Risk Management

- Enterprise Risk with IT
- Software Project Risks
- Risk identification
- Risk projection (estimation)
- Risk mitigation, monitoring, and management

Problems with IT in Enterprise

- High complexity of IT environments
- Communication gap between business and IT managers
- Disappointing IT service levels from internal IT functions and also from outsourced IT providers
- IT costs are perceived to be out of control
- Unsatisfactory ROI/productivity gains on technology investments
- Impaired organizational flexibility and nimbleness to change
- Frequent resort to *ad hoc* solutions due to many constraints

Five Major Components of IT Governance

- IT principles – high level statements about how IT is used
- IT architecture – set of technical choices to guide the organization
- IT infrastructure strategies – technical infrastructure needed to deliver reliable, secure and efficient services
- Business applications – process of identifying needed applications
- IT investment and prioritization – mechanism for making decisions about project approvals and budgets

– Weill and Ross (MIT), 2004

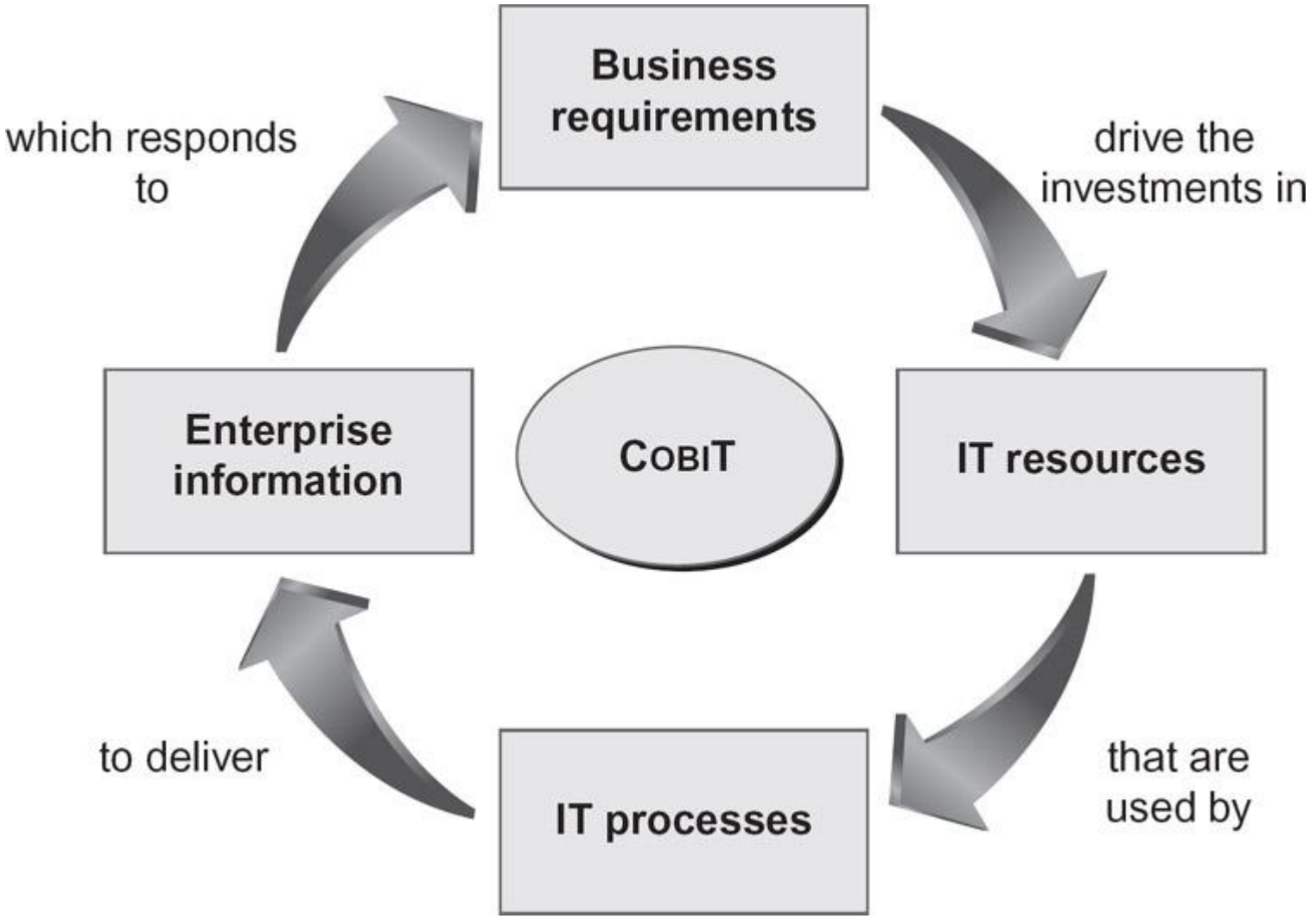
COBIT for IT Governance

- Control Objectives for Information and Related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts.
- COBIT practices are focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong.
- COBIT supports IT governance by providing a framework to ensure that
  - IT is aligned with the business
  - IT enables the business and maximizes benefits
  - IT resources are used responsibly
  - IT risks are managed appropriately

