LECTURE 10: PROJECT RISK MANAGEMENT

Yeganeh M. Hayeri
SYS 660
Spring 2019

PROJECT RISK MANAGEMENT

A representative approach for project risk management

Best practices for project risk management

Human issues

Technical issues

Revisiting ordinal misuse

OVERVIEW

In this lecture we are going to cover the US DoD approach to project risk management as a representative example

- US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

Even if you do not end up in the defense industry, it is likely that the risk management approach at your organization will include similar elements

As we walk through the approach, we will note some of the methodological issues that we have discussed earlier in the class

The intent of this lecture is not to endorse a particular approach to project risk management, but instead to expose you to an approach that you may see

DEFINITION OF A PROJECT RISK

"Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints."

- US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

According to the guide, a risk has three components:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at the present time of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

DEFINITION OF A PROJECT RISK

We see a specialized version of the definitions we discussed in the last lecture

- Recall that we defined a risk as the probability and severity of an adverse event

Here, the adverse consequences take the form of project performance shortfalls

We also have a variation on the risk triplet

- What can go wrong? What is its likelihood? What are the consequences?

The key difference is that triggering event, “What can go wrong?” is termed the root cause

AN ISSUE VS. A RISK

A key distinction that is critical to make in project management is that of an issue versus a risk

- An issue is an adverse event that is already underway, thus it is not a risk

The DoD guide has a useful test to tell the difference:

- "If a root cause is described in the past tense, the root cause has already occurred, and hence, it is an issue that needs to be resolved, but it is not a risk."

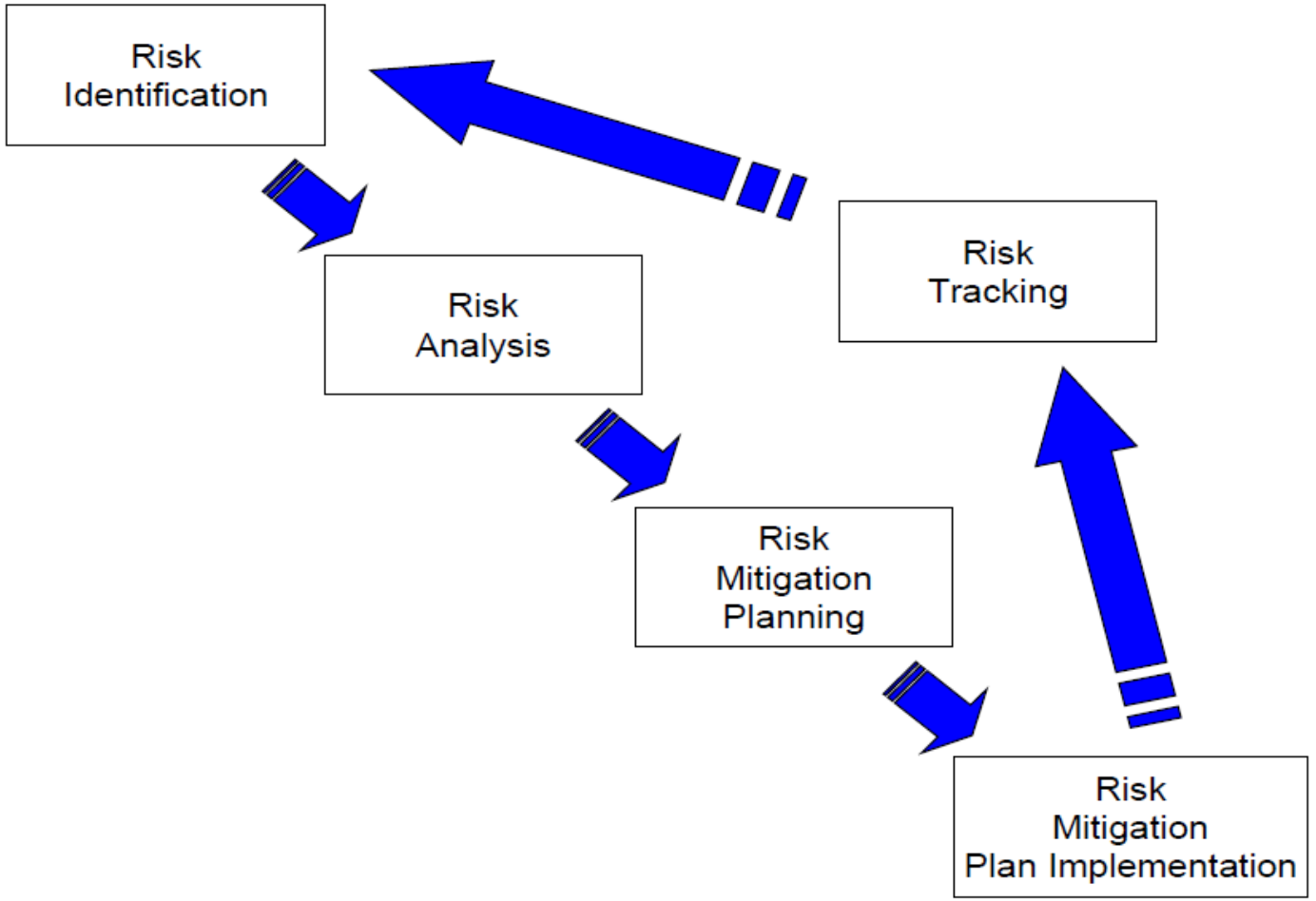
Obviously, it is very important to manage issues

