Successful Management of Information Security Projects

Approach, Tools and Techniques

Dr. Horst Walther
SiG Software Integration GmbH
31. Oktober 2001

Agenda

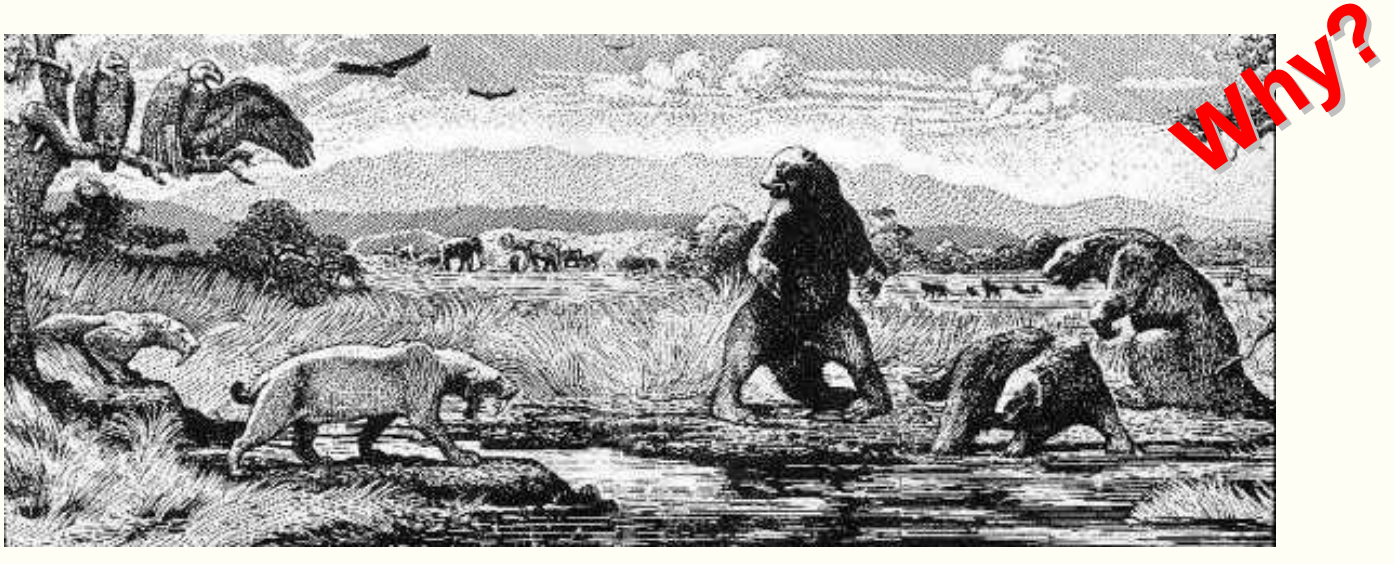
- Real world projects - the bitter truth.
- IT Projects – What is special?
- 101 of Traditional Project Management
- IS Projects – What is special?
- First you need a project
- The Mission
- Work breakdown Structure
- Communication - The big picture
- Quality Assurance
- Reporting
- Project meetings
- Planning Tools
- Project Standards
- Project post mortem – lessons learned
- Summary - Factors of success and failure

Real world projects - the bitter truth.

Project management is often perceived as a "struggle in the tar pit" …

- The strongest creatures fail first
- The harder they fight, the deeper they sink
- Adding manpower to a late IT project still makes it later

Is there an escape path?

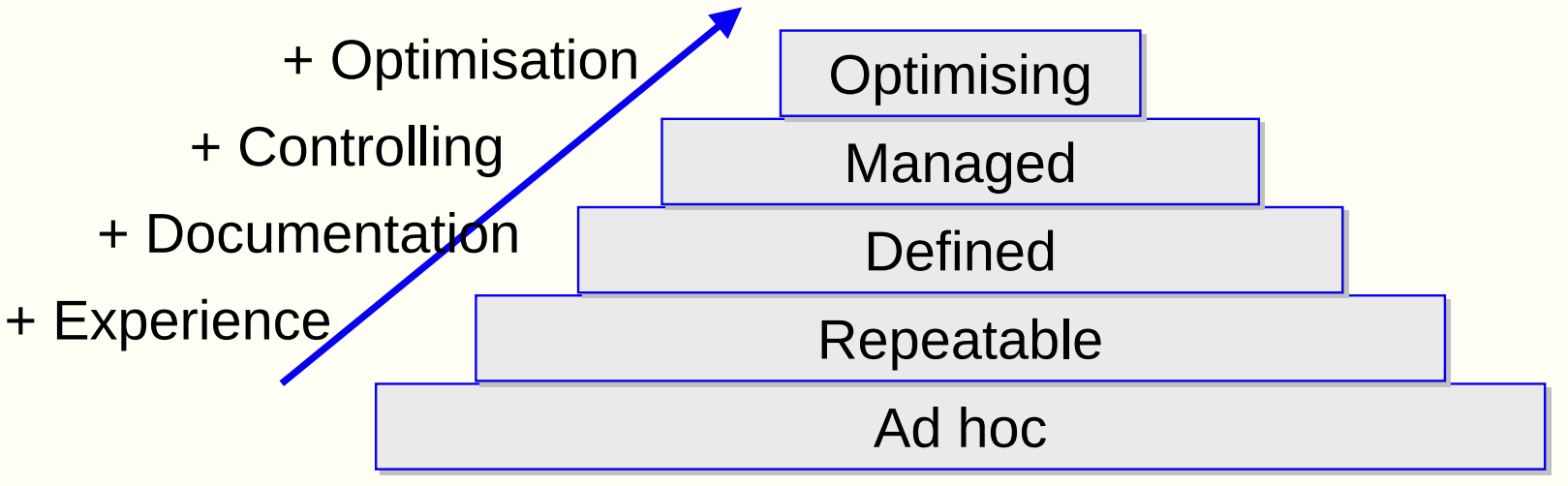


IT Projects – What is special?

- Management of IT Projects has more in common with “**ordinary” management**, that most IT project managers think.
- But if 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
- **Effort** is critical – not sequence.
- IT–projects are **communication bound**

CMM for Project Management

- Project Management is just another management task
- It needs a mature process.
- The process maturity can be improved according to the Capability Maturity Model (CMM from the SEI) in 5 levels.



101 of Traditional Project Management I

- **Mission**
  - Develop project objectives and define the project scope.
- **Requirements**
  - Build a network of measurable achievements & sub-achievements.
- **Mandate**
  - Define the project charter, including authority & accountability structures.
- **Risks**
  - Define the project **risks** (threats, potential damages, probabilities)
  - Find options for risk **reduction**
- **Work Breakdown Structure**
  - Build the work breakdown structure from the project plan.
  - Define the summary tasks, sub-tasks and **individual ownerships** with completion dates.
  - Lay out a WBS that provides clear assignments for your team and a **foundation for tracking** actual results.

101 of Traditional Project Management II

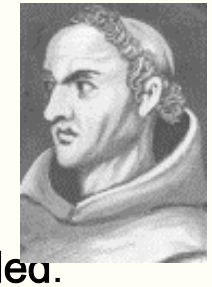
- Predecessor Network
  - Use the software to create predecessor relationships between assignments, yielding a network of tasks.
- Resource Assignments
  - Assign project team members to tasks
  - quantify the duration and get commitment to accountability and schedule.
  - Prepare for change of people's schedules and task assignments.
- Critical Path
  - Use critical path and PERT to analyse the network of tasks.
  - Always keep options for shortening the project duration.
- Team Leadership
  - Resolve team conflicts and avoid potential problems.
  - Define the leadership style and actions required of the PM.
- Tracking & Status Reporting
  - Get status data from the team, update the project plan, identify problems.
  - Propose solutions in status reports to the project sponsor.

