

**EUROPEAN IDENTITY & CLOUD
CONFERENCE 2012**
Thought Leadership & Best Practice in Digital ID, Cloud and GRC



Dr. Horst Walther
senior analyst, KuppingerCole
horst.walther@kuppingercole.com

Best Practices for Lean, Efficient and Focused Information Security Projects

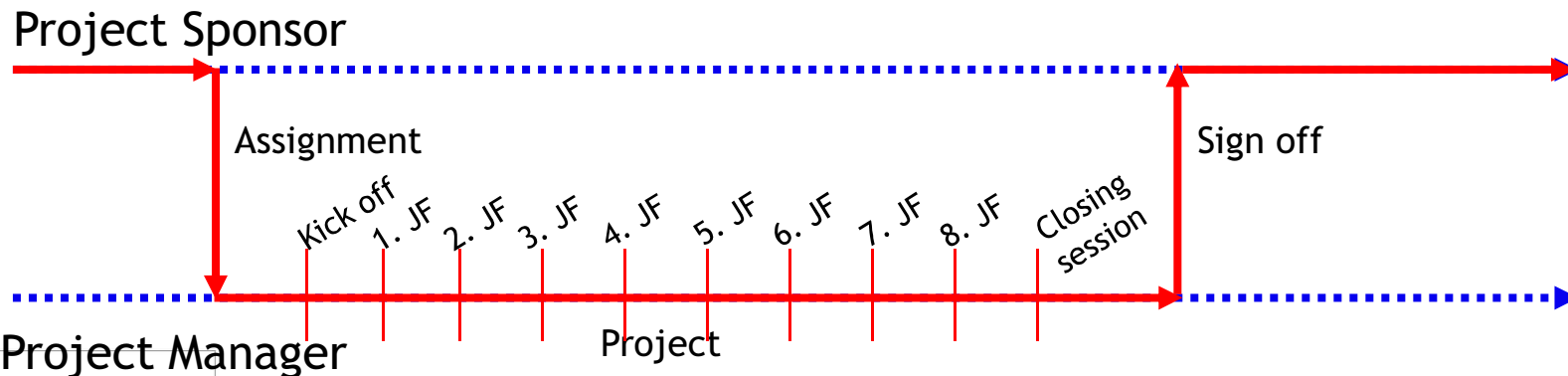
2012-04-19 | 14:00 - 14:30

summary

- IS project have much in common with general purpose project.
- So, good general project management is required anyway.
- But some specific challenges apply to IS projects in particular.
- Success factors are ...
 - Risk driven
 - C-level sponsor
 - Clear focus & responsibilities
 - Active communication
 - Long-term view
 - Agile approach
- But key success factor is addressing the challenges up-front.

For tasks “too big to fail” First you need a project

- **Visible C-level management commitment**
 - The corporation wants to move things
 - Not just the CISO fights his lost fights
- **Reasonably defined**
 - Mission, **requirements**, project plan ... to feel comfortable with
 - If fundamental data is missing: perform a **feasibility study**
- **Explicitly assigned and mandated**
 - You take the **responsibility** for success and failure
 - Or “Just say no”



Projects - IT projects - IS projects IS project most often are IT projects - So what is special?

- Management of IT Projects has more in common with “ordinary” management, that most IT project managers think.
- But it offers more **specific issues**, than most general managers can imagine.
- You just have to **do your homework** – but you should know, what you are dealing with.
- **Complexity** is the enemy - keep it as **simple** as possible (Occams razor)
- **Effort** is critical – not sequence.
- IT-projects are **communication bound**

