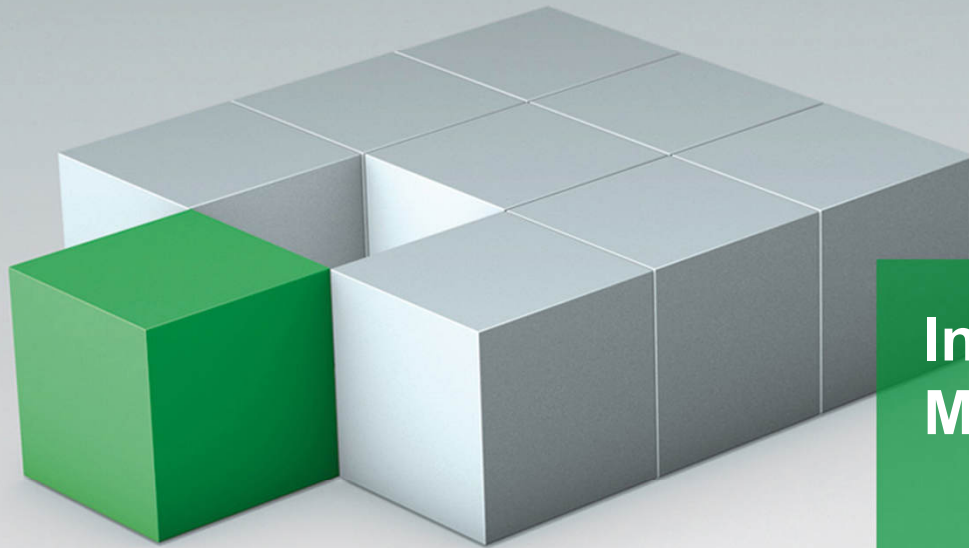SQS. Excellence through Independence

# Integrating Test and Risk Management

**Dr. Daniel Simon**, Dr. Frank Simon
SQS Research
03 September 2012, QUATIC Lisbon

SQS Software Quality Systems AG

# Agenda

## Introduction

- About SQS

- TIMBUS context / Overall motivation

## TM and RM

- What is TM?

- What is RM / ERM?

## Integration of TM and RM

- Use Cases / Examples

## Summary

## SQS Group

## At a glance: SQS is the leader in independent software testing and quality management services.

» *The global leader in independent software testing and quality management services – majority of its business in Europe* «

Financial Times, 21 August 2007

- Almost 30 years of prosperous operations

- Over 5,000 completed projects

- The customer base includes 36 FTSE-100 companies, half of the DAX 30 companies and nearly a third of the STOXX-50 companies

- The SQS philosophy is **to increase success and efficiency of IT projects by using efficient solutions**
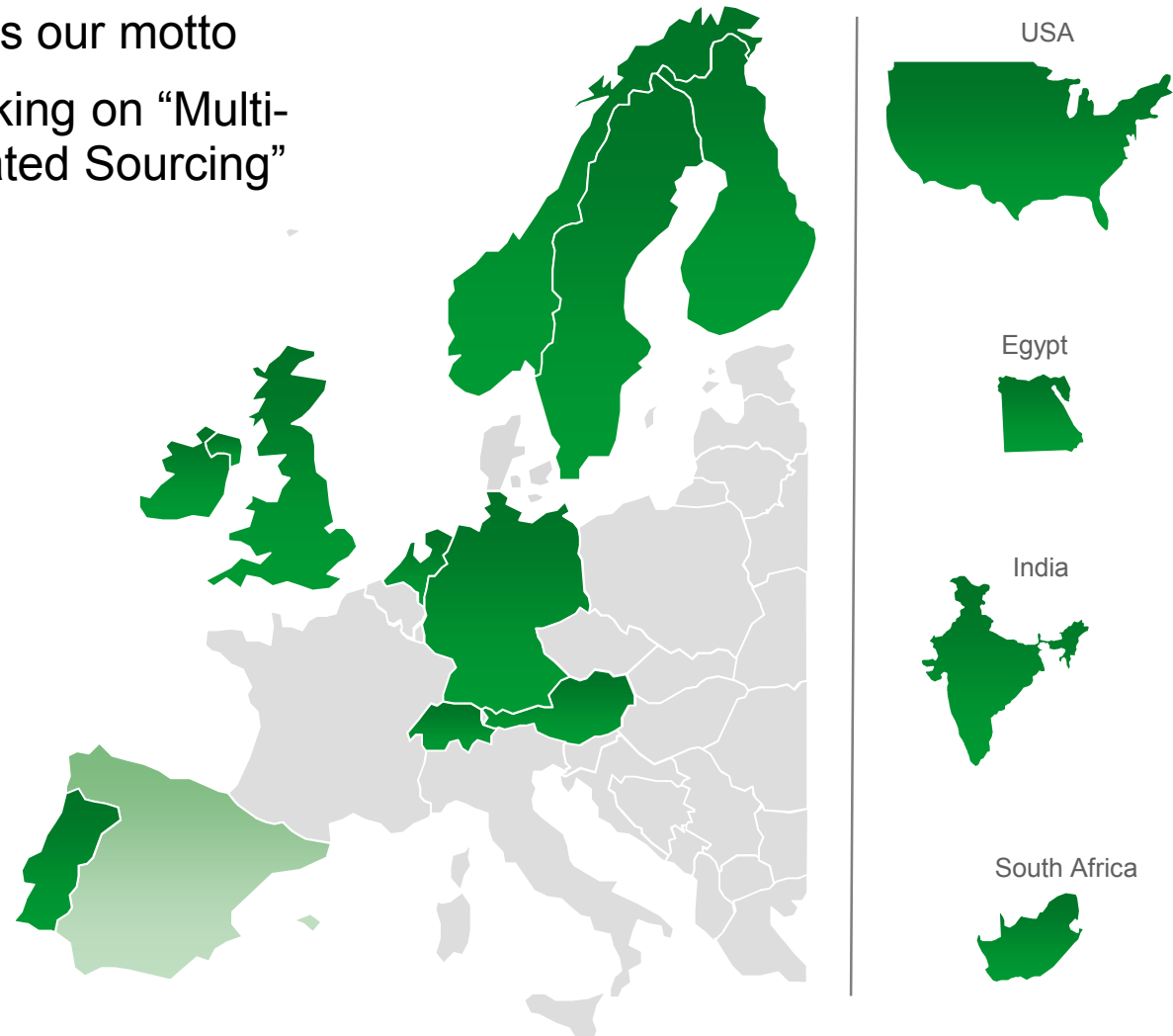
SQS is listed on the AIM London

# SQS is represented throughout the world
## Wherever our clients are located.

- "Follow the customers" is our motto

- for Offshore we are working on "Multi-language Customer-related Sourcing" (MLCS) strategy