Information Security Projects – What is special?

Ubiquitous occurrence	Isolated security issues occur on all levels, from strategic to implementation detail.
No Paying customer	often triggered by internal considerations
Isolated activities	sometimes there's no obvious relationship to the affected IT–Systems
Bad image	security is often perceived as an inhibitor
Part-time members	Non–fulltime members tend to disappear
Trade-offs	Full security is an illusion
Global approach	Global projects add considerably to effort and skill requirements.

Guideline: Occam's Razor

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



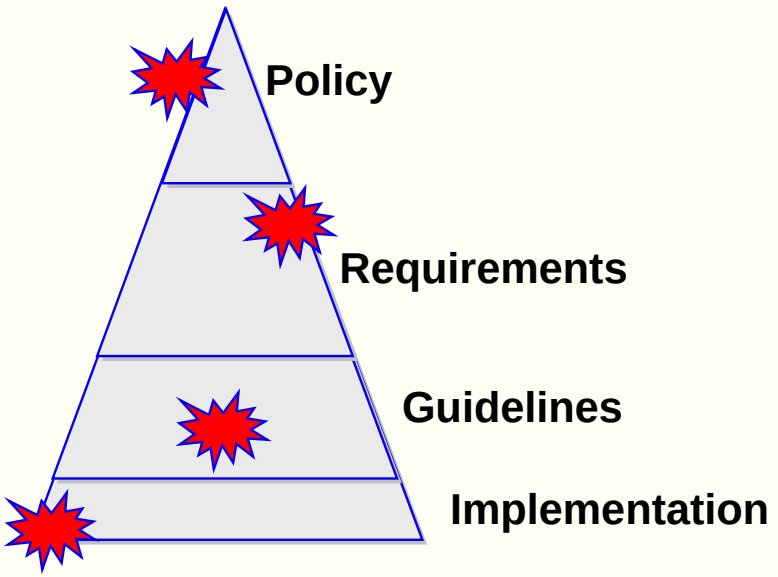
William of Ockham, born in the village of Ockham in Surrey (England) about 1285, was the most influential philosopher of the 14th century and a controversial theologian.

- 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 – *Ubiquitous occurrence*

Security issues occur on every task level.

- You will need technicians, process designers, managers.
- You will get **heterogeneous** teams
- Many **specialists** are involved for special purposes only.e.
- **Writings skills** are essential to explain experts results to the public.

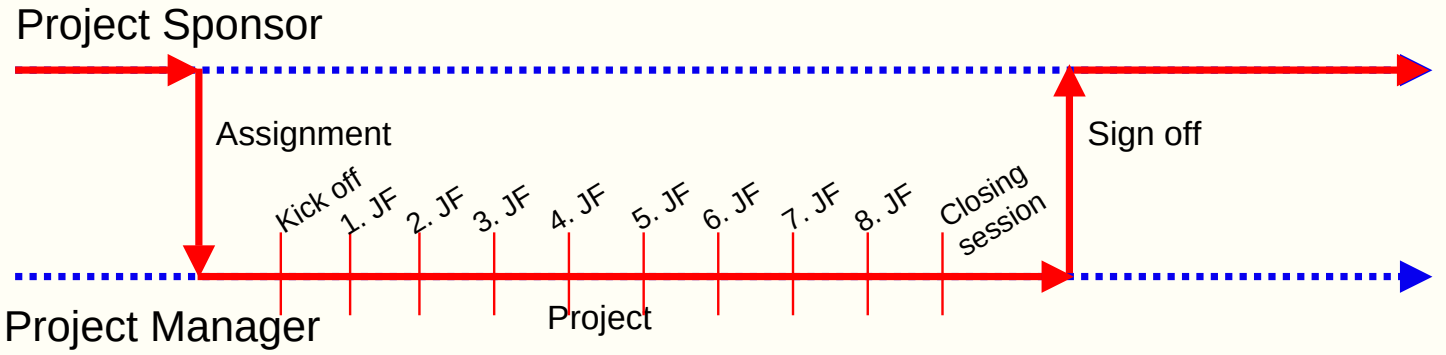


Sidestep - What did we learn from QM?

- **Quality** is “Meeting the customers expectation”
  - Regardless if you offer products or services, to internal or external “customers”
- Security covers a distinct set of the overall **Q-criteria**
- Security is an enabler for **trust**
  - Trust is easier to sell than security
- If **TQM** is a valid assumption, Total Security Management is the challenge. There are no security islands.
- Security-**Tradeoffs** are no accident.
- Target Quality is defined to deliver a “*good-enough* solution”

First you need a project

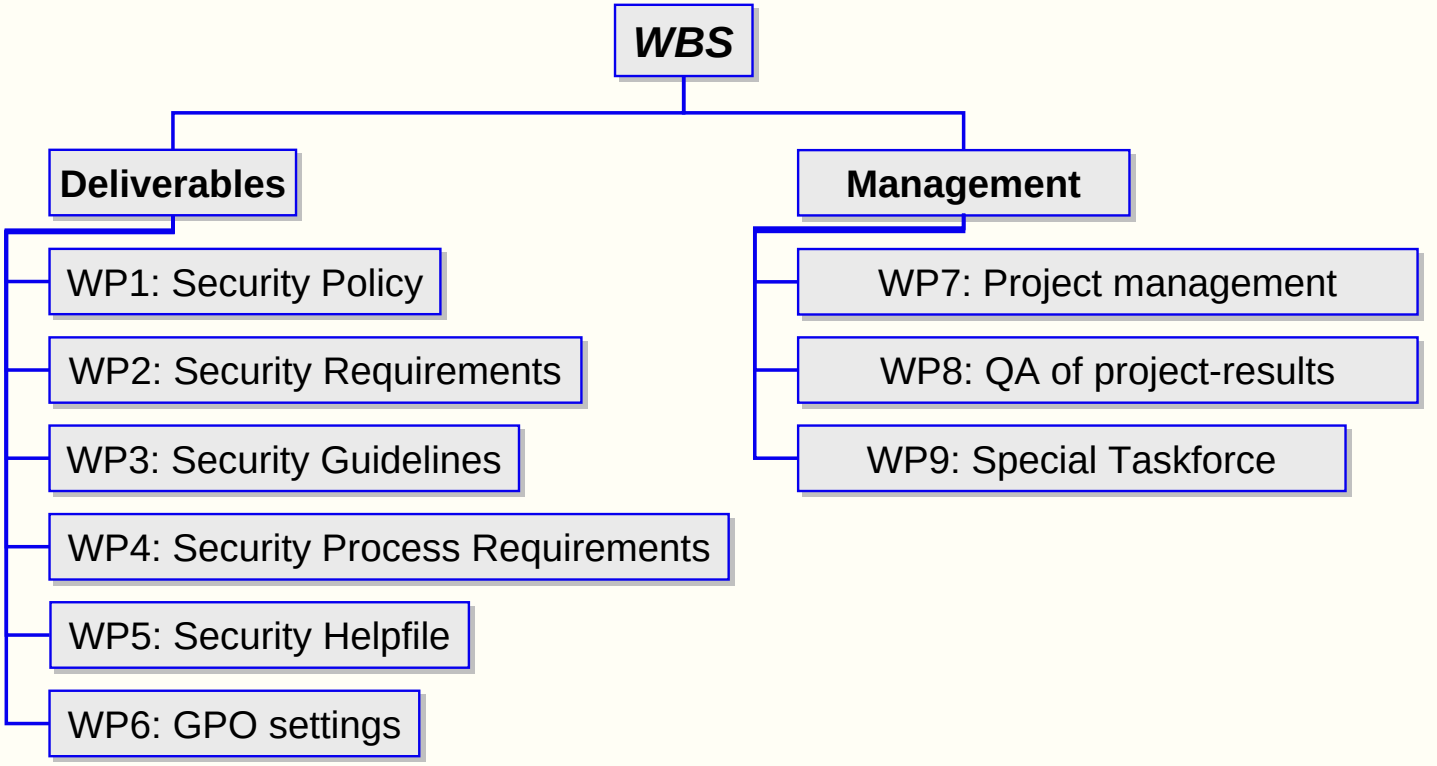
- **Temporary** management task
- Reasonably defined
  - Mission, **requirements**, project plan … to feel comfortable with
  - If fundamental data is missing: perform a **feasibility study**
- Explicitly assigned and mandated
  - You take the **responsibility** for success and failure
  - Or “Just **say no**”