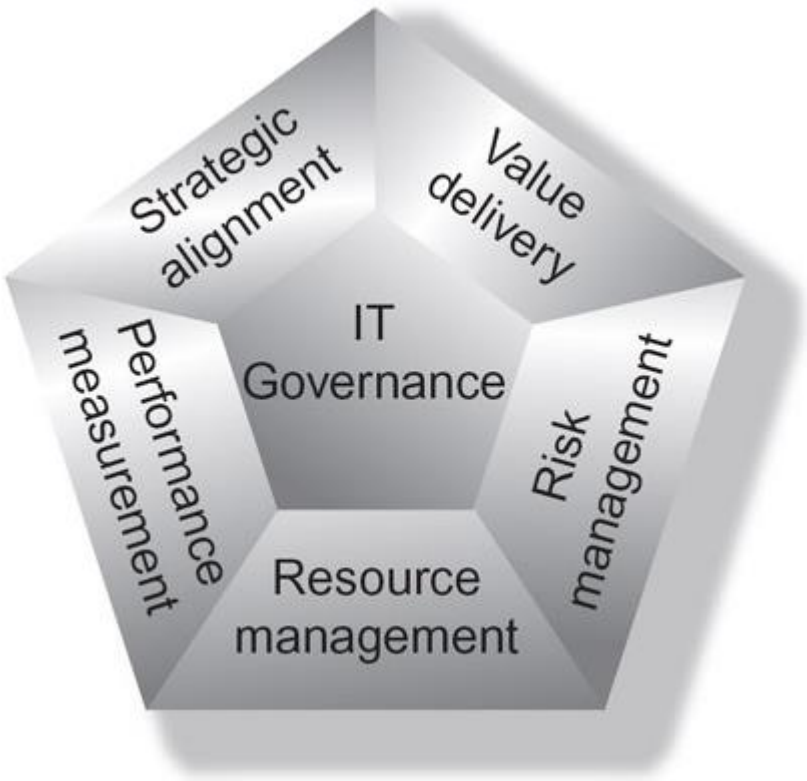
Some Pain Points addressed by COBIT 5

- Business frustration with failed initiatives, rising IT costs and a perception of low business value
- Significant incidents related to IT risk, such as data loss or project failure
- Outsourcing service delivery problems, such as consistent failure to meet agreed-on service levels
- Failure to meet regulatory or contractual requirements
- IT limiting the enterprise's innovation capabilities and business agility
- Regular audit findings about poor IT performance or reported IT quality of service problems
- Hidden and rogue IT spending
- Duplication or overlap between initiatives or wasting resources, such as premature project termination
- Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
- IT-enabled changes failing to meet business needs and delivered late or over budget
- Board members, executives or senior managers who are reluctant to engage with IT, or a lack of committed and satisfied business sponsors for IT
- Complex IT operating models

Basic COBIT principle



IT governance focus areas



Strategic alignment focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

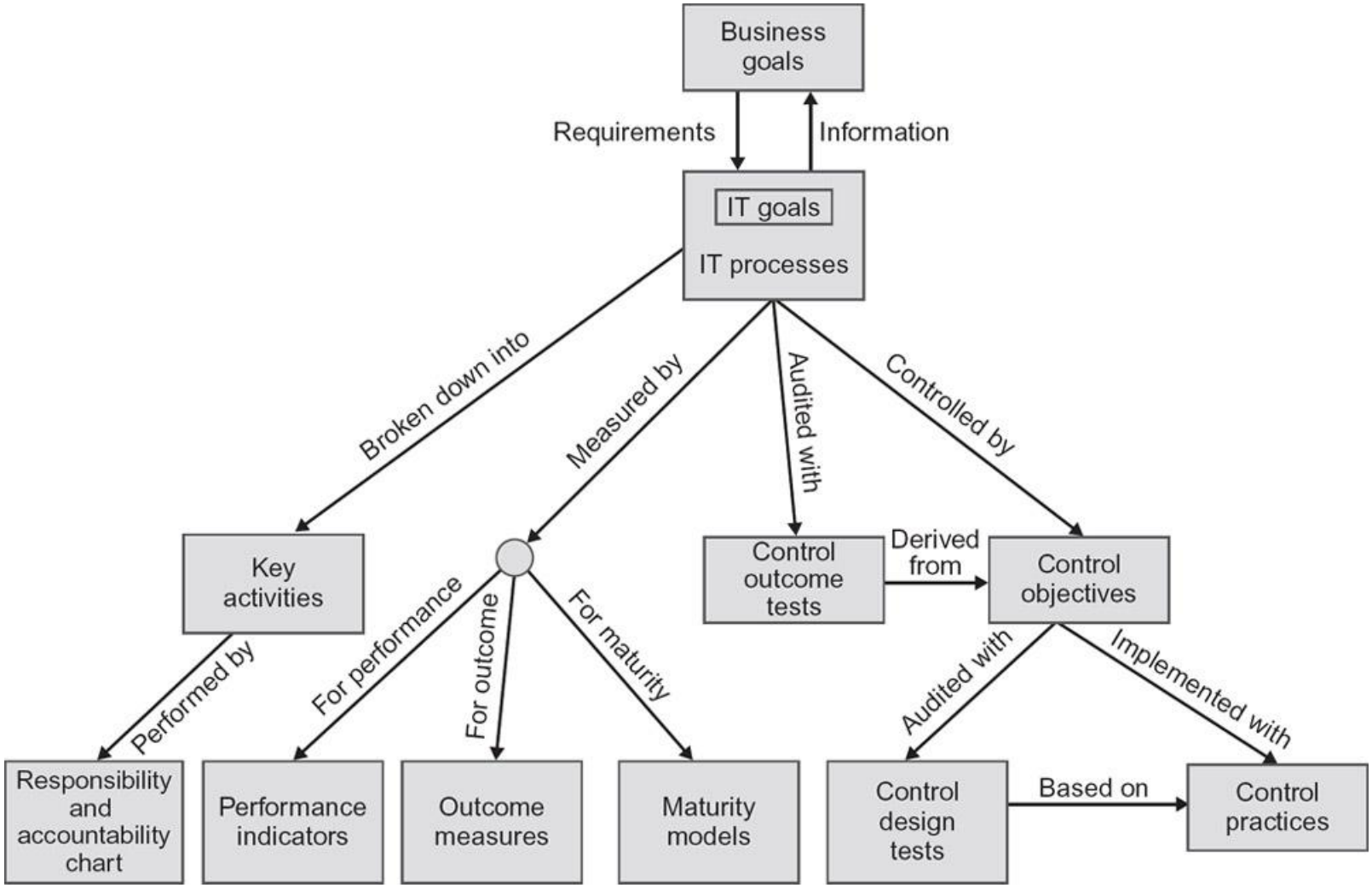
Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

Resource management is about the optimal investment in, and the proper management of, critical IT resources: ***applications, information, infrastructure and people***. Key issues relate to the optimization of knowledge and infrastructure.

Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.