**Locations**
- Austria
- Germany
- Egypt
- Finland
- India
- Ireland
- Netherlands
- Norway
- Portugal

- South Africa
- Sweden
- Switzerland
- United Kingdom
- USA

**Partnership**
- Spain

USA

Egypt

India

South Africa

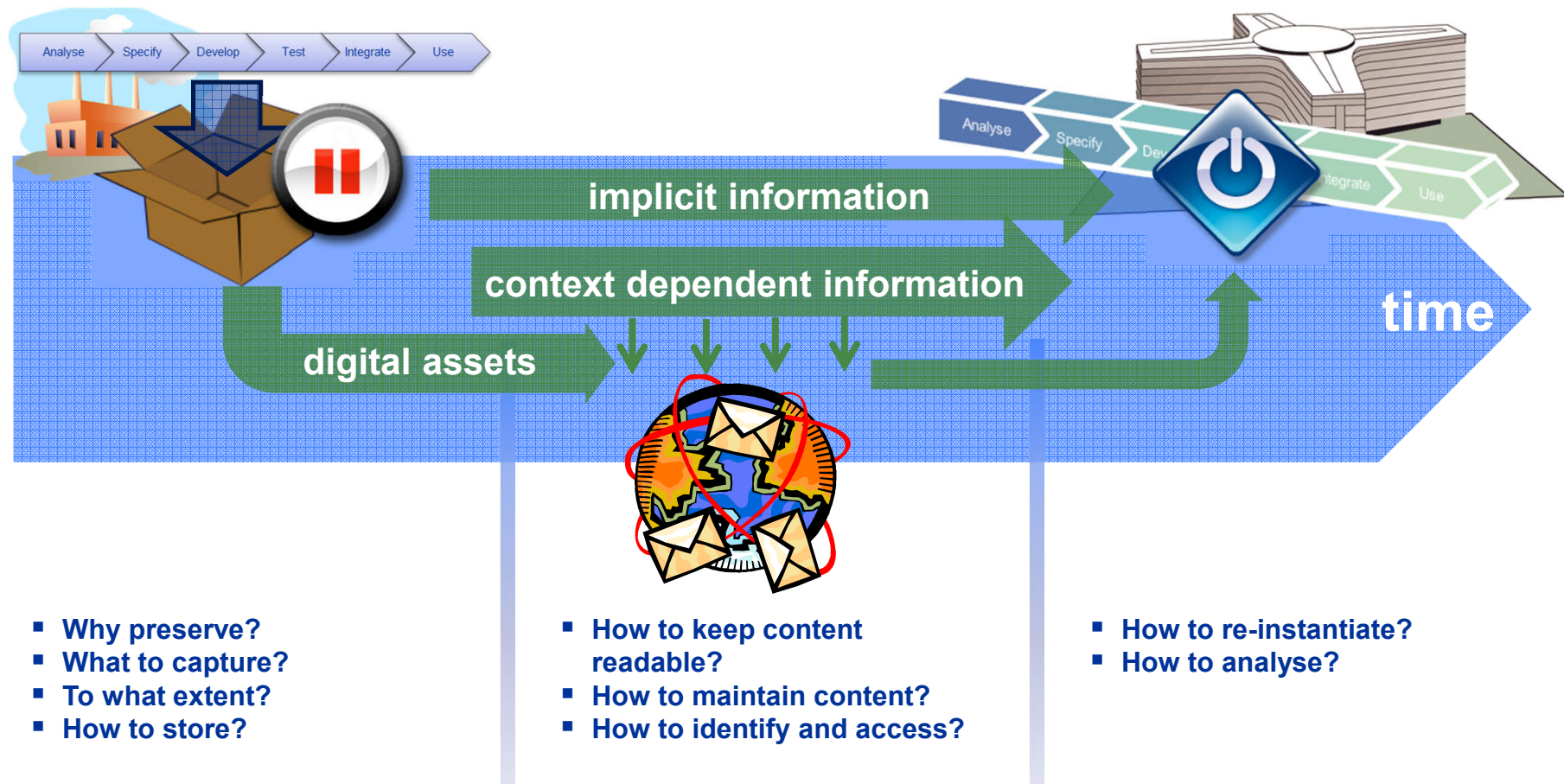# EC funded TIMBUS goes the next mile for Digital Preservation:  Facts

- Title:     "Digital Preservation for Timeless Business Processes and services"

- Ref.No.:   269940

- Duration:  April 2010 to March 2013

- Funding:   8M€ funding by 7th Framework Programme (FP7) of EC

- Consortium:

| CMS | DPC | INESC-ID | Intel |
|---|---|---|---|
| Caixa Mágica | DigitalPreservationCoalition | inesc id lisboa | intel |
| **iPharro** | **KIT** | **LIP** | **LNEC** |
| iPharro | KIT Karlsruher Institut für Technologie | LIP | LNEC |
| **SAP** | **SBA** | **SQS** | **WWU** |
| SAP | secure sba-research.org | SQS Excellence through Independence | Westfälische Wilhelms-Universität Münster |

# EC project TIMBUS: Digital Preservation Services (http://www.timbusproject.net/)



- Why preserve?
- What to capture?
- To what extent?
- How to store?

- How to keep content readable?
- How to maintain content?
- How to identify and access?

- How to re-instantiate?
- How to analyse?

EC focus is on "preserving digital things over time"; novel in TIMBUS: this starts from complex business processes and their supporting IT rather than "simple" objects such as newspapers, email, photos, etc.

# SQS view on TIMBUS: DP + Improvements for existing Services.

**Carve out**

**Transfer**

**Integrate**

Analyse | Specify | Integrate | Use

implicit information

context dependent information

digital assets

time

- **What projects or programmes?**
- **What processes and test assets?**
- **What additional resources and interfaces?**
- **What cost models?**

- Wh
- Wh
- To
- Ho

- How
  read
- How
- How

- **How to migrate?**
- **How to maintain assets?**
- **How to search and access?**
- **What costs?**

- Ho
- Ho

- **How to integrate?**
- **How to revitalise processes and interfaces?**
- **What costs?**

Results from TIMBUS support us in transitioning testing activities from our clients to our test centres to offer Managed Services by changing the focus from "time" to "shift in organisation, location, owner".