- Hence the common phrase, "fighting fires," in project management

The problem is that there is a tendency to focus too much attention on managing issues as opposed to risks

As a result, some of those unmanaged risks become issues

DOD RISK MANAGEMENT PROCESS



Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

RISK IDENTIFICATION

Candidate risks can be identified through examination of a number of different sources:

- Requirements
- Critical technologies list
- Work breakdown structure
- Project schedule and budget
- Technical documentation
- Project staffing plan
- Lessons learned from past projects

The objective is to identify what can go wrong in each of these areas

The goal should be to identify all credible risks and worry about prioritizing them later

RISK IDENTIFICATION

The DoD Risk Management Guide suggests the following areas as sources of risk:

Threat

- In the DoD context this refers to uncertainty in the assessment of a military adversary, but in a commercial context it is critical to consider the actions and capabilities of your competitors

Requirements

- Risky requirements and changing requirements are one of the leading causes of project failure! When developing commercial products, consider uncertainty in the market/customer assessments.

Technical baseline

- How risky is the proposed system configuration?

Test and evaluation

- The purpose of test and evaluation is to burn down risk. Will your test program accomplish that?

Modeling and simulation

- Model risk is an often overlooked problem. First, there are risks associated with implementing any custom developed models and simulations. Second, there are the risks associated with V&V of those simulations. Finally, there is the risk that an error in the model will lead to a latent problem in your physical system.

RISK IDENTIFICATION

Technology

- Immature technologies are a leading cause of project failure for any system that is making use of "bleeding edge" technologies. However, even systems using mature technologies need to be wary of using such technologies in new application areas and interaction effects from combining technologies in a new way.

Logistics

- Are there any risks to supporting the system once it is built? For example: supplier end of life issues, warranty issues, spares availability, skill sets required to maintain the system, etc.

Production/facilities

- Are there any risks to actually producing the system? For example, specialized production equipment, long-lead time items, rare materials, specialized skills, etc?

Concurrency

- Overlapping project phases is a substantial source of risks. How much rework will be required if design changes are made during production?

Industrial capabilities

- Do your suppliers have the necessary capabilities to design and build the system and its components? What is their process maturity?

RISK IDENTIFICATION

Cost

- What are the uncertainties in the project life-cycle cost estimates? Depending the type of project, these could be substantial.

Management

- Are management teams and approaches qualified and sufficient for the nature of the project? For example, an inexperienced PM on a complex project could be a substantial risk.

Schedule

- Projects always have schedule risks. Identify the activities critical to realizing the schedule. PERT, CPM and other scheduling techniques can be useful here.

External Factors

- Look outside the project for risks. Are there key stakeholders who are wavering? Could a shift in market conditions jeopardize the project?

RISK IDENTIFICATION

Budget

- How sensitive is the project to changes in the budget? This is especially important for government projects due to the capricious nature of the budgeting process, but it can also be an issue for commercial projects as well.

Earned Value Management System

- Examining the EVMS is another way to identify schedule and cost risks.
- EVMS helps project managers to measure project performance. It is a systematic project management process used to find variances in projects based on the comparison of worked performed and work planned.