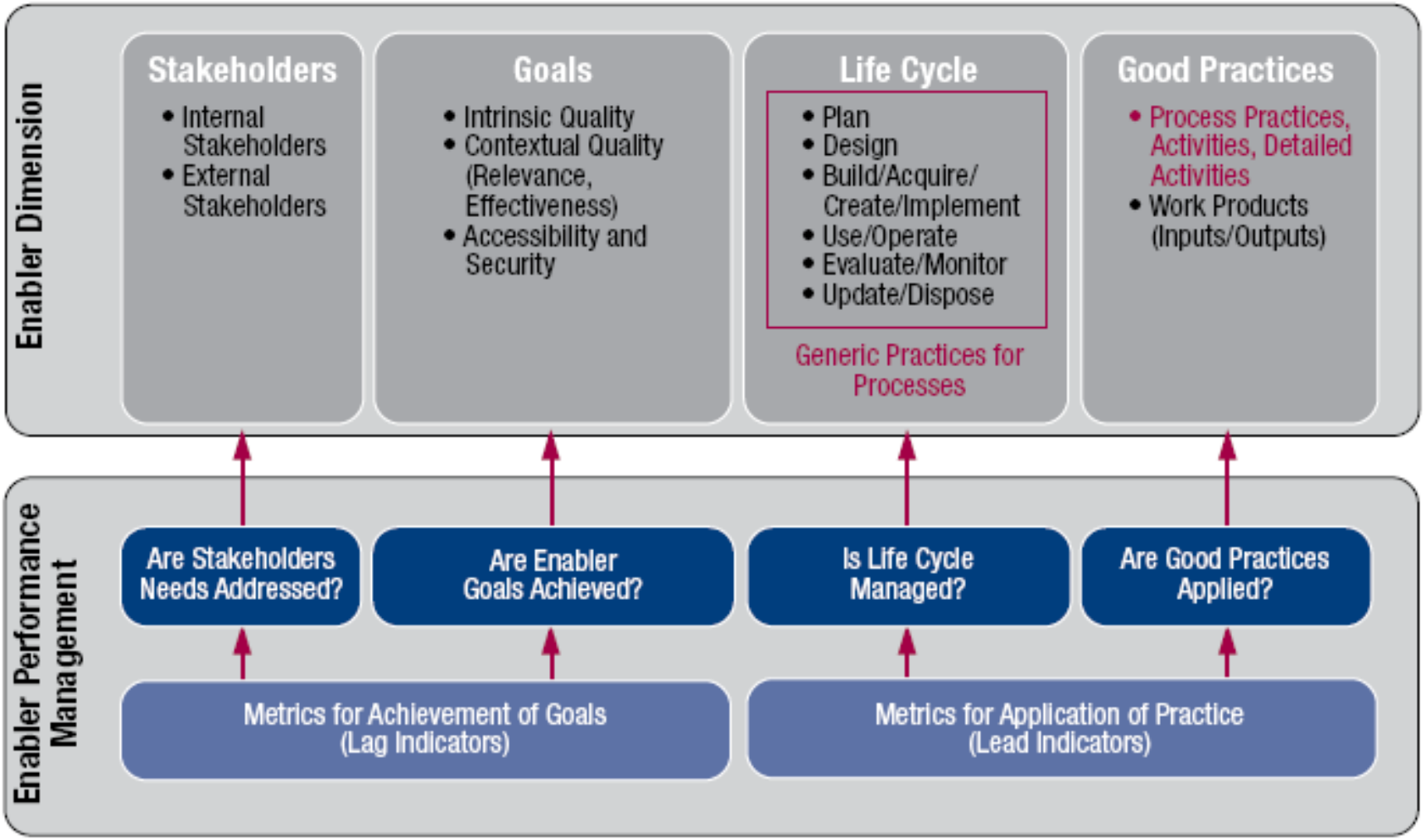
Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Interrelationships of COBIT components



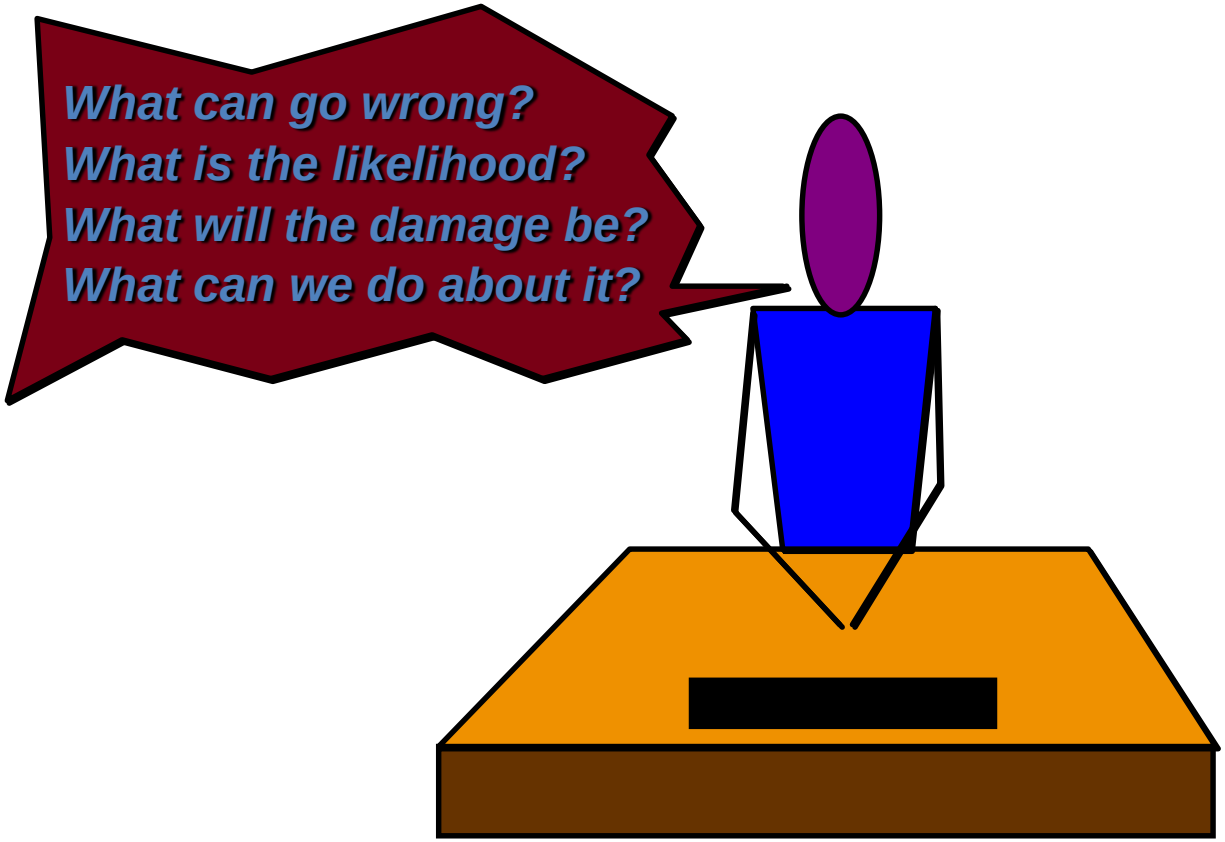
"Information Technology Risk Management in Enterprise Environments.." by Jake Kouns and Daniel Minoli John Wiley & Sons © 2010

