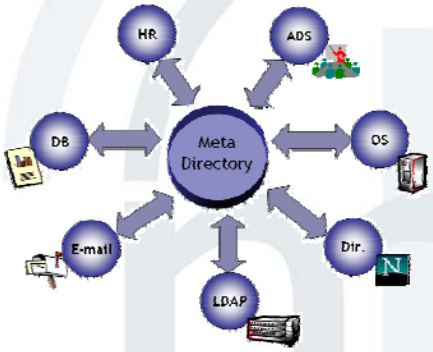
IFIP FIDIS Summer School 2007:

Enterprise Identity Management – What's in it for Organisations?



Denis Royer
Johann Wolfgang Goethe University Frankfurt
Chair for Mobile Business and Multilateral Security

Agenda

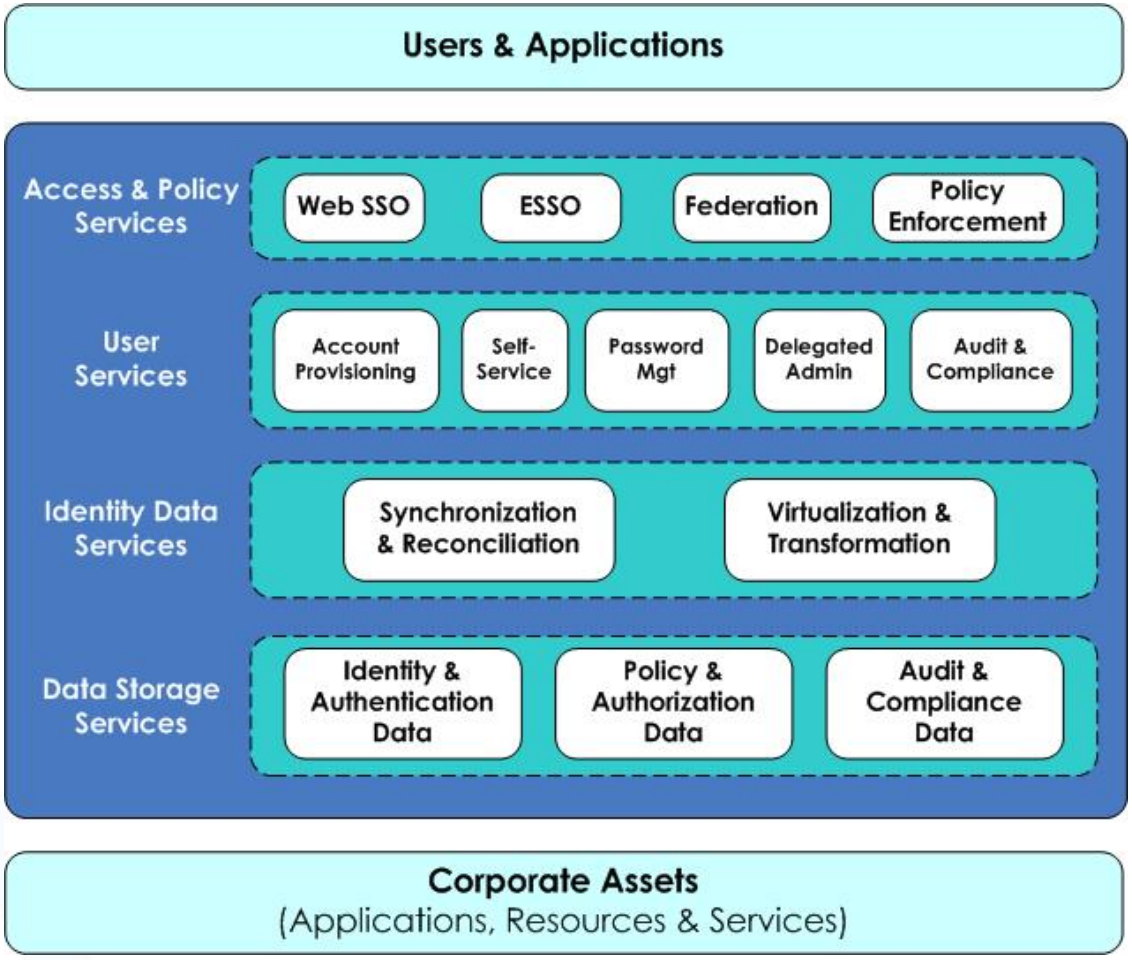
- Introduction
  - The Need for IdM in Organisations
  - Driving Factors for IDM
  - The Cost Side of IdM
- Evaluation of IdM
  - Prerequisites
  - The Evaluation Process
- Conclusion / Discussion