STATING PROJECT RISKS

A good way to ensure that you have properly identified a risk is to state it in the form of an "If…then" statement

If <event occurs> then <consequence occurs>

This format ensures that you are considering both the root cause or triggering event and the resulting consequence

By stating all risks in this format, it can help weed out both issues that aren't really risks and poorly thought out risks

- For example, "risk of cost increase" is not a well formed risk statement because there is no trigger event
- "If the experimental manufacturing process fails to meet reliability requirements, production costs will increase." is a well formed risk statement

EXAMPLES OF ENGINEERING AND PROGRAM RISKS

If our vendor discontinues support for the selected server model in the next three years, then we could be forced to make expensive upgrades sooner than expected

If the experimental engine doesn't meet requirements by PDR, we will be forced to redesign much of the system

If we do not hire a qualified database administrator within three months, we will not meet our delivery schedule

If we do not meet this requirement, then the sponsor will reduce funding for future versions of the system

If this new pharmaceutical drug causes too many side effects, the company will subject to class-action law suits

RISK ANALYSIS

The purpose of the risk analysis phase is to measure each risk

According to the DoD Risk Management Guide this consists of three components:

- Considering the likelihood of the root cause occurrence;
- Identifying the possible consequences in terms of performance, schedule, and cost; and
- Identifying the risk level using the Risk Reporting Matrix…

All available information and evidence should be used to assess the likelihood and consequence of each risk

This is typically done using ordinal scales for likelihood and consequence as shown on the subsequent slides