COBIT 5: Enabling Processes (cont.)



Software Project Risks

Project Risks



The time to repair the roof is when the sun is shining.

John F. Kennedy

Definition of Risk

- A risk is a potential problem – it might happen and it might not
- Conceptual definition of risk
  - Risk concerns future happenings
  - Risk involves change in mind, opinion, event, action, place, etc.
  - Risk involves choice and the uncertainty that choice entails
- Two characteristics of risk
  - Uncertainty – the risk may or may not happen, that is, there are no 100% risks (those, instead, are called constraints)
  - Loss – the risk becomes a reality and unwanted consequences or losses occur

Risk Categorization – Approach #1

- Project risks
  - They threaten the project plan
  - If they become real, it is likely that the project schedule will slip and that costs will increase
- Technical risks
  - They threaten the quality and timeliness of the software to be produced
  - If they become real, implementation may become difficult or impossible
- Business risks
  - They threaten the viability of the software to be built
  - If they become real, they jeopardize the project or the product

(More on next slide)

Risk Categorization – Approach #1 (continued)

- Sub-categories of Business risks
  - **Market risk** – building an excellent product or system that no one really wants
  - **Strategic risk** – building a product that no longer fits into the overall business strategy for the company
  - **Sales risk** – building a product that the sales force doesn't understand how to sell
  - **Management risk** – losing the support of senior management due to a change in focus or a change in people
  - **Budget risk** – losing budgetary or personnel commitment

Risk Categorization – Approach #2

- Known risks
  - Those risks that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed, and other reliable information sources (e.g., unrealistic delivery date)
- Predictable risks
  - Those risks that are extrapolated from past project experience (e.g., past turnover)
- Unpredictable risks
  - Those risks that can and do occur, but are extremely difficult to identify in advance

– Charette

Reactive vs. Proactive Risk Strategies

- Reactive risk strategies
  - "Don't worry, I'll think of something"
  - The majority of software teams and managers rely on this approach
  - Nothing is done about risks until something goes wrong
    - The team then flies into action in an attempt to correct the problem rapidly (fire fighting)
  - Crisis management is the choice of management techniques
- Proactive risk strategies
  - Steps for risk management are followed (see next slide)
  - Primary objective is to avoid risk and to have a contingency plan in place to handle unavoidable risks in a controlled and effective manner

Reactive Risk Management

- Project team reacts to risks when they occur
- Mitigation—plan for additional resources in anticipation of fire fighting
- Fix on failure—resource are found and applied when the risk strikes
- Crisis management—failure does not respond to applied resources and project is in jeopardy

Proactive Risk Management

- Formal risk analysis is performed
- Organization corrects the root causes of risk
  - TQM concepts and statistical SQA
  - Examining risk sources that lie beyond the bounds of the software
  - Developing the skill to manage change

Steps for Risk Management

1) Identify possible risks; recognize what can go wrong

2) Analyze each risk to estimate the likelihood (probability) that it will occur and the consequences (impact) if it does occur

3) Rank the risks by probability and impact
   - Impact may be negligible, marginal, critical, and catastrophic

4) Develop a contingency plan to manage those risks having high probability and high impact

Risk Management Options

The PMBOK suggests four techniques for dealing with project risks:

- **Risk acceptance:** Allocate contingency time and/or funds that can be used to absorb the impact if one of the risks eventuates.
- **Risk transference:** Assign responsibility for the risks to another party.
- **Risk avoidance:** Find alternative processes that do not include these risks.
- **Risk mitigation:** Find ways to make the risks less likely to eventuate, or to reduce the impact when they do.

Risk Identification

Background

- Risk identification is a systematic attempt to specify threats to the project plan
- By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary
- Generic risks
  - Risks that are a potential threat to every software project
- Product-specific risks
  - Risks that can be identified only by those a with a clear understanding of the technology, the people, and the environment that is specific to the software that is to be built
  - This requires examination of the project plan and the statement of scope
  - "What special characteristics of this product may threaten our project plan?"

Risk Item Checklist

- Used as one way to identify risks
- Focuses on known and predictable risks in specific subcategories (see next slide)
- Can be organized in several ways
  - A list of characteristics relevant to each risk subcategory
  - Questionnaire that leads to an estimate on the impact of each risk
  - A list containing a set of risk component and drivers and their probability of occurrence

Known and Predictable Risk Categories

- **Product size** – risks associated with overall size of the software to be built
- **Business impact** – risks associated with constraints imposed by management or the marketplace
- **Customer characteristics** – risks associated with sophistication of the customer and the developer's ability to communicate with the customer in a timely manner
- **Process definition** – risks associated with the degree to which the software process has been defined and is followed
- **Development environment** – risks associated with availability and quality of the tools to be used to build the project
- **Technology to be built** – risks associated with complexity of the system to be built and the "newness" of the technology in the system
- **Staff size and experience** – risks associated with overall technical and project experience of the software engineers who will do the work

Risk Due to Product Size

Attributes that affect risk:

- **estimated size of the product in LOC or FP?**
- **estimated size of product in number of programs, files, transactions?**
- **percentage deviation in size of product from average for previous products?**
- **size of database created or used by the product?**
- **number of users of the product?**
- **number of projected changes to the requirements for the product? before delivery? after delivery?**
- **amount of reused software?**