Goals and Objective

- Security related technologies often lack strategic focus for the decision makers.
- Decision makers will not invest into security technologies and infrastructures without analysing the costs and benefits.
- Evaluation schemes are needed to help identifying potentials and support the decision making process.

➔ *A generic approach how to tackle these issues is presented.*

Enterprise Identity Management



Identity lifecycle

- *Enrolment* - Creation of accounts for new employees: issuance of the credentials and setting of the access permissions.
- *Management* - Maintenance of accounts: in a changing working environment (promotions, change of departments, etc,) the user and access management needs to handle the access permission (e.g. for minimising liabilities).
- *Support* - Password management: issue new passwords or reset passwords that are “lost”.
- *Deletion* - End of lifecycle: revoke or freeze accounts or entitlements.

(Enterprise) Identity Management

- **Organisational:** Software systems that help to facilitate one or more of the 4 As: Authorisation, Authentication, Administration, and Audit
- **Technological:** Cluster of different technologies:
  - Single Sign-On (SSO)
  - Meta Directories
  - PKI Infrastructures
  - Access Management Systems
  - …
- Therefore, IdM is a framework of different technologies, not a specific product.

Problems of IT Security Investments

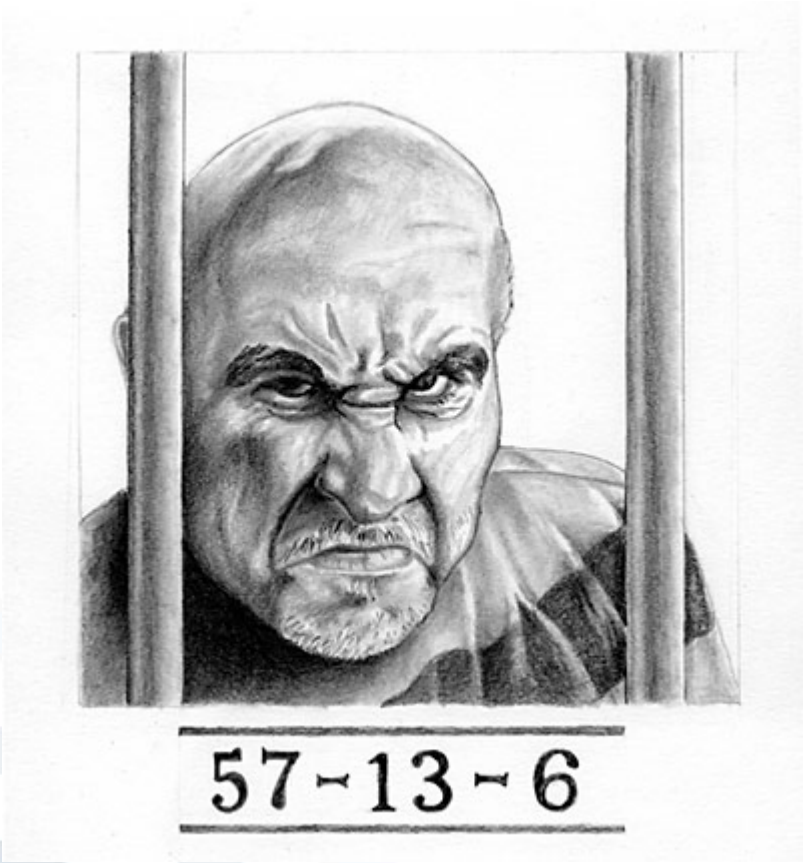
- Many problems inherited from general IT investments.
- Also additional problems:
  - “How can the arguments be overcome that security investments do not generate any revenue?”
  - “How can an IT security investment be established as cost-effective, when the best that could happen is that “nothing” happens?”
  - “How can the optimal level of the total IT security investments be determined?”