The Mission

- Insist on a agreed **mission**
- List the top-level **deliverables**
- Keep the mission **short**
- The mission must be **measurable**
- In case of a mission impossible – **just say “No”**
- Explicitly state what is **not** the **mission**

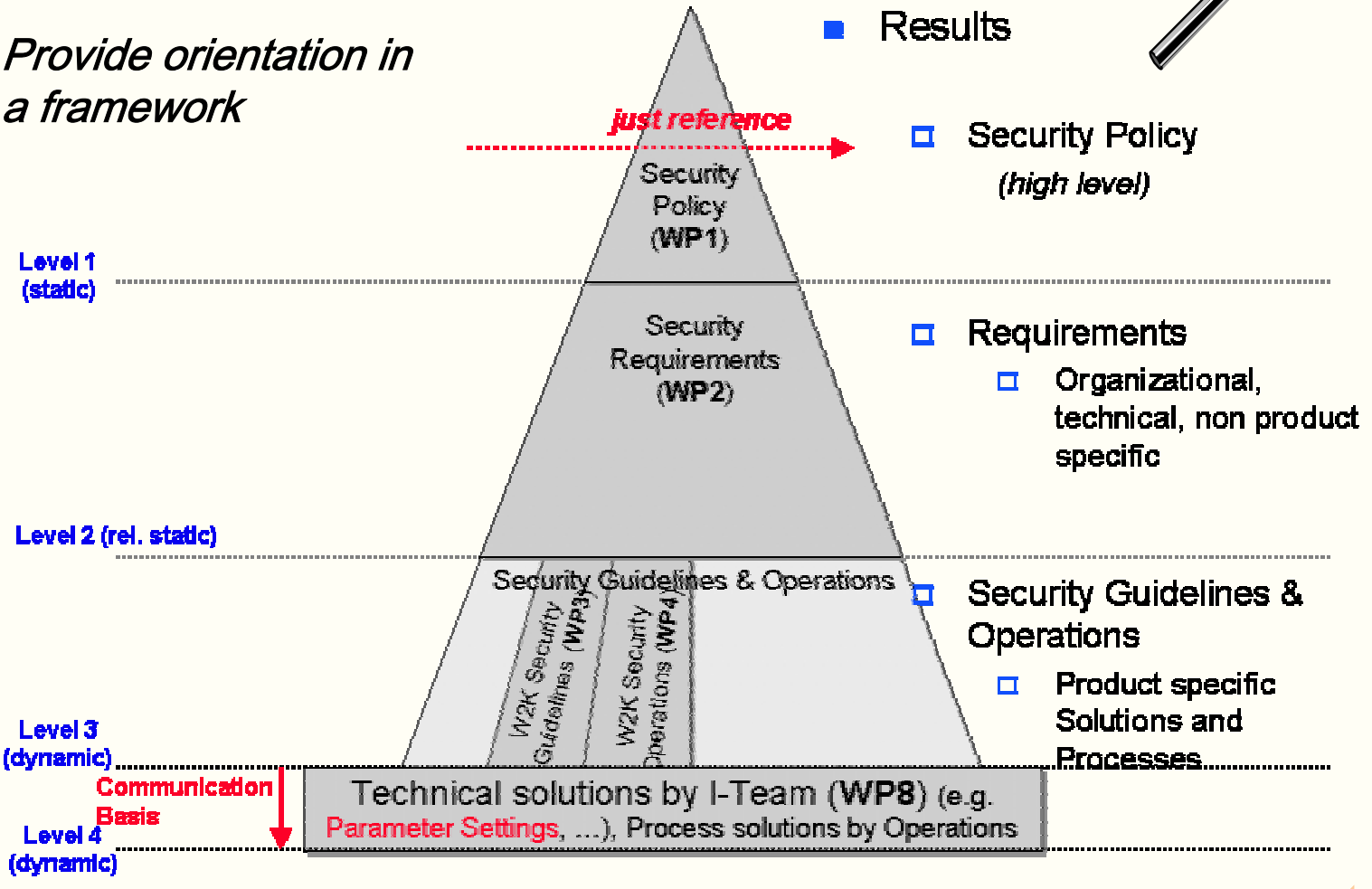
Work breakdown Structure



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

Communication - The big picture

Provide orientation in a framework



One more word on communication …

Adding manpower to a late IT project still makes it later.

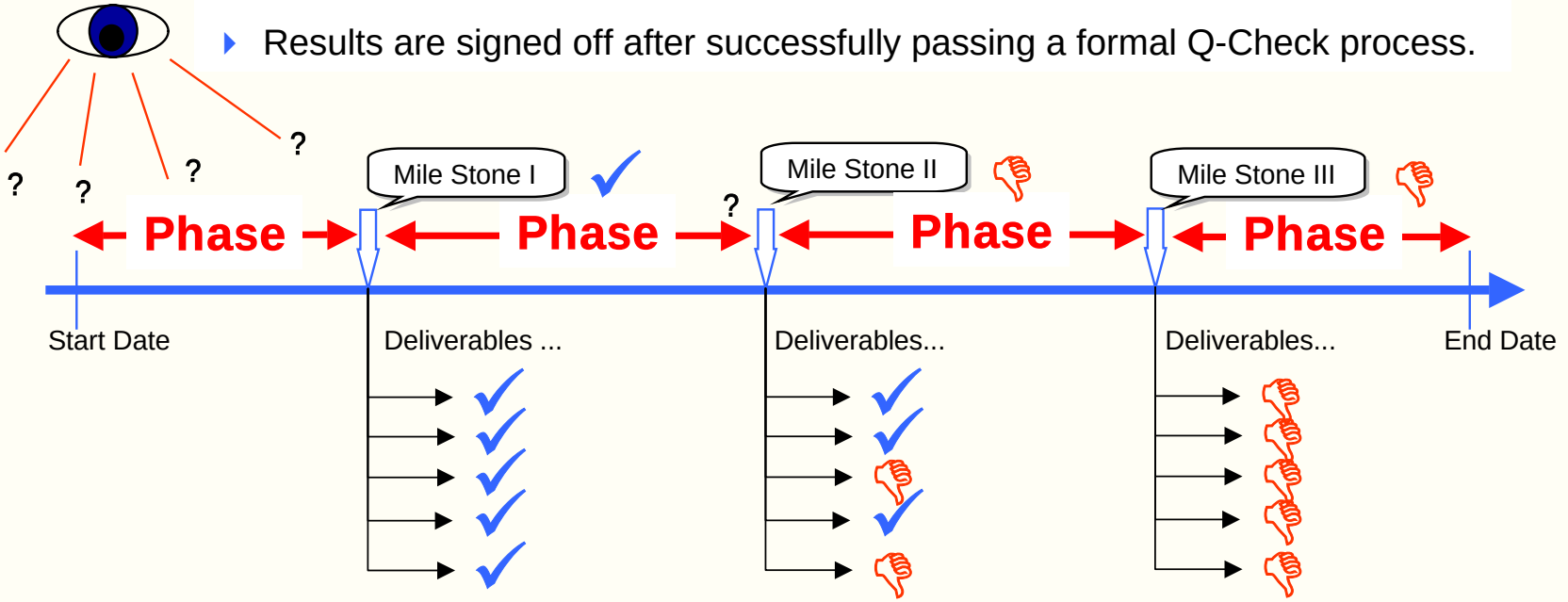
Principles of QA

- **Full coverage** - Each result will be checked for quality and formally singed off
- The **expert principle -** Project results are assessed by experts ...
  - Following a formal process
  - colleagues, internal or external experts
  - Reviews including meetings or in documents-flow based way.
  - Comments und sign off decision are documented by review minutes.