SCORING LIKELIHOOD

Likelihood

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

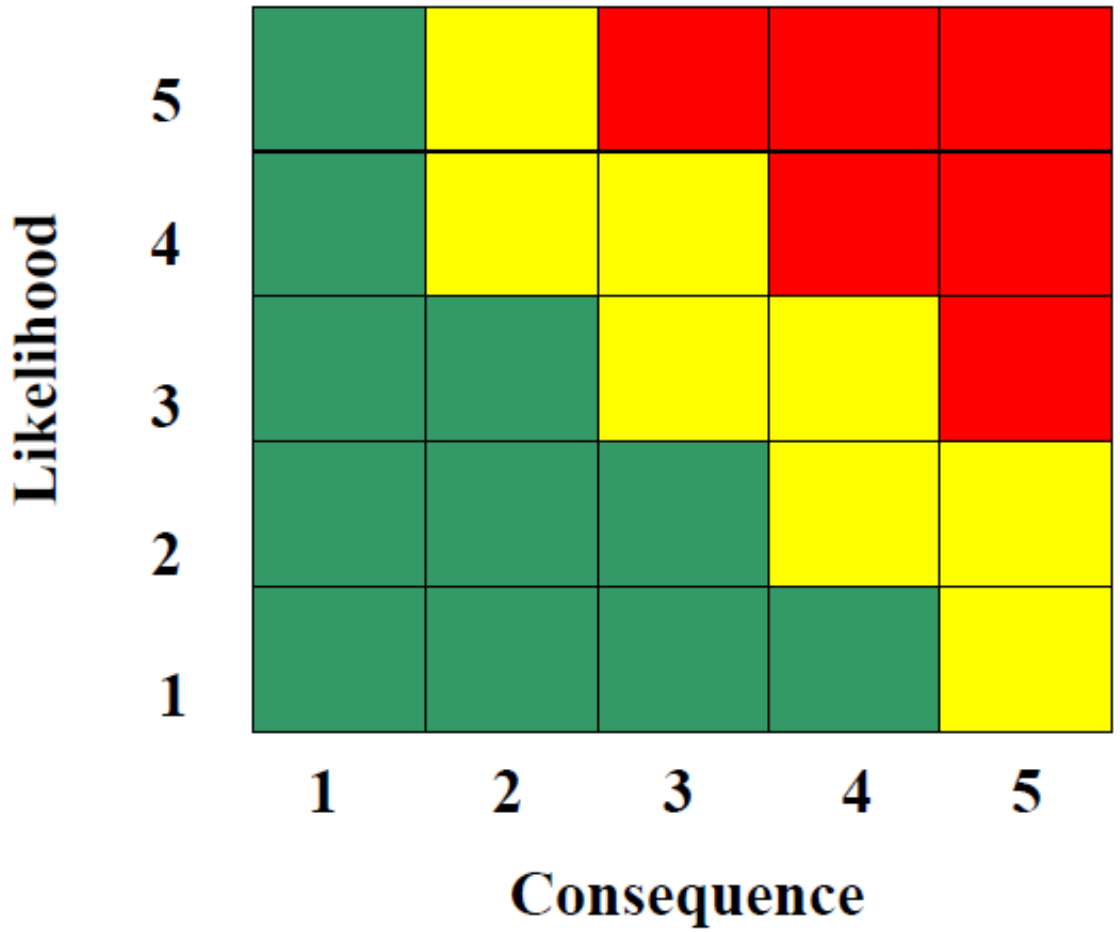
SCORING CONSEQUENCE

Consequence

Level	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates. **Slip < _*_ month(s)**	Budget increase or unit production cost increases. **< _*_ (1% of Budget)**
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. **Slip < _*_ month(s)** **Sub-system slip > _*_ month(s) plus available float.**	Budget increase or unit production cost increase **< _*_ (5% of Budget)**
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected. **Slip < _*_ months**	Budget increase or unit production cost increase **< _*_ (10% of Budget)**
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. **Slip > _*_ months**	Exceeds APB threshold **> _*_ (10% of Budget)**

Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

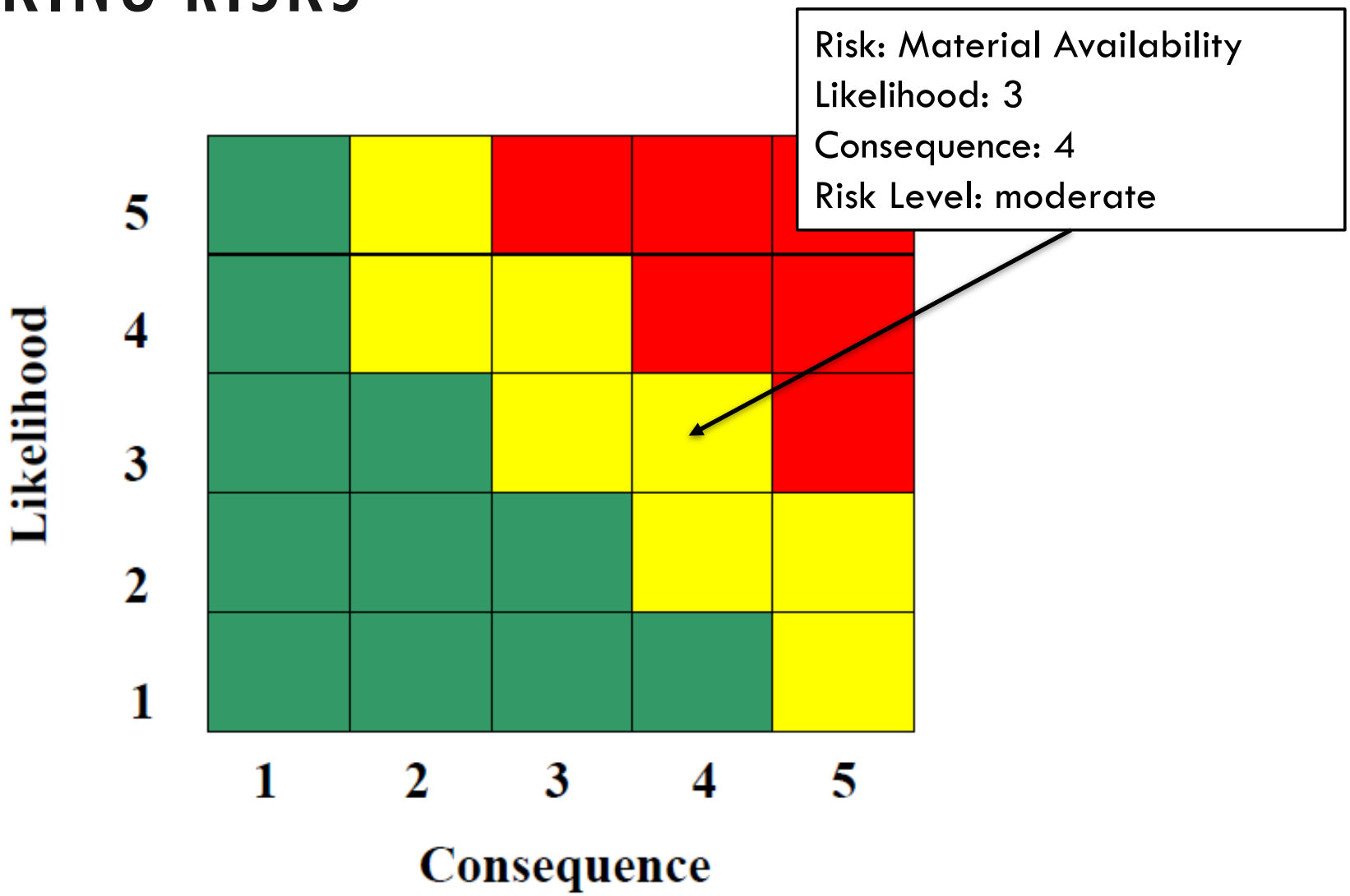
RISK MATRIX



Risk Level
Red = high
Yellow = moderate
Green = low

Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

RANKING RISKS



Source: US Department of Defense, *Risk Management Guide for DoD Acquisition*, 6th ed., Version 1.0, August 2006.

RISK MITIGATION PLANNING

After risks are assessed and ranked using the risk matrix, the next logical step is to determine what to do about the most important risks

The DoD Risk Management Guide identifies the following options:

- Avoiding risk by eliminating the root cause and/or the consequence,
- Controlling the cause or consequence,
- Transferring the risk, and/or
- Assuming the level of risk and continuing on the current program plan.

While the step is called risk mitigation planning, technically, controlling the cause or consequence is the only option that involves mitigation

RISK MITIGATION PLANNING

If the decision is made to mitigate a risks, a plan is developed to execute the mitigation

This involves identifying who, what, when and with what resources

The risk mitigation plan is essentially planning a new sub-task for the project

Obviously risk mitigation consumes resources, so not every risk can be mitigated

Thus, one typically starts with the most critical risks and works downward until the available resources are consumed

This is why proper risk ranking is so critical

RISK MITIGATION PLAN IMPLEMENTATION

A key issue with risk mitigation efforts is that the plan has to be implementable

- For example, if a mitigation requires actions outside of a supplier's statement of work, a contract modification may be required
- Consequently, this can be a non-trivial step

The DoD Risk Management Guide identifies the following objectives:

- Determines what planning, budget, and requirements and contractual changes are needed,
- Provides a coordination vehicle with management and other stakeholders,
- Directs the teams to execute the defined and approved risk mitigation plans,
- Outlines the risk reporting requirements for on-going monitoring, and
- Document the change history.

RISK TRACKING

Risk tracking accomplishes two things:

- It allows management to assess the efficacy of risk mitigation efforts
- It allows management to keep track of risks that are on the watch list in case circumstances change

The DoD Risk Management Guide highlights the following objectives:

- Communicating risks to all affected stakeholders,
- Monitoring risk mitigation plans,
- Reviewing regular status updates,
- Displaying risk management dynamics by tracking risk status within the Risk Reporting Matrix, and
- Alerting management as to when risk mitigation plans should be implemented or adjusted.

