A project of the

EUROSAI
IT Working Group

A methodology for IT self-assessment by SAI's

Based on

COBIT®

Version: 2.0
February, 2004

PREFACE

It is with great pleasure that we present a methodology that can be used by SAI's to perform a self-assessment as to the maturity of their IT-processes. Such a self-assessment helps SAIs to discover, understand and close possible gaps in their own IT-environment. Such an IT self-assessment needs to be done regularly.

The present version of this self-assessment methodology is based on the experience gained by applying an earlier draft in three SAI's. In Denmark, Lithuania and Spain a successful test of the methodology took place. The methodology for IT self-assessment appeared to work well and only a few minor changes had to be made. We want to thank the three above-mentioned SAIs for helping us improve the methodology.

This IT self-assessment methodology has the advantage of being compatible with the CobiT framework (Control Objectives for Information Technology). CobiT is wellknown worldwide. It was originally an audit framework. That might have a beneficial effect: experiences with the IT self-assessment could also be useful in the audit practice of a SAI. The methodology outlined here is easy to use. It can be amended to suit particular objectives. With repetition, the methodology will become even more effective. Based on future practical experiences, updating of the methodology may be needed.

The Eurosai Training Committee supported the idea of organising a training event concerning IT self-assessment based on CobiT. This training could be scheduled before applying a self-assessment. SAI Portugal offered to host the event end of September or the beginning of October 2004.

Benchmarking could be a long term perspective. Enough SAIs first have to become familiar with IT self-assessment before benchmarking becomes a realistic option. Another direction for future research is the use of CobiT in auditing.

Finally, we hope that there will be volunteers to try it out, and that SAIs will accept this methodology and take advantage of it. This will ensure longer-term success for improving SAIs organisations and for the development of this self-assessment tool. Several members of our project group are available to act as moderators and facilitate a local IT self-assessment workshop.

Michel Huissoud, Switzerland, manager of this project
Henk van der Geest, The Netherlands
Dainius Jakimavicius, Lithuania
Rune Johannessen, Norway
Paul Mantelaers, The Netherlands
Marjan Podgorsek, Slovenia
Alberto Rubio, Spain

Contents

1 Introduction 5

1.1 Objectives and goals for this project 5

1.1.1 Objective 5

1.1.2 Goals 6

1.2 Requirements for the self-assessment tool 6

1.3 Confidentiality and communication of results 6

1.4 What is self-assessment? 6

1.5 What are the advantages of self-assessment? 7

1.6 The use of benchmarking in self-assessments 7

1.7 Why have we chosen CobiT? 7

1.7.1 The place of CobiT in the audit community 7

1.7.2 A short description of the CobiT framework 8

1.7.3 Experiences with CobiT as a self-assessment tool 9

1.8 How can the results be implemented? 10

1.8.1 Self-assessment and Goal Identification 10

1.8.2 Gap Analysis 10

1.8.3 Project Classification 10

1.8.4 Project Prioritisation 11

2 IT Self-Assessment: the Methodology 12

2.1 Preparing an SA workshop 12

2.1.1 Decide to perform an SA 12

2.1.2 Invite a moderator 13

2.1.3 Appoint a contact person 13

2.1.4 Set a date for the SA workshop 13

2.1.5 Invite participants 13

2.1.6 Preparation by the moderator 13

2.1.7 Preparation by the participants 14

2.1.8 Pre-workshop presentation 14

2.1.9 Arranging facilities 14

2.2 Conducting a workshop 14

2.2.1 Overview 14

2.2.2 Phase 1: Introduction. 15

2.2.3 Phase 2: Business processes and IT. 15

2.2.4 Phase 3: Selection of IT-processes to be assessed. 17

2.2.5 Phase 4: Determination of maturity levels of selected IT-processes. .. 18

2.2.6 Phase 5: Design of the action plan. 19

2.2.7 Phase 6: Evaluation. 19

2.2.8 Phase 7: Presentation. 20
3 Conclusion 21
3.1 Workshop reporting 21
3.2 Ongoing monitoring 21

1 Introduction

During the XVII INCOSAI in Seoul, October 2001, the INTOSAI Governing Board made a proposal to regionalize its activities. At the meeting of EUROSAI members held in Seoul, the Netherlands Court of Audit (NCA) expressed its readiness to take the lead in the establishment of an Information Technology Working Group within the European region. At the meeting of the EUROSAI Governing Board, which took place in Copenhagen, Denmark on 7th March 2002, the NCA's proposal for the establishment of the working group was endorsed, and the EUROSAI Working Group on Information Technology was later formed.

The first meeting of the EUROSAI Information Technology Working Group was held in The Hague on 30th September and 1st October 2002 and a decision list was agreed upon. One of these activities was to start a project, which would produce a self-assessment tool for SAIs based on the existing framework of CobiT. Subgroup 1, consisting of Switzerland (lead), Slovenia, Norway, The Netherlands, Lithuania and Spain, was established to perform this work.

The project team started its work by preparing discussion papers on topics such as:

- What is self-assessment and what are its advantages,
- What is the place of CobiT in the audit community, are there any experiences with CobiT as a tool for self-assessment and what other frameworks are available?

During a meeting in Bern, March 2003, these papers were discussed and a framework for a methodology was decided upon. Activities to turn this framework into a practical methodology were listed and responsibilities assigned. It was also decided to conduct four pilots, in Lithuania, Spain, France and Denmark, in an attempt to test the method.

During summer 2003, a script and corresponding slideshow were developed, and several forms including Excelprograms were prepared. The pilots took place at the end of 2003 and the beginning of 2004. In December 2003, in Bern, the results of the pilots were evaluated and changes were made in method, forms, guide and slideshow.

1.1 Objectives and goals for this project

1.1.1 Objective

1. To contribute to the work of the SAI's, by insuring the quality and performance of the SAI's own IT environment and by promoting awareness of IT Governance.

2. To develop the capacity of SAIs to meet their strategic goals through the use of IT (e.g. in relation to internal management, more effective audits and skills development of staff).

1.1.2 Goals

The goal of the project is to develop a self-assessment tool for use in the SAI. Furthermore, SAI's will be able to benchmark their environment against CobiT's standards for best practice, and identify opportunities for improvement.

The use of the tool by a SAI will have various other benefits:

1. Contribute to awareness in the SAI organisation about how to control Information Technology, so that it delivers the information the organisation needs, and how to manage the risks and secure the infrastructure.
2. Give the auditors and the SAIs a first experience of self-assessment and of CobiT as a tool for evaluation of IT systems and IT governance.
3. Learn about the CobiT methodology and get experience in using CobiT as a tool for the SAIs.
4. Give the SAIs assessments of their own IT environment.

1.2 Requirements for the self-assessment tool

Furthermore, the self-assessment tool must meet the following requirements:

- Easy to use
- Cover all relevant IT-processes in the SAI
- Can be applied in other environments outside the SAI
- Self-explanatory (clear documentation)
- Independent of software
- Generate discussions and dialog
- Generate results which permit comparison
- Contribute to quality improvements

1.3 Confidentiality and communication of results

The results of the workshops are property of the SAIs. Communication of the results for external benchmarking will take place in cooperation with the SAIs involved. The principle is that no information relating to the SAIs' IT function is disclosed without approval.

1.4 What is self-assessment?

Self-assessment is a powerful way to gather information and educate the participants. It is a generic term that covers processes whereby an organization's

personnel evaluate their own risks and controls with the help of a facilitator or moderator. Assessments can be performed by means of workshops, meetings or questionnaires and may be applied to projects, processes, business units and functions. Basically it could be applied in any area of a company or organisation.

Whatever format is used, the goal is the same: To help organisations assess the likelihood of achieving their objectives by using the knowledge of the people responsible for meeting them.

1.5 What are the advantages of self-assessment?

The successful implementation of self-assessment could have a number of specific benefits:

1. Encourages direct involvement by the people involved in IT.
2. Leads to better allocation of scarce resources by involving the organisations' own people in the evaluation process.
3. Contributes to awareness in the organisation.
4. Aligns business unit objectives with corporate goals.
5. Fosters a sense of ownership of risks and controls.
6. Builds teamwork in addressing risks.
7. Improves communication within business units and across the organisation.
8. Raises awareness about the effect that soft controls can have on the overall health of the control systems.

1.6 The use of benchmarking in self-assessments

Benchmarking refers to systematic comparisons by two or more organisations of their processes and/or results in their respective organisations in order to learn about best practices (superior performance or methods or approaches that lead to exceptional performance) and implement them in ways suited to their own organisation.

The result of a self-assessment may be used for benchmarking. Advantages are:

- A SAI can position itself in relation to other SAIs;
- Insights into best practices can generate ideas for possible control measures.

1.7 Why have we chosen CobiT?

1.7.1 The place of CobiT in the audit community

The Information Systems Audit and Control Foundation (ISACA) is a leading global professional organisation representing individuals in more than 100 countries and

comprising all levels of IT – executive, management, middle management and practitioner. The association is working to fulfil the role of a central, harmonizing source of IT control practice standards for the world, and has formed strategic alliances with other groups in the financial, accounting, auditing and IT professions.

Together with the IT Governance Institute and others sponsors they have designed and created the Control Objectives for Information and related Technology (CobiT). CobiT is a global open standard for control over information technology, enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards, e.g. ISO9000, SPICE and ITIL.

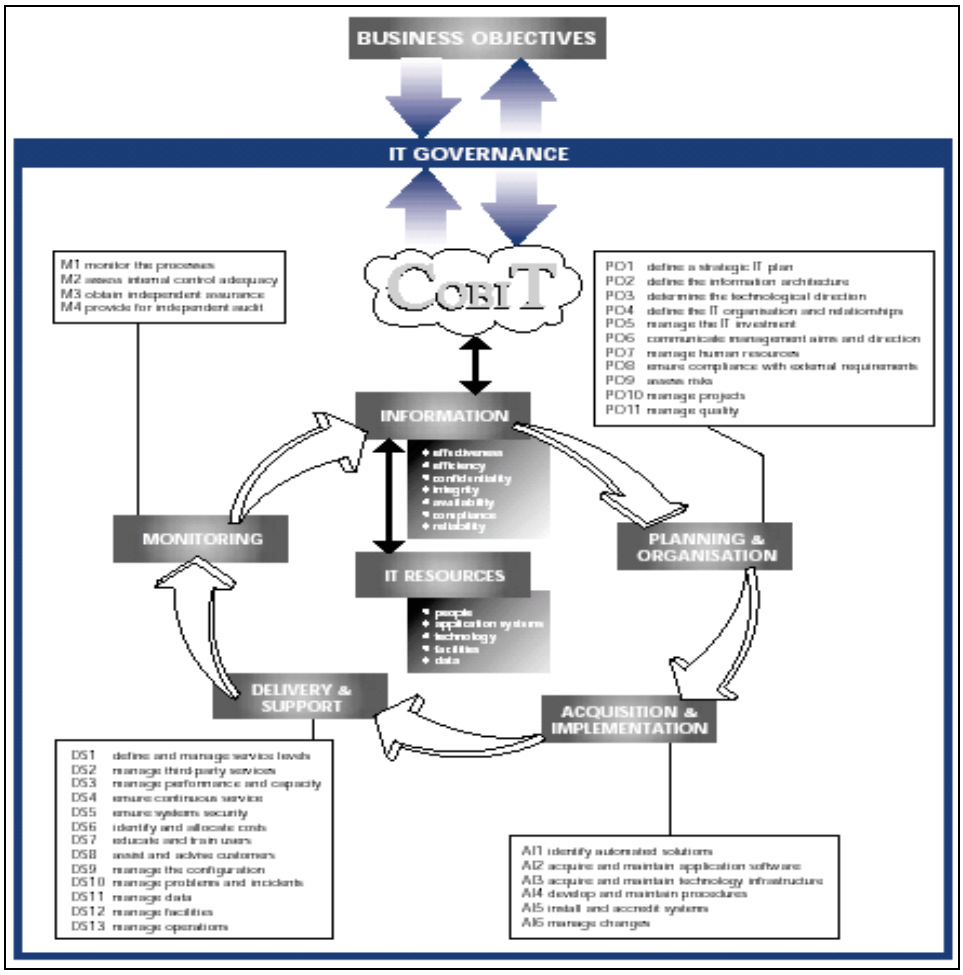
The complete CobiT package consists of the following components:

- **Management Guidelines** composed of Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators.
- **The Executive Summary** consisting of an Executive Overview, which explains CobiT's key concepts and principles.
- **Framework** which provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives.
- **Audit Guidelines** that enable the review of IT-processes against control objectives.
- **Control Objectives** that provide the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.
- **Implementation Tool Set**, which contains Management Awareness and IT Control Diagnostics, Implementation Guide, frequently asked questions, case studies from organisations currently using CobiT and slide presentations that can be used to introduce CobiT into organisations.

The global representation of ISACA and its active promotion of the CobiT framework as a tool for IT governance and auditing, as well as a global open standard for control over information technology (www.isaca.org), has made CobiT one of the dominating tools for auditors in the IT area.