  ... But signed off by a third party.
- **Atomicity** - A result is considered done by 0% or by 100%.
- **Transparency -** Results are published to a defined public.
- **Documentation** - In an accessible way – to learn from our mistakes.
- The **minimum principle -** regulations as concise as possible

Q-Check & Sign off

- Results are completed by **0 %** (not signed off) or by **100** % (signed off).
- Results are signed off after successfully passing a formal Q-Check process.



Mile Stone completed
- All Results are signed off

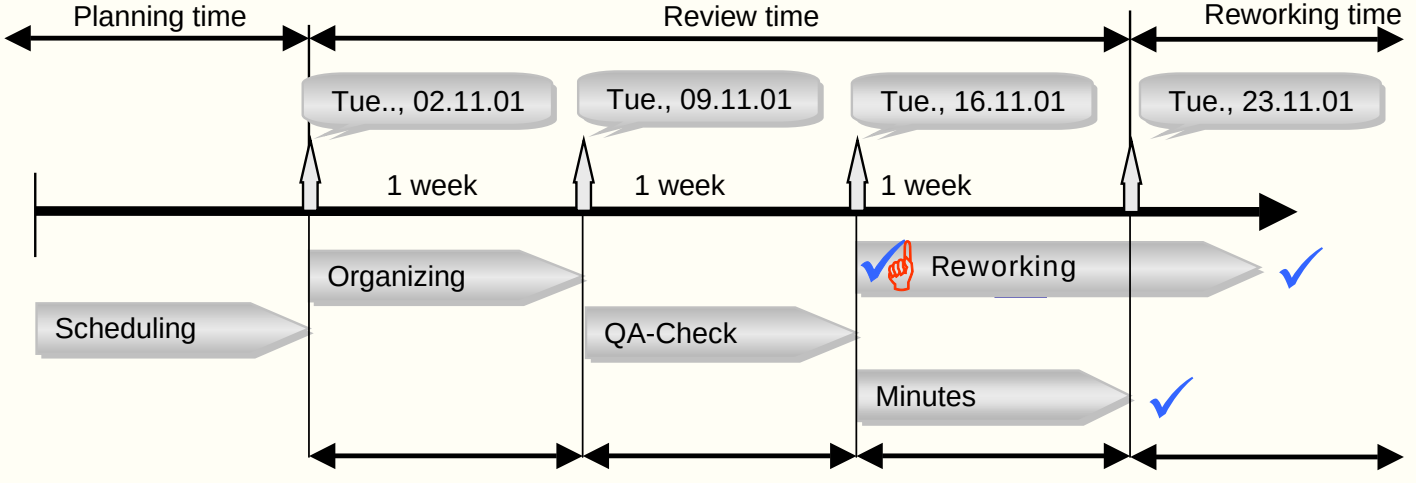
Miles Stone not completed
- Not all Results are signed off

Miles Stone not completed
- There are no results

Defined per Phase ...
- Participants
- Tasks
- Results

The Review Process

- The **Author** signals a ready for review result to QM.
- QM names a **Moderator** and calls **experts** for participating the Review.
- The Reviewers deliver their comments **prior** to the Meeting.
- They classify flaws in a precise way
  - Minor flaws lead to **conditions**
  - Major flaws lead to **rejection**
- A Review is not a interrogation but a **service** for the Author
- The Recorder documents decisions in **Review minutes**.
- QM **signs off** the result, rejects it or imposes conditions (while signing off).



Reporting

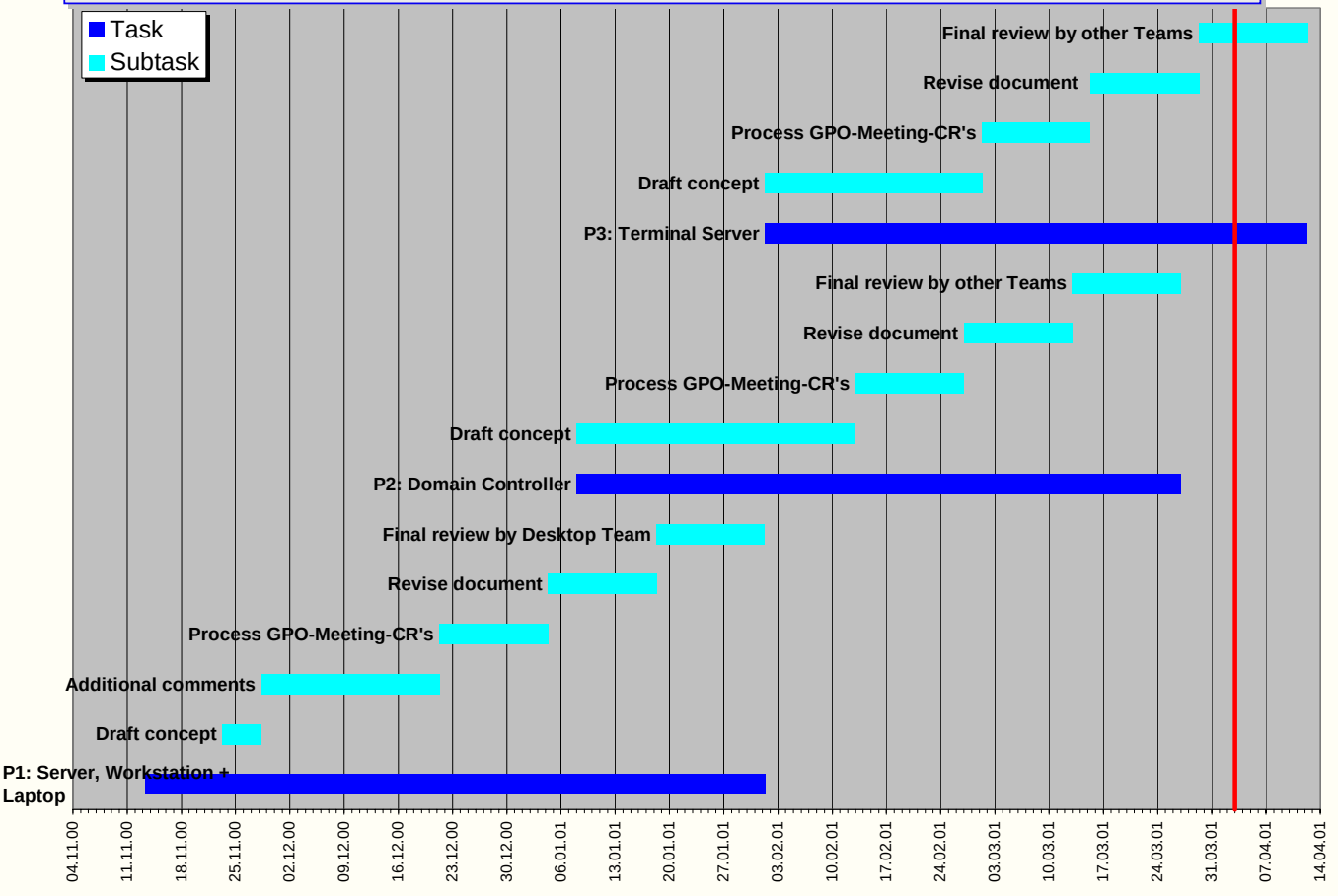
- Let team members report via **time sheets**.
- **Period** is weekly (e.g. each Friday by noon)
- Provide necessary **Forms** to the team.
- Consolidate the weekly work reports and set up a monthly **Status report**.
- Store a **pdf-version** of the monthly status report in the project folder.