Driving Factors for IdM

- Amongst a variety of driving factors for introducing IdM into an organisation, the most prerelevant appear to be:
  - Risk management / IT security soals
  - Value creation goals (e.g. efficiency, cost reduction)
  - *Compliance goals*

- The goals itself are not mutually exclusive - However there are overlaps.

Example: The CIO and Compliance



- Legislative mandates
  - Sarbanes-Oxley
  - Basel 2
- *Goals:* accountability, fraud prevention, & reporting
- Instruments needed to build up infrastructures and to control them
- Otherwise risk of serving "*jail time*" for the CIO.

The cost side

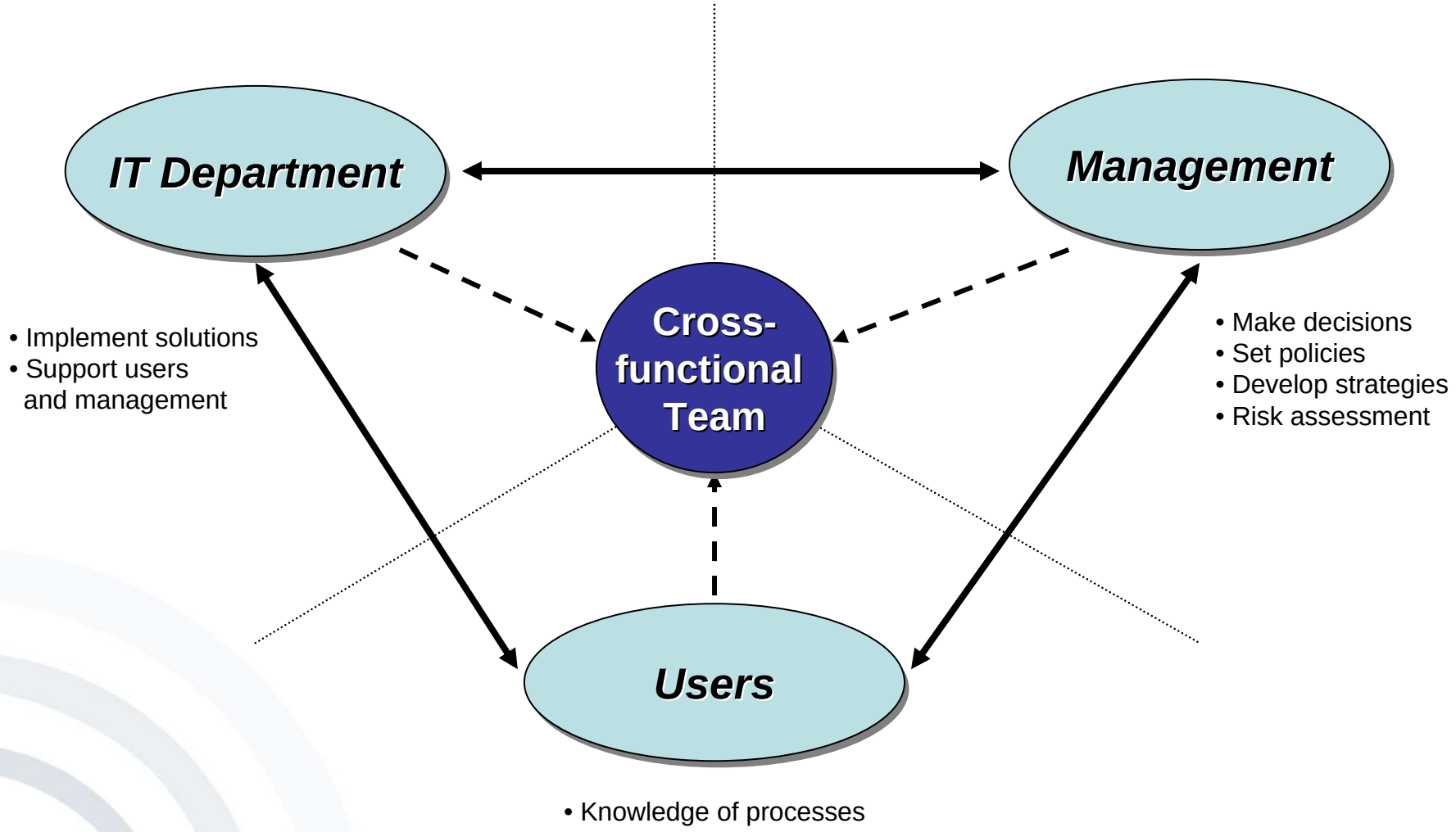
- IdM is not a purely technology driven topic, as it intervenes with the infrastructure and the processes in an organisation.
- The nature of the projects differ considerably, depending on the inherent requirements.
- The lifecycle costs (e.g. introduction, running costs, etc.) need to be integrated as well.