1.7.2 A short description of the CobiT framework

In CobiT, processes are defined as a series of linked control objectives. At the highest level, processes are grouped together into four domains: Planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. In order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. The following diagram illustrates this concept:



1.7.3 Experiences with CobiT as a self-assessment tool

CobiT is an instrument that allows many sorts of self-assessment. The most extensive way is described in an exposure draft published in December 2002 from the ISACA under the title “Control risk self-assessment (CRSA)”. This methodology is defined as an empowering method/process by which management and staff of all levels collectively identify and evaluate IS related risks and controls. The IT auditors of Swiss life (largest insurance company and real estate owner in Switzerland) have done an IT-CRSA with the procedure described in the Management Guide.

Another way is described in the Management Guide. On the basis of a form the participants should for each process answer these questions: Importance? / Performance? / Who does it? / Audited? / Formally? / Who is accountable? Many firms have been carrying out this kind of self-assessment successfully.

- Philips conducted pilots based on the maturity models in the management guidelines in combination with a summary of the control objectives. The pilots were carried out as self-assessments in about 130 business units.

1.8 How can the results be implemented?

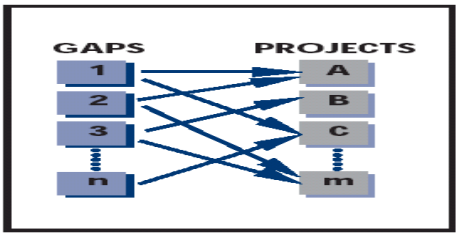
There are many ways to address the results of a self-assessment. Depending on the size, complexity and the maturity of the SAI's IT department there will be a range of variations in types and numbers of topics that are identified. Our suggested methodology for implementing results could be used in both small, medium and big sized IT departments, but it is important to emphasise that the process must be adjusted, and in some cases simplified, so that it is suitable for the SAI.

1.8.1 Self-assessment and Goal Identification

For each of the processes on the forms, the SAI uses the measurement scales to define its estimated positions, by assessing which one of the positions best describes its current status. The organisation also needs to consider where it would like to go on the scale as a result of its IT strategy. The more important the process is for the organisation, the higher it should be on the scale.

1.8.2 Gap Analysis

In many cases the two self-assessment markers (where one is and where one wants to be) will be separated by a gap. This gap needs to be described in detail to facilitate use of the results, in order to plan a series of projects/activities that will take the organisation towards its strategic goals for security and control of IT. The gap analysis process will compile a list of all the actions needed to close the gaps between the 'current status' markers and their corresponding 'strategic goal' markers. This list of gaps could also be used to plan a matching list of projects/activities that will carry out these actions. There will probably in some cases be a many to many mapping between gaps and projects as illustrated in the diagram below:



The Excel-spreadsheets that form part of this methodology contain options for making graphical representations of two gaps:

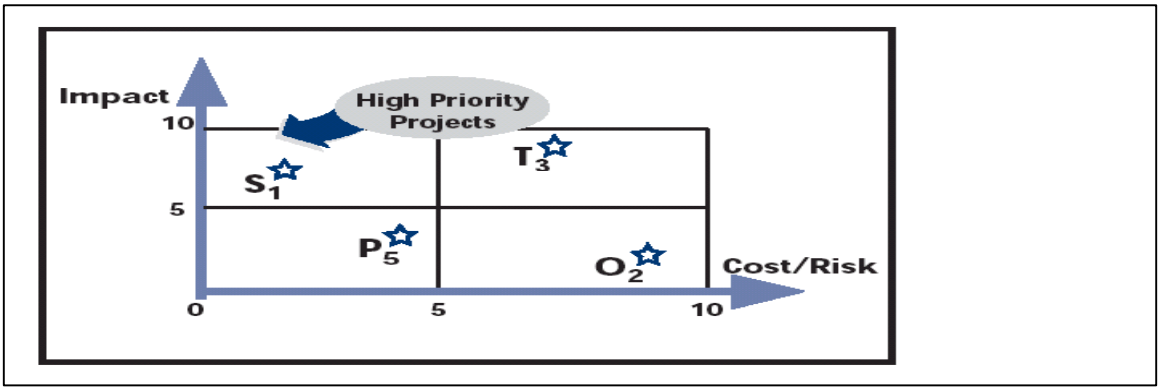
- Importance of shortcomings in the quality of present systems;
- Importance of shortcomings in the quality of future systems.

1.8.3 Project Classification

For the ease of planning and communication, it could be recommendable that the projects/activities are classified according to type, for example Strategic initiatives (S), Tactical projects (T), organisational improvements (O) or procedural developments (P). Each project/activity is then tagged with a unique sequential label as shown in the diagram below:

1.8.4 Project Prioritisation

The objective of prioritising projects/activities is usually to identify those where quick wins can be achieved. The best candidates are usually those where the gaps are small, the cost of closing the gap is low, risk of failure is low and impact on business profit will be greatest. Projects/activities should therefore be assessed for impact and cost/risks. The results of these assessments could also be the basis for an action plan for the future. The projects/activities could be plotted on a chart which becomes a management decision support tool, showing the relative impacts and costs/risks, as shown in the diagram below where impact and cost/risk are measured on a scale from 0 to 10.



2 IT Self-Assessment: the Methodology

This chapter contains a description of the methodology that can be used by a SAI to prepare for and to conduct an IT Self-Assessment (SA). The intended user of the methodology description is the moderator of the SA. But it is also useful as background information for workshop participants. The methodology consists of five components:

1) Way of working: description of the various steps that need to be taken during the workshop. Chapter 2 is structured according to these steps.
2) Way of modelling: several forms play a prominent role during the workshop. Most of them are used by the participants to model various aspects of a SAIs IT. The content and use of each form will be described as part of the way of working.
3) Way of supporting: spreadsheets have been developed to generate statistics. These statistics will be used to generate discussion between participants. The content and use of the spreadsheets will also be described as part of the way of working.
4) Way of presenting: a PowerPoint presentation is developed to support the presentations by the moderator. During each step (way of working) one or more slides are available.
5) Way of preparing: both the moderator and the participants need to prepare themselves for the workshop. This issue will be dealt with in a separate paragraph (2.1).

A very important characteristic of an IT Self-Assessment supported by this methodology is the crucial role of discussion during almost every phase between representatives from the business processes (demand side) and IT-specialists (supply side). It is necessary that the conclusions of these discussions including the underlying evidence be documented for future use.

Point of departure for the methodology is that the moderator is an external expert and not one of the employees of the SAI.

This chapter is split up into two sections: the preparation (par. 2.1) and the execution (par. 2.2) of the SA-workshop.

2.1 Preparing an SA workshop

2.1.1 Decide to perform an SA

First of all, a SAI needs to decide to perform an SA. When an SA has not been done in the past, it will be necessary to convince the management of the SAI of the benefits of such an investment. SAI-representatives in the Eurosai IT WG play an important role here. Information from SAI's that took part in the pilots (Denmark,

Lithuania and Spain) could be helpful. An SA workshop only makes sense when it is supported by the higher management (and/or the AG). They are the ones to take part in the workshop (next to others) and what is more, they should act upon the results of the SA. Proposals for change will be at stake and there should be ex ante preparedness to take the proposals that result from the SA into consideration in a careful manner. When (part of) the higher management is not able to participate in the SA, it is even more important that they are prepared to take the findings of the SA very seriously. In that case, these higher managers should be invited to attend the presentation of the final results of the SA (see Chapter 2.2.8, phase 7: presentation).

2.1.2 Invite a moderator

The SAI should invite someone from outside the SAI to act as independent experienced moderator during the SA workshop. An outsider has the advantage of a more objective approach. This outweighs the disadvantage of a more complex preparation phase. Preferably, the moderator should speak the local language. If this is not possible, the participants should be able to understand the international language spoken by the moderator and one of the participants should be available to translate a summary of the discussions and conclusions for the moderator.

2.1.3 Appoint a contact person

One of the members of the SAI's management team needs to be the 'owner' of the project. He/she should act as a link between the SAI and the moderator and also take care of the internal part of the preparation.

2.1.4 Set a date for the SA workshop

Adequate planning is crucial in conducting a successful SA workshop. The contact person and moderator agree on a date for the workshop. A workshop requires between 1 and 2 days. It is an option to start the workshop in the afternoon of the first day and to continue the next day. Losing momentum could be a drawback of this option. Moderator and contact person also need to decide how, when, and to whom the workshop results will be communicated.

2.1.5 Invite participants

Moderator and contact person decide whom to invite for the workshop. Both IT- and business-professionals should be invited and within both categories managers as well as non-managers should be involved. It is important to invite a user of the SAI's key information systems as well as a senior employee from the help desk. As well as the consideration of having the necessary knowledge/information available for the workshop, other (more local) circumstances may influence the composition and size of the group. However, all important business processes should be represented. The total number of participants should be somewhere between 8 and 12 people.

2.1.6 Preparation by the moderator

The moderator needs to familiarise himself with the methodology and with the SAI. He will read the manual and look at the PowerPoint presentation. Next to that, he will study documents regarding the SAI that are made available to him by the contact person. In such a way the moderator will become familiar with the processes,

activities, risks, controls and areas of emphasis in the workshop. This may involve obtaining relevant policies, plans, laws, regulations and contracts; organizational information, financial information, previous audit results, industry best practices, details of problems affecting the area and, where possible, details of challenges and opportunities expected to arise in the future.

2.1.7 Preparation by the participants

The participants prepare themselves by studying the documents provided to them by the contact person on request of the moderator. At least the following documents should be provided to the participants:

- This methodology (including a copy of the forms that will be used).
- The executive summary and the management guidelines (pages 22-97) of CobiT.
- Pages 23-27 of CobiT's control objectives guideline.

If possible, the documents should be provided in the local language.

2.1.8 Pre-workshop presentation

One option is to arrange an introductory meeting a few weeks before a workshop will take place for the first time. Such a meeting could be used by the moderator to perform phase 1 (introduction) and its main purpose is to stimulate the participants to prepare themselves for the workshop. Whether such a preparatory meeting is feasible or not depends on the availability of the moderator and the participants. Such a meeting is also a good opportunity for the moderator to meet the AG, higher managers and the contact person to achieve a common understanding about the SA process and to define the scope and the issues to be resolved in the workshop.

2.1.9 Arranging facilities

The contact person is responsible for the arrangement of the following facilities:

- Meeting room.
- 2 interconnected laptops.
- Beamer.
- Flip-over.
- Handouts of the various presentations (see annex 1).
- Copies of empty forms (see annexes 2, 3 and 4).
- Copies of the evaluation forms (see annex 5).

2.2 Conducting a workshop

2.2.1 Overview

The IT self-assessment methodology consists of the following 7 phases:

1) Introduction.
2) Business processes and IT.

3) Selection of IT-processes to be assessed.
4) Determination of maturity levels of selected IT-processes.
5) Design of the action plan.
6) Evaluation.
7) Presentation (optional).

Each of these 7 phases will be described in the next paragraphs. The description of each phase will contain an overview of the subphases and their contents, the estimated duration and the outcome of the phase. Reference will be made to the slides of the PowerPoint presentation (see annex 1) that is part of this methodology.

2.2.2 Phase 1: Introduction.

The participants and moderator are expected to introduce themselves, mentioning their name, their position within the SAI, and their experience in areas such as auditing, IT and the use of CobiT.

The moderator gives a presentation (using slides 1-17; see annex 1) covering the following topics:

- The background of the self-assessment. A brief overview of the establishment of the Eurosai WG IT, its members, the results if the first meeting in The Hague in 2002 and of the second meeting in Bern in 2004. One of the four projects resulting from the meeting in the Hague was the project to develop a CobiT-based methodology for IT self-assessment. This project was led by Switzerland. Lithuania, The Netherlands, Norway, Slovenia and Spain participated.
- A short explanation of the two essential elements of self-assessment: why IT self-assessment and why CobiT?
- The methodology.
- Conclusions and questions.

Estimated duration: 60 minutes

Outcome of this phase: understanding by the participants of the background of the self-assessment, its objectives and the value of its results for the SAI. Participants are aware of their role (it is a self-assessment) and that of the moderator and that they are not expected to discuss the methodology during the self-assessment. Comments about the methodology are appreciated during phase 6 (evaluation).

It is an option to do this phase a few weeks before the workshop. In that case the introduction during the workshop can be minimised.

2.2.3 Phase 2: Business processes and IT.

This phase consists of 3 sub phases.

- **Introduction (slides 18-21).**

The moderator introduces the second phase by giving an overview of the objective of the phase, an explanation of the (various columns of the) Business Value Chain Form (see annex) and a preview of the steps to be taken.

The Business Value Chain[1] Form consists of five (sets of) columns. The third column refers to all relevant primary and secundary business processes of the SAI (see sub phase 2.2). The first two (sets of) columns refer to the importance of (current and future) IT-systems for the business processes (see sub phase 2.3). The fourth column focuses on the quality of the current IT systems. Important questions regarding the IT support are:

a. Does IT support this business process (no = 0)?
b. What is the importance of the current IT systems for this business process (5 point scale)?
c. What is the quality of the current IT systems as perceived from the point of view of this business process (6 point scale)?