Project meetings

- **Jour fixe** – weekly or bi-weekly at a fixed weekday
- **Participants** – All actually active Team members (and optionally guests).
- **Location** - Provide a fixed location or rotate in a defined order.
- **Minutes** – Decisions, presented Results and Assignments will be documented in minutes, sent to the participants and stored in a project folder.
- **Assignments** - Assign **tasks**, track them and control the results.
- Cut lengthy **discussions** by assigning a surveying task as the foundation for a decision.

Planning Tools

- More often than not ... MS Excel is sufficient



Project Standards (example)

- **Policies & guidelines** - Follow the rules and regulations of „*Corporate SecurityManual* “
- **Exchange format** – Define exchange formats e.g.
  - *Office 2000* format within the teams and
  - PDF-documents for distribution of results.
- **Project folder** - Use a Lotus Domino DB or Intranet Pages to store the project results and other relevant documentation.
- **Communication** – We will make use of Internet-Mail or Lotus NOTES (Text, RTF, HTML)
- **Encryption** – Use PGP if no corporate solution is in place.

Project post mortem – *lessons learned*

- What did we achieve?
  - Sell your successes
- Which are the goals, that we did not reach?
  - What were the reasons?
- What are the Lessons we had to learn?
  - The effort
  - Type of project
  - Formal project management - There's often "room for improvement"
  - Given a second chance – which changes would you apply?
- Process improvement (CMM level 5)
  - If there's an owner for the project management process suggest changes for process optimisation.

Summary - Factors of success and failure

- IS – Project Management is **simple** – but not easy.
- Just do your „**homework**“- but with special emphasis.
- Make sure, that it is really a **project**.
- Tie your contribution to a “real” **business need**.
- Be suspicious on **granted internal resources** – augment them with contractual staff.
- Insist on **regular** team meetings, keep them short. Document them.
- **Track** assignments – There’s no escape from responsibility.
- Don’t believe in **tools** - Just use them appropriately.
- Use a **rigorous QA-Process** to achieve visibility and management-buy-in
- **Sell** your results
  - “*We enable trust*”, rather than “*We need to impose restrictions due to security reasons*”
  - Be aware, that you write a piece of technical literature
  - Publish concise documents, be aggressively visible.

Workshop …

Telling from experience

key factors
for success and failure
of IS projects

Dr. Horst Walther
SiG Software Integration GmbH
31. Oktober 2001

Questions - What is your experience?

- Why did your projects have **Success**?
- Why did a project fail **failure**?
- What are the key factors **underemphasized** here?
- Which ones are **overemphasized** here?
- To which statements do you **agree**?
- Where do you **disagree**?
- Is there an **important message** you want to tell us?

Answers - From our experience …(1)

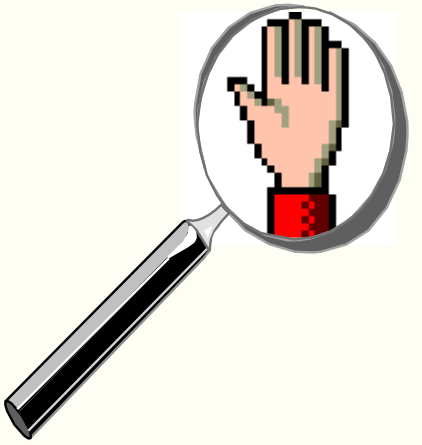
- Small projects offer special challenges
  - On small sites projects often consist of just one team member.
  - The mapping of all necessary project roles to one person requires considerable discipline.
- Moving Targets require adequate treatment
  - Change requests have to be handled formally
  - A change request process and a change decision board have to be established.
- Duration is a success factor too
  - Projects should be kept short.
  - 9 Months are a natural duration.
  - Most projects are cancelled after 2 years duration.

Answers - From our experience …(2)

- The fear factor is important
  - Highly visible and obviously important projects have better chances to keep the team members motivated to meet the deadlines.
- Regulations must be adapted to the project size
  - Large projects,
  - Medium projects, and
  - Small projects & maintenance

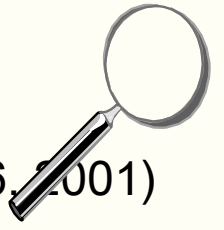
  … need to be regulated to a different level.
- Strong sponsorship is essential
  - In some cases the presence of the project sponsor is necessary even during critical project meetings.
  - Project sponsors presence is needed to demonstrate management support
- Be brave, tell the truth
  - On the long run ignoring reality to please your boss doesn't pay off.

Stop,
Appendix



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

Failures - Management's Deadly Sins



- Management's Deadly Sins Survey (SANS 2001, May 16, 2001)
  - 101 Responses

The Deadly Sin	Sin Index
Mistaking Half–baked Ideas as Projects	2.9
Poor Sponsorship	3.3
Under Skilled Project Managers	3.5
Not Monitoring Project Vital Signs	3.6
Failing to Deploy a Robust Project Management Process	3.5
Average Sin Index	**3.4**