**SQS Client**

**SQS Test centre**

# No project is without risk
## The art lies in early recognition and management of risk!

**The earlier a risk is recognised,**

- the earlier derived risks can be assessed (impact analysis),

- the earlier mitigation actions can be planned and executed

- the better the negative effects can be limited

- the lower the cost
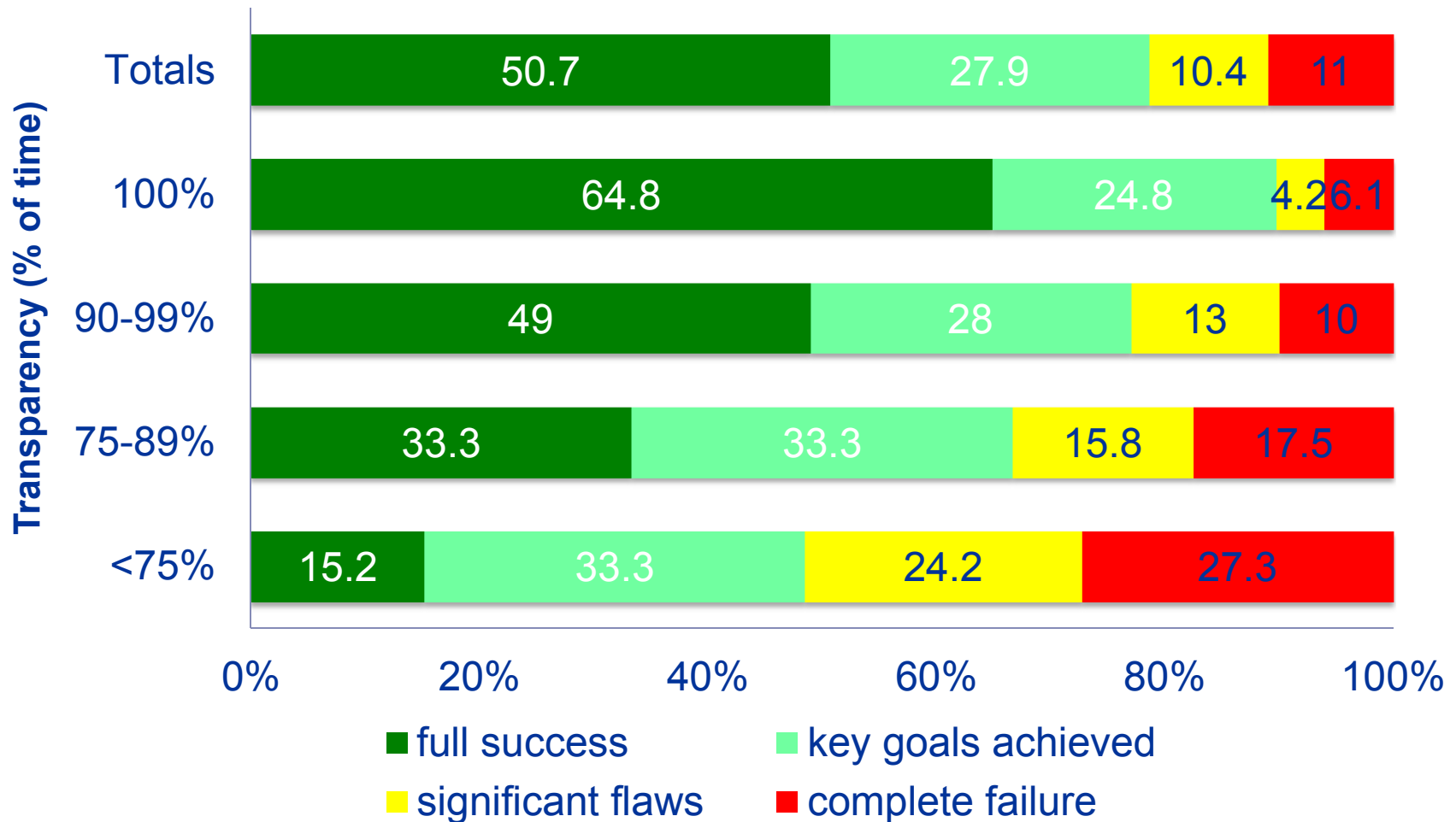
- the sooner feedback-loops can be established

**Project Plan**
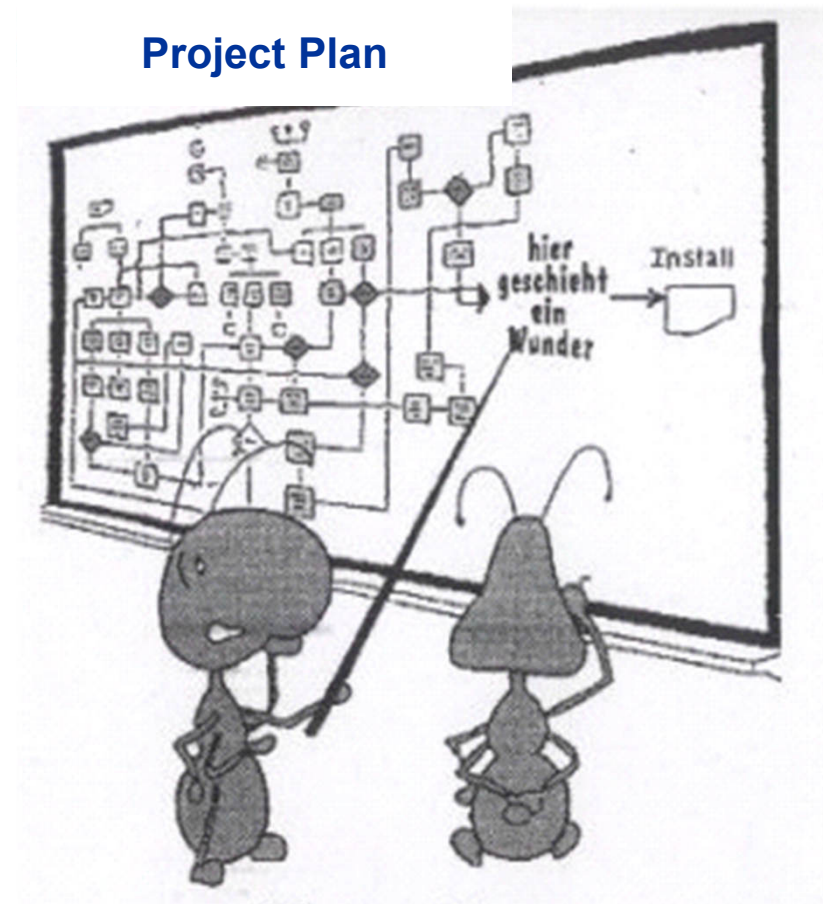
Project success depends on transparency

# Only 15.2% of IT projects that had transparency less than 75% of the time were a full success.

**Project success (time, cost, quality)**



**Transparency (% of time)**

| | | | |
|---|---|---|---|
| Totals | 50.7 | 27.9 | 10.4 | 11 |
| 100% | 64.8 | 24.8 | 4.2 | 6.1 |
| 90-99% | 49 | 28 | 13 | 10 |
| 75-89% | 33.3 | 33.3 | 15.8 | 17.5 |
| <75% | 15.2 | 33.3 | 24.2 | 27.3 |

0%  20%  40%  60%  80%  100%

■ full success   ■ key goals achieved
■ significant flaws   ■ complete failure

# ISTQ Fundamental Test Process

**Testing** is *"the process consisting of all life cycle activities, both static and dynamic, concerned with planning, preparation and evaluation of software products and related work products to determine that they satisfy specified requirements, to demonstrate that they are fit for purpose and to detect defects."*