   The combination of assessments b and c (only relevant when question a is answered 'yes') gives the following insight:

		Importance of current IT system		
		low	*medium*	*high*
Quality of current IT system	*Low*			
	Medium			
	High			

   Systems that are not very important (for the effectiveness of the efficiency of a business process) can be of high quality i.e. in terms of the information they provide (see the various characteristics in the CobiT handbook:). But other options are possible too. A system can be very important but its quality can be low because of low availability, high response times, insufficient information etc.

d. What is the importance of the future IT systems for this business process (5 point scale)?

- **Determination of the list of business processes (slides 22-23)**

  What are the important processes, looking at the goal of the SAI? Two examples of lists of processes are presented. However, the participants have to make their own choice. Just to structure the discussion, a distinction is made between primary and secondary processes. As to the required level of detail of the description: more detail is required as long as this gives a better insight into the IT-support of the various (sub)processes. The participants are asked to write the processes on the flip-over. The processes are registered in

[1] The value chain of an organization is its system of mutually dependent primary and secondary processes. See: Porter, M.E and V.E. Millar: "How information gives you competitive advantage", in: *Harvard Business Review,* July-august, 1985.

a spreadsheet and the new BVC-forms are printed to be used during the last sub phase (assessment of IT-support).

- **Assessment of the IT support of the business processes (slides 24-25).**

  Each participant scores the IT support of the business processes from the various perspectives described above: present support (yes/no; 1, 0) importance of the present IT systems (l1, 2, 3, 4 or 5), importance of future IT systems (low/medium/high; 1, 2, 3, 4 or 5) and quality of the present IT systems (low/medium/high; 0, 1, 2, 3, 4 or 5). The BVC-form with the relevant business processes is used for the scoring. The individual scores are imported into a spreadsheet and a few statistics are calculated. Based on these scores, a group consensus process takes place to come to an agreement about the scores. Documenting the evidence underlying the agreed score is very important! The moderator should see this is done.

Estimated duration: 75 minutes.

Outcome of this phase: the participants agree about their business processes and about the level of present and future IT-support. Their view as to the IT-support will still be rather general. During the next phase, this view will become more detailed and precise.

2.2.4 Phase 3: Selection of IT-processes to be assessed.

This phase consists of 5 sub phases.

- **Introduction (slides 26-29).**

  The moderator introduces the third phase by giving an overview of the objective of the phase, an explanation of the (four columns of the) CobiT-form and a preview of the steps to be taken.

- **Introduction of IT processes (slides 30-34).**

  Introduction of the CobiT-processes is necessary, because in the next sub phase participants are expected to determine their relevance. Participants may have read the management summary, which contains descriptions of the IT processes. First of all, the four domains are introduced. For each domain a few processes are described.

- **Determination of the relevance of IT-processes by each participant (slide 35).**

  The first column of the CobiT-form is used to score the relevance of each IT-process (scores 0-2).

- **Calculation of statistics (slide 36).**

  The individual scores are imported into a spreadsheet. Statistics are calculated. An overview is made of the IT-processes arranged in decreasing order of importance.

- **Agree on the selection of 15 most important processes (slides 37-38).**

  The participants discuss the results and come to an agreement. Documenting the evidence underlying the agreed selection of processes is very important! The moderator should see this is done.

Estimated duration: 90 minutes.

Outcome of this phase: The individual scores on the relevance of each IT-process are used as a basis for the consensus process which leads to agreement about the relative importance of each IT-process (including documented evidence).

2.2.5 Phase 4: Determination of maturity levels of selected IT-processes.

This phase consists of 3 sub phases.

- **Introduction (slides 39-40)**

  The moderator introduces the fourth phase by giving an overview of the objective of the phase and a preview of the steps to be taken.

- **Introduction of maturity levels (slide 41).**

  General introduction of levels 0-5. Each participant has a copy of the management overview, which contains a description of the maturity levels for each IT process.

- **Determine maturity levels (slide 42).**

  Each individual uses the CobiT-form to determine the maturity level of the selected IT-processes. These maturity levels are imported into a spreadsheet and on the basis of average scores a group discussion will lead to agreement on the maturity levels. Evidence of the chosen level has to be provided (and documented): why on this level and not on the next one? Are there any risks associated with this level? Which business processes are influenced by the fact that maturity levels are as they are? This information has to be written on the flip-over, using a format like the one below (the second column contains an example for process PO1):

Cobit-process:	PO1 Define a Strategic IT Plan
Maturity level:	2
Shortcomings:	Policy not known, no business planning system
Risks:	Communication problem, alignment problem
Business process involved:	Every business process may be influenced

  During this phase, the discussion should focus on present maturity levels and not on required maturity levels. The latter will be included in the discussion about future actions (next phase).

  Option: skip the individual voting and determine maturity levels through a group discussion. Each participant can be invited to lead the discussion about one of the IT-process and to summarize the findings of the group on the flip-over.

Estimated duration: 90 minutes.

Outcome of this phase: determination of the agreed maturity level of the selected IT-processes (including documented evidence).

2.2.6 Phase 5: Design of the action plan.

This phase consists of 4 sub phases.

- **Introduction (slides 43-46).**

  The moderator introduces the fifth phase by giving an overview of the objective of the phase and a preview of the steps to be taken. The action form is introduced. The first columns of the form (the problems and the possible consequences) have already been filled out in the previous phase (see flip-over).

  During this phase the participants should keep the BVC-form and the CobiT-form in mind and ask themselves whether the IT-support problems that were raised are covered by appropriate actions.

- **Design solutions for each problem (slides 47-48).**

  The participants discuss the action(s) that could be taken to solve an identified problem. They take the overviews that were drawn up during subphase 4.3 as their point of departure. For each problem, one or more solutions can be suggested. Participants also discuss who is responsible for this action.

- **Combine solutions into projects (slide 49).**

  If possible: combine actions into a project.

- **Assign priorities (slide 50).**

  Use stickers (red and green) to assign priorities. Red stickers reflect the importance from a business point of view: the higher the better. Green stickers reflect the cost/risk point of view: the lower the better. Each participant has to use 10 stickers of each colour, with a maximum of two for each action.

Estimated duration: 60 minutes.

Outcome of this phase: List of actions (projects) for improvements (including documented evidence as to the priority setting: costs/drawbacks and benefits/advantages).

2.2.7 Phase 6: Evaluation.

Each participant is requested to fill out the questionnaire (see annex 5). After that, there is an opportunity to discuss experiences. One of the participants will be invited to present the action list in phase 7 (slide 51).

Estimated duration: 30 minutes.

Outcome of this phase: An overview of the opinions of participants about the workshop.

2.2.8 Phase 7: Presentation.

All interested SAI employees are invited to attend a presentation about the background of the pilot and its findings. Several slides that were used during the various phases of the workshop could be presented, next to a few slides about the results.

Estimated duration: 60 minutes.

Outcome of this phase: the AG, higher management and other people interested are aware of what has been done during the workshop and of the benefits for their SAI.

3 Conclusion

3.1 Workshop reporting

- Each SA exercise should produce a report. In general, the substance of the report will be created during the workshop, by way of a listing and description of relevant findings, risks, performance weaknesses and actions proposed.
- One of the outputs of the SA workshop will be an action plan in the format of **finding and action form** (the proposed form could also be modified if there are other users' requirements). The SA moderator could also issue a formal report on the SA process and outcomes, including relevant background, context, performance and risk ratings and other material in accordance with SAI reporting standards. In the formal report the conclusions from "**Questionnaire evaluation"** should also be included. Within 2 weeks after workshop completion the formal report should be presented to the sponsor and other relevant parties in SAI.

3.2 Ongoing monitoring

- An important part of SA is that IT departments, the audit units or other process owners must revisit their performance and risk assessments regularly (twice a year) and monitor the implementation of action plans. The tools provided for SA can also act as support in achieving this. Follow-up workshops could also be reconsidered, as well as occasional meetings with IT and/or business unit representatives to discuss performance and risk management issues and concerns.
- Monitor the implementation of the agreed actions, in accordance with normal audit and assurance practice and ISACA IS Auditing Standard 080 Follow-Up Activities.

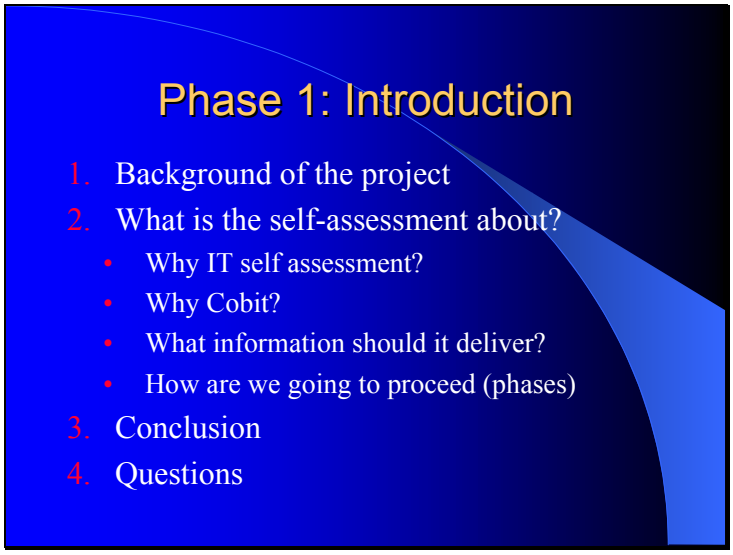
Annex 1: PowerPoint-slides

Dia 1

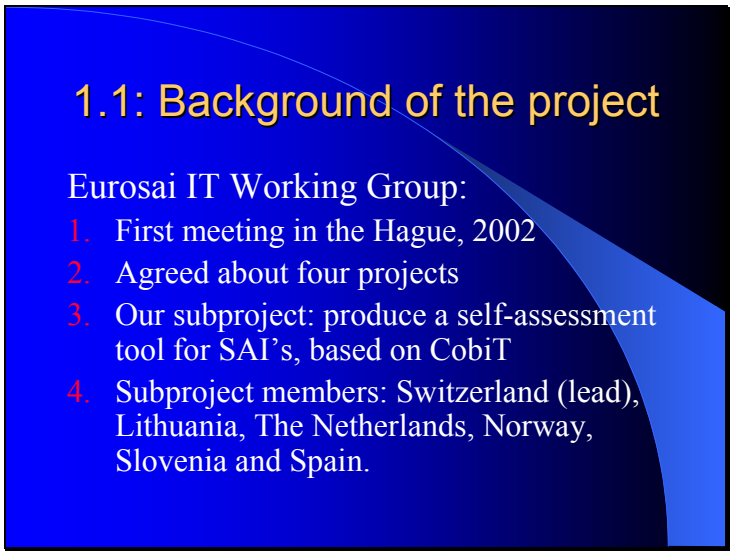
Dia 2


Agenda
Welcome, who is who?
IT self assessment:
– Introduction (phase 1)
– Phases 2-6:
• Introduction
• Execution
– Phase 7: presentation
• Content and method
• SAI

Dia 3


Phase 1: Introduction
1. Background of the project
2. What is the self-assessment about?
• Why IT self assessment?
• Why Cobit?
• What information should it deliver?
• How are we going to proceed (phases)
3. Conclusion
4. Questions

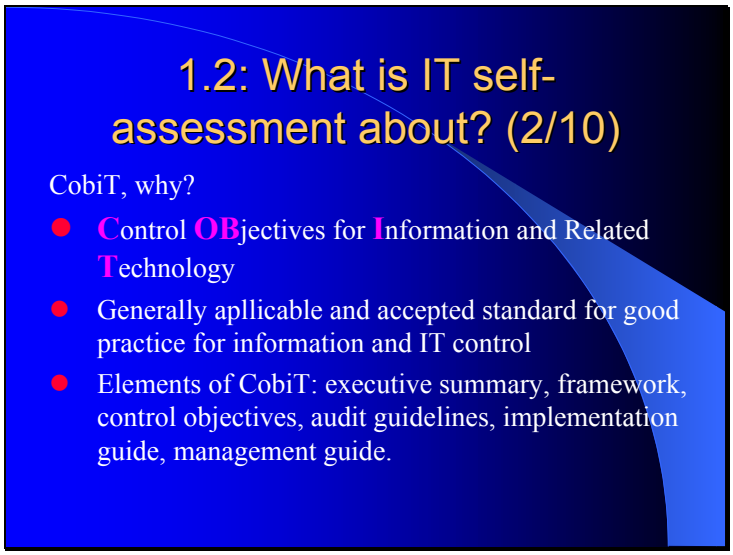
Dia 4


1.1: Background of the project
Eurosai IT Working Group:
1. First meeting in the Hague, 2002
2. Agreed about four projects
3. Our subproject: produce a self-assessment tool for SAI's, based on CobiT
4. Subproject members: Switzerland (lead), Lithuania, The Netherlands, Norway, Slovenia and Spain.