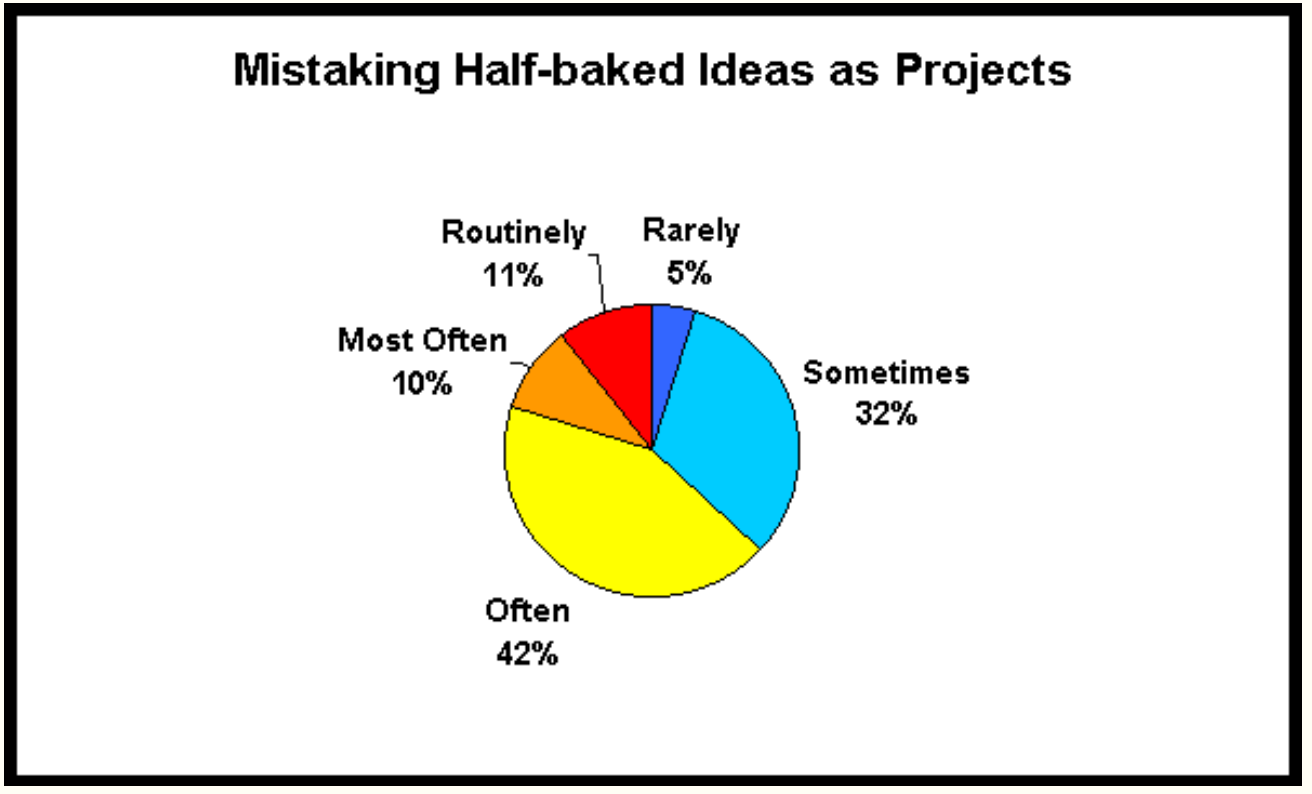
Sin Index

Value 0.0 - 1.0 Project Nirvana
Value 1.1 - 2.0 Cloud Nine
Value 2.1 - 3.0 Can be Saved
Value 3.1 - 4.0 Project Purgatory
Value 4.1 - 5.0 Project Hell

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which about 96,000 system administrators, security professionals, and network administrators share their experiences. SANS was founded in 1989.

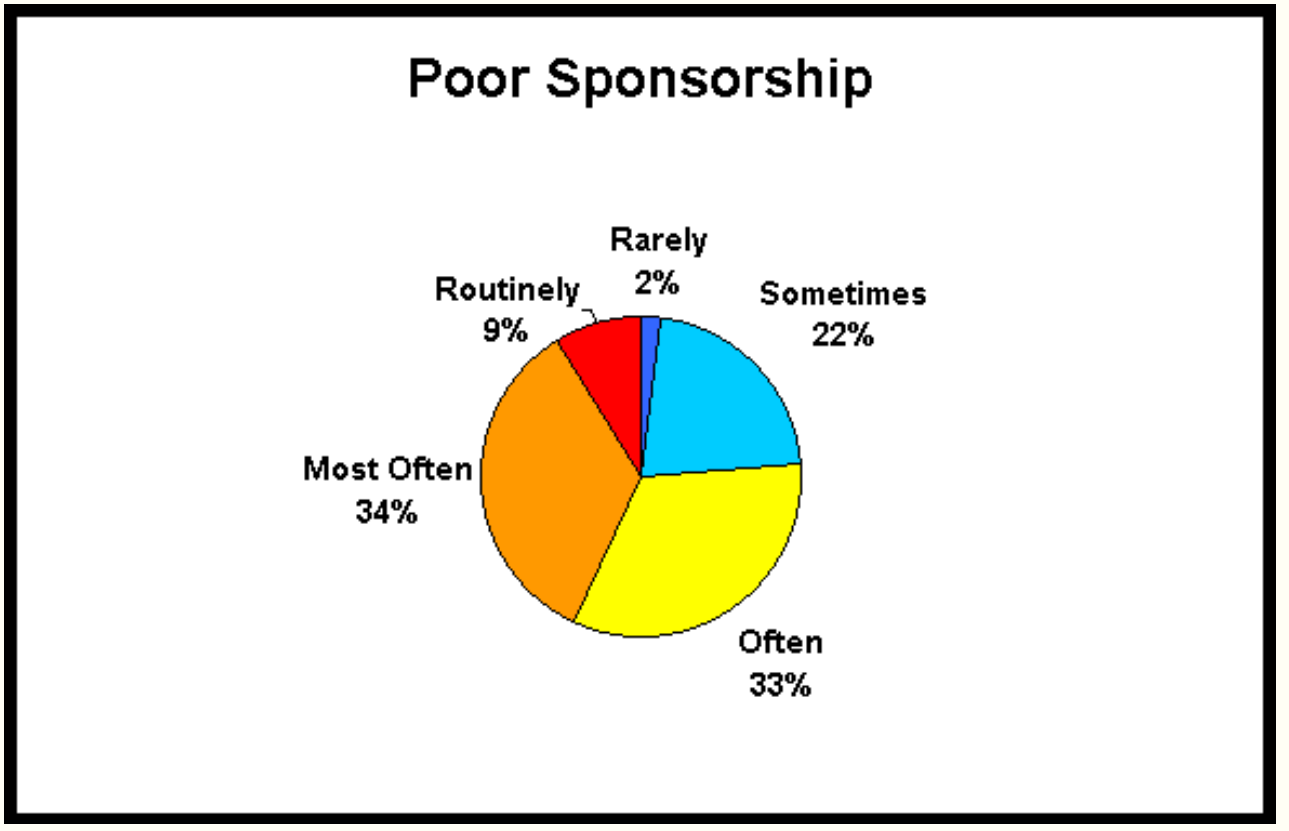
Sin #1: Half baked ideas

- Results reported from the SANS Institute ...



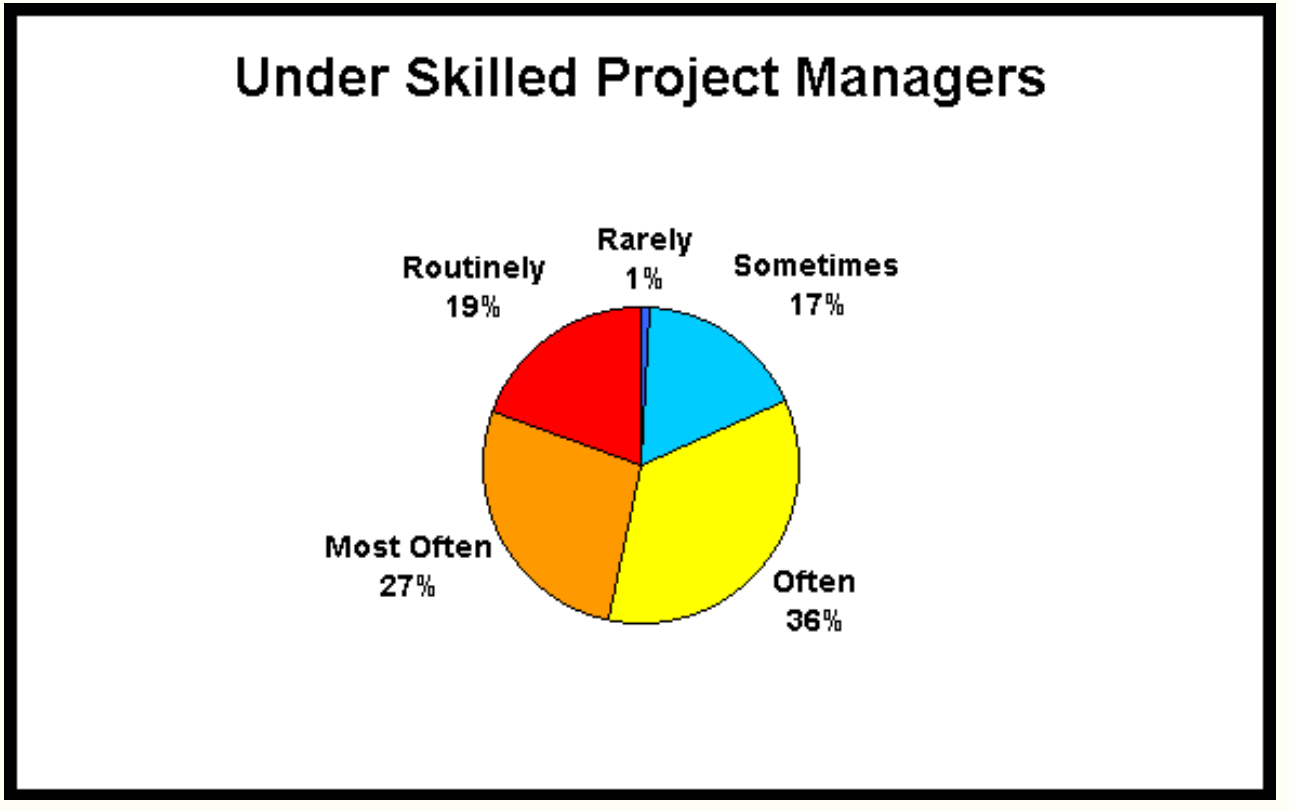
Sin #2: Poor Sponsorship

- Results reported from the SANS Institute ...