Bottom line: There are high saving potentials, bundled with high costs.

The Paradox of the Return on IdM Investment

- Need for a holistic approach, since IdM has a high impact on the organisational structure.
- However, organisations tend to fail to see the big picture and cannot achieve the return aimed at. [Dos Santos]
- **Solution:** build cross-functional teams
  - Enable strategic thinking
  - Better estimate costs and benefits
  - Overcome possible “language” barriers

IdM Stakeholders



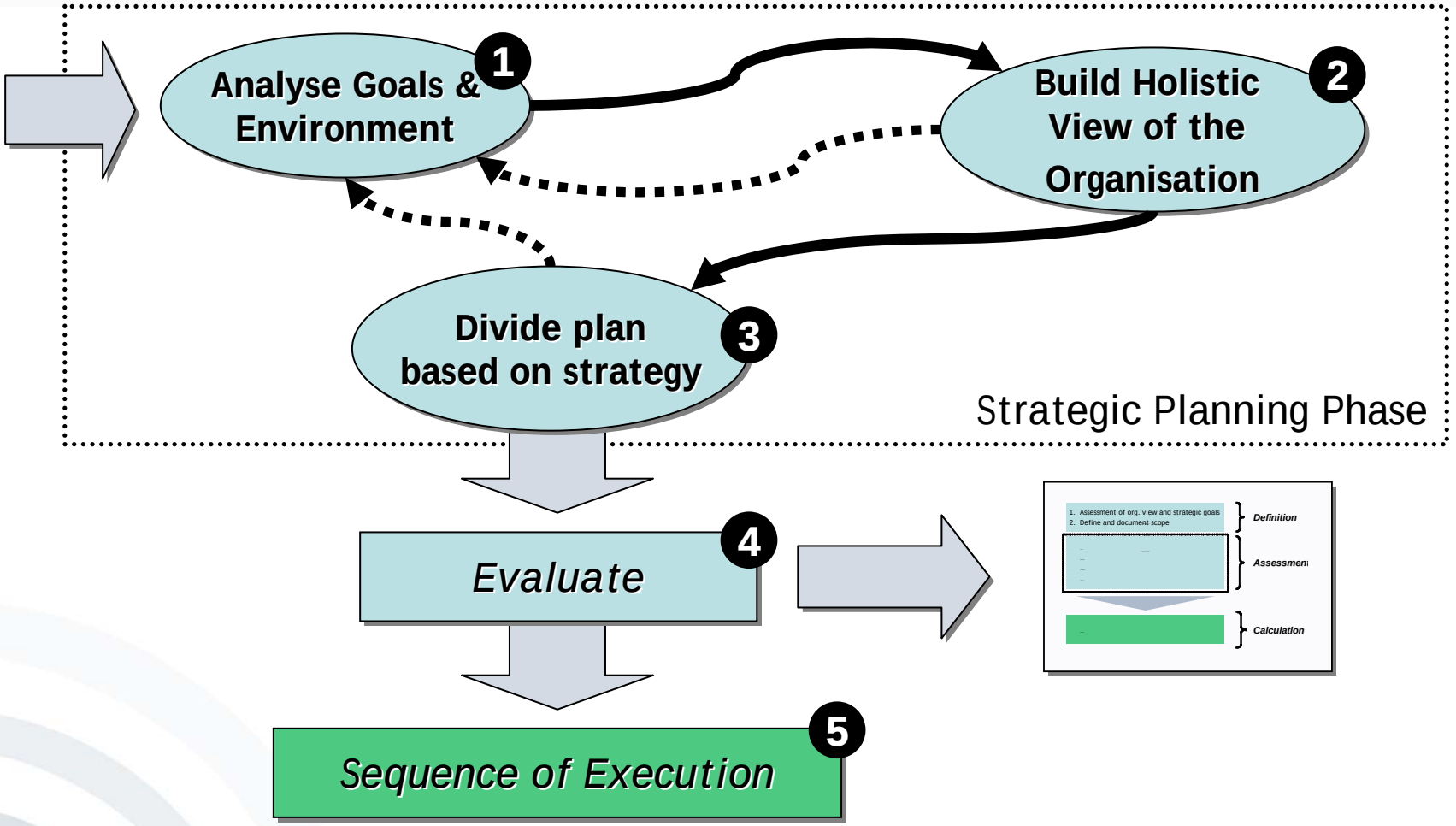
Agenda

- Introduction
  - The Need for IdM in Organisations
  - Driving Factors for IDM
  - The Cost Side of IdM
- Evaluation of IdM
  - Prerequisites
  - The Evaluation Process
- Conclusion / Discussion

Prerequisites for the Analysis

- Underlying assumptions need to be realistic (e.g. by using reference/benchmark projects).
- Complete view on costs
- Impact of the different factors on each other
- Usage of finance-mathematical methods
- Usage of scenarios to cope with uncertainty
- *For decision support:*
  - It is not possible to gather all data in an acceptable timeframe
  - Some degree of compromise is needed
  - Results only need to be sufficiently accurate for decision making