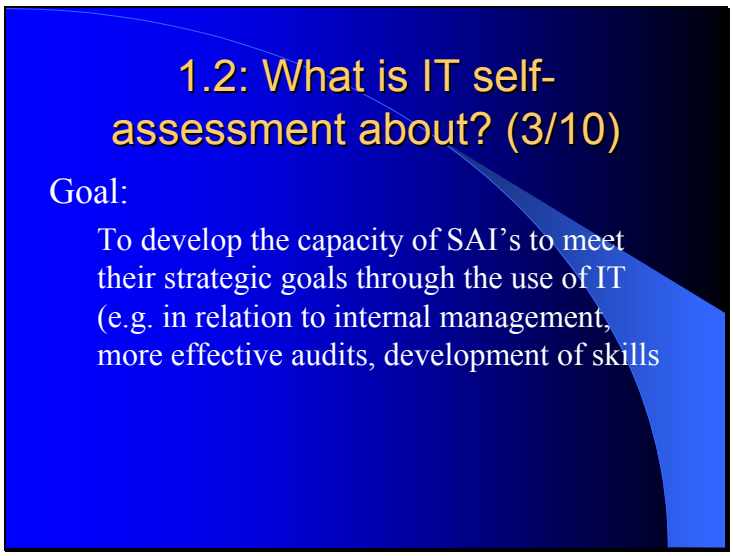
Dia 5


1.2: What is IT self-assessment about? (1/10)
IT self assessment, why?
IT is an integral part of business
IT governance is an integral part of corporate governance
IT is critical, strategic to the business
Expectations and reality don't match
IT hasn't got the attention it deserves
IT involves huge investments and risks
IT governance!

Dia 6


1.2: What is IT self-assessment about? (2/10)
CobiT, why?
Control OBjectives for Information and Related Technology
Generally apllicable and accepted standard for good practice for information and IT control
Elements of CobiT: executive summary, framework, control objectives, audit guidelines, implementation guide, management guide.

Dia 7


1.2: What is IT self-assessment about? (3/10)
Goal:
To develop the capacity of SAI's to meet their strategic goals through the use of IT (e.g. in relation to internal management, more effective audits, development of skills

Dia 8

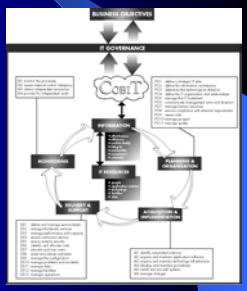
1.2: What is IT self-assessment about? (4/10)

1. What information should it deliver? (5-8/10)
2. How are we going to do the pilot? (9-10/10)

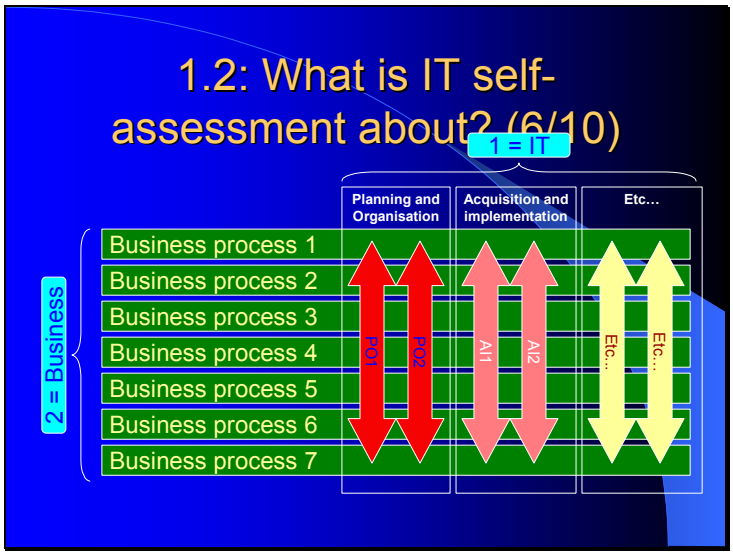
Dia 9

1.2: What is IT self-assessment about? (5/10)

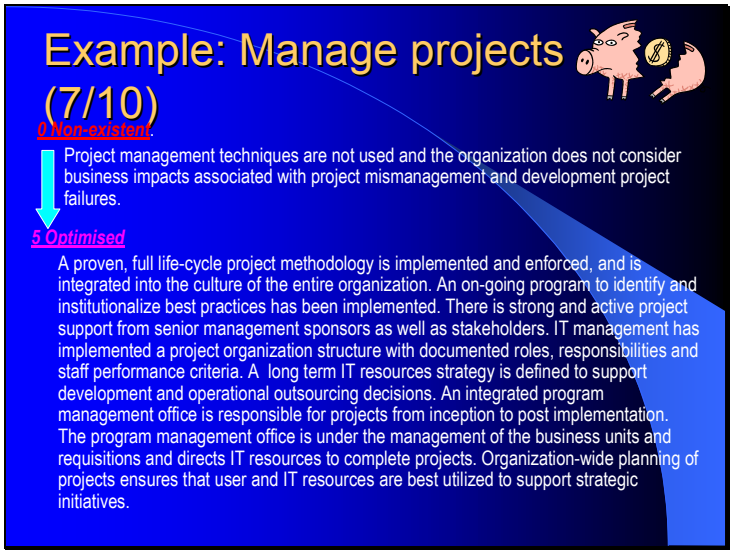
- Key: alignment between business and IT
- Two dimensions of the analysis:
  - Business processes (users)
    - Most important processes in achieving goals; IT-support?
  - IT-processes (IT-staff)
    - Which are the most important?
    - Maturity levels



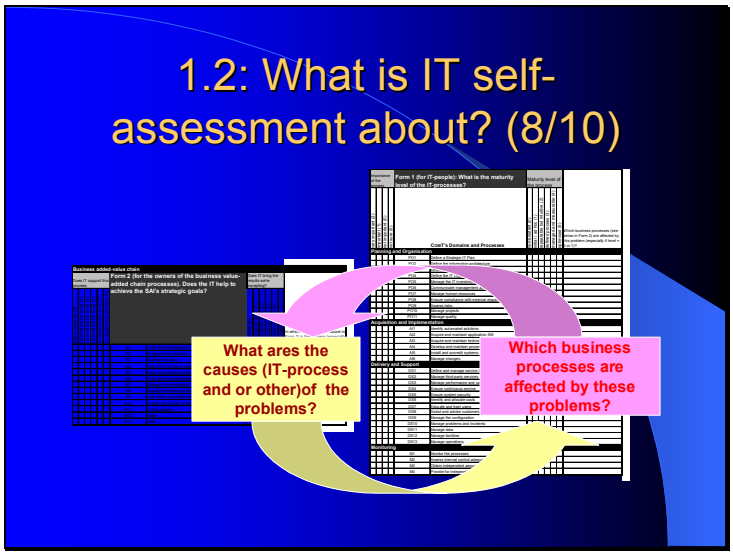
Dia 10


1.2: What is IT self-assessment about? (6/10)
1 = IT
Planning and Organisation
Acquisition and implementation
Etc…
2 = Business
Business process 1
Business process 2
Business process 3
Business process 4
Business process 5
Business process 6
Business process 7
PO1
PO2
AI1
AI2
Etc…
Etc…

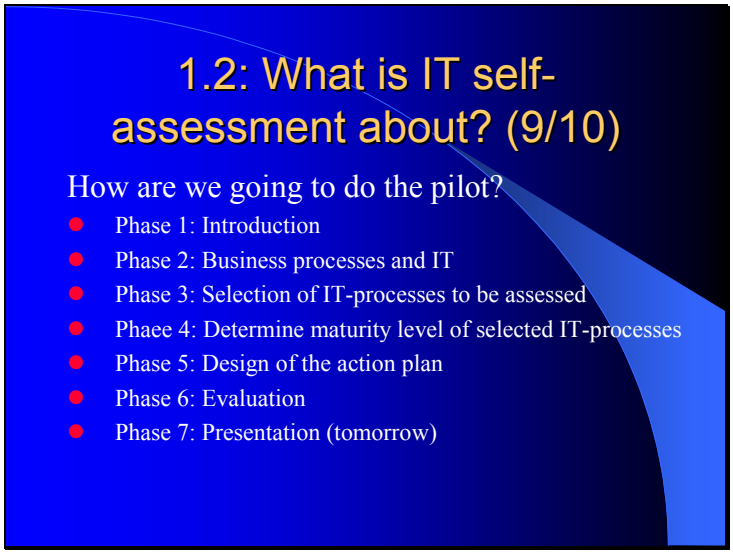
Dia 11


Example: Manage projects (7/10)
0 Non-existent
Project management techniques are not used and the organization does not consider business impacts associated with project mismanagement and development project failures.
5 Optimised
A proven, full life-cycle project methodology is implemented and enforced, and is integrated into the culture of the entire organization. An on-going program to identify and institutionalize best practices has been implemented. There is strong and active project support from senior management sponsors as well as stakeholders. IT management has implemented a project organization structure with documented roles, responsibilities and staff performance criteria. A long term IT resources strategy is defined to support development and operational outsourcing decisions. An integrated program management office is responsible for projects from inception to post implementation. The program management office is under the management of the business units and requisitions and directs IT resources to complete projects. Organization-wide planning of projects ensures that user and IT resources are best utilized to support strategic initiatives.

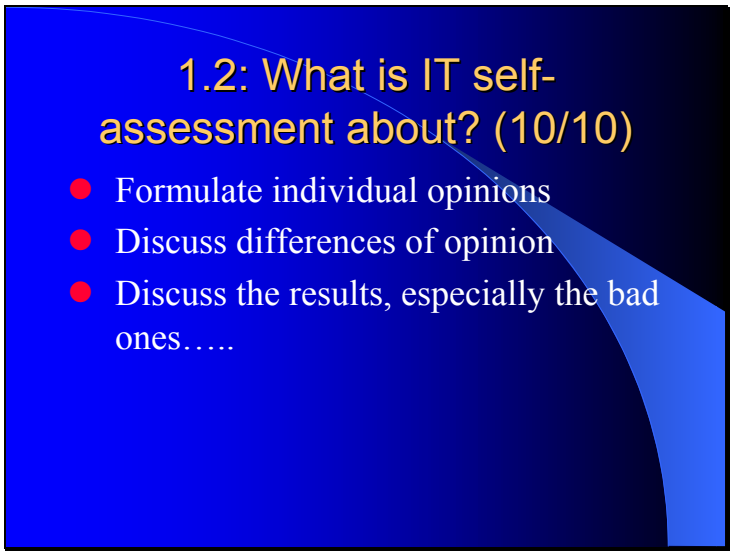
Dia 12


1.2: What is IT self-assessment about? (8/10)
What ares the causes (IT-process and or other)of the problems?
Which business processes are affected by these problems?

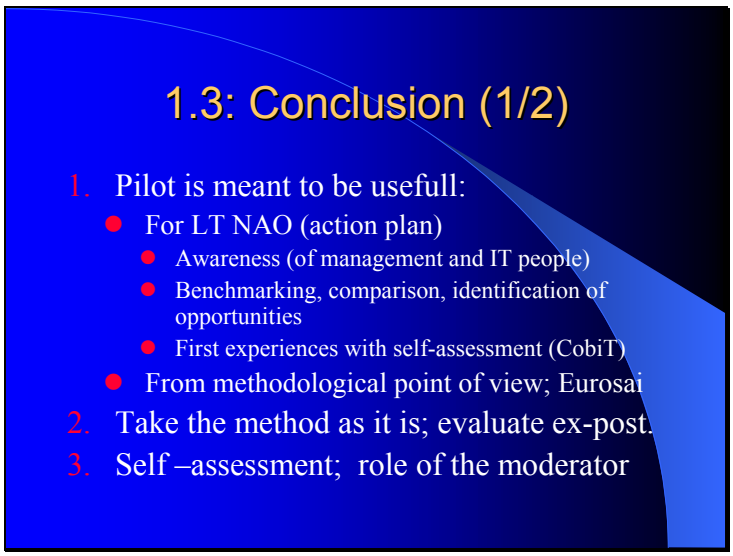
Dia 13


1.2: What is IT self-assessment about? (9/10)
How are we going to do the pilot?
Phase 1: Introduction
Phase 2: Business processes and IT
Phase 3: Selection of IT-processes to be assessed
Phaee 4: Determine maturity level of selected IT-processes
Phase 5: Design of the action plan
Phase 6: Evaluation
Phase 7: Presentation (tomorrow)

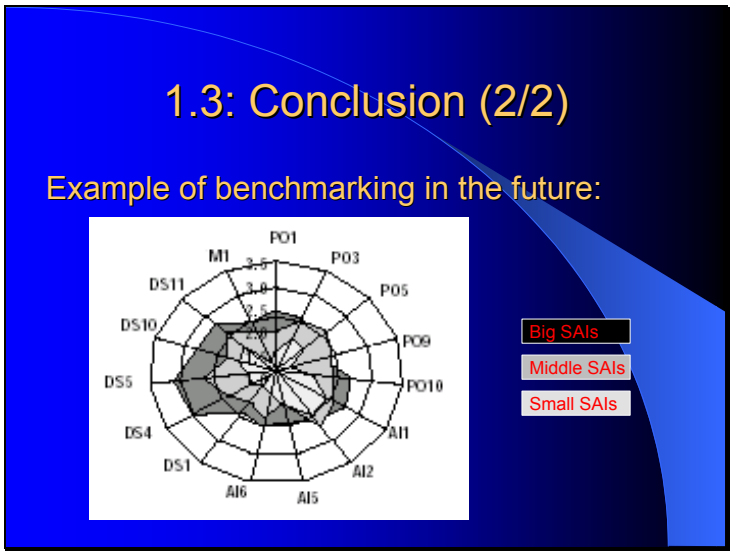
Dia 14


1.2: What is IT self-assessment about? (10/10)
Formulate individual opinions
Discuss differences of opinion
Discuss the results, especially the bad ones…..

