RISK ANALYSIS AND MANAGEMENT

LESSON 5 – CCS 6

NOTES PREPARED BY ASST. PROF. MELODY ANGELIQUE C. RIVERA
FACULTY, COLLEGE OF COMPUTER STUDIES, SILLIMAN UNIVERSITY

No man is worth his salt who is not ready at all times to risk his well-being, to risk his body, to risk his life, in a great cause.

~ Theodore Roosevelt

RISK

- ***The chance of a negative event***
- A chance that something unexpected will happen

- It is the combination of **threats** and **vulnerabilities**:

  Risk = Threats x Vulnerabilities

effect of uncertainty on objectives
~ Definition of Risk, ISO 31000

- This definition leaves the possibility open that risks can produce positive outcomes. This is no doubt based on the philosophy that problems represent opportunities

THREAT

- ***Something bad that might happen***

- From a security perspective the first threat that pops to mind is a **security attack**
- A threat can range from innocent mistakes made by employees to natural disasters

THREAT (CONT.)

- **Categories of Threats**
  - *Acts of human error or failure*
    - accidents, employee mistakes
  - *Compromises to intellectual property*
    - Piracy, copyright infringement
  - *Deliberate acts of espionage or trespass*
    - Unauthorized access and/or data collection
  - *Deliberate acts of information extortion*
    - Blackmail of information disclosure
  - *Deliberate acts of sabotage or vandalism*
    - Destruction of systems or information
  - *Deliberate acts of theft*
    - Illegal confiscation of equipment or information

VULNERABILITY

Vulnerability is the birthplace of innovation, creativity and change
~ Brene Brown

- **Common definition:**

  "weakness" or an "inability to cope“

  - these definitions are completely wrong from a security and risk management perspective

- **Better definition:**

  “exposure”

VULNERABILITY (CONT.)

- For example:

Connecting a system to the Internet can represent a vulnerability

- It exposes a system to a DDoS (Distributed Denial of Service) attack
- But connecting a system to customers via the Internet isn't likely to be considered a weakness from a business perspective

IS RISK GOOD OR BAD?

- IT security professionals tend to think of risk as bad
  - They might define it as **the chance a threat will exploit vulnerabilities** or the "chance that something bad will happen“
- Risk management professionals treat risks as potentially positive
  - From a business perspective risk can be considered a good thing

RISK MANAGEMENT

- *the process of identifying, analyzing and responding to risk factors throughout the life of a project and in the best interests of its objectives*
  - It is the process of identifying and controlling potential losses
  - It is a standard business practice that is applied to investments, programs, projects, operations and commercial agreements
- **Proper risk management** implies control of possible future events
- It is proactive rather than reactive
- It will reduce not only the likelihood of an event occurring, but also the magnitude of its impact

RISK MANAGEMENT (CONT.)

Reactive Risk Management

- Project team reacts to risks when they occur
- Mitigation – plan for additional resources in anticipation of fire fighting
- Fix on failure – resources 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 the risk
  - Examining risk sources that lie beyond the bounds of the software
  - Developing the skill to manage change

RISK MANAGEMENT (CONT.)

Seven (7) steps of Risk Management

RISK MANAGEMENT (CONT.)

1. **Identification**
   - Giving all stakeholders an opportunity to identify risks
   - This can increase acceptance of a program or project as everyone is given a chance to document all the things that might go wrong
   - The diverse perspectives of stakeholders helps to develop a comprehensive list of risks
   - It is also possible to use databases of issues with that occurred with similar business processes, programs or projects in your industry
   - Knowledge sources such as l*essons-learned* and the *risk registers of historical projects* can also be used

RISK MANAGEMENT (CONT.)

2. **Analysis**
   - Developing context information for each risk such as moment of risk.

3. **Probability & Impact**
   - Assessing the probability and impact of each risk
   - These can be single estimates such as high, medium and low
   - Alternatively, they can be a probability distribution that model multiple costs and associated probabilities for each risk

RISK MANAGEMENT (CONT.)

4. **Risk Treatment**
   - Planning a treatment for each risk such as acceptance, mitigation, transfer, sharing or avoidance
   - Risks that are both low impact and low probability typically aren't treated

5. **Residual Risk**
   - Assess residual risk including secondary risks that result from risk mitigation, transfer or sharing

RISK MANAGEMENT (CONT.)

6. **Risk Control**
   - Implement identified controls for risk mitigation, sharing, avoidance and transfer