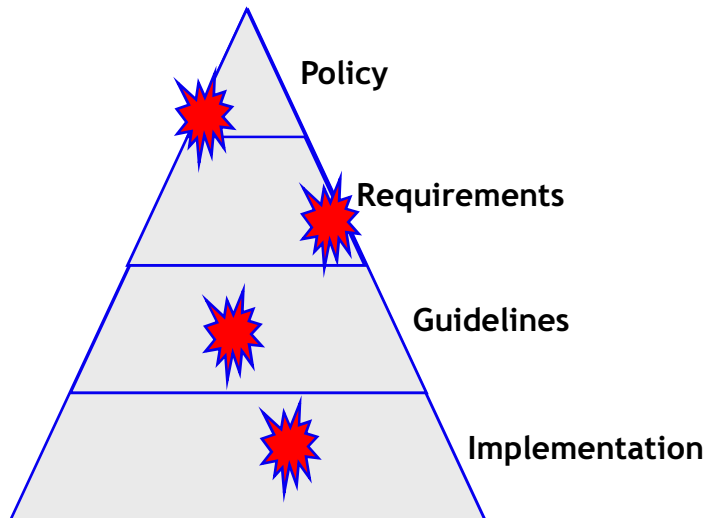
Projects - IT projects - IS projects

When it comes to IS projects - What is special here?

- **Ubiquitous occurrence**
Security issues may occur on any management level
- **Cross-company character**
end-to-end IT security touches multiple corporate functions
- **No paying customer**
often triggered by internal considerations
- **Unclear priorities**
You will drivers from operation risk to set priorities right
- **Differing process maturity**
no islands of order in an ocean of chaos
- **Trade-offs**
Full security is an illusion
- **Wrong project scope**
An implementation project cannot reorganise the corporation.
- **Bad image**
security is often perceived as an inhibitor
- **Part-time members**
Non-fulltime members tend to disappear
- **Global approach**
Global projects add considerably to effort and skill requirements.

Ubiquitous occurrence

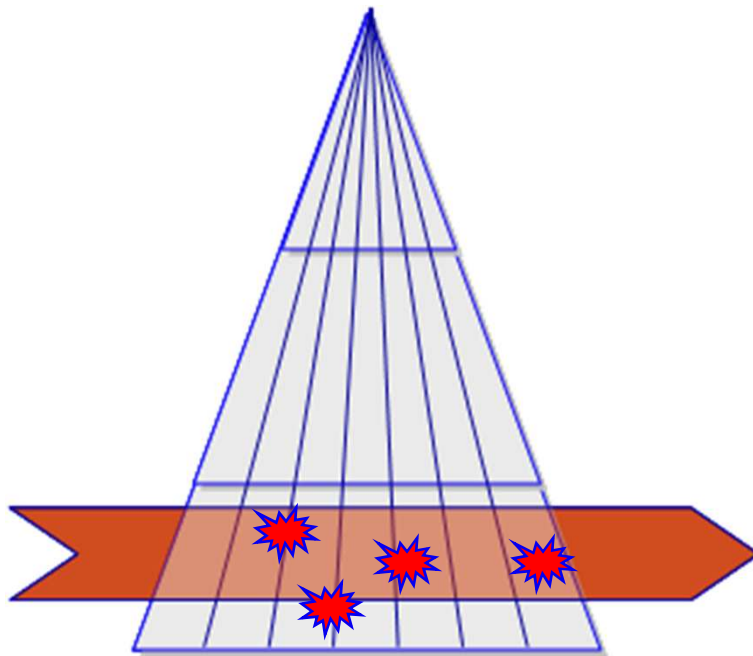
Security issues may occur on any management level.



- Operational - managerial / tactical, even strategic issues to be addressed.
- This may be true within a **single project**,
- You will need technicians, process designers, managers.
- Some **specialists** are involved for special purposes only.
- Team building of **heterogeneous** teams becomes a challenge.
- **Communication skills** are essential to explain experts' results to the public.

Cross-company character

end-to-end IT security touches multiple corporate functions



Complexity factors

- IS typically has to be ensured in processes are across the company.
- There are **multiple Stakeholders** from different corporate levels involved in a project.
- 3 to 5 mal times higher **Communication complexity** compared to „normal“ IT-projects.
- Typical **Change Management Process**

actions

- Strengthen the project management!
- Add an extra reserve for communication!
- Insist on a power sponsor for your project!

