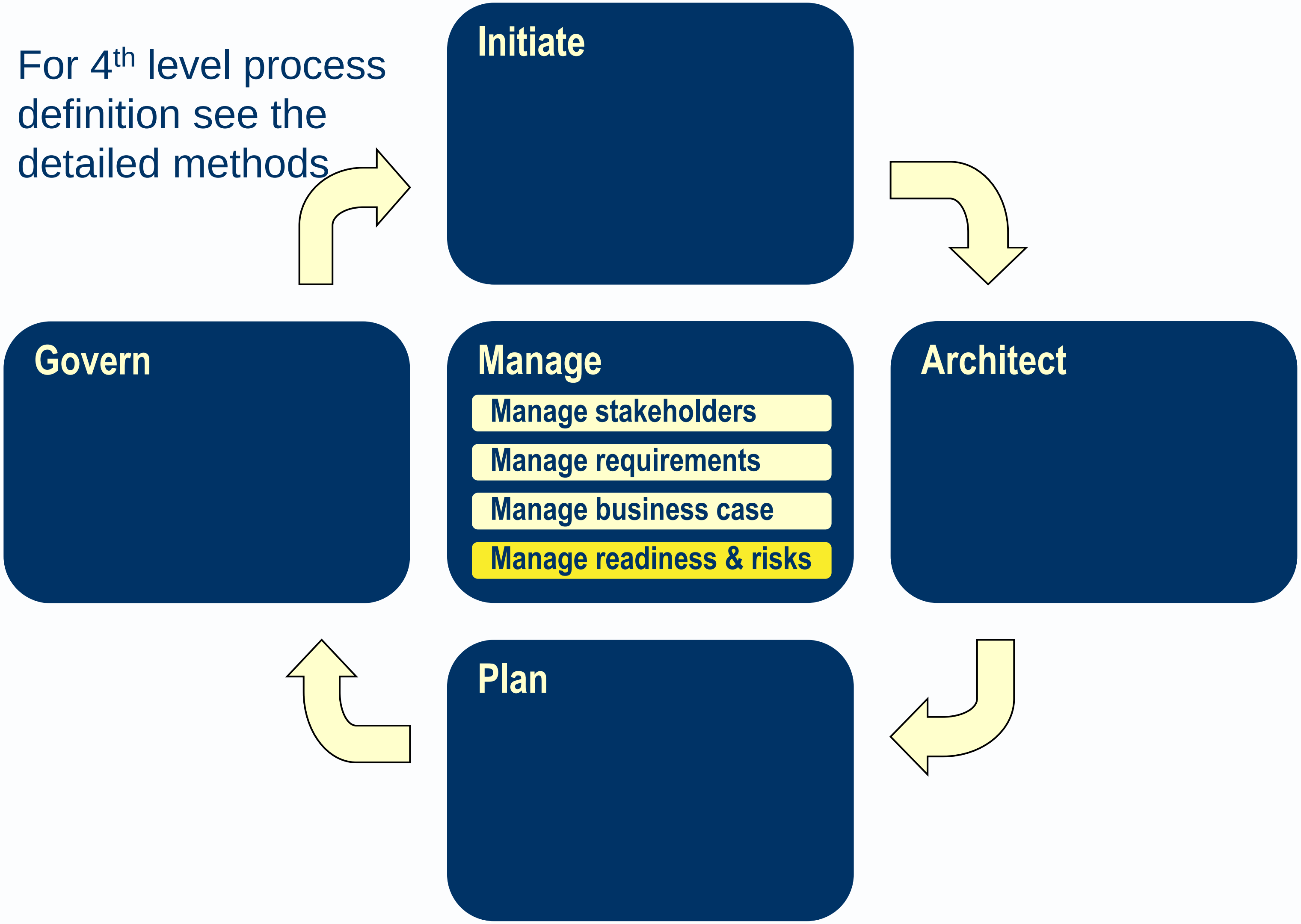
Avancier Methods (AM)
MANAGE

Manage readiness and risks

Manage readiness & risks

- For 4th level process definition see the detailed methods



Assess risks

Risk analysis	Analysis of vulnerabilities that threaten the ability of a target system to meet requirements, especially non-functional requirements, including security. Risk analysis is needed before architecture definition starts in earnest, and then several times later in the process, and at several levels of design.