**Test Management** *covers the planning, estimating, monitoring and control of test activities*.

**ISTQB Glossary**

Test Planning & Control

Test Analysis & Design

↓

Test Implementation & Execution

↓

Evaluating Exit Criteria & Reporting

↓

Test Closure Activities
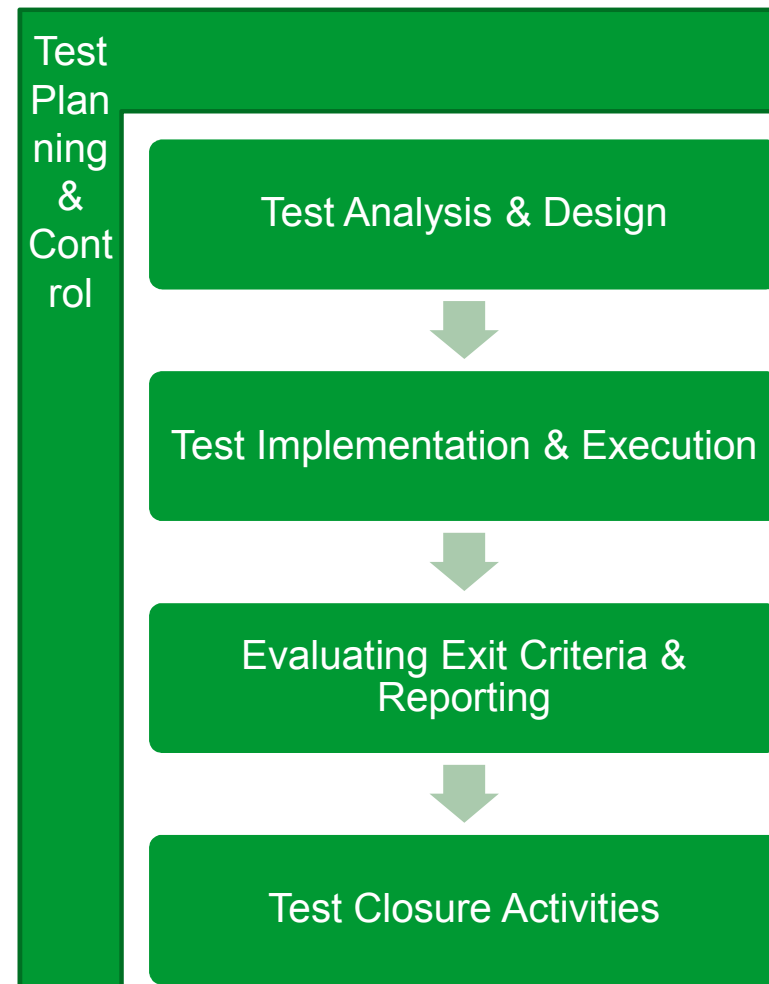
# Generic Test Process (based on ISO 29119)

**Test Management**

Test Planning → Test Monitoring & Control → Test Completion

**Dynamic Testing**

Test Design & Implementation → Test Execution → Test Incident Reporting
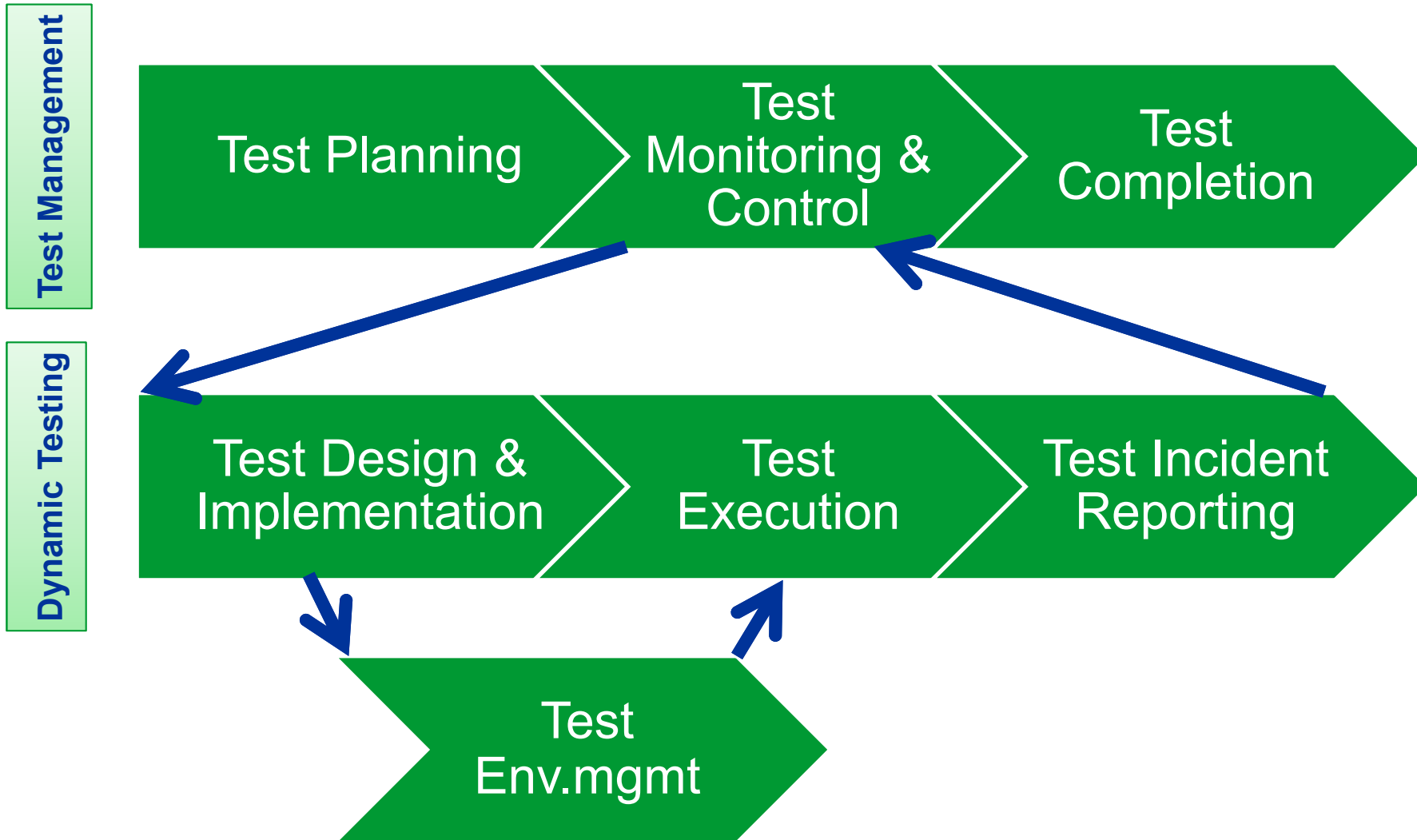
Test Env.mgmt

# Evolution of Risk Management

## Traditional

- Risks managed in **silos**
- Concentrates on physical hazards and **financial risks**
- Insurance orientation
- **Ad hoc** / one-off projects

## Current State

- A variety of approaches to improving risk management
- A recognition that a **holistic approach** is appropriate and preferable
- An acknowledged need to improve risk management
- Risk Management can improve overall capital management and thus enhance corporate value and competitiveness