Risk Due to Business Impact

Attributes that affect risk:

- **affect of this product on company revenue?**
- **visibility of this product by senior management?**
- **reasonableness of delivery deadline?**
- **number of customers who will use this product**
- **interoperability constraints**
- **sophistication of end users?**
- **amount and quality of product documentation that must be produced and delivered to the customer?**
- **governmental constraints**
- **costs associated with late delivery?**
- **costs associated with a defective product?**

Risks Due to the Customer

Questions that must be answered:

- **Have you worked with the customer in the past?**
- **Does the customer have a solid idea of requirements?**
- **Has the customer agreed to spend time with you?**
- **Is the customer willing to participate in reviews?**
- **Is the customer technically sophisticated?**
- **Is the customer willing to let your people do their job—that is, will the customer resist looking over your shoulder during technically detailed work?**
- **Does the customer understand the software engineering process?**

Risks Due to Process Maturity

Questions that must be answered:

- **Have you established a common process framework?**
- **Is it followed by project teams?**
- **Do you have management support for software engineering**
- **Do you have a proactive approach to SQA?**
- **Do you conduct formal technical reviews?**
- **Are CASE tools used for analysis, design and testing?**
- **Are the tools integrated with one another?**
- **Have document formats been established?**

Technology Risks

Questions that must be answered:

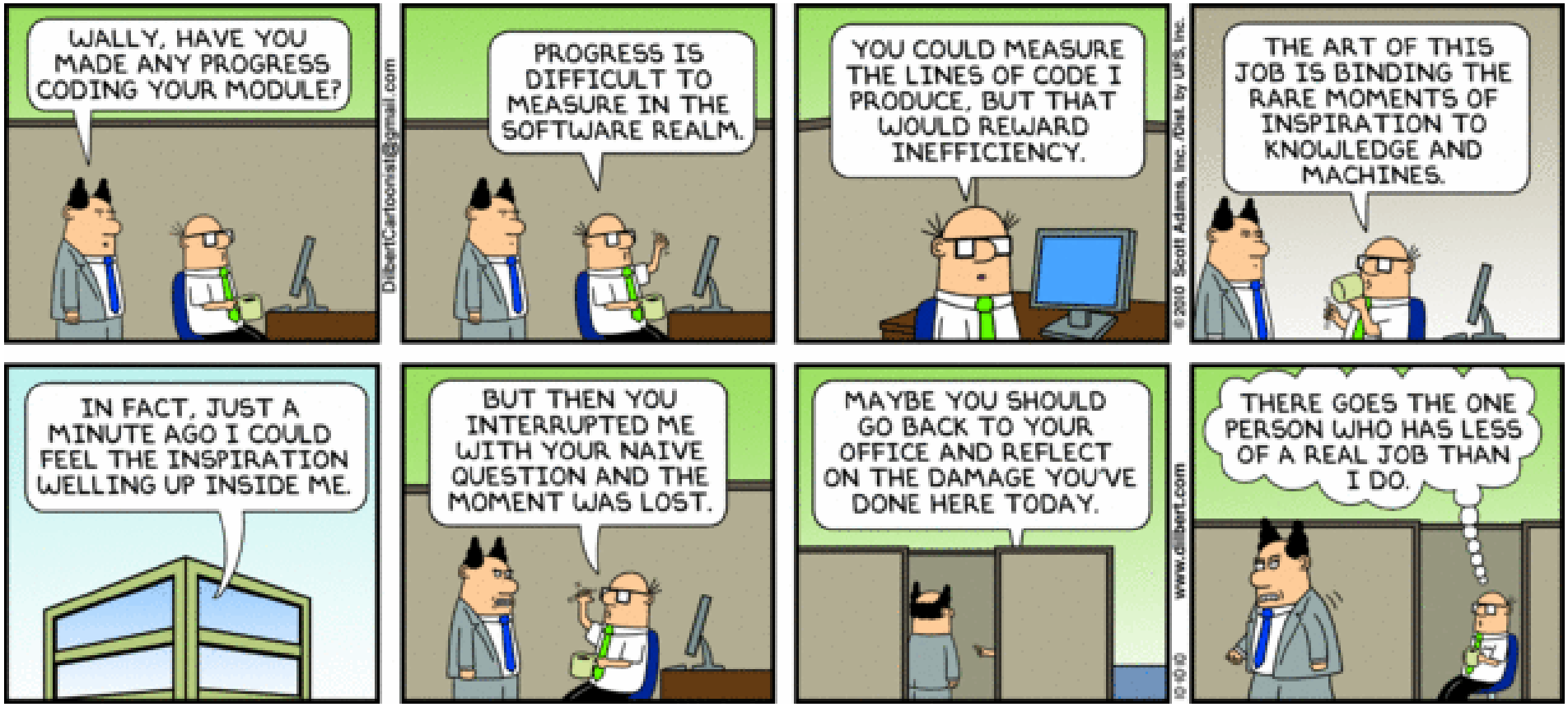
- **Is the technology new to your organization?**
- **Are new algorithms, I/O technology required?**
- **Is new or unproven hardware involved?**
- **Does the application interface with new software?**
- **Is a specialized user interface required?**
- **Is the application radically different?**
- **Are you using new software engineering methods?**
- **Are you using unconventional software development methods, such as formal methods, AI-based approaches, artificial neural networks?**
- **Are there significant performance constraints?**
- **Is there doubt the functionality requested is "do-able?"**

Staff/People Risks

Questions that must be answered:

- **Are the best people available?**
- **Does staff have the right skills?**
- **Are enough people available?**
- **Are staff committed for entire duration?**
- **Will some people work part time?**
- **Do staff have the right expectations?**
- **Have staff received necessary training?**
- **Will turnover among staff be low?**

Software Development is full of risks



Questionnaire on Project Risk

(Questions are ordered by their relative importance to project success)

1) Have top software and customer managers formally committed to support the project?
2) Are end-users enthusiastically committed to the project and the system/product to be built?
3) Are requirements fully understood by the software engineering team and its customers?
4) Have customers been involved fully in the definition of requirements?
5) Do end-users have realistic expectations?
6) Is the project scope stable?

-Keil et al.