No paying customer often triggered by internal considerations

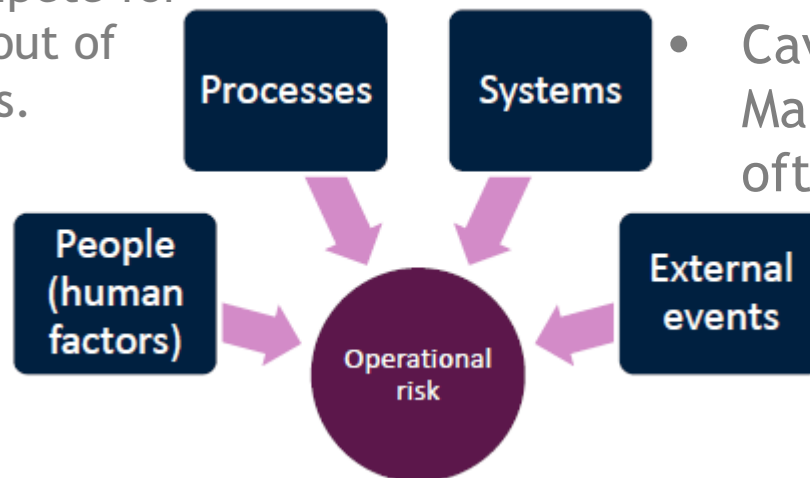
- Often more security does not lead to increase sales.
- For infrastructure, awareness or culture it is hard to find an appropriate cost centre.
- It is often hard to come-up with a positive **business case** for investments into IT-security.
- As IT Security is often seen as an **inhibitor** to business there is no credit for taking ownership.

- Let risk considerations drive the decision.
- Business is about **taking risks**.
- IT security feed into **operational** and / or **reputational** risk.
- If risk management is not sufficiently rooted within the corporation - insist on **C-Level sponsorship**.
- Establishing a risk culture spread the risk awareness to all corporate levels.

Unclear priorities

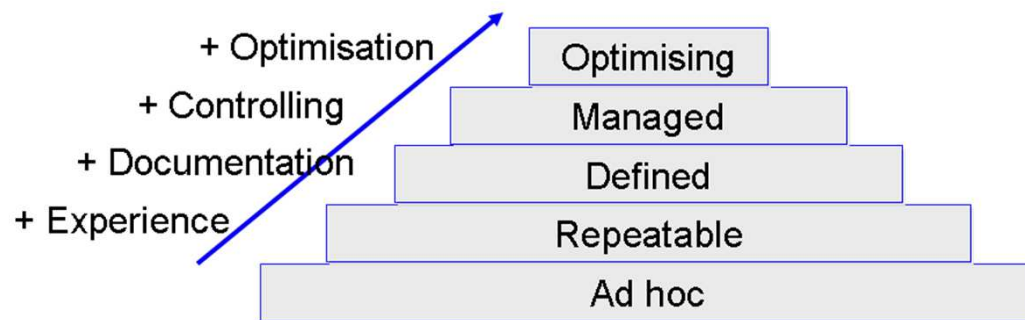
You will need drivers from operational risk to set priorities right

- Often deadlines are set which cannot be shifted
- Even if not - quick success is expected
- The size of the task often is overwhelming
- Everything seems to equally important
- Departments compete for resources to get out of the auditors focus.
- What has to be done 1st?
- What may come later?
- It all boils down to risks considerations
- Operational & reputational risks
- Good enough security = risk based security
- Priorities of tasks result from ordering them by their risk.
- Caveat: Dept. „risk Management“ quite often is not managing the risks.