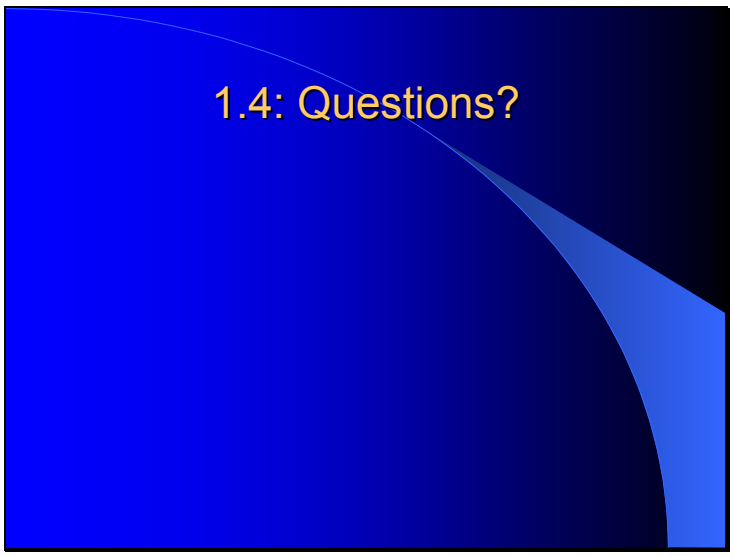
Dia 15


1.3: Conclusion (1/2)
1. Pilot is meant to be usefull:
For LT NAO (action plan)
Awareness (of management and IT people)
Benchmarking, comparison, identification of opportunities
First experiences with self-assessment (CobiT)
From methodological point of view; Eurosai
2. Take the method as it is; evaluate ex-post.
3. Self –assessment; role of the moderator

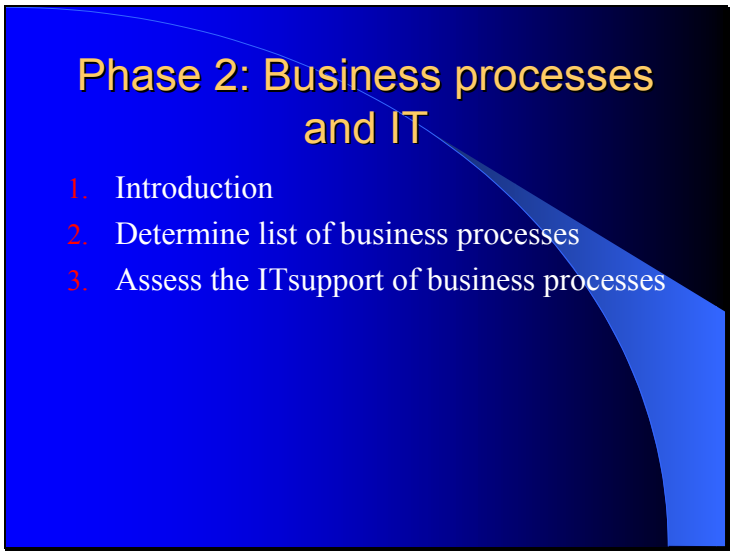
Dia 16


1.3: Conclusion (2/2)
Example of benchmarking in the future:
PO1
PO3
PO5
PO9
PO10
AI1
AI2
AI5
AI6
DS1
DS4
DS5
DS10
DS11
M1
Big SAIs
Middle SAIs
Small SAIs

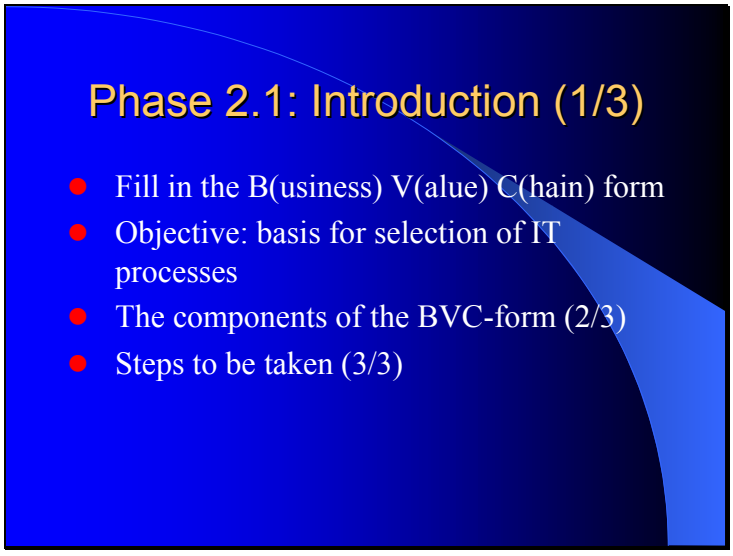
Dia 17


1.4: Questions?

Dia 18


Phase 2: Business processes and IT
1. Introduction
2. Determine list of business processes
3. Assess the ITsupport of business processes

Dia 19


Phase 2.1: Introduction (1/3)
Fill in the B(usiness) V(alue) C(hain) form
Objective: basis for selection of IT processes
The components of the BVC-form (2/3)
Steps to be taken (3/3)

Dia 20

Phase 2.1: Introduction (2/3)

Business added-value chain

What is the importance of the current IT systems for this business process?						What is the importance of the future IT systems for this business process?						BVC Form 1 (for the owners of the business value-added chain processes). Does the IT help to achieve the SAI's strategic goals?		What is the quality of the current IT systems?						In which IT-process (see in Form 2) is the problem (especially if quality level = 0 or 1)?
high (5)	importance level (4)	importance level (3)	importance level (2)	low (1)	no application software (0)	high (5)	importance level (4)	importance level (3)	importance level (2)	low (1)	no application software (0)			very low (0)	quality level (1)	quality level (2)	quality level (3)	quality level (4)	very high (5)	
												B1	Audit Risk Management							
												B2	Organise the missions							
												B3	Analyse the data							
												B4	Test the IT by the IT-Audit							
												B5	Report the results to the auditee							
												B6	Track the implementation of the recommandations							
												B7	Manage the knowledge							
												B8	Manage finances and human ressources							
												B9	Administer and archive the dossiers							
												B10	Publish the results of the audits							
												B11	Communicate							
												B12	other ...							
												B13	other...							

Dia 21

Phase 2.1: Introduction (3/3)

- Steps to be taken:
  - Determine list of business processes (2.2)
  - Assess IT support of business processes (2.3)
    - Individual scoring of every business process
    - Statistics
    - Group process:
      - Reach consensus on IT support
      - Determine relevant IT processes and evidence

Dia 22

Phase 2.2: Determine list of processes (1/2)

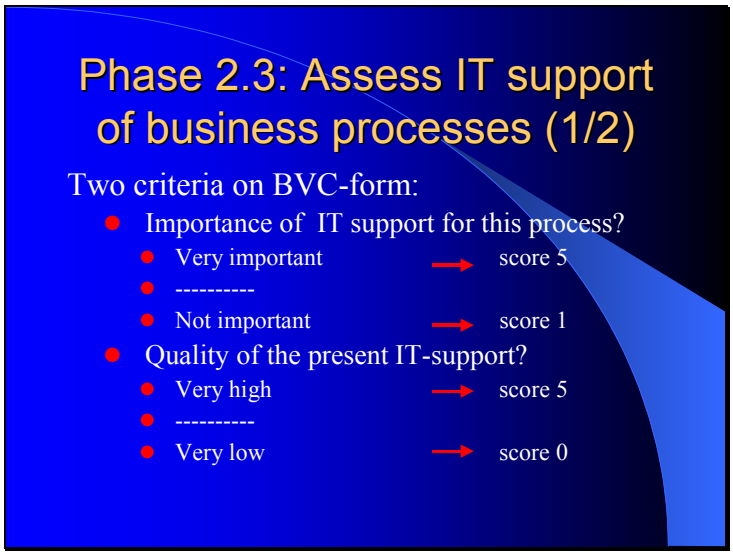
1. List on BVC-form is just a proposal
2. An example: the audit process at the Netherlands Court of Audit (2/2)
   - Auditing, but also exchange of knowledge
3. Main distinction: primary – secundary
4. Determine your SAI's primary processes
5. Determine your SAI's secundary processes

Dia 23

Phase 2.2: Determine list of processes (2/2)

Audit process at the Netherlands Court of Audit:

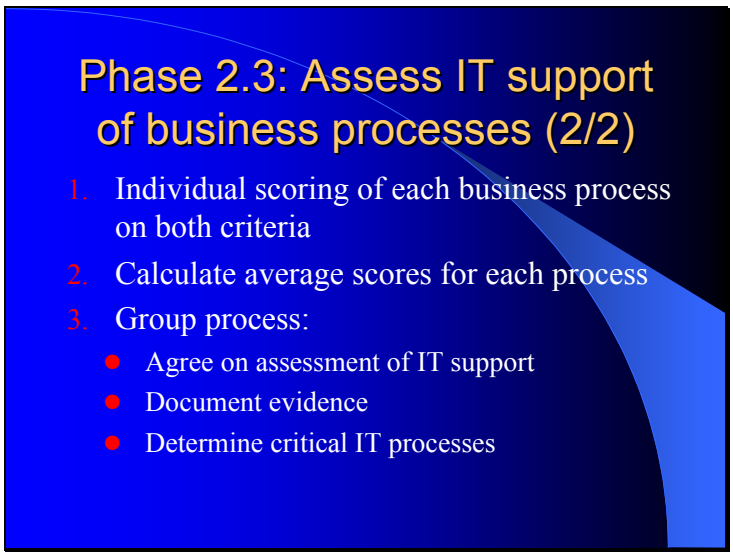
Dia 24


Phase 2.3: Assess IT support of business processes (1/2)
Two criteria on BVC-form:
Importance of IT support for this process?
Very important → score 5

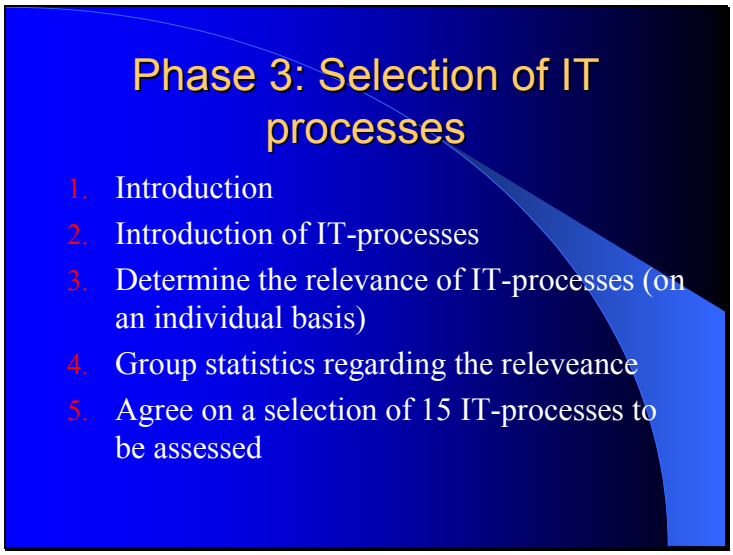
Not important → score 1
Quality of the present IT-support?
Very high → score 5

Very low → score 0

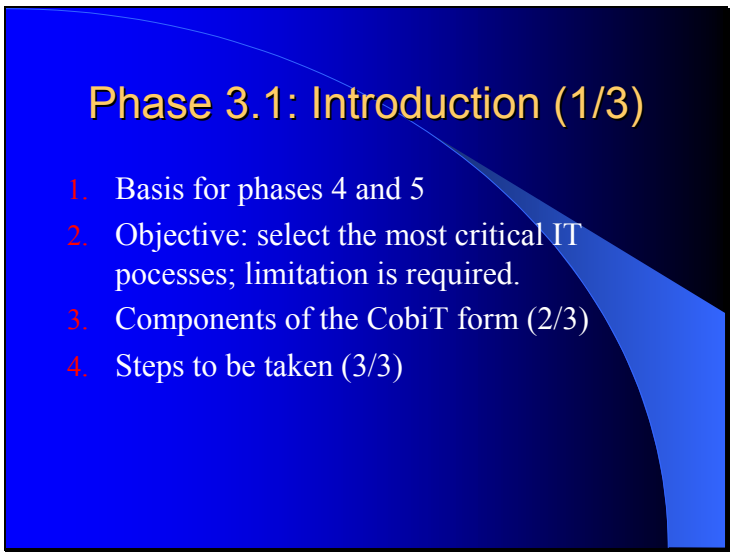
Dia 25


Phase 2.3: Assess IT support of business processes (2/2)
1. Individual scoring of each business process on both criteria
2. Calculate average scores for each process
3. Group process:
Agree on assessment of IT support
Document evidence
Determine critical IT processes