## Emerging

- **Centralized mgt**., with exec-level coordination
- **Integrated consideration of all risks**, firm-wide
- Opportunities for hedging, diversification
- **Continuous and embedded**

# What is risk?

## Variations of definitions for the term "risk" are

- popular: *the possibility of suffering loss*

- ISO 31000: *the effect of uncertainty on objectives, whether positive or negative*

  → "quality risk" = possibility of suffering due to quality issues


- Along with a **probability** that the effect occurs: $0 < prob < 1$

- **Impact**: the effect of a risk occurs, either quantitative (€€€) or qualitative

- **Mitigation** – measures and actions to reduce the likelihood of the effect to occur  or to limit the impact

- **Risk exposure**: probability x potential loss

- **Risk Reduction Leverage**: RRL = (REbefore - REafter) / cost of intervention

- **Risk Exposure Matrix** (dimensions)

  ☐ probability

  ☐ impact

# ISO 31000 Risk Management Process



Establishing the context

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Communication and Consultation

Risk Assessment

Monitoring and review

# "Establishing the context" and "Risk Identification"
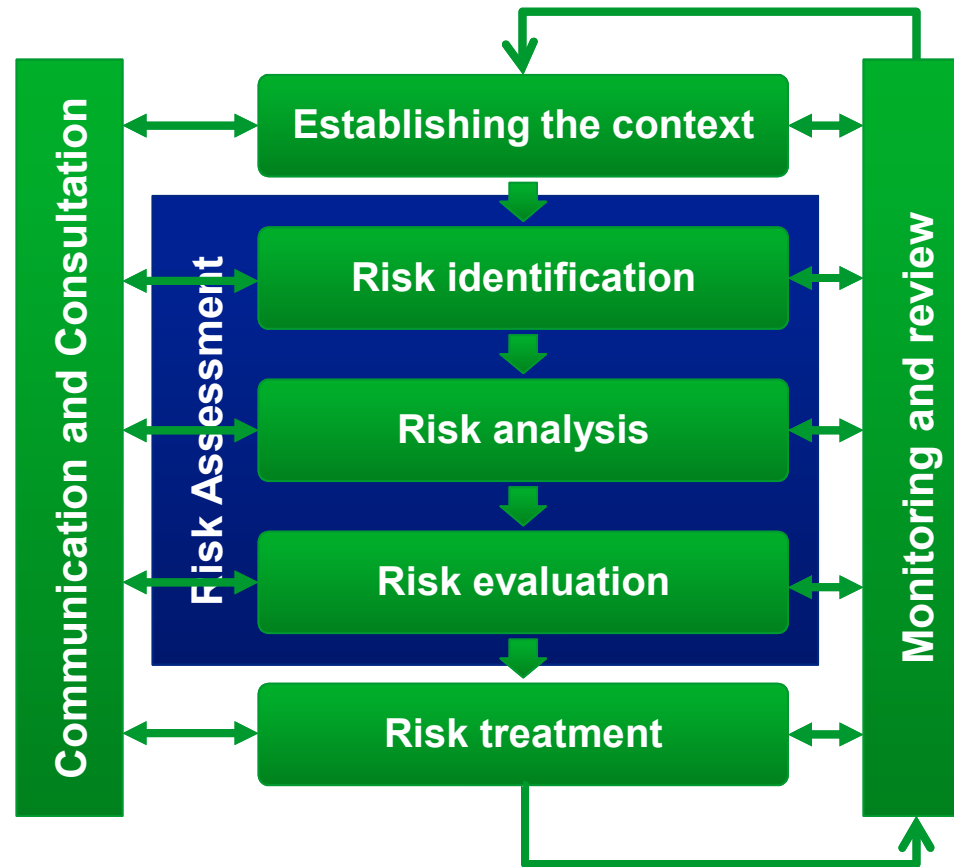
## Establishing the context

- defining the external and internal parameters … setting the scope and risk criteria

- articulating project goals and strategy

- describes the environment of organisation and the project

- external stakeholders, key drivers and trends with impact on project objectives, and cultural, economic and regulatory constraints are considered.

- decisions about the types of consequences to be included

- how consequences are quantified

- how risk levels will be determined

- when risks require treatments or are acceptable

## Risk identification

- discovering, identifying and documenting risks

- risk sources and causes

- their impact area, the events and the potential consequences at a high level.

- methods:
  - brainstorming,
  - questionnaires
  - inspection

- leverage the multidisciplinary experience

- be as open minded and holistic as possible, because any risk not identified in this step cannot be evaluated in the following steps.

- maximum accuracy and completeness: use systematic approaches e.g. QRM

# "Risk Analysis" and "Risk Evaluation"

## Risk analysis

- developing a deep understanding of the risk

- causes and sources of risks are inspected as to analyse the consequences

- reconnaissance and controls

- vulnerabilities of components and adverse effects as the consequence:
  - □ qualitative manner; and
  - □ quantitative impact

- probabilities are estimated and underpinned with indicators

## Risk evaluation

- applying the results of risk analysis and make decisions about measures

- evaluating indicators and controls in order to quantify the risks

- results of quantification used to decide whether the risks are acceptable or treatments are required

- treatment options include:
  - □ avoiding the risk;
  - □ taking or increasing risk;
  - □ removing the risk source;
  - □ changing the likelihood;
  - □ changing the consequences;
  - □ sharing the risk; and
  - □ retaining the risk by informed choice.

# Test Management can be regarded as a particular Risk Management activity. As such, both disciplines are complementary.

# Target Alignment (steps 1, 3, 2, 4)

## "Target alignment"

- improving alignment of risk contexts and risk identification from the risk management function with "Test planning & control" and "Test analysis & design" from the testing function