Differing process maturity

No islands of order in an ocean of chaos



Complexity factors

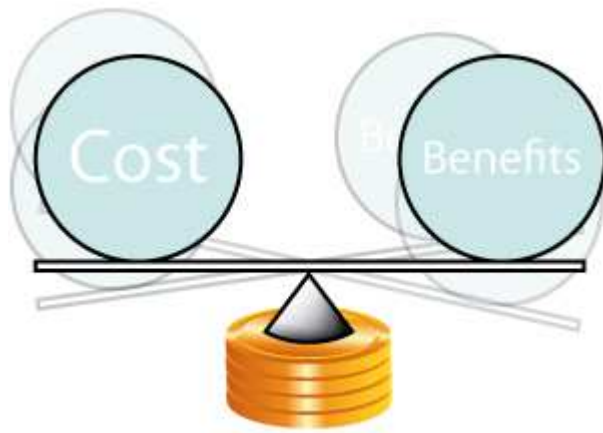
- At higher levels of **maturity** of the management processes (e.g. according to CMMi) the introduction of processes, -rules, -roles, -policies becomes easier.
- You can't implement mature & auditable processes in a low maturity **process environment**.
- The top-down definition e.g. of roles needs defined processes.

actions

- Launch IS-projects according to the maturity level as implemented in the environment.
- Suicide is not a option: occasionally „*just say no*”!

Trade-offs

Full security is an illusion

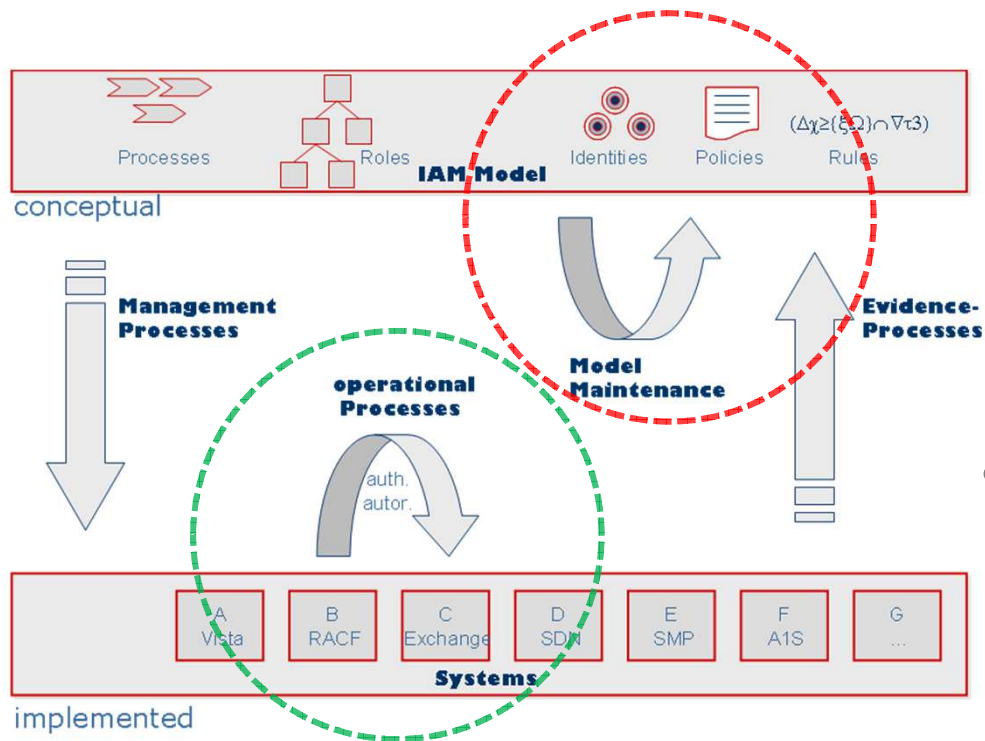


- A 100% security possibly may bring your operations to a grinding halt.
- But how much security is enough?

- Let risk management define the „good-enough security“.
- Address high risks first.
- Always look for low hanging fruits.
- Process huge tasks in an stage, agile approach.
- Yes, you may skip tasks as well!

Wrong project scope

An implementation project cannot reorganise the corporation.



Avoiding the scope trap e.g. for IAM projects


Complexity factors

- Implementation project will have a hard job when having to reorganise the corporation first.
- Model definitions require their own Definition projects before or in parallel to the Implementation.

actions

- Break your work down into loosely coupled work packages
- Define own projects for the model definition before or in parallel to the Implementation.
- A program made up of several agile projects often is a better solution.