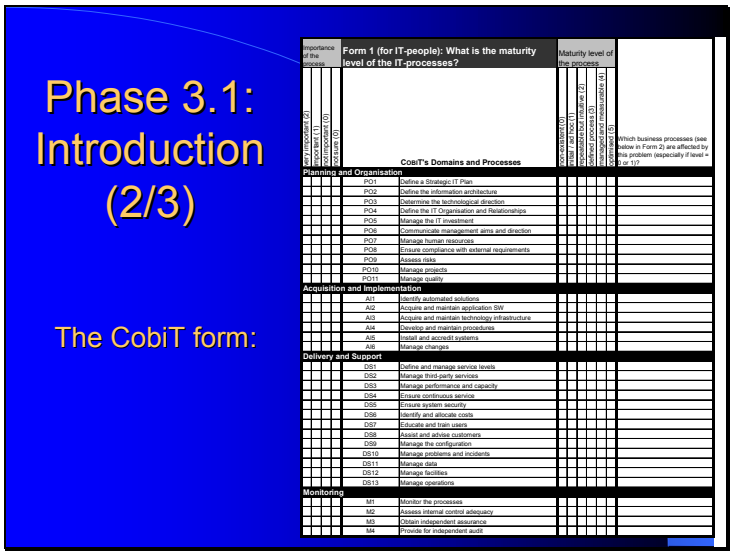
Dia 26


Phase 3: Selection of IT processes
1. Introduction
2. Introduction of IT-processes
3. Determine the relevance of IT-processes (on an individual basis)
4. Group statistics regarding the releveance
5. Agree on a selection of 15 IT-processes to be assessed

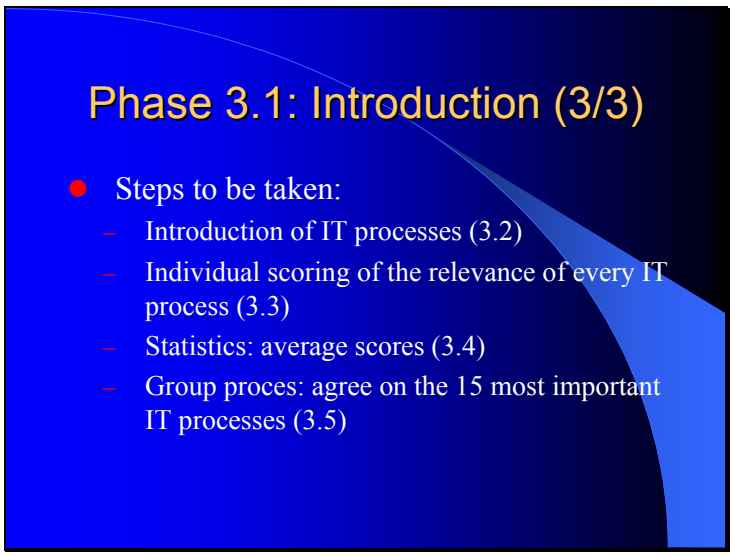
Dia 27


Phase 3.1: Introduction (1/3)
1. Basis for phases 4 and 5
2. Objective: select the most critical IT pocesses; limitation is required.
3. Components of the CobiT form (2/3)
4. Steps to be taken (3/3)

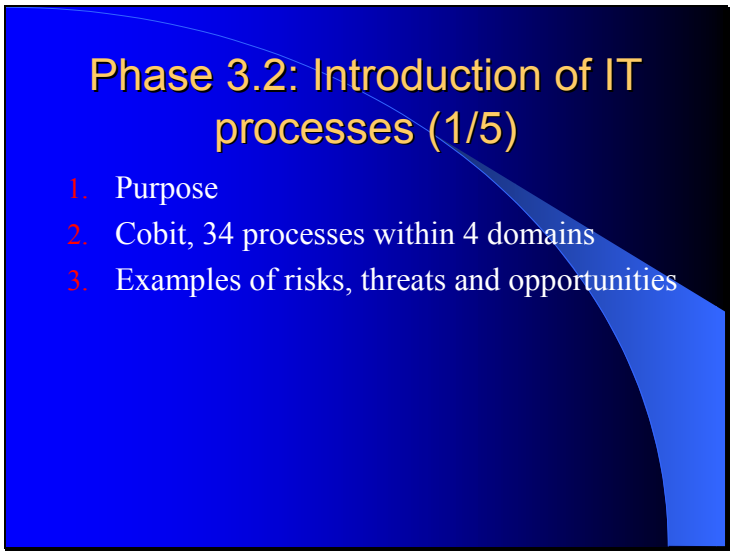
Dia 28


Phase 3.1: Introduction (2/3)
The CobiT form:
Form 1 (for IT-people): What is the maturity level of the IT-processes?
Maturity level of the process
CobiT's Domains and Processes
Planning and Organisation
PO1 Define a Strategic IT Plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT Organisation and Relationships
PO5 Manage the IT investment
PO6 Communicate management aims and direction
PO7 Manage human resources
PO8 Ensure compliance with external requirements
PO9 Assess risks
PO10 Manage projects
PO11 Manage quality
Acquisition and Implementation
AI1 Identify automated solutions
AI2 Acquire and maintain application SW
AI3 Acquire and maintain technology infrastructure
AI4 Develop and maintain procedures
AI5 Install and accredit systems
AI6 Manage changes
Delivery and Support
DS1 Define and manage service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure system security
DS6 Identify and allocate costs
DS7 Educate and train users
DS8 Assist and advise customers
DS9 Manage the configuration
DS10 Manage problems and incidents
DS11 Manage data
DS12 Manage facilities
DS13 Manage operations
Monitoring
M1 Monitor the processes
M2 Assess internal control adequacy
M3 Obtain independent assurance
M4 Provide for independent audit

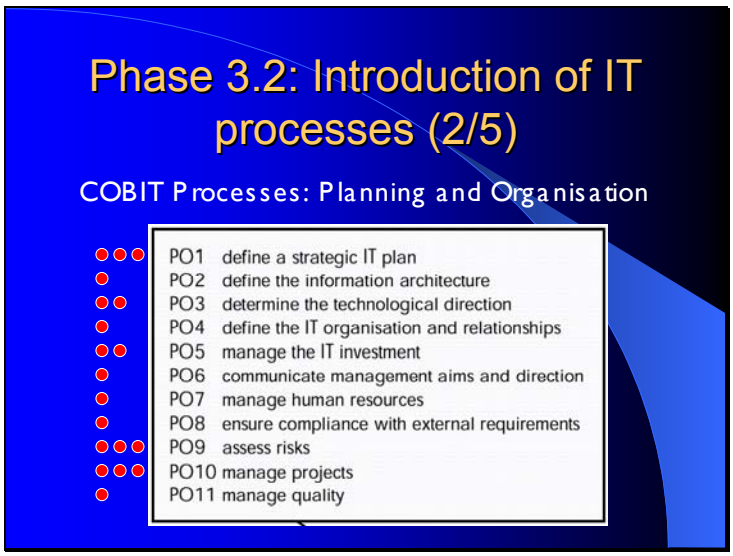
Dia 29


Phase 3.1: Introduction (3/3)
Steps to be taken:
Introduction of IT processes (3.2)
Individual scoring of the relevance of every IT process (3.3)
Statistics: average scores (3.4)
Group proces: agree on the 15 most important IT processes (3.5)

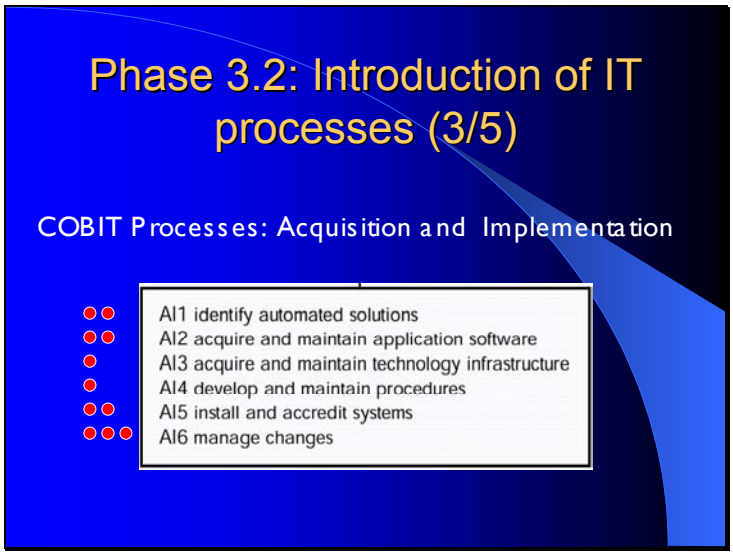
Dia 30


Phase 3.2: Introduction of IT processes (1/5)
1. Purpose
2. Cobit, 34 processes within 4 domains
3. Examples of risks, threats and opportunities

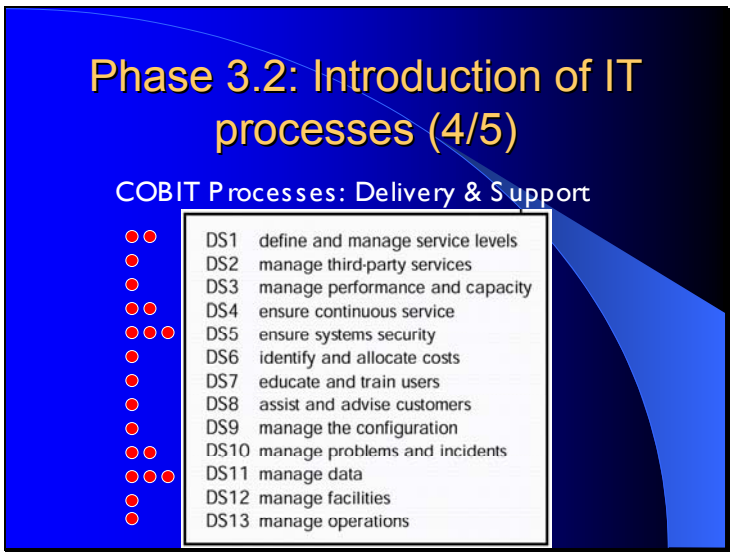
Dia 31


Phase 3.2: Introduction of IT processes (2/5)
COBIT Processes: Planning and Organisation
PO1 define a strategic IT plan
PO2 define the information architecture
PO3 determine the technological direction
PO4 define the IT organisation and relationships
PO5 manage the IT investment
PO6 communicate management aims and direction
PO7 manage human resources
PO8 ensure compliance with external requirements
PO9 assess risks
PO10 manage projects
PO11 manage quality

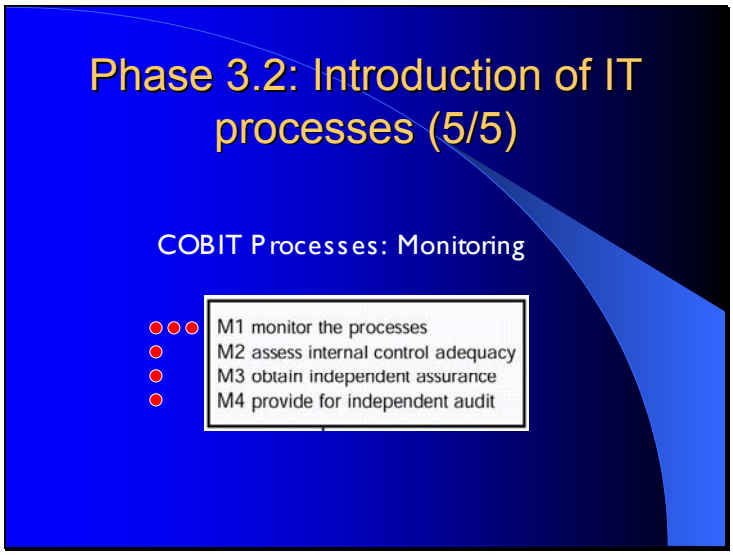
Dia 32


Phase 3.2: Introduction of IT processes (3/5)
COBIT Processes: Acquisition and Implementation
AI1 identify automated solutions
AI2 acquire and maintain application software
AI3 acquire and maintain technology infrastructure
AI4 develop and maintain procedures
AI5 install and accredit systems
AI6 manage changes

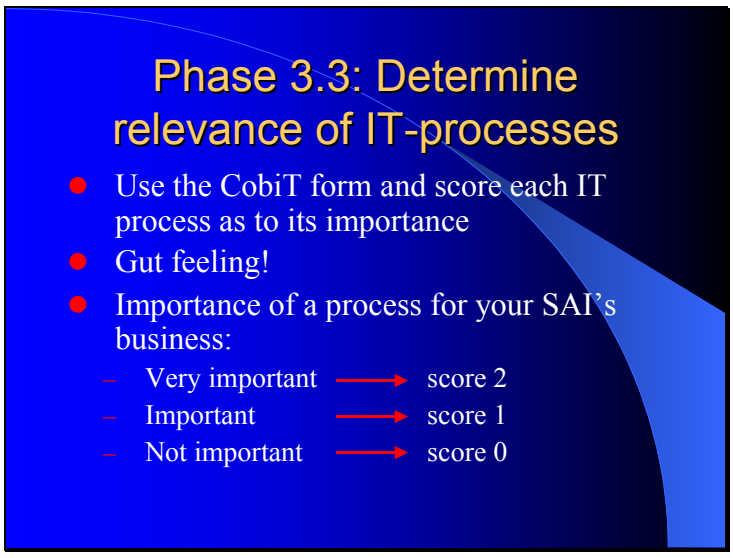
Dia 33


Phase 3.2: Introduction of IT processes (4/5)
COBIT Processes: Delivery & Support
DS1 define and manage service levels
DS2 manage third-party services
DS3 manage performance and capacity
DS4 ensure continuous service
DS5 ensure systems security
DS6 identify and allocate costs
DS7 educate and train users
DS8 assist and advise customers
DS9 manage the configuration
DS10 manage problems and incidents
DS11 manage data
DS12 manage facilities
DS13 manage operations