RISK TRACKING

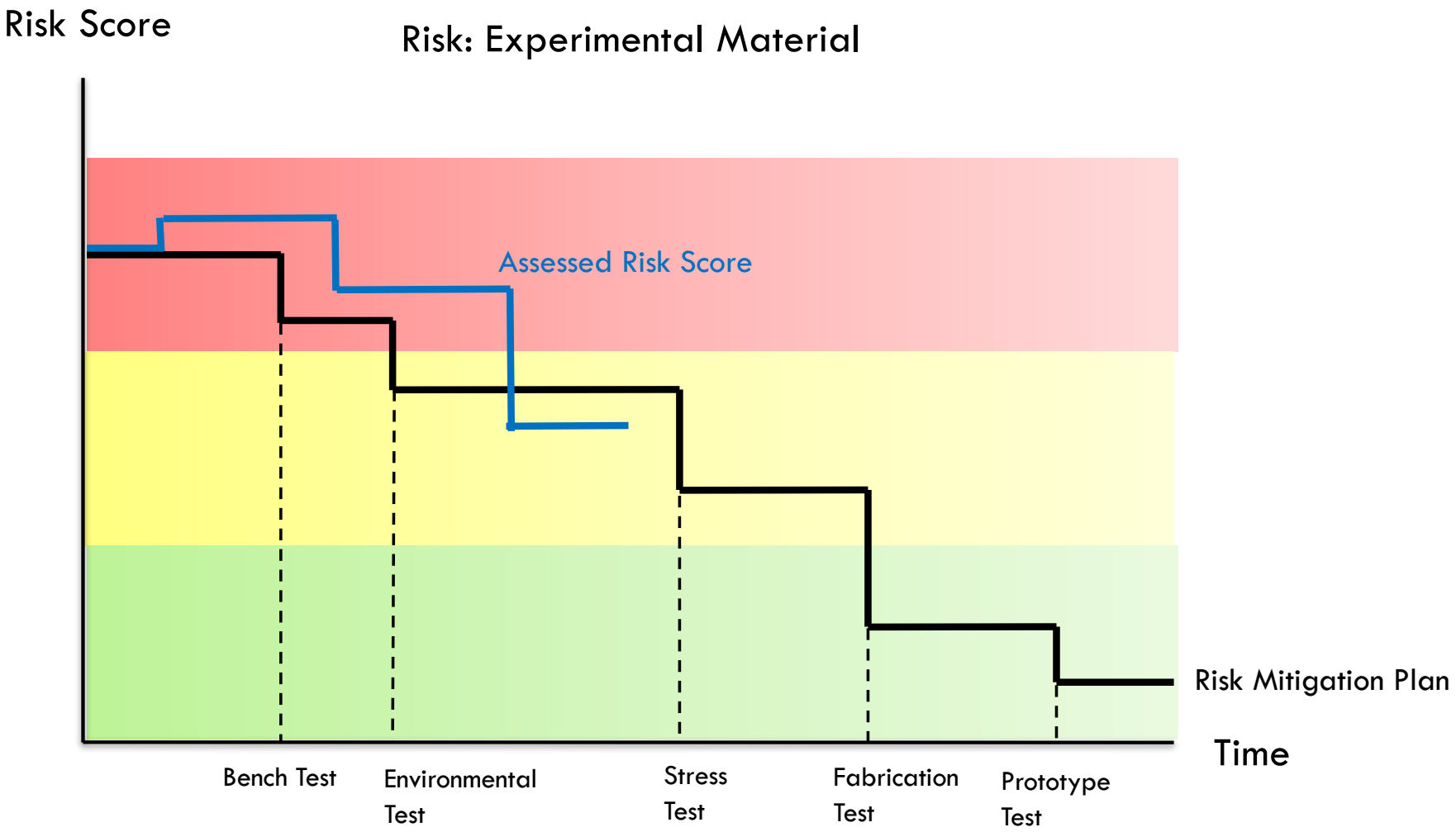
The key to risk tracking is to periodically reassess the likelihood and consequence rating of each tracked risk

There should also be a mechanism to introduce a newly identified risk

While not covered in the DoD Risk Management Guide, risk burn down charts are a popular means for tracking risks within the government contracting community

- These charts multiply the likelihood and consequence scores to obtain an numerical risk score
- The anticipated changes in this score due to risk mitigation activities are plotted against a timeline
- Actual assessments are plotted over time and deviations can trigger corrective actions

RISK BURN DOWN CHART



ISSUES WITH BURN DOWN CHARTS

The big pro of these charts is that they force the project team to actually pay attention to their risks and the efficacy of their plans

However, there are some issues..

We have already discussed the issues with multiplying ordinal numbers

- It's not clear how big of a deviation from the plan is "bad"

Even if the ordinal scales are roughly linear, the risk score is a form of expected value

- High probability, low consequence events are weighted equally with low probability, high consequence events

The plan path is the path if everything goes perfectly

- Every test is a success, etc.

ISSUES WITH BURN DOWN CHARTS

From my personal experience, I feel like risk burn down charts create the false impression among some decision makers that risks can be eliminated with hard work

This leads them to plan programs that take big risks under the assumption that these risks can simply be “burned down”

If an experimental technology is simply not going to work, no risk mitigation plan is going to reverse that

What a risk mitigation plan typically does is allow you to fail fast so that you still have time to switch to a fallback option or cancel the project before too many resources are expended

It does not actually make the impossible possible. So if you don’t have a fallback position, you are in trouble

SUMMARY RISK SHEETS

A common project risk management practice is to build a summary risk sheet for each risk that is under mitigation or on the watch list

Such a sheet might contain

- Risk title
- If…then statement
- Description
- Risk owner
- Current risk matrix assessment
- Mitigation plan
- Burndown chart

These sheets allow management to quickly assess the status of a given risk and may be reviewed at regular status meetings