Bad image security is often perceived as an inhibitor

- Information security often is perceived as a road block for day-to-day activities.
 - Management often feels embarrassed by audit findings.
 - They try to tend to launch undercover activities to cope with them.
 - Instead sometimes a culture change is required.
 - IS specialist often are suboptimal communicators
- 
- Sell your project within the corporation.
 - “*We enable trust*”, rather than “*We need to impose restrictions due to security reasons*”
 - No clandestine activities due to „embarrassing“ audit findings.
 - There is no way to hide.
 - Plan & staff for project communication / marketing up-front.

Part-time members Non-fulltime members tend to disappear



persons with business domain knowledge are rare creatures

Complexity factors

- The availability of specialists with **domain knowledge** often turns out to be the bottle neck in role- und process definitions.
- Their involvement is essential for the **requirements definition** and the **QA**.
- Waiting times (for specialists) are driving the overall effort.
- While in projects they tend to disappear.

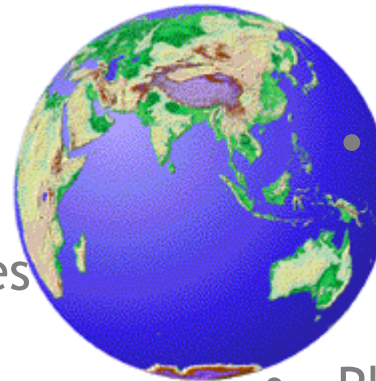
actions

- Assign the project responsibility to the **business departments**.
- Think of **splitting projects** to business definition and an implementation part.

Global approach

Global projects add considerably to effort and skill requirements.

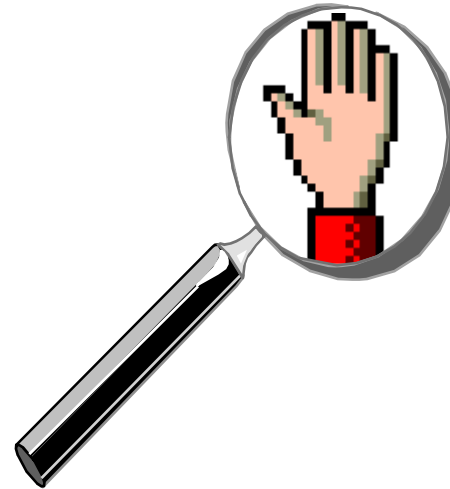
- Regulation may differ by region.
- One-size-fits-all might not be the right approach for all subsidiaries.
- But the chain may break at its weakest link.
- The responsibility for remote security measures often still stays with the headquarters.
- Global PM causes considerable on-top complexity.
- Factor-in a 1.5 times higher communication overhead for global projects.
 - Not all security issues can be handled globally in a uniform way.
 - Assign regional responsibility - but support them from the headquarters.
- Plan for a phased roll-out - a big bang approach rarely works.



Any questions ?



S_{top,}
A_{ppendix}



From here on the back-up-slides follow ...