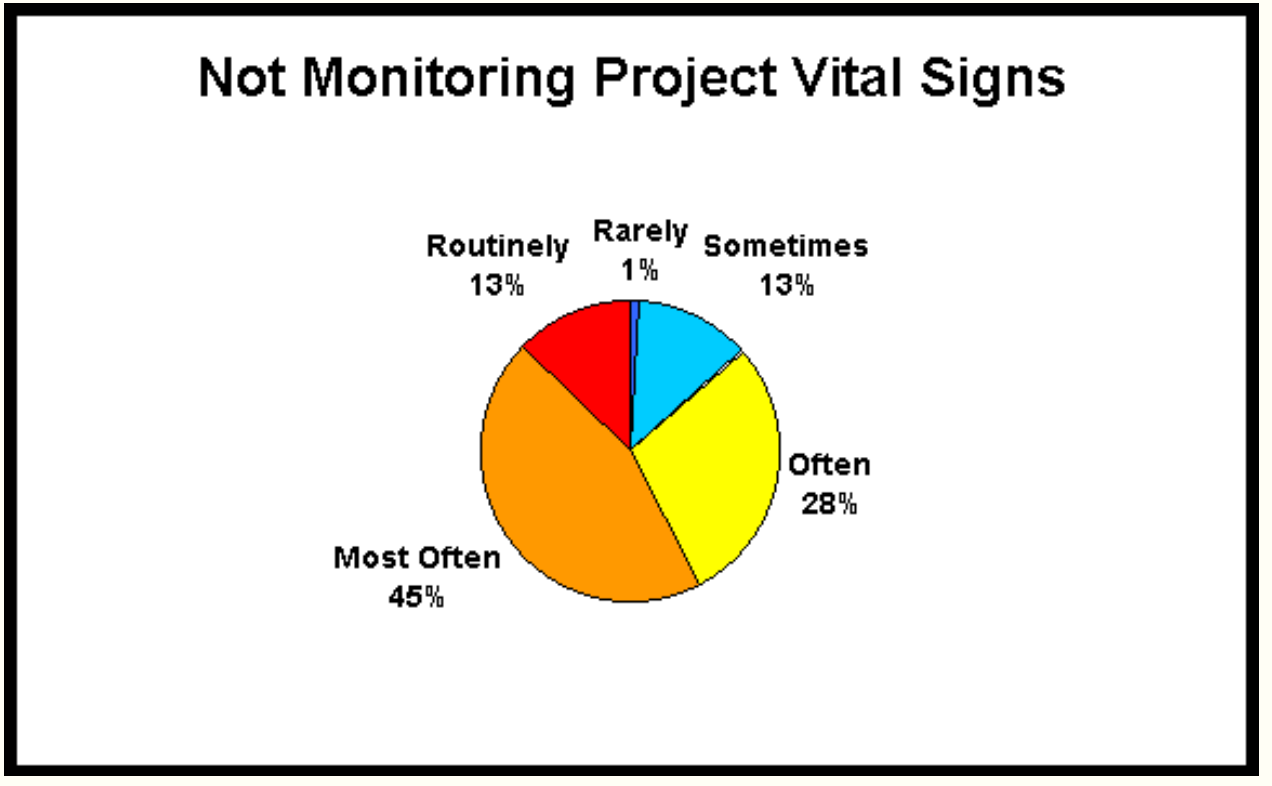
Sin #3: Under Skilled Project Managers

- Results reported from the SANS Institute ...



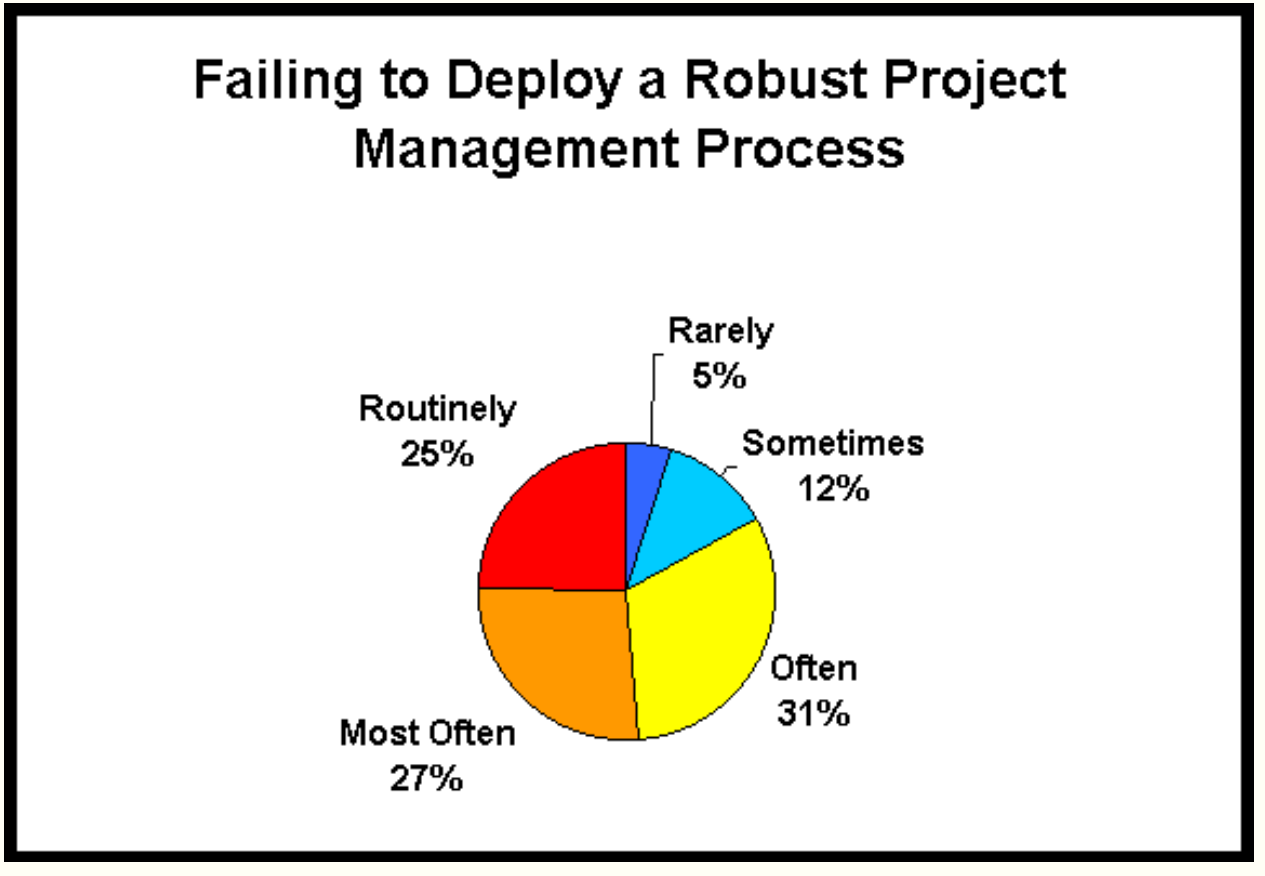
Sin#4: Poor Monitoring

- Results reported from the SANS Institute ...