# Operation and Implementation (steps 5, 6, 4)
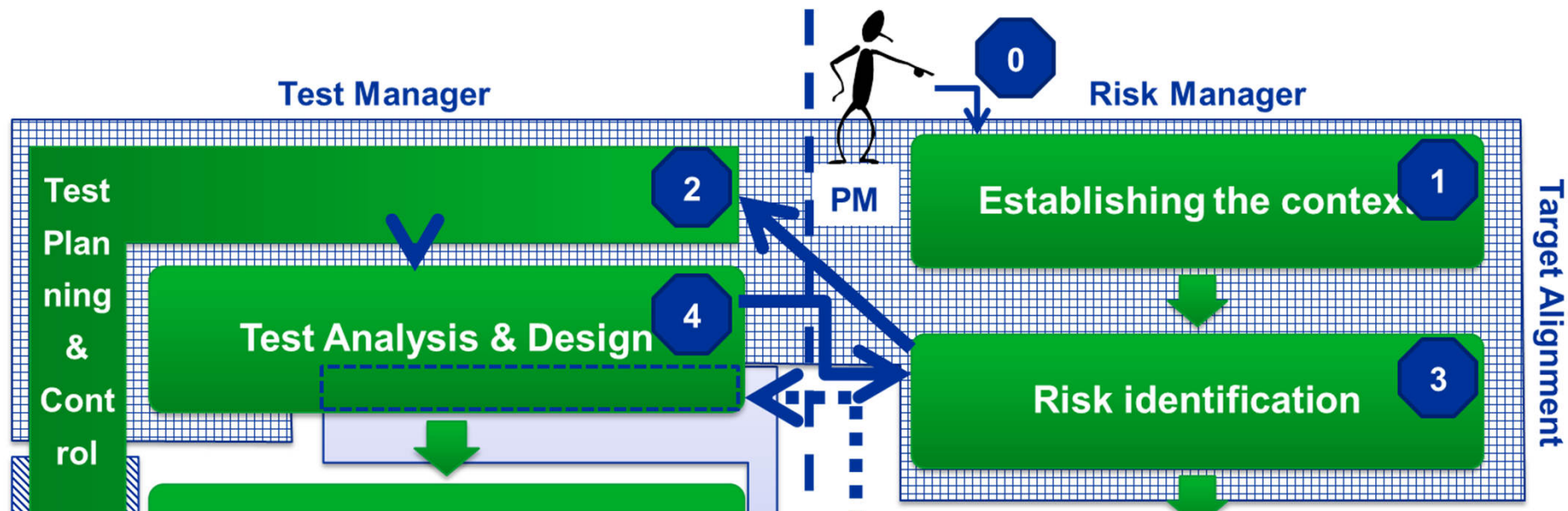
## "Operation and implementation"

- supporting "Risk analysis" and "Risk evaluation" in risk management and "Test analysis & design" and "Evaluating exit criteria and reporting" in the fundamental test process by the exchange of their respective insights

# Mitigation & Adjustment (steps 7, 9, 2)
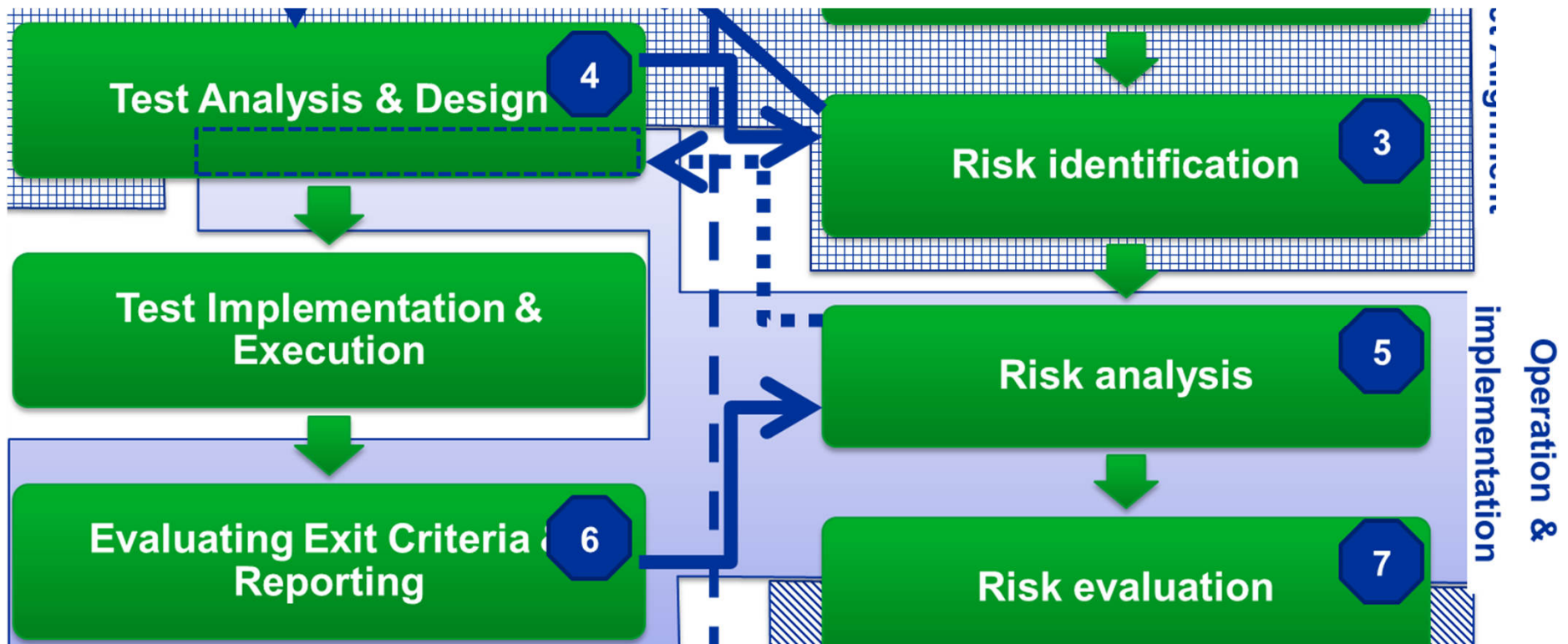
## "Mitigation and adjustment"

- managing risks and adjusting the current planning for testing by teaming up "Risk evaluation" and "Risk treatment" steps with "Test planning and control"