(More on next slide)

Questionnaire on Project Risk (continued)

7) Does the software engineering team have the right mix of skills?
8) Are project requirements stable?
9) Does the project team have experience with the technology to be implemented?
10) Is the number of people on the project team adequate to do the job?
11) Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built?

-Keil et al

Risk Components and Drivers

- The project manager identifies the risk drivers that affect the following risk components
  - **Performance risk** - the degree of uncertainty that the product will meet its requirements and be fit for its intended use
  - **Cost risk** - the degree of uncertainty that the project budget will be maintained
  - **Support risk** - the degree of uncertainty that the resultant software will be easy to correct, adapt, and enhance
  - **Schedule risk** - the degree of uncertainty that the project schedule will be maintained and that the product will be delivered on time
- The impact of each risk driver on the risk component is divided into one of four impact levels
  - Negligible, marginal, critical, and catastrophic
- Risk drivers can be assessed as impossible, improbable, probable, and frequent

-U S Air Force

Examples of common project, product, and business risks

Risk	Affects	Description
Staff turnover	Project	Experienced staff will leave the project before it is finished.
Management change	Project	There will be a change of organizational management with different priorities.
Hardware unavailability	Project	Hardware that is essential for the project will not be delivered on schedule.
Requirements change	Project and product	There will be a larger number of changes to the requirements than anticipated.
Specification delays	Project and product	Specifications of essential interfaces are not available on schedule.
Size underestimate	Project and product	The size of the system has been underestimated.
CASE tool underperformance	Product	CASE tools, which support the project, do not perform as anticipated.
Technology change	Business	The underlying technology on which the system is built is superseded by new technology.
Product competition	Business	A competitive product is marketed before the system is completed.

Examples of different risk types

Risk type	Possible risks
Technology	The database used in the system cannot process as many transactions per second as expected. (1) Reusable software components contain defects that mean they cannot be reused as planned. (2)
People	It is impossible to recruit staff with the skills required. (3) Key staff are ill and unavailable at critical times. (4) Required training for staff is not available. (5)
Organizational	The organization is restructured so that different management are responsible for the project. (6) Organizational financial problems force reductions in the project budget. (7)
Tools	The code generated by software code generation tools is inefficient. (8) Software tools cannot work together in an integrated way. (9)
Requirements	Changes to requirements that require major design rework are proposed. (10) Customers fail to understand the impact of requirements changes. (11)
Estimation	The time required to develop the software is underestimated. (12) The rate of defect repair is underestimated. (13) The size of the software is underestimated. (14)

Risk Projection (Estimation)

Background

- Risk projection (or estimation) attempts to rate each risk in two ways
  - The probability that the risk is real
  - The consequence of the problems associated with the risk, should it occur
- The project planner, managers, and technical staff perform four risk projection steps (see next slide)
- The intent of these steps is to consider risks in a manner that leads to prioritization
- By prioritizing risks, the software team can allocate limited resources where they will have the most impact

Risk Projection/Estimation Steps

1) Establish a scale that reflects the perceived likelihood of a risk (e.g., 1-low, 10-high)
2) Delineate the consequences of the risk
3) Estimate the impact of the risk on the project and product
4) Note the overall accuracy of the risk projection so that there will be no misunderstandings

Contents of a Risk Table

- A risk table provides a project manager with a simple technique for risk projection
- It consists of five columns
  - Risk Summary – short description of the risk
  - Risk Category – one of seven risk categories (slide 22)
  - Probability – estimation of risk occurrence based on group input
  - Impact – (1) catastrophic (2) critical (3) marginal (4) negligible
  - RMMM – Pointer to a paragraph in the Risk Mitigation, Monitoring, and Management Plan

Risk Summary	Risk Category	Probability	Impact (1-4)	RMMM

(More on next slide)

Developing a Risk Table

- List all risks in the first column (by way of the help of the risk item checklists)
- Mark the category of each risk
- Estimate the probability of each risk occurring
- Assess the impact of each risk based on an averaging of the four risk components to determine an overall impact value (See next slide)
- Sort the rows by probability and impact in descending order
- Draw a horizontal cutoff line in the table that indicates the risks that will be given further attention

Assessing Risk Impact

- Three factors affect the consequences that are likely if a risk does occur
  - **Its nature** – This indicates the problems that are likely if the risk occurs
  - **Its scope** – This combines the severity of the risk (how serious was it) with its overall distribution (how much was affected)
  - **Its timing** – This considers when and for how long the impact will be felt
- The overall risk exposure formula is RE = P x C
  - P = the probability of occurrence for a risk
  - C = the cost to the project should the risk actually occur

Risk Exposure Example

- **Risk identification.** Only 70 percent of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.
- **Risk probability.** 80% (likely).
- **Risk impact.** 60 reusable software components were planned. If only 70 percent can be used, 18 components would have to be developed from scratch (in addition to other custom software that has been scheduled for development). Since the average component is 100 LOC and local data indicate that the software engineering cost for each LOC is $14.00, the overall cost (impact) to develop the components would be 18 x 100 x 14 = $25,200.
- **Risk exposure.** RE = 0.80 x 25,200 ~ $20,200.

Risk types and examples

Risk	Probability	Effects
It is impossible to recruit staff with the skills required for the project (3).	High	Catastrophic
Organizational financial problems force reductions in the project budget (7).	Low	Catastrophic
The organization is restructured so that different management are responsible for the project (6).	High	Serious
The time required to develop the software is underestimated (12).	High	Serious
Key staff are ill at critical times in the project (4).	Moderate	Serious
Faults in reusable software components have to be repaired before these components are reused. (2).	Moderate	Serious
Changes to requirements that require major design rework are proposed (10).	Moderate	Serious

Risk types and examples

Risk	Probability	Effects
The database used in the system cannot process as many transactions per second as expected (1).	Moderate	Serious
Software tools cannot be integrated (9).	High	Tolerable
The size of the software is underestimated (14).	High	Tolerable
Customers fail to understand the impact of requirements changes (11).	Moderate	Tolerable
Required training for staff is not available (5).	Moderate	Tolerable
The rate of defect repair is underestimated (13).	Moderate	Tolerable
Code generated by code generation tools is inefficient (8).	Moderate	Insignificant