Guideline: Occam's Razor



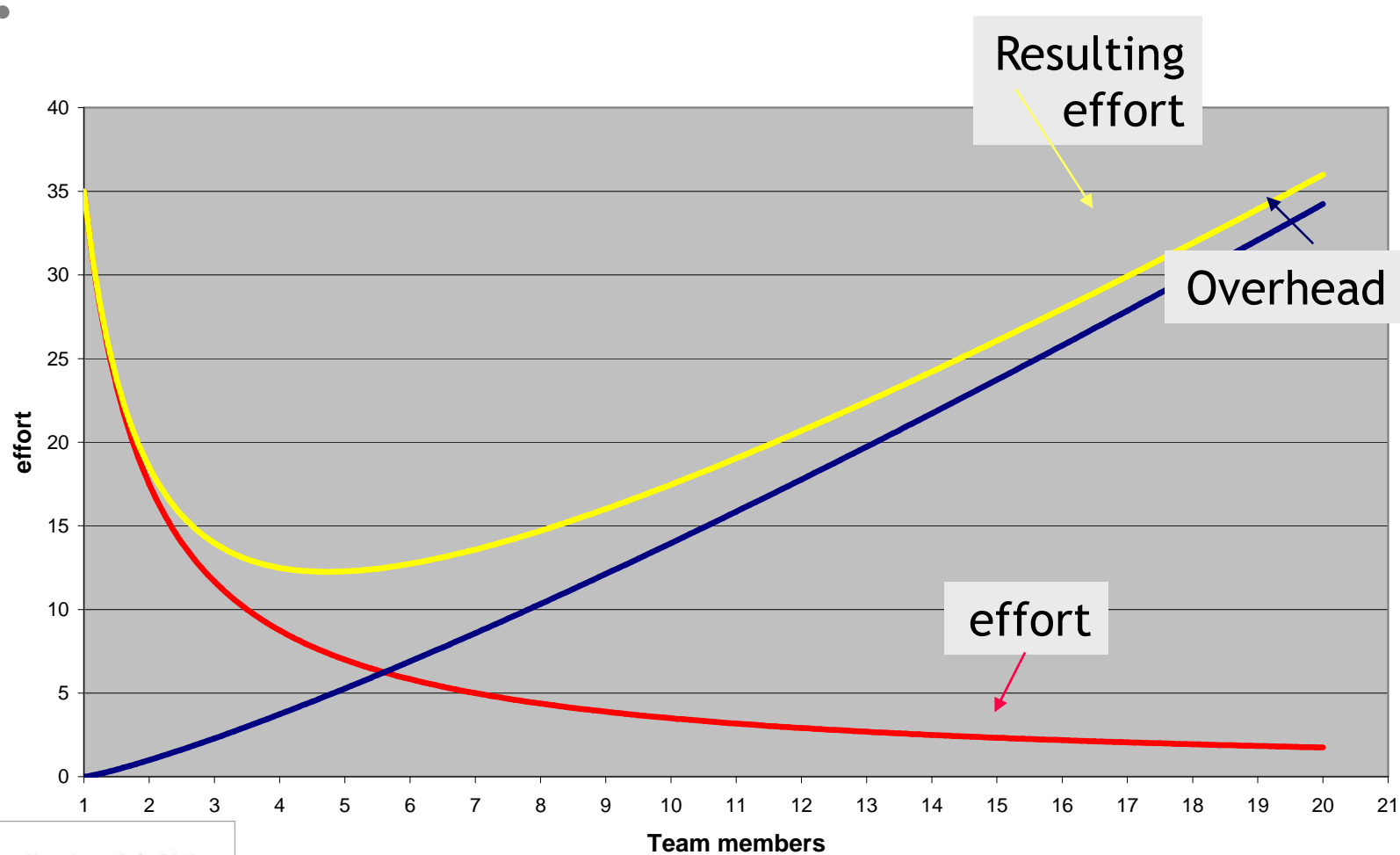
One should not increase, beyond what is necessary, the number of entities required to explain anything.