Approach

- Risk management is about reducing the probability of a forecast risk event and/or recovering from its occurrence as an issue.
- About identifying, classifying and managing risks, including those arising from unpreparedness.
- Note that “readiness assessment” carried out in the Architect phase often provides a specific collection of risks to do with the business or IT function not being ready to accept or implement changes

Identify and catalogue risks

1. **Identify and catalogue risks**
2. Classify and prioritise risks
3. Define risk mitigation and containment actions
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. Recognise when a risk event occurs as an issue
6. After risk becomes issue, take risk recovery/containment actions

Identify and catalogue risks

- Risks are commonly listed in a Risks, Assumptions, Issues and Dependencies (RAID) catalogue.
- Assumptions and dependencies can turn into risks
- Risk turn into issues.

RAID catalogue

RAID catalogue	A catalogue of risks, assumptions, issues and dependencies, maintained separately from requirements and from solution documentation. Cf. Risk Register in PRINCE2.
Risk	A potential problem; an event that will cause an issue if it occurs.
Assumption	Statement that, if not true, could turn into a risk or issue that threatens the success of a project.
Issue	A problem that needs resolution. Sometimes the realisation of a pre-identified risk, or an assumption that turned out to be false.
Dependency (risk sense)	A dependency of a project upon an external actor or deliverable, not under the management of the project manager.

Identify risks

Avancier

- What are you trying to protect?
- What are sources of risk?

- Predict likely issues in order to anticipate them
- Every issue you have ever experienced could in theory have been logged as a risk beforehand

- Focus on the ‘iron triangle’ of
  - scope,
  - cost and
  - time.

- Consider people, processes, technologies, and locations/environments.

Likely areas of project management risk

Avancier

After PMBOK

- Scope
- Cost
- Deadline/Time
- Procurements
- Human resources
- Cost of poor quality
- Communications
- The flow of process

After Avancier survey

1. Functional requirements are unclear and will change.
2. Non-functional requirements are unclear and will demand additional design.
3. Initial estimates are inaccurate and will turn out to be underestimates.
4. Process is largely unknown and not agreed, leading to inefficiency.
5. People are not trained/able/motivated enough, leading to inefficiency.
6. Technologies are unknown/buggy/ill-chosen, leading to inefficiency.

Different kinds of business – different kinds of risk

Avancier

- A stock trading system moving £100M/day.
- A SME dealing with auto-parts.
- A government department logging claims for grants from farmers.
- They are all different.

- Consider security especially.
- Security requirements need to be stated and analyzed just as much as any other functional requirement.
- Security functionality should be tested.

Look for business & IT readiness risks

- Analyse and report how prepared the relevant departments are ready for the transformation that is being planned.
- If need be, produce a readiness factor catalogue of the kind below

Readiness factor	Responsible party	Current Readiness level	Required Readiness level	Actions to raise Readiness level	Target completion date
A		Low	High	xxxx	99/99/99
B		Moderate	High	xxxx	99/99/99
C		High	High	xxxx	99/99/99
D		Low	Moderate	xxxx	99/99/99
E		Low	Low		
F		Low	High	xxxx	99/99/99

Record risk events

- A risk event has a description and a potential time period in which it may occur.

- Risk events (described as when they happen) might include
  - *"key supplier has gone bust"* and
  - *"the project has gone over budget."*

- The first is an all-or-nothing event, though you may see it coming.
- The second is an event on a continuum that might be sub divided into
  - Project has gone 5% over budget
  - Project has gone 15% over budget
  - Project has gone 30% over budget, etc.

Record risks

- Help managers to create and maintain a RAID catalogue.

- Try not to clutter up the architecture definition itself with RAID.
- Refer only to key ones where it helps.

Classify and prioritise risks

1. Identify and catalogue risks
2. **Classify and prioritise risks**
3. Define risk mitigation and containment actions
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. Recognise when a risk event occurs as an issue
6. After risk becomes issue, take risk recovery/containment actions

Classify and prioritise risks

- A risk manager should strive to define the likelihood and impact of a risk.
- A common way to classify and priorities risks is using a grid such as the one below.