Sin #5: Weak Project Management Process

- Results reported from the SANS Institute ...



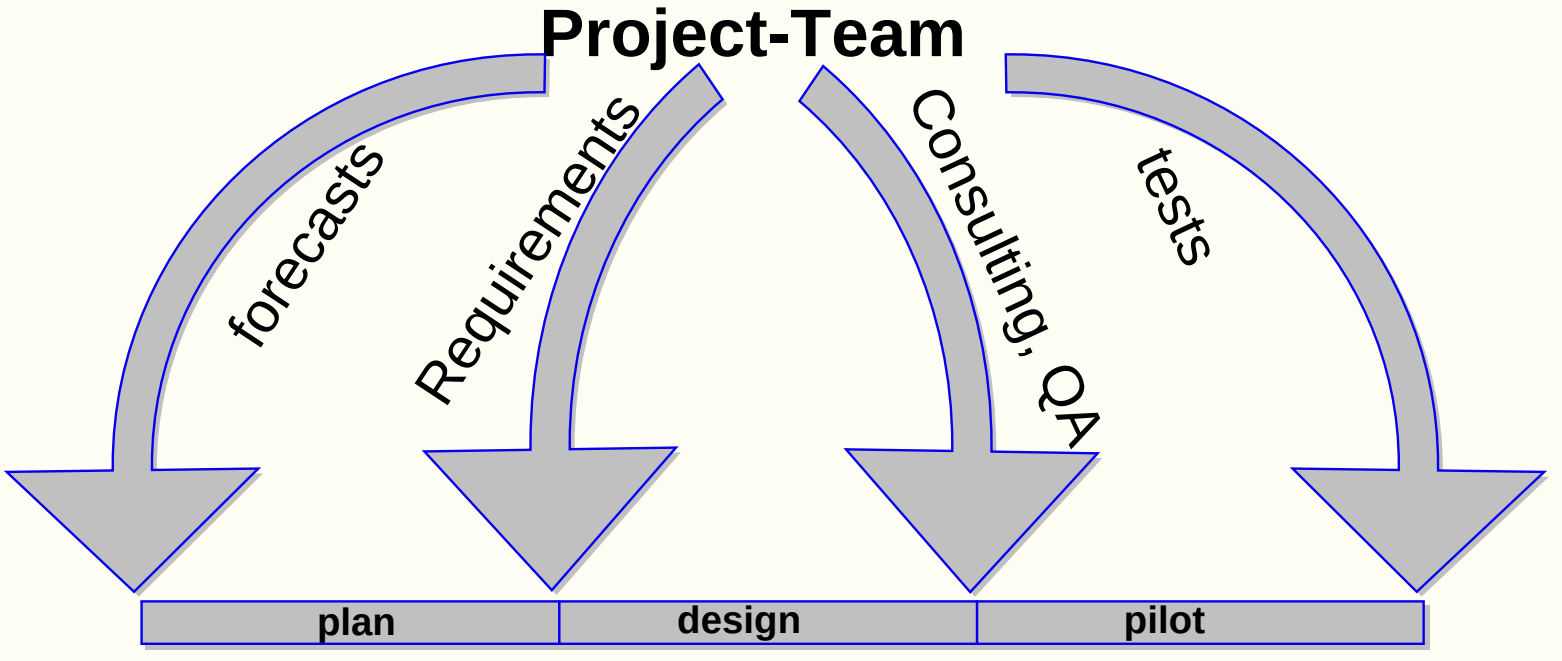
Sin-Index 3.4 = Project Purgatory

The fire is hot; the good news is that you are still in the frying pan.

- When it comes to competent **project management**, your organization doesn't have a clue.
- In your current environment, practically **every idea**, no matter how lame, **becomes a project**.
- Your project managers are experts in the art of **"estimate-to-please."**
- Project managers and team members receive **insufficient** project management training.
- Management's solution is to acquire site licenses to **project management software** – you might as well attach afterburners onto a mule.
- When a project is successful, it is due to heroic performances by a few individuals, or just **"dumb" luck**.

… The patient is in critical condition.

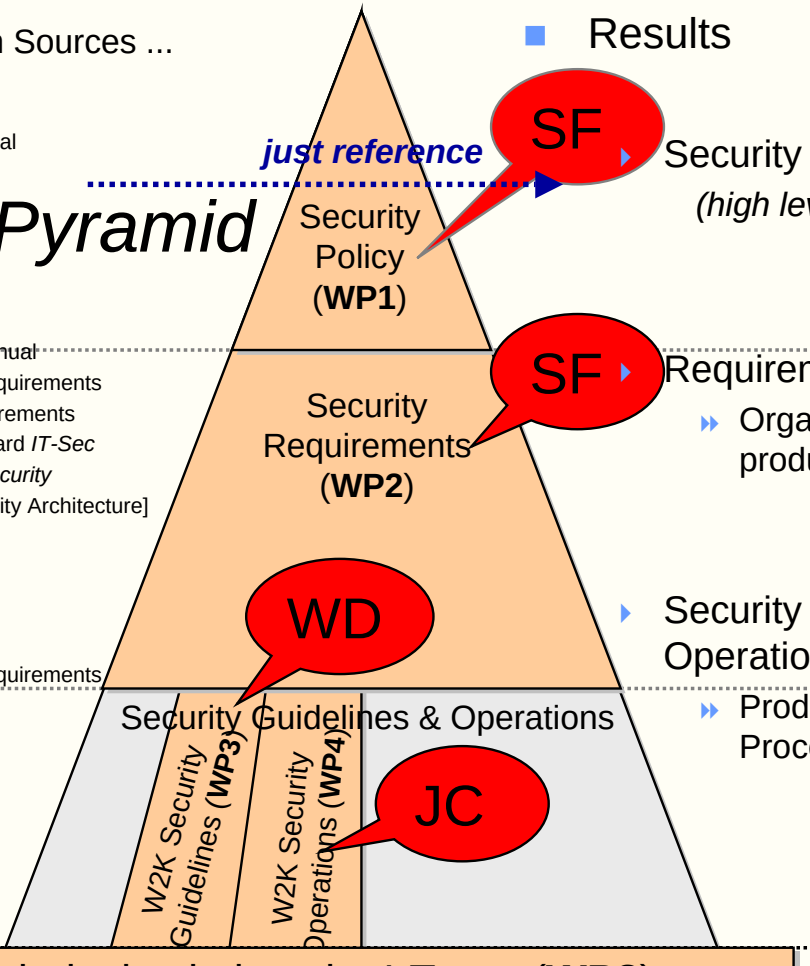
Security –Where to apply?



Positioning of Deliverables in a ”Big Picture”

- Existing Information Sources ...
  - Corporate Policy Manual
- Results

The Security Pyramid



Security Policy *(high level)*

Level 1 (static)

1. Corporate Security Manual
2. Corporate Network Requirements
3. London regional Requirements
4. Central Institute Standard *IT-Sec*
5. Central Institute *NT-Security*
6. [Central Institute Security Architecture]
7. [DoD Orange book]
8. [BSI GSHB]

Requirements
- Organizational, technical, non product specific

Level 2 (rel. static)

- Corporate Network Requirements
- NT Admin Manual
- Discussion by IT

Security Guidelines & Operations
- Product specific Solutions and Processes

Level 3 (dynamic)

Communication Base

Level 4 (dynamic)

Technical solutions by I-Team (**WP8**) (e.g. Parameter Settings, ...), Process solutions by Operations