REVIEWING AND UPDATING RISKS

It is important to regularly review and update risk assessments and mitigation plans

How often this is done and the level of involvement will vary depending the size of the project and the management approach

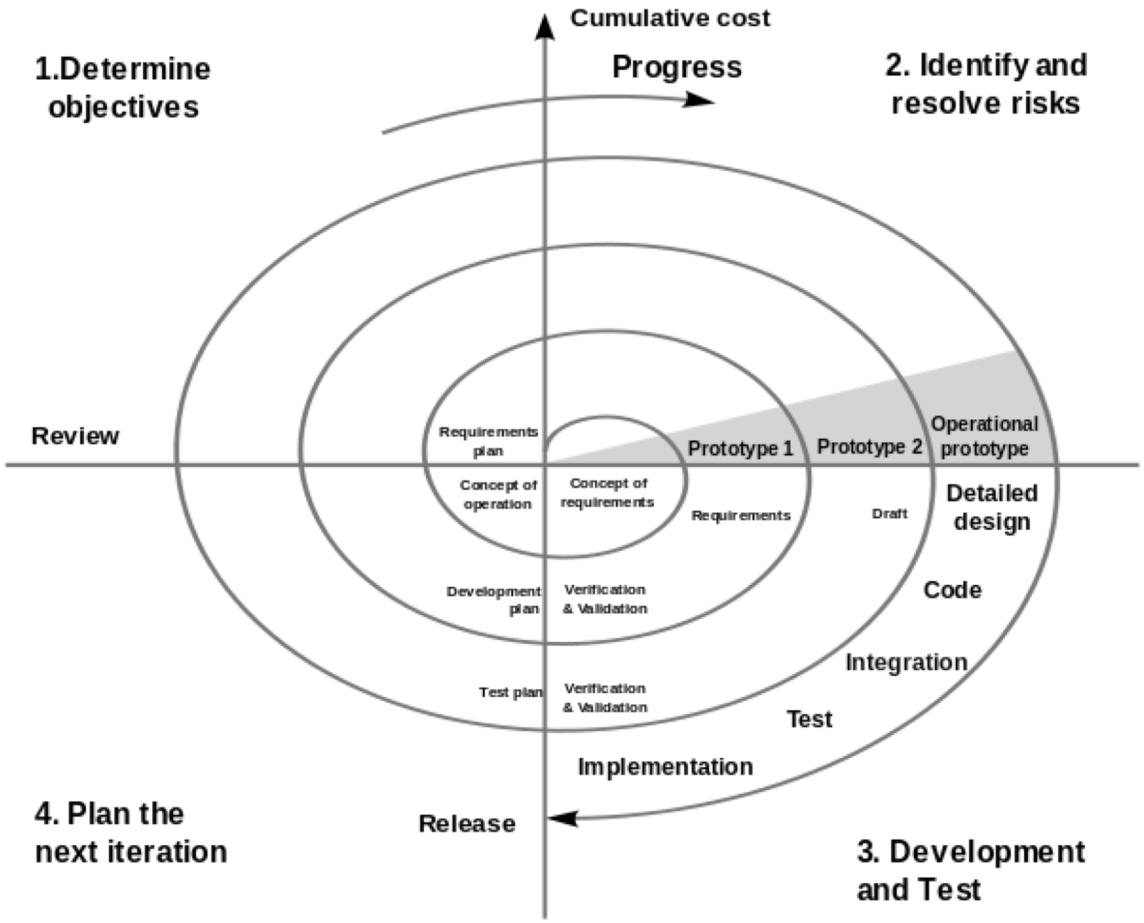
An internal project risk board may meet on a frequent basis

- E.g., every other week

Additional team members and stakeholders may get involved for major status review or milestones

SPIRAL MODEL

- The spiral model explicitly builds risk reduction into the process
- The idea is to reduce the risk of building the wrong system



BEST PRACTICES

Employ a documented risk management plan

- Use a consistent process and avoid ad hoc risk management approaches

Maintain a risk database

- Avoid having the risks documented in word files on someone's computer. Doing so makes it extremely difficult to status and manage risks.