Risk Mitigation, Monitoring, and Management

Background

- An effective strategy for dealing with risk must consider three issues

  (Note: these are not mutually exclusive)

  - Risk mitigation (i.e., avoidance)
  - Risk monitoring
  - Risk management and contingency planning

- Risk mitigation (avoidance) is the primary strategy and is achieved through a plan
  - Example: Risk of high staff turnover (see next slide)

(More on next slide)

Background (continued)

- During risk monitoring, the project manager monitors factors that may provide an indication of whether a risk is becoming more or less likely
- Risk management and contingency planning assume that mitigation efforts have failed and that the risk has become a reality
- RMMM steps incur additional project cost
  - Large projects may have identified 30 – 40 risks
- Risk is not limited to the software project itself
  - Risks can occur after the software has been delivered to the user

(More on next slide)

Background (continued)

- Software safety and hazard analysis
  - These are software quality assurance activities that focus on the identification and assessment of potential hazards that may affect software negatively and cause an entire system to fail
  - If hazards can be identified early in the software process, software design features can be specified that will either eliminate or control potential hazards

Background (continued)

Strategy for Reducing Staff Turnover

- Meet with current staff to determine causes for turnover (e.g., poor working conditions, low pay, competitive job market)
- Mitigate those causes that are under our control before the project starts
- Once the project commences, assume turnover will occur and develop techniques to ensure continuity when people leave
- Organize project teams so that information about each development activity is widely dispersed
- Define documentation standards and establish mechanisms to ensure that documents are developed in a timely manner
- Conduct peer reviews of all work (so that more than one person is "up to speed")
- Assign a backup staff member for every critical technologist

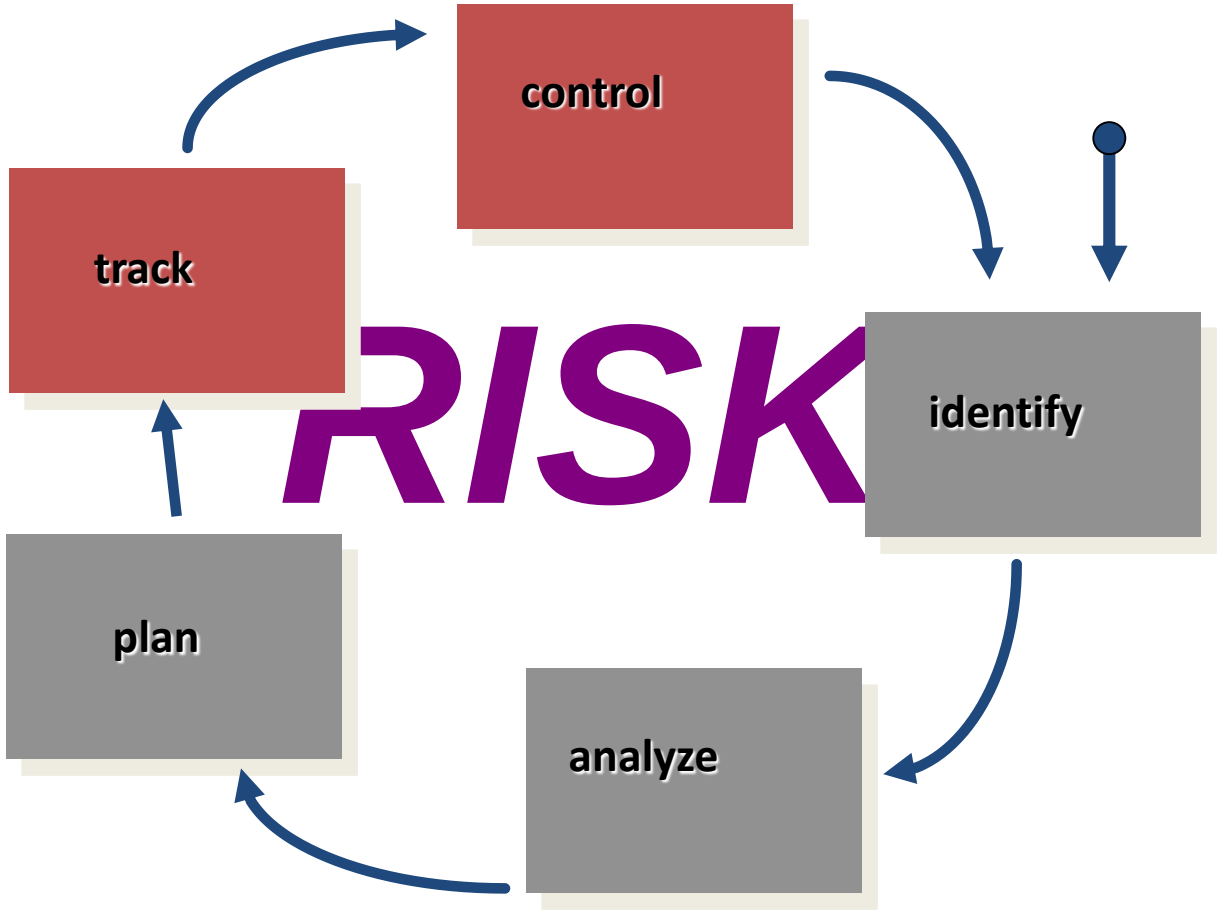
Risk Mitigation, Monitoring, and Management

- mitigation—how can we avoid the risk?
- monitoring—what factors can we track that will enable us to determine if the risk is becoming more or less likely?
- management—what contingency plans do we have if the risk becomes a reality?