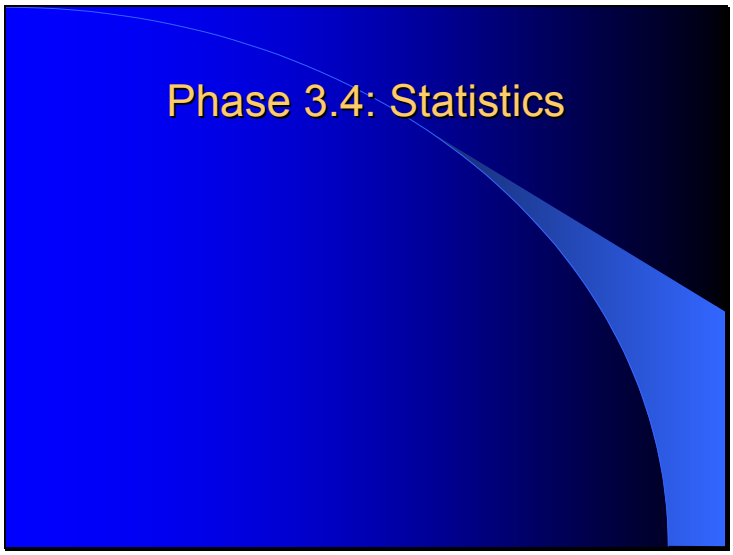
Dia 34


Phase 3.2: Introduction of IT processes (5/5)
COBIT Processes: Monitoring
M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit

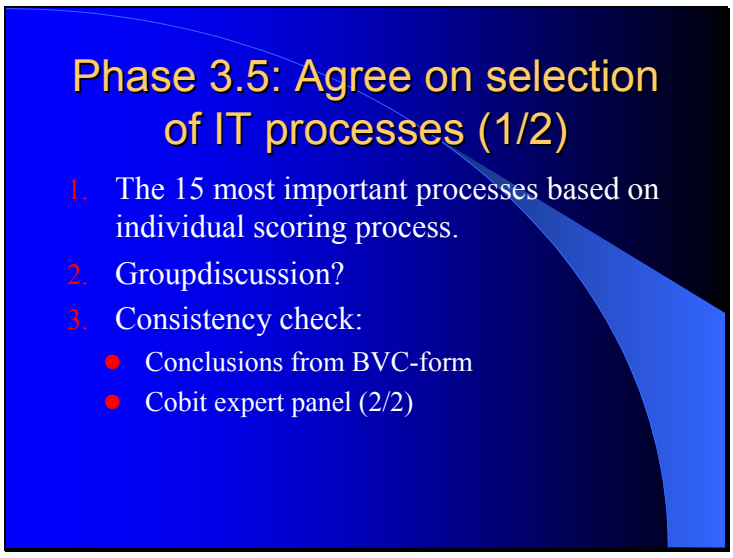
Dia 35


Phase 3.3: Determine relevance of IT-processes
Use the CobiT form and score each IT process as to its importance
Gut feeling!
Importance of a process for your SAI's business:
Very important → score 2
Important → score 1
Not important → score 0

Dia 36


Phase 3.4: Statistics

Dia 37


Phase 3.5: Agree on selection of IT processes (1/2)
1. The 15 most important processes based on individual scoring process.
2. Groupdiscussion?
3. Consistency check:
Conclusions from BVC-form
Cobit expert panel (2/2)

Dia 38

Phase 3.5: Agree on selection of IT processes (2/2)

High importance:	Medium importance:
PO1: define a strategic plan PO9: assess risks PO10: manage projects	PO3: determine the technological direction PO5: manage the IT investment
AI6: manage changes	AI1: identiy automated solutions AI2: acquire and maintain application software AI5: install and accredit systems
DS5: ensure systems security DS11: manage data	DS1: define and manage service levels DS4: ensure continuous service DS10: manage problems and incidents
M1: monitor the processes	

Dia 39

Phase 4: Determine maturity of selected IT processes

1. Introduction
2. Introduction of maturity levels
3. Determine maturity level

Dia 40

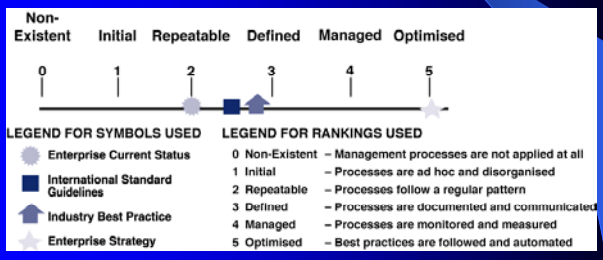
Phase 4.1: Introduction

1. Objective: determine maturity level of important IT-processes as a basis for improvement
2. Steps to be taken:
   - Introduction of maturity levels (4.2)
   - Determination of maturity levels (4.3)
     - Individual determination of the maturity level of each IT process
     - Statistics
     - Group process: consensus and evidence

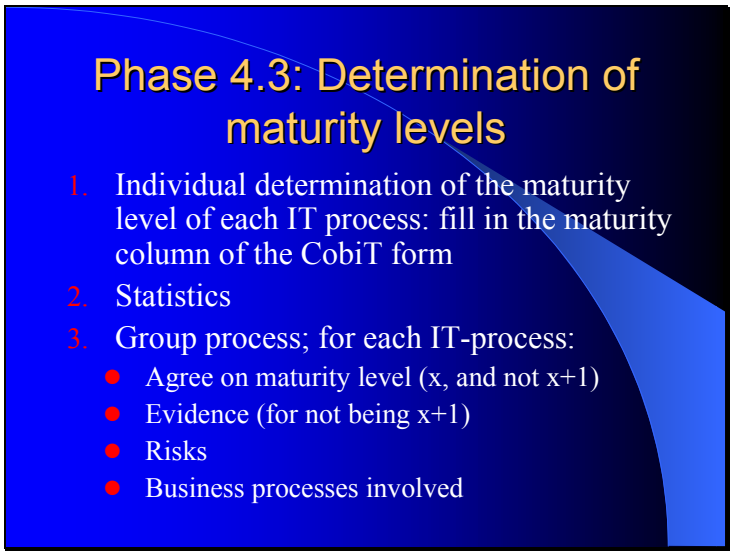
Dia 41

Phase 4.2: Introduction of maturity levels

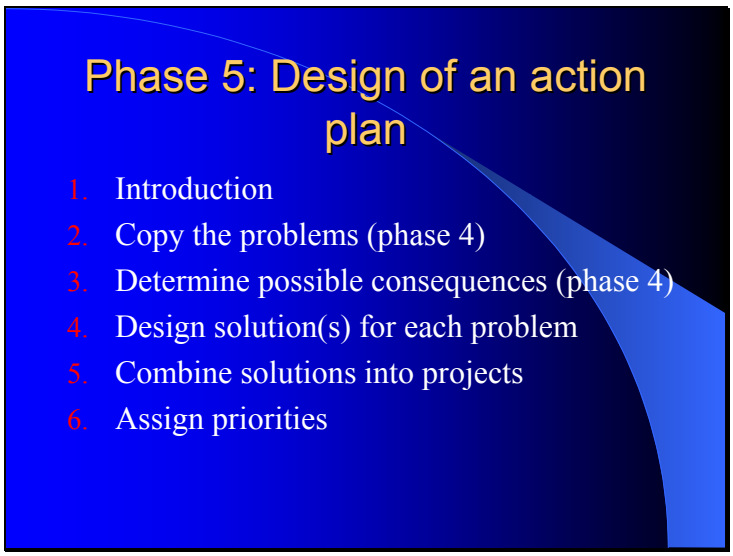
Maturity Models for Self-Assessment



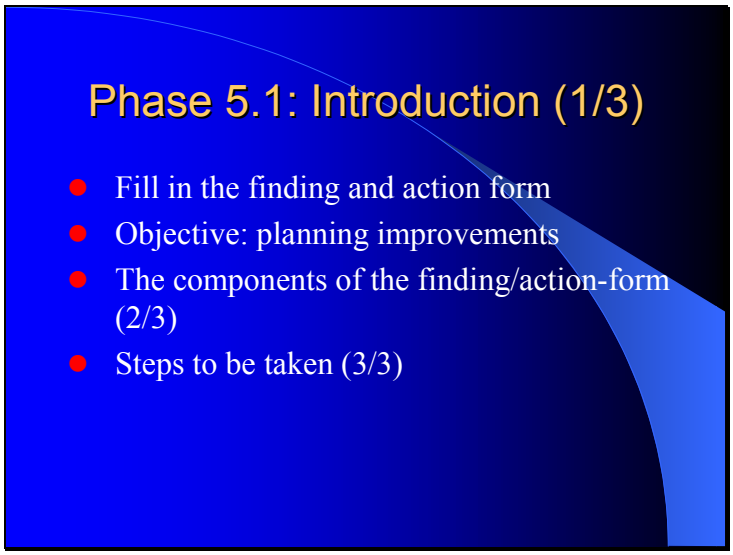
Dia 42


Phase 4.3: Determination of maturity levels
1. Individual determination of the maturity level of each IT process: fill in the maturity column of the CobiT form
2. Statistics
3. Group process; for each IT-process:
- Agree on maturity level (x, and not x+1)
- Evidence (for not being x+1)
- Risks
- Business processes involved

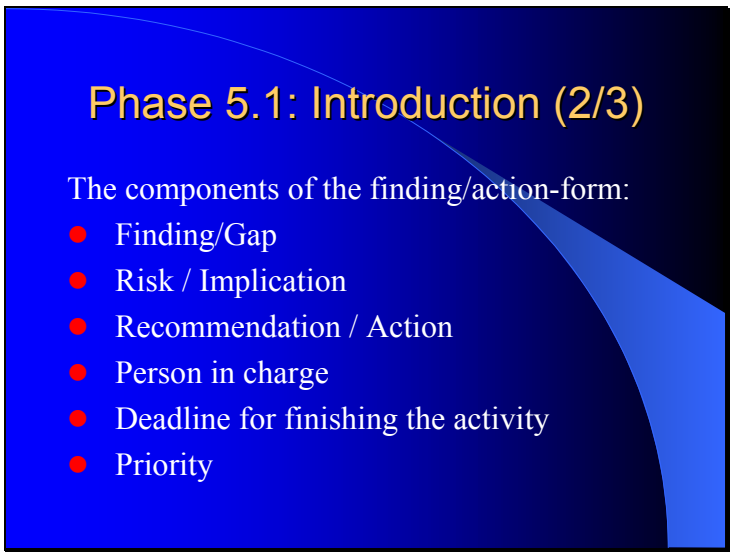
Dia 43


Phase 5: Design of an action plan
1. Introduction
2. Copy the problems (phase 4)
3. Determine possible consequences (phase 4)
4. Design solution(s) for each problem
5. Combine solutions into projects
6. Assign priorities

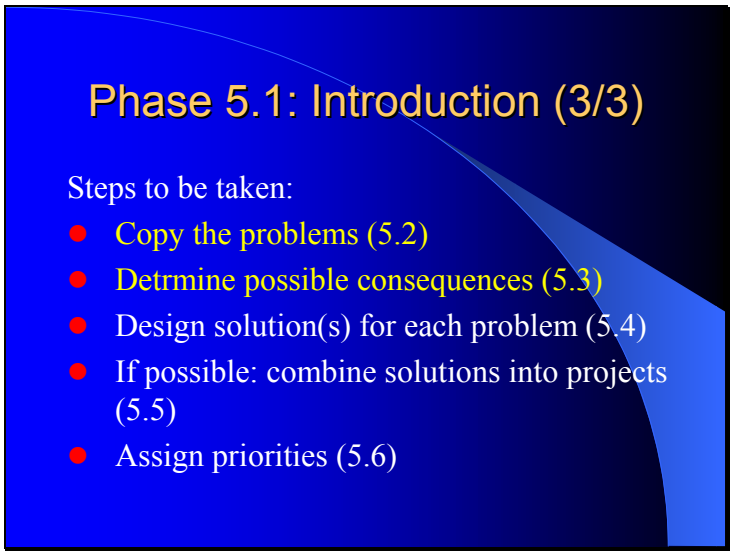
Dia 44


Phase 5.1: Introduction (1/3)
Fill in the finding and action form
Objective: planning improvements
The components of the finding/action-form (2/3)
Steps to be taken (3/3)