**Test Manager**

**Risk Manager**

**0**

**PM**

Test Planning & Control

**2** Test Analysis & Design **4**

**1** Establishing the context

**3** Risk identification

Test Implementation & Execution

**5** Risk analysis

**6** Evaluating Exit Criteria & Reporting

**7** Risk evaluation

**8** Test Closure Activities

**9** Risk treatment

© SQS Software Quality Systems AG | Integration

21
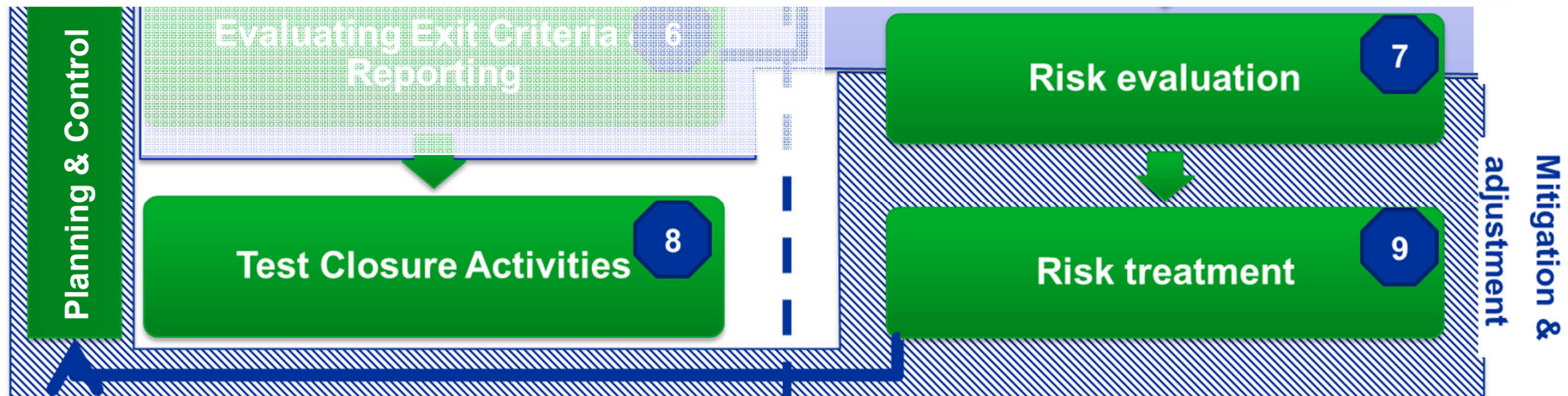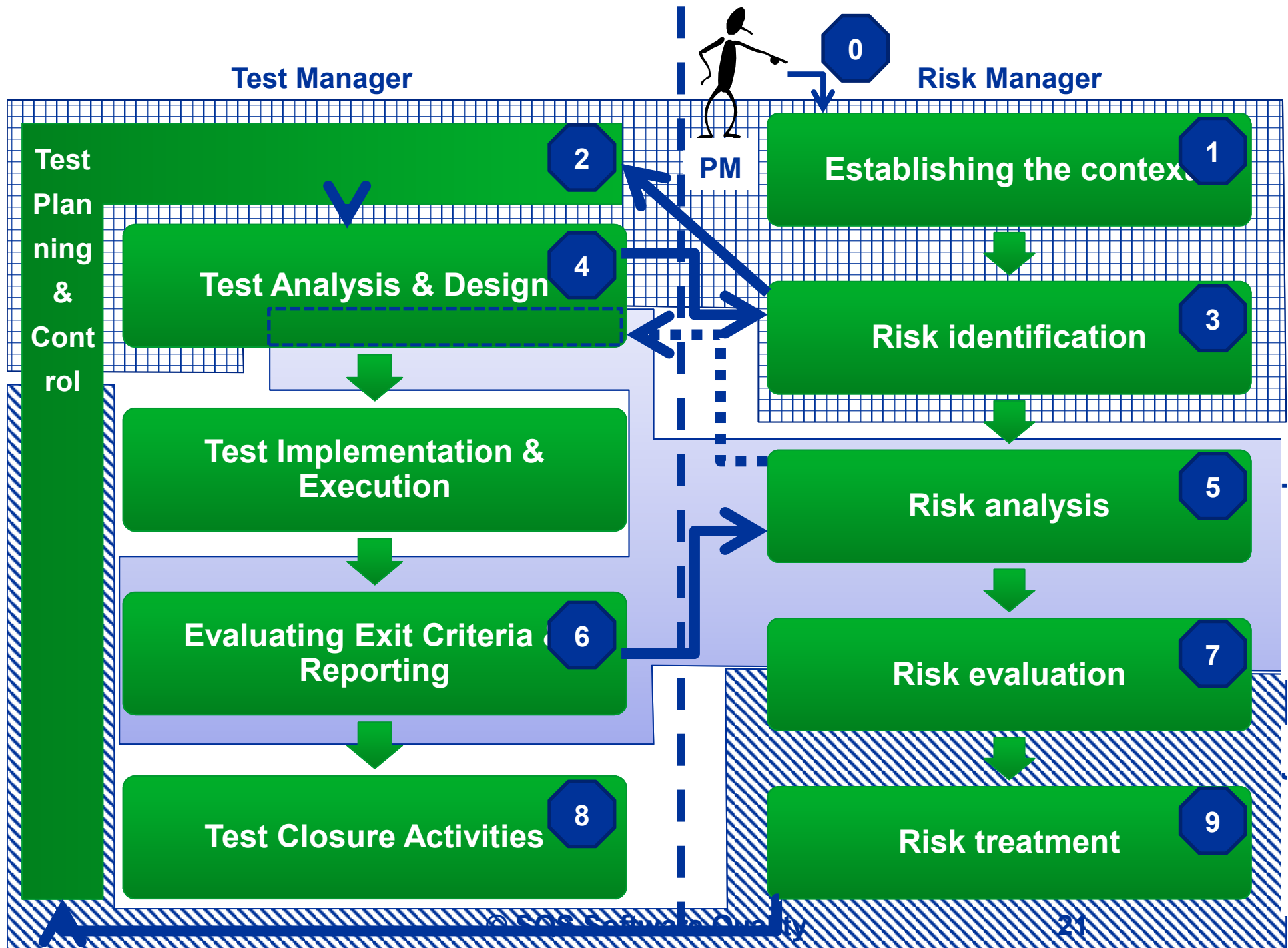
# Roadmap of risk areas was laid out for "Target Alignment".