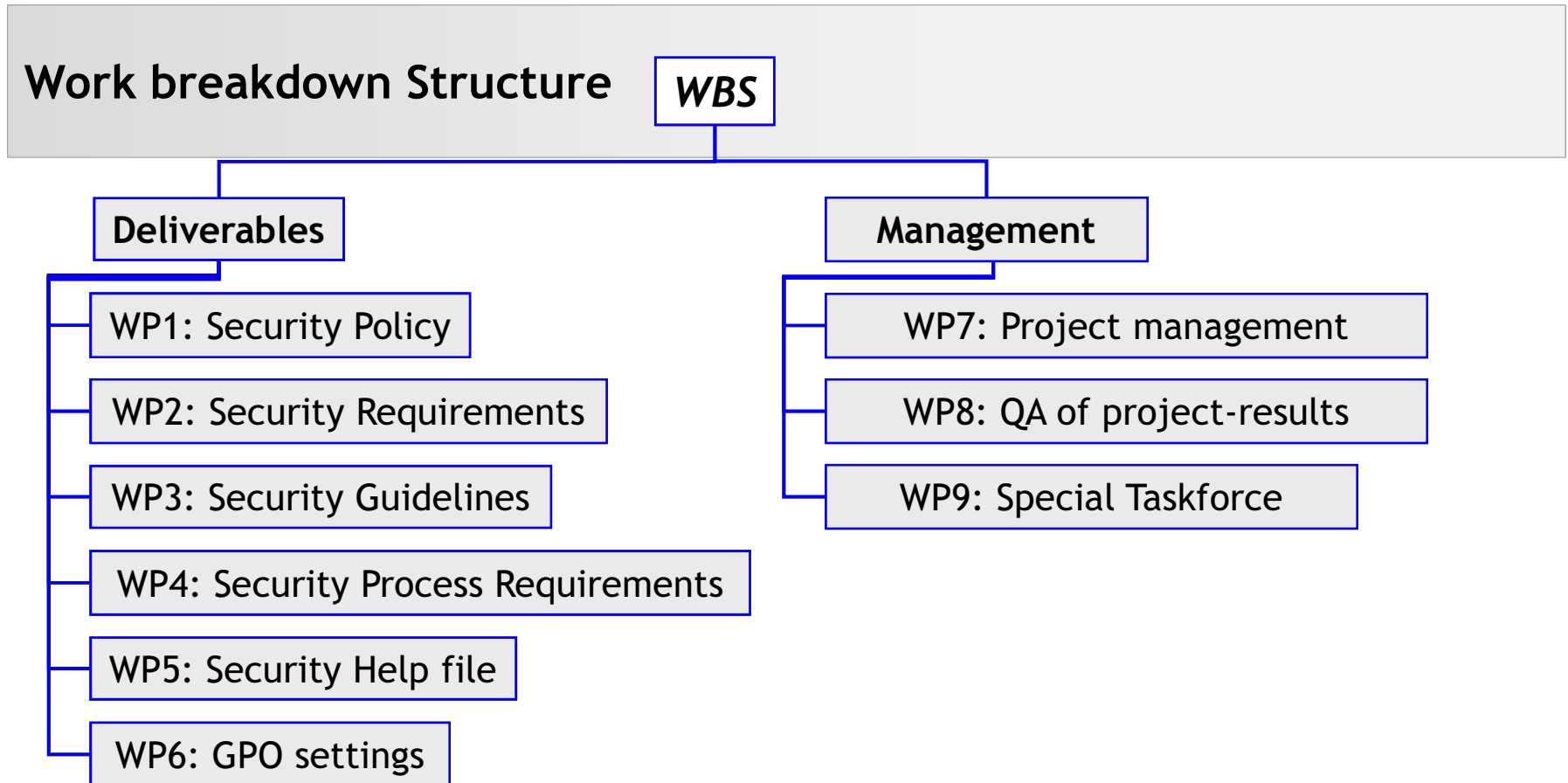
William of Ockham, born in the village of Ockham in Surrey (England) about 1285, was the most influential philosopher of the 14th century and a controversial theologian.



- One should not make more assumptions than the **minimum needed**.
- This principle is often called the **principle of parsimony** or **simplicity**.
- It underlies all **scientific modelling** and theory building.
- **Choose simplest** model from a set of otherwise equivalent ones of a given phenomenon.
- In any given model, Occam's razor helps to "*shave off*" the concepts, variables or constructs that are **not really needed** to explain the phenomenon.
- Developing the model will become much **easier**, and there is **less chance** of introducing **inconsistencies, ambiguities** and **redundancies**.

IS projects are communications bound ...





- Break the work down
- Name and number the work packages WP1 ... WPn
- Assign WP-Ownerships
- Set safe delivery dates

The Future of Information Security - Today.

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company **KuppingerCole** provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

Kuppinger Cole Ltd.

Headquarter
Arnheimer Str. 46
D-40489 Düsseldorf | Germany

Phone +49 (211) 23 70 77-0
Fax +49 (211) 23 70 77-11

www.kuppingercole.com
clients@kuppingercole.com