The RMMM Plan

- The RMMM plan may be a part of the software development plan or may be a separate document
- Once RMMM has been documented and the project has begun, the risk mitigation, and monitoring steps begin
  - Risk mitigation is a problem avoidance activity
  - Risk monitoring is a project tracking activity
- Risk monitoring has three objectives
  - To assess whether predicted risks do, in fact, occur
  - To ensure that risk aversion steps defined for the risk are being properly applied
  - To collect information that can be used for future risk analysis
- The findings from risk monitoring may allow the project manager to ascertain what risks caused which problems throughout the project

Risk Management Paradigm



Seven Principles of Risk Management

- **Maintain a global perspective**
  - View software risks within the context of a system and the business problem that is is intended to solve
- **Take a forward-looking view**
  - Think about risks that may arise in the future; establish contingency plans
- **Encourage open communication**
  - Encourage all stakeholders and users to point out risks at any time
- **Integrate risk management**
  - Integrate the consideration of risk into the software process
- **Emphasize a continuous process of risk management**
  - Modify identified risks as more becomes known and add new risks as better insight is achieved
- **Develop a shared product vision**
  - A shared vision by all stakeholders facilitates better risk identification and assessment
- **Encourage teamwork when managing risk**
  - Pool the skills and experience of all stakeholders when conducting risk management activities

– SEI (Software Engineering Institute)

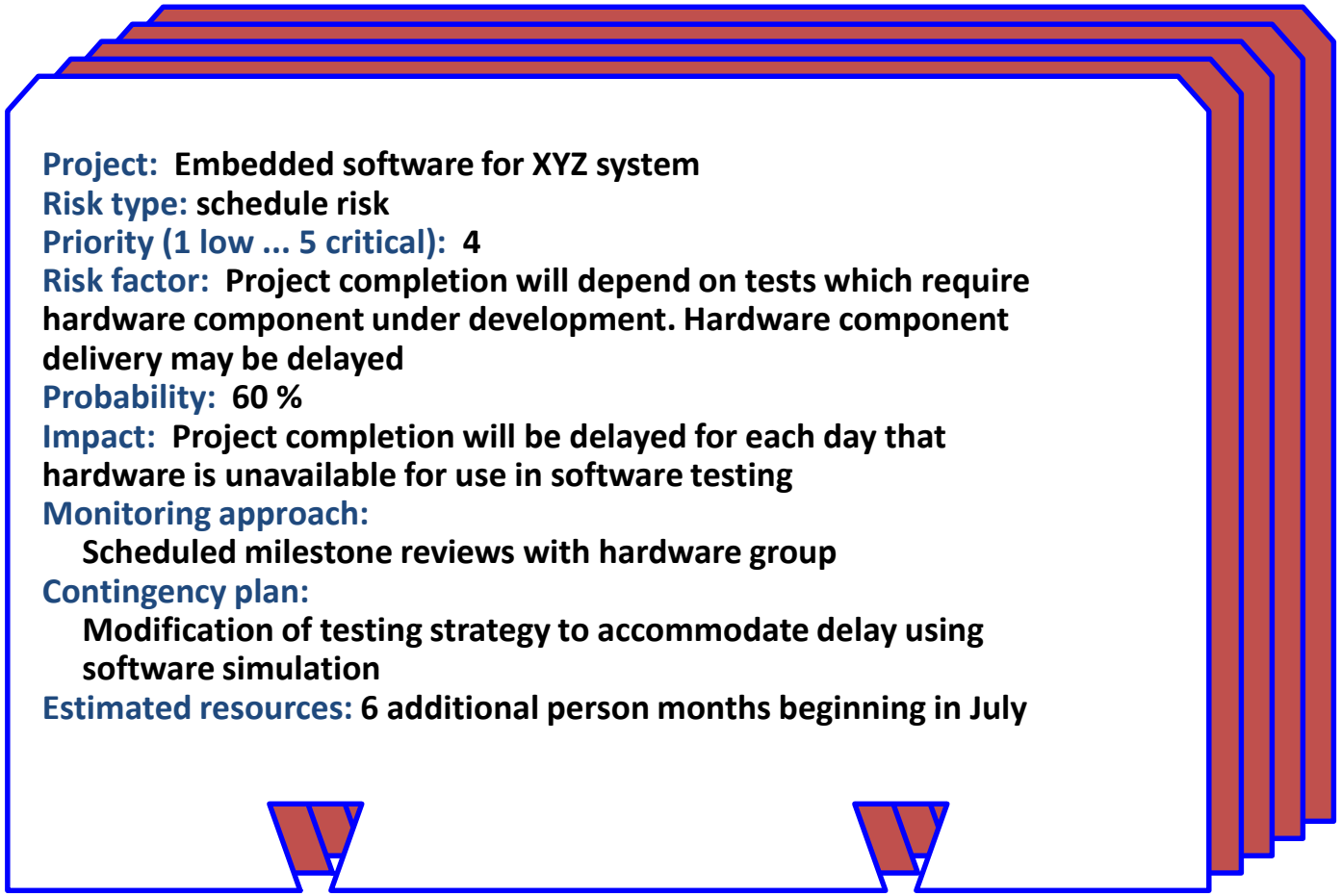
Strategies to help manage risk

Risk	Strategy
Organizational financial problems	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business and presenting reasons why cuts to the project budget would not be cost-effective.
Recruitment problems	Alert customer to potential difficulties and the possibility of delays; investigate buying-in components.
Staff illness	Reorganize team so that there is more overlap of work and people therefore understand each other's jobs.
Defective components	Replace potentially defective components with bought-in components of known reliability.
Requirements changes	Derive traceability information to assess requirements change impact; maximize information hiding in the design.

Strategies to help manage risk

Risk	Strategy
Organizational restructuring	Prepare a briefing document for senior management showing how the project is making a very important contribution to the goals of the business.
Database performance	Investigate the possibility of buying a higher-performance database.
Underestimated development time	Investigate buying-in components; investigate use of a program generator.

Recording Risk Information



Risk Information Sheet (RIS), proposed by Williams, Walker, Dorofee, is a complete documentation for each risk. RIS is preferred by some practitioners over RMMM.

Summary of Risk Management

- Risks are potential problems that might affect the successful completion of a software project.
- Whenever much is riding on a software project, common sense dictates risk analysis
  - Yet, most project managers do it informally and superficially, if at all
- Risks involve uncertainty and potential losses. Risk analysis and management is intended to help a software team understand and manage uncertainty during the development process.
- The time spent in risk management results in
  - Less upheaval during the project
  - A greater ability to track and control a project
  - The confidence that comes with planning for problems before they occur
- Risk management can absorb a significant amount of the project planning effort…but the effort is worth it
- The work product is called a Risk Mitigation, Monitoring, and Management Plan (RMMM) or a set of Risk Information Sheets (RIS).