Identify risk owners

- If someone isn't held accountable for managing the risk, it won't happen

Regularly review risks

- It's very easy to perform an initial risk assessment at the beginning of the project and then never get around to looking at it again

BEST PRACTICES

Allow anyone to submit a risk

- The people in the "trenches" may have the best information on where the risks lie

Include your mitigation plans in the project schedule

- Once you generate a risk mitigation plan, it needs to become part of the project plan
- If it isn't, it won't get executed
- For example, if your mitigation plan calls for an additional test, add that test to the project master schedule

Use checklists for risk identification and assessment

- Checklists based on past experience can help avoid repeating the mistakes of the past

HUMAN ISSUES

Shooting the messenger

- Team members may be afraid to report a risk for fear of getting blamed

Fear of cancellation

- Program management my try to suppress critical risks out of the fear that a more risky program will be cancelled in favor of a less risky one

"If we don't do our" job risks

- People have a tendency to identify risks like, "If we don't do a good job with the design, the product won't work as intended"
- While technically a risk, these are not the kind that we are looking for

HUMAN ISSUES

Estimating probabilities

- As we have already discussed, humans are bad at estimating probabilities
- In my experience, people just go with their gut when assessing a project risk rather than collecting any evidence

How hard can it be?!

- People have a tendency to underestimate the difficulty of a task that is outside of their area of expertise
- The availability heuristic at work!

TECHNICAL ISSUES

Root causes versus systemic risks

- The root cause approach doesn't always make sense when the risks are systemic in nature
- A systemic risk is a result of the structure of the system
- Consequently, the "cause" of an adverse event may be an incidental trigger event
- There is no "root cause" in the chain of causality

Multiple independent failures

- The one at time risk approach discussed in this lecture may not identify adverse events that can be caused multiple independent failures that are insignificant in of themselves
- I would be surprised if someone came up with a risk using this process that took the form, "If the cooling system fails, and the control system fails, and the backup valve fails, then there will be an explosion"

TECHNICAL ISSUES

Multiplying ordinal scores

- The risk burn down charts multiply ordinal numbers
- We will revisit this issue again on the next slide

Non-linear to ordinal scales

- When using ordinal numbers in quantitative scoring metrics such as expected value, one is implicitly applying a linear scale
- When the underlying scale is non-linear as it was in the methodology we discussed, the results are distorted and risks can be misprioritized

Range compression

- When using risk matrices, some of the boxes substantially compress ranges
- For example, the “not likely” box covers the probability range of 0 to 10%
- There is gigantic difference between a 10% chance of a nuclear meltdown and a 0% chance of a nuclear meltdown

ORDINAL MISUSE EXAMPLE

Consider the following example scales for scoring risks

Score	Consequence
5	Loss of life
4	Loss of mission
3	Degraded mission performance
2	Minor inconvenience
1	No effect

Score	Likelihood
5	Very likely
4	Highly likely
3	Somewhat likely
2	Possible
1	Unlikely

Because we are using an ordinal scale, all we know is that "Loss of life" is worse than "Loss of mission," but we do not know how much worse.

ORDINAL MISUSE EXAMPLE

As we have discussed previously, a popular way to rank risks is to multiply an ordinal value for consequence by an ordinal value for likelihood

Imagine that we had two risks:

- A highly likely chance for loss of mission (Likelihood = 4, Consequence = 4)
- A somewhat likely chance for loss of life (Likelihood = 3, Consequence = 5)

Using the scales from previous slide, these risks would be scored 16 and 15 respectively

If you were the decision maker would you consider a somewhat likely chance for loss of life to be a lower priority than a loss of mission?

The problem is that once you multiply ordinal numbers, you implicitly assume that their ratios are meaningful

- Is loss of mission only twice as bad as a minor inconvenience? It would probably be much worse in the minds of most decision makers.

SUMMARY

As we have discussed, there are some significant methodological issues associated with the typical approach to project risk management

- Using ordinal scoring can result in misprioritization
- Risk matrices introduce range compression

So why do organizations continue to use and, in fact, advocate these types of methods?

Once again, the value is in the exercise: It is a major achievement to get most organizations to think about risk at all

The value is generated when members of a project actively engage in identifying, prioritizing, and developing plans to mitigate risks rather than just letting things happen

SUMMARY

So the takeaway here is to use your judgment

Look for circumstances when shortcomings can cause problems

- If your risk has to do with the difficulty of hiring a qualified database administrator in time to meet the project schedule, then the presented methods are likely sufficient
- If your risk has to do with an engineering disaster such as a plane crashing, a bridge collapsing, or a nuclear reactor failing, then use a more sophisticated and QUANTITATIVE method