Likelihood Impact	Low	Medium	High
High			Highest risk
Medium			
Low	Lowest risk		

Scoring risks

- A matrix of 16 or 25 cells might be used, but
- Quantification is often too imprecise for > 9 cells.
- Do not multiply probability x impact.
- Multiplying sounds scientific, but is misleading pseudo science.
- If you must use maths, then add rather than multiply.

Likelihood Impact	Low	Medium	High
High	3 + 1	3 + 2	3 + 3
Medium	2 + 1	2 + 2	1 + 2
Low	1 + 1	1 + 2	1 + 3

Avancier

Ranking risks

- Not only according to the impact and the likelihood but also
- The time and resources available for risk mitigation

Impact	Likelihood / frequency	Level of risk
High	High	**6 Very high**
High	Medium	**5 High**
Medium	High	**5 High**
Low	High	**4 Medium**
High	Low	**4 Medium**
Medium	Medium	**4 Medium**
Medium	Low	**3 Low**
Low	Medium	**3 Low**
Low	Low	**2 Very low**

- A 100% likely risk is in fact an issue - to be dealt with now.
- Whether we call it risk or issue, the management question is:
- How much time and money to invest in addressing it?

Define risk mitigation and containment actions

Avancier

1. Identify and catalogue risks
2. Classify and prioritise risks
3. **Define risk mitigation and containment actions**
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. Recognise when a risk event occurs as an issue
6. After risk becomes issue, take risk recovery/containment actions

Define risk mitigation and containment actions

- A risk manager should strive to define risk mitigation and containment procedures (aka controls).
- Focusing attention of course on the highest risks.

- You may:
  - Tolerate - accept the risk.
  - Treat - improve controls.
  - Transfer - insure yourself.
  - Terminate - don’t do it.

Before risk event occurrence, take risk avoidance/mitigation actions

1. Identify and catalogue risks
2. Classify and prioritise risks
3. Define risk mitigation and containment actions
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. Recognise when a risk event occurs as an issue
6. After risk becomes issue, take risk recovery/containment actions

Reviewing the RAID log on a regular basis

- Add, update and delete RAID catalogue entries to reflect changed circumstances.
- Look forward, look for clues as to likely events.
- Is there a trend? Are things getting worse or better?

Example

- In the example, you would want to monitor the supplier's financial health.
- You want one or more reports on a regular basis about the supplier's finances.
- Reports might be classified for simplicity as red/amber/green. If the reports turn amber or red, you need to take action.
- Perhaps make sure the supplier is paid on time; perhaps start shopping around for a new supplier; etc.

- Hopefully, taking avoidance/mitigation actions shifts the risk event likelihood or impact back to low.

Beware these factors

- Both quantifications come with a wide error margin.
- Risks are like estimates, the further ahead you document them, the less accurate they are.
- Likelihood and impact will change from week to week.
- Most risks are not all-or-nothing. E.g.

Risk: estimate exceeds reality	The likelihood is	The impact is
< 10%	< 50%	aaa
11-20%	30%	bbb
21-40%	10%.	ccc
41-80%	5%.	ddd
81-160%	3%.	eee
16-320%	1%.	fff
>320%	1%.	ggg

Recognise when a risk event occurs as an issue

Avancier

1. Identify and catalogue risks
2. Classify and prioritise risks
3. Define risk mitigation and containment actions
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. **Recognise when a risk event occurs as an issue**
6. After risk becomes issue, take risk recovery/containment actions

Recognise when a risk event occurs as an issue

Avancier

- In the example, the risk event occurrence is the point in time you find the supplier has gone bust.
- That is, the moment the risk turns into an issue in the RAID catalogue.

After risk becomes issue, take risk recovery/containment actions

1. Identify and catalogue risks
2. Classify and prioritise risks
3. Define risk mitigation and containment actions
4. Before risk event occurrence, take risk avoidance/mitigation actions
5. Recognise when a risk event occurs as an issue
6. **After risk becomes issue, take risk recovery/containment actions**

After risk becomes issue, take risk recovery/containment actions

- Now, we need to recover e.g. we engage a new key supplier; start retooling; etc.
- We also need to measure the success of the recovery.

Read also

- The associated paper with cautionary notes

Manage readiness & risks

- For 4th level process definition see the detailed methods