts about project risk management and software testing.

AGENDA

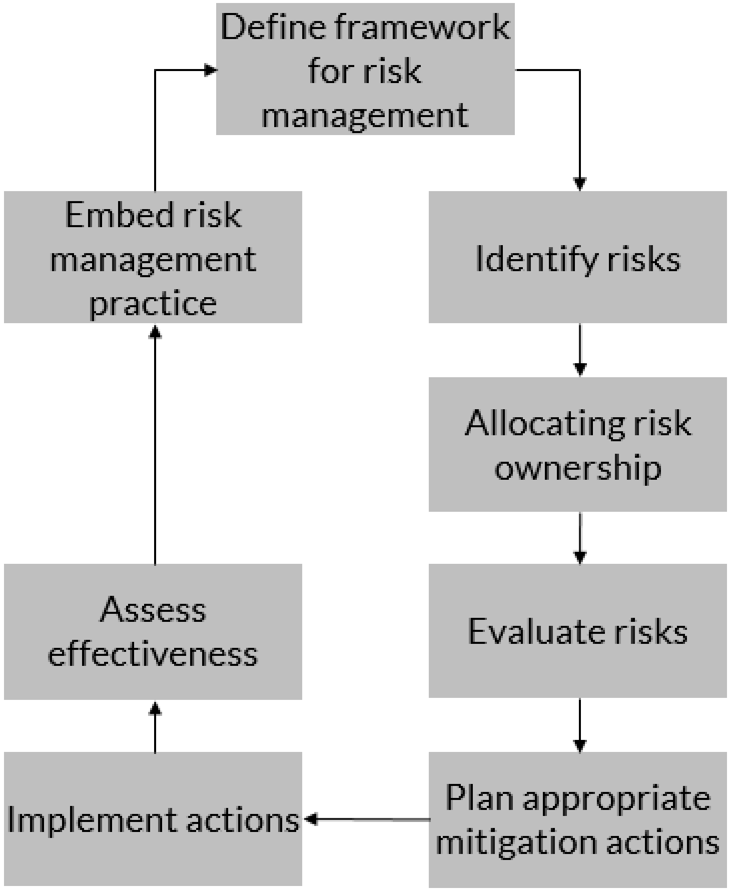
1	RISK	How can we manage project risks?
2	TESTING	What does software testing entails?
3	SUMMARY	What was covered in this section?

SUMMARY – RISK MANAGEMENT

Project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, and quality.

Project risk management refers to identifying, analyzing, and responding to risk throughout the life of a project and in the best interests of meeting project objectives.

Risk Management Process



Define framework for risk management
Identify risks
Allocating risk ownership
Evaluate risks
Plan appropriate mitigation actions
Implement actions
Assess effectiveness
Embed risk management practice

SUMMARY – RISK MITIGATION ACTIONS

Risks with high probability and high impact should be managed.

Each risk has a range of possible mitigation actions summarized as 'the four Ts':

Transfer	Transfer the risk to the third party best placed to manage it.
Terminate	Terminate the risk by adjusting the programme so that the risk no longer applies.
Tolerate	Tolerate the risk - basically the 'do nothing' option. Typically used for 'low-impact' risks.
Treat	Treat the risk by identifying and implementing mitigating actions that address either the probability or impact of the risk and so contain it at an acceptable level.

SUMMARY – TESTING

Testing a program means running it under controlled conditions, such as to observe its output or results.

Failure	the physical manifestation of a defect It happens when a software component produces an incorrect result or does not perform the correct action.
Fault	a manifestation of an error in software, also known as Defect or Bug.
Error	a mistake made by a software developer (human action)

Software Testing Process:

- Requirement Analysis
- Test planning
- Test cases designing
- Test environment setup
- Test execution -> Defect reporting
- Test closure

BIBLIOGRAPHY

REFERENCES

- Identifying and Managing Project Risks – Essential tools for failure-proofing your project, Tom Kendrick, AMACOM, third edition, 2015, ISBN-13 978-0814436080

- Foundations of Software Testin – ISTQB Certification, Rex Black, Erick van Veenendaal, Dorothy Graham, Cengage Learning, ISBN 978-1408044056

ONLINE RESOURCE

- Project Risk Management Handbook: A Scalable Approach, Risk Management Task Group, Clatrans, 2012, http://www.dot.ca.gov/projmgmt/documents/Project_Risk_Management_Handbook.pdf
- Software Testing Fundamentals—Concepts, Roles, and Terminology John E. Bentley, Wachovia Bank, Charlotte NC, paper 141-30, http://www2.sas.com/proceedings/sugi30/141-30.pdf

Many thanks!

Elsa Estevez

ecestevez@gmail.com