Operationalisation



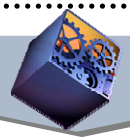
Evaluation Process

1. Assessment of org. view and strategic goals
2. Define and document scope

Definition

3. Define Costs
4. Estimate tangible benefits
5. Document intangible benefits
6. Document risks

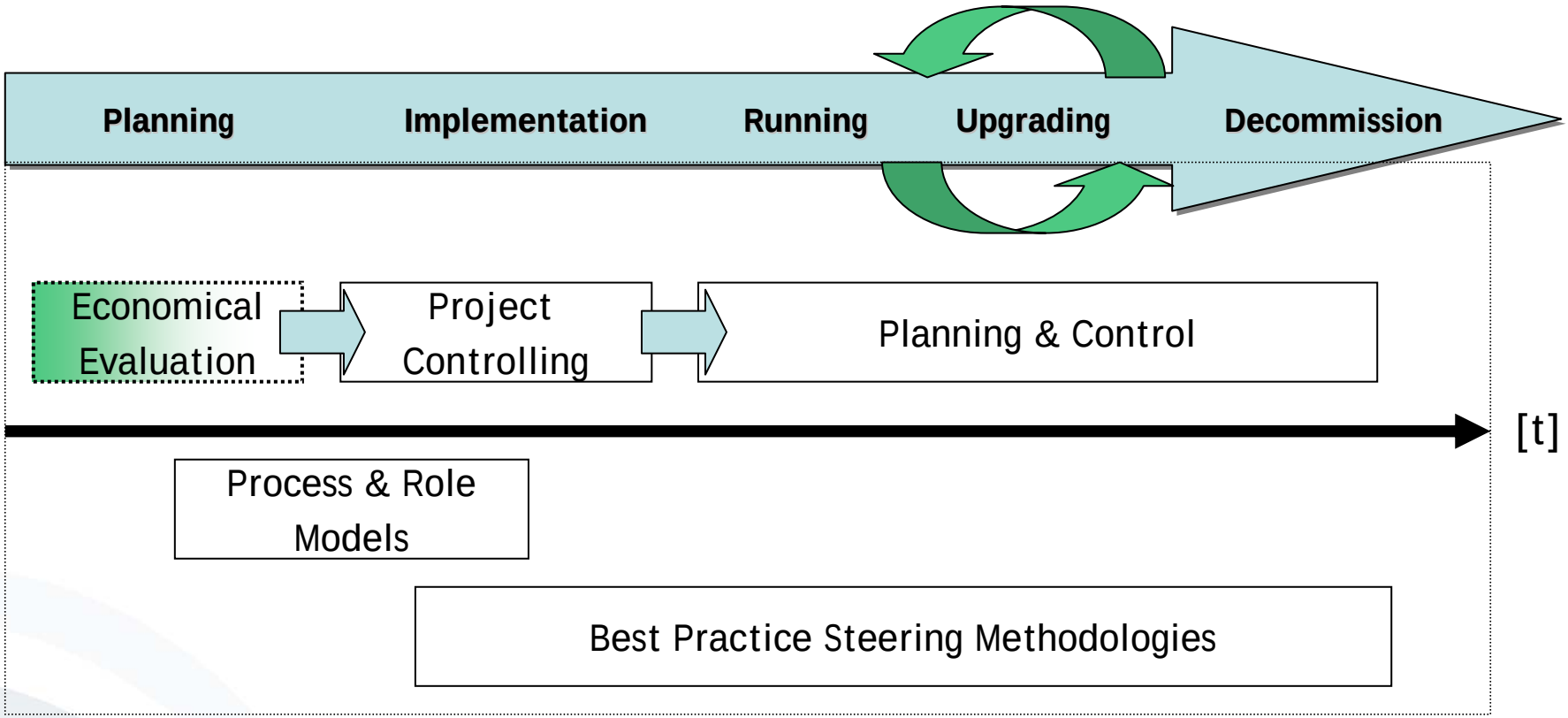
Assessment



7. Calculate potential return

Calculation

Lifecycle View



Agenda

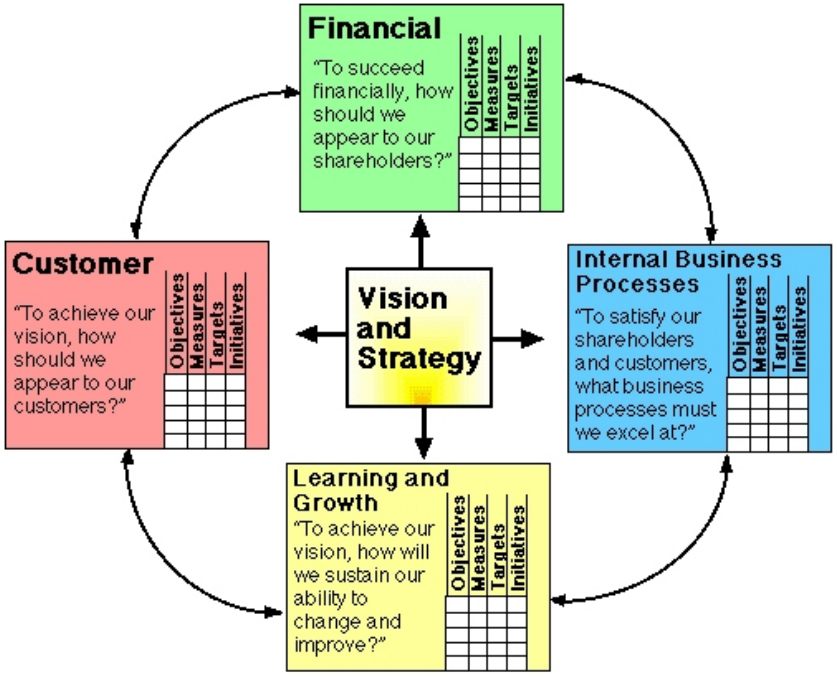
- Introduction
  - The Need for IdM in Organisations
  - Driving Factors for IDM
  - The Cost Side of IdM
- Evaluation of IdM
  - Prerequisites
  - The Evaluation Process
- Conclusion / Discussion

Conclusion

- The proposed evaluation process should help to assess costs and benefits in a formalised way.
  - Associated risks
  - Facilitate the decision process
  - More transparent assessment of introduction
- Cross-functional team
- Planning of IdM strategy

How to Proceed?

- Build a complete evaluation and steering scheme as a decision support tool for organisations
  - Based on ROSI?
  - Based on a specific IT Security Balanced Scorecard?
  - …



[Kaplan & Norton]

Thank you for your attention!
Any Questions?

denis.royer@m-chair.net

- Decision support instruments
- Return on Security Investment (ROSI)
- More holistic approach to make evaluations comparable in the way they are conducted.