## clients risk context setting (applying QRM framework)
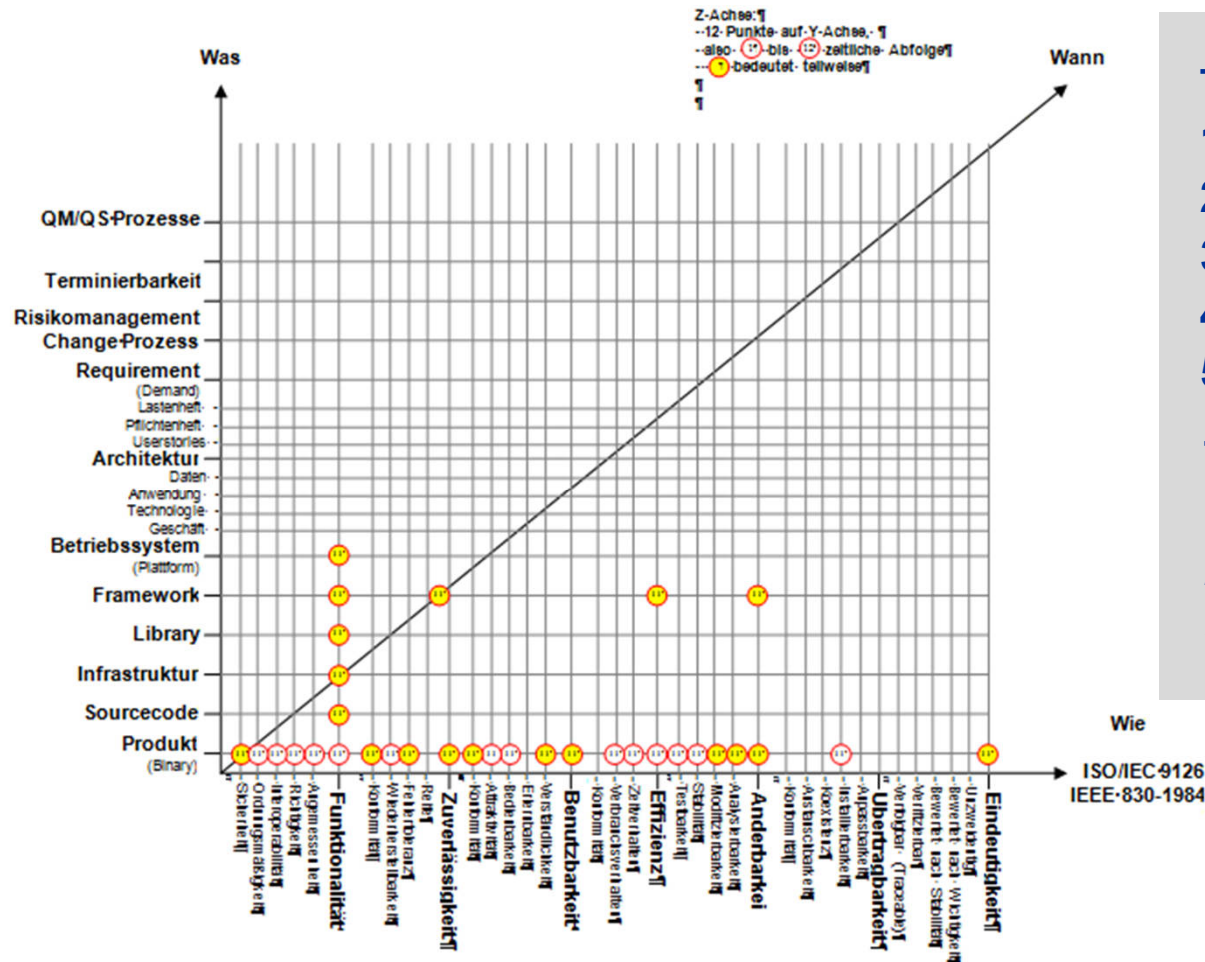


**Top 5 Objects (Draft):**
1) Test cases
2) Requirements
3) Source-codes
4) Executables
5) Architectures

**Top 3 Attributes (Draft):**
1) Functionality
2) Reliability
3) Efficiency

# A first set of risk indicators for test related artefacts has been created for "Operation and Implementation".

## First set of indicators for object <<testcase>> and Top-3 attributes

- No testcases existent
- No testcases covering security existent
- No negative testcases existent
- No testcases covering performance existent
- No testcases covering resource utilisation existent
- A testcase doesn't have corresponding test data
- A testcase doesn't have corresponding entry- and exit criteria
- A testcase has no expected results.
- A testcase does not contain any test steps
- A test step has no specified goal.
- A test step has more than one goal ('and', or, 'or' as part of the test goal).
- A testcase is not related to any committed requirement

## First set of indicators for object <<requirements>> and Top-3 attributes

- No requirements existent
- No requirements covering security existent
- No requirements covering performance existent
- A requirement covering performance is formulated without using any number
- A requirement does contain DON'T-words (like should, could, might, etc.)
- A requirement exists without an assigned risk level
- A committed requirement without a committed test case exists
- A testcase related to a requirement has test data but creates a negative test result

Example for a client

# "Mitigation & Adjustment" supported by a dashboard Landing Page

Example for a client
# Dashboard: Department Director´s View

Example for a client
# Dashboard: Unit Directors View

## Example for a client
## Dashboard: Project Manager´s View /1/2

# Dashboard: Project Manager´s View  2/2



KPI system - report level 3 (for project managers)
results for individual projects    **synthetical test data**    `<<<`

| last report date | 02.09.2011 | ID | 508 | please choose project name >>> |
|---|---|---|---|---|

name of project     L_____g SAP

name of org unit     S_____

| | requirements do not contain DON'T-words | ⬤○ | 0 |
|---|---|---|---|
| | requirements exists with an assigned risk level | ⬤○ | 0 |
| | committed requirements with a committed test cases exists | ○🔴 | 5 |
| | testcases related to requirements have no test data with negative test results | ⬤○ | 0 |

## list of indicators for test cases

| type of indicator: | description of indicator: | status of indicator: | number of violations: |
|---|---|---|---|
| ▢ | test cases are existent | ○🔴 | 1 |
| ▢ | test cases covering security existent | ○⬤ | 0 |
| ▢ | negative test cases existent | ○⬤ | 0 |
| ▢ | test cases covering performance existent | ○⬤ | 0 |
| ▢ | test cases covering resource utilisation existent | ○⬤ | 0 |

# Example for a client
## Dashboard: Engineer's View

Summary

## Integration of TM and RM has proven beneficial for organisation as Test Managers and Risk Managers can support each other.

- both TM and RM are established processes and usually executed in isolation

- synergies can be leveraged when integrating TM and RM for
  - Target alignment
  - Operation and implementation
  - Mitigation and adjustment

of the activities in TM and RM

- mostly, organisation specific interfaces have to be vitalised and new communication channels have to be initiated

SQS. Excellence through Independence
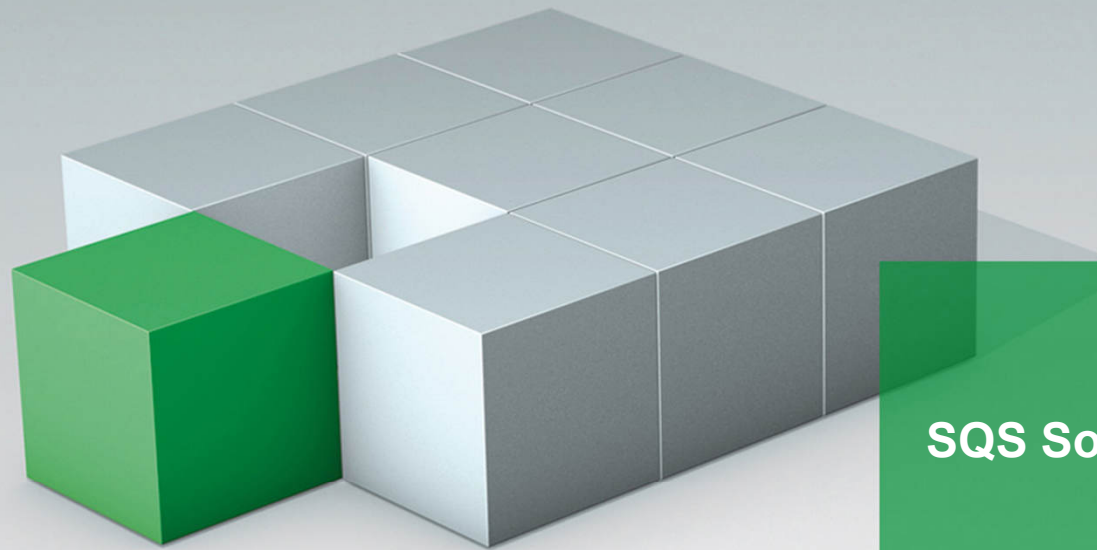
**SQS Software Quality Systems AG**

Stollwerckstraße 11 | 51149 Cologne, Germany
Phone: +49 22 03 91 54-0 | Fax: +49 22 03 91 54-15
E-Mail: research@sqs.com
Internet: www.sqs.com

Thank you for your attention