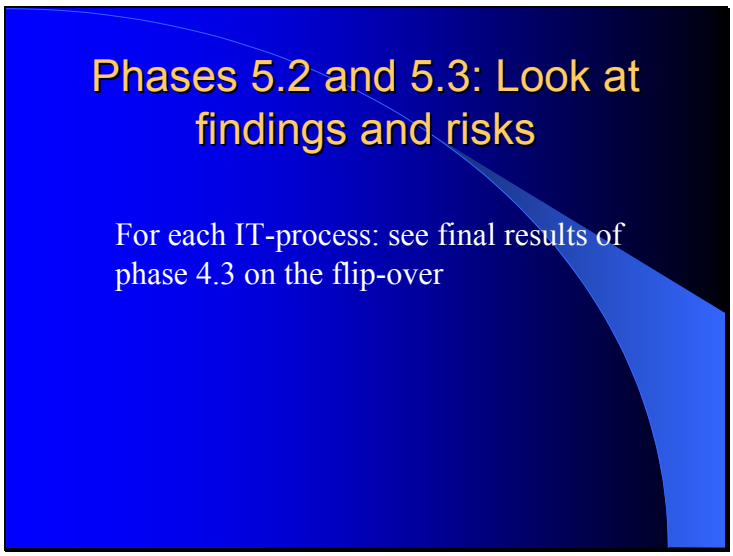
Dia 45


Phase 5.1: Introduction (2/3)
The components of the finding/action-form:
Finding/Gap
Risk / Implication
Recommendation / Action
Person in charge
Deadline for finishing the activity
Priority

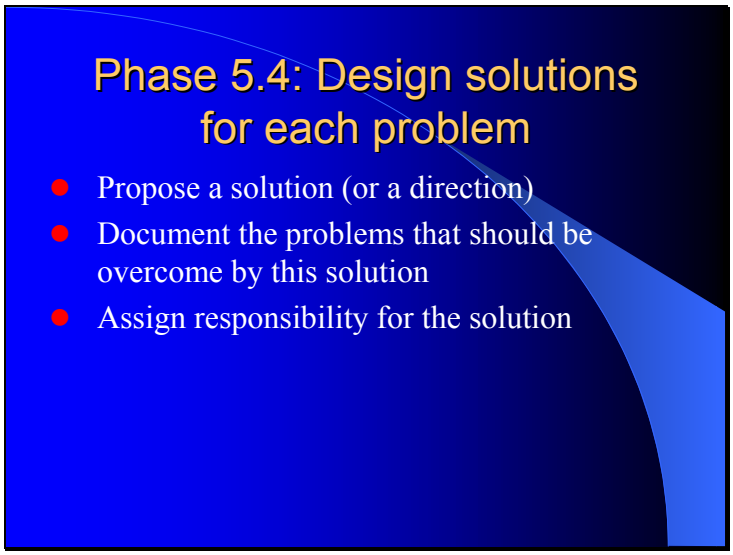
Dia 46


Phase 5.1: Introduction (3/3)
Steps to be taken:
Copy the problems (5.2)
Detrmine possible consequences (5.3)
Design solution(s) for each problem (5.4)
If possible: combine solutions into projects (5.5)
Assign priorities (5.6)

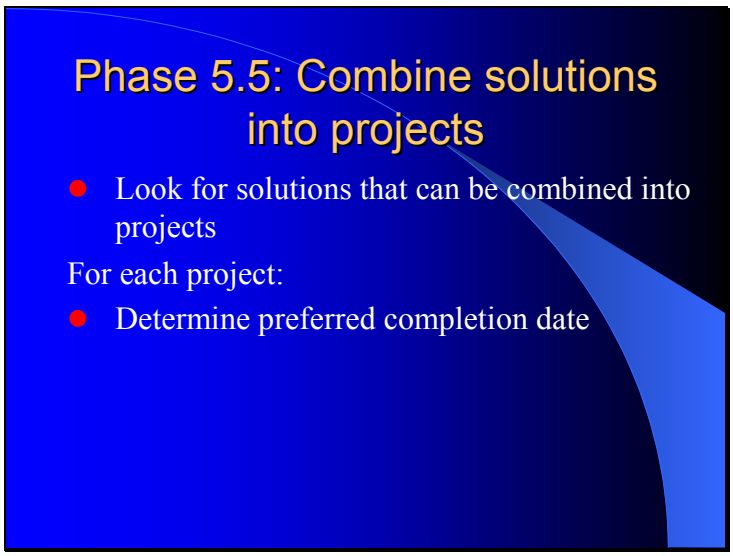
Dia 47


Phases 5.2 and 5.3: Look at findings and risks
For each IT-process: see final results of phase 4.3 on the flip-over

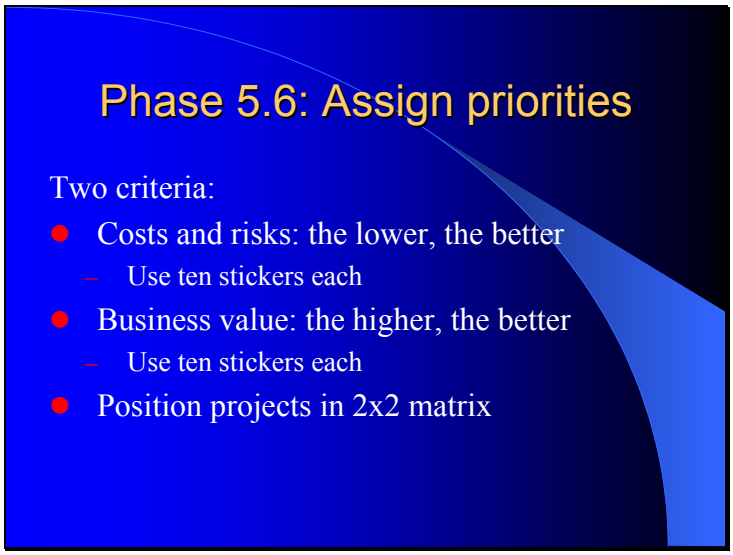
Dia 48


Phase 5.4: Design solutions for each problem
Propose a solution (or a direction)
Document the problems that should be overcome by this solution
Assign responsibility for the solution

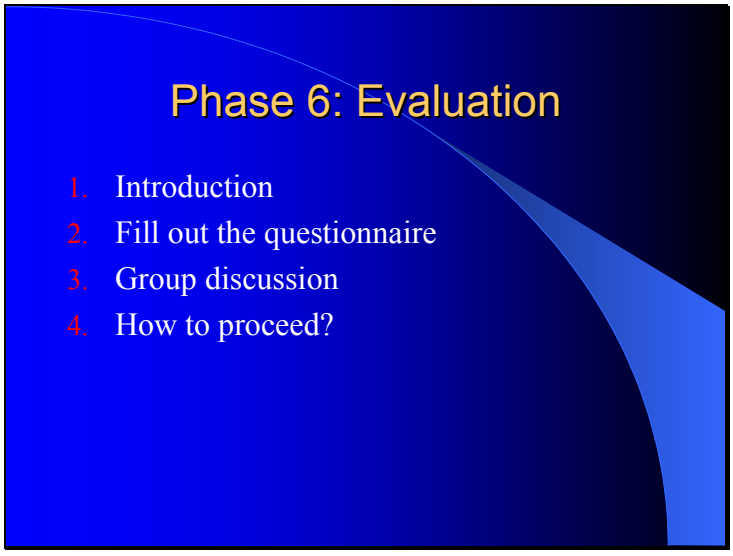
Dia 49


Phase 5.5: Combine solutions into projects
Look for solutions that can be combined into projects
For each project:
Determine preferred completion date

Dia 50


Phase 5.6: Assign priorities
Two criteria:
Costs and risks: the lower, the better
Use ten stickers each
Business value: the higher, the better
Use ten stickers each
Position projects in 2x2 matrix

Dia 51


Phase 6: Evaluation
1. Introduction
2. Fill out the questionnaire
3. Group discussion
4. How to proceed?

Annex 2: The Cobit Form

Importance of the process				CobiT Form 2: What is the maturity level of the IT-processes?		Maturity level of the process						
very important (2)	important (1)	not important (0)	not sure (0)	CobiT's Domains and Processes		non-existent (0)	initial / ad hoc (1)	repeatable but intuitive (2)	defined process (3)	managed and measurable (4)	optimised (5)	Remarks:
Planning and Organisation												
				PO1	Define a Strategic IT Plan							
				PO2	Define the information architecture							
				PO3	Determine the technological direction							
				PO4	Define the IT Organisation and Relationships							
				PO5	Manage the IT investment							
				PO6	Communicate management aims and direction							
				PO7	Manage human resources							
				PO8	Ensure compliance with external requirements							
				PO9	Assess risks							
				PO10	Manage projects							
				PO11	Manage quality							
Acquisition and Implementation												
				AI1	Identify automated solutions							
				AI2	Acquire and maintain application SW							
				AI3	Acquire and maintain technology infrastructure							
				AI4	Develop and maintain procedures							
				AI5	Install and accredit systems							
				AI6	Manage changes							
Delivery and Support												
				DS1	Define and manage service levels							
				DS2	Manage third-party services							
				DS3	Manage performance and capacity							
				DS4	Ensure continuous service							
				DS5	Ensure system security							
				DS6	Identify and allocate costs							
				DS7	Educate and train users							
				DS8	Assist and advise customers							
				DS9	Manage the configuration							
				DS10	Manage problems and incidents							
				DS11	Manage data							
				DS12	Manage facilities							
				DS13	Manage operations							
Monitoring												
				M1	Monitor the processes							
				M2	Assess internal control adequacy							
				M3	Obtain independent assurance							
				M4	Provide for independent audit							

Annex 3: The Business Value Chain Form

Business added-value chain																		
What is the importance of the current IT systems for this business process?						What is the importance of the future IT systems for this business process?						BVC Form 1: Does the IT help to achieve the SAI's strategic goals?		What is the quality of the current IT systems ?					
high (5)	importance level (4)	importance level (3)	importance level (2)	low (1)	no application software (0)	high (5)	importance level (4)	importance level (3)	importance level (2)	low (1)	no application software (0)			very low (0)	quality level (1)	quality level (2)	quality level (3)	quality level (4)	very high (5)	In which IT-process (see in Form 2) is the problem (especially if quality level = 0 or 1)?
												B1	Audit Risk Management							
												B2	Organise the missions							
												B3	Analyse the data							
												B4	Test the IT by the IT-Audit							
												B5	Report the results to the auditee							
												B6	Track the implementation of the recommandations							
												B7	Manage the knowledge							
												B8	Manage finances and human ressources							
												B9	Administer and archive the dossiers							
												B10	Publish the results of the audits							
												B11	Communicate							
												B12	other …							
												B13	other…							

Annex 4: The Findings and Actions Form

Findings and Actions form					
Finding/ Gap Description	**Risk / implication**	**Recommendation / action description**	**Person in charge**	**Deadline for finishing activity**	**Priority 1-10**

Annex 5: The Evaluation Forms

Questionnaire on the evaluation of the SAI's IT Self-assessment EUROSAI IT Working Group

Introduction

- Objectives: To obtain concrete proposals for improvements to the SAI's IT Self-assessment process and its guidelines.

The completion of the questionnaire is the responsibility of the entire Self-assessment group.

General: identification of the SAI and application of the SAI's IT Self-assessment
Note: one representative should answer the following 7 questions
of the Self-assessment group.

Nr	Question	Answer
1	Briefly describe the use of the IT in your SAI?	

2	Is IT critical to the business?	
3	Are there any IT-management functions outsourced?	
4	How many persons are in your IT-department?	
5	Was the SAI's IT Self-assessment applied in the whole or in a part of the organization or in the IT-department?	
6	How many people took part in the Self-assessment process?	
7	Who were involved in the Self-assessment group?	

Questionnaire on the evaluation of the SAI's IT Self-assessment EUROSAI IT Working Group

Introduction

- Objectives: To obtain concrete proposals for improvements to the SAI's IT Self-assessment process and its guidelines.

Evaluation of the self-assessment by each member of the self-assessment group:

Nr	Question:	Answer:
1	Do you have any previous experience with self-assessment? (yes/no)	
2	Do you have any experience with COBIT? (yes/no)	
3	In your opinion, were the right persons involved in the self-assessment group? (yes/no) If no, how should the self-	

	assessment group be composed?	
4	Do you think that you had sufficient support, in terms of information and explanations (before and during the self-assessment process), for carrying out the SAI's IT self-assessment? (yes/no) If no, what was missing?	
5	If your organization were to repeat the SAI's It self-assessment, what steps would you take to improve the process?	
6	Did the results of the self-assessment come up to your expectations? Please explain?	
7	Did you prepare an action plan for the future?	
8	Having carried out the self-assessment, what do you think are its main advantages and disadvantages for the functioning of your organization?	

9	Do you think that the SAI's IT self-assessment is an effective management tool in itself? Why?	
10	Is repetition of the self-assessment process at some time useful?	

The methodology and the guidelines

Nr	Question	Answer
1	Please give your comments regarding the first dimension of the analysis, indicating any problems you have in understanding the COBIT-processes, as well as suggestions for improvement?	
2	Do you find the information about the maturity levels enough to do scoring?	
3	Do you think the documentation, the forms and the guidelines are clear and explained in sufficient depth to carry out the self-assessment exercise? If not, please specify?	
4	Would you be prepared with other SAI's to exchange experiences (yes/no) and become involved in benchmarking?	
5	Do you think the SAI's IT self-assessment could be useful in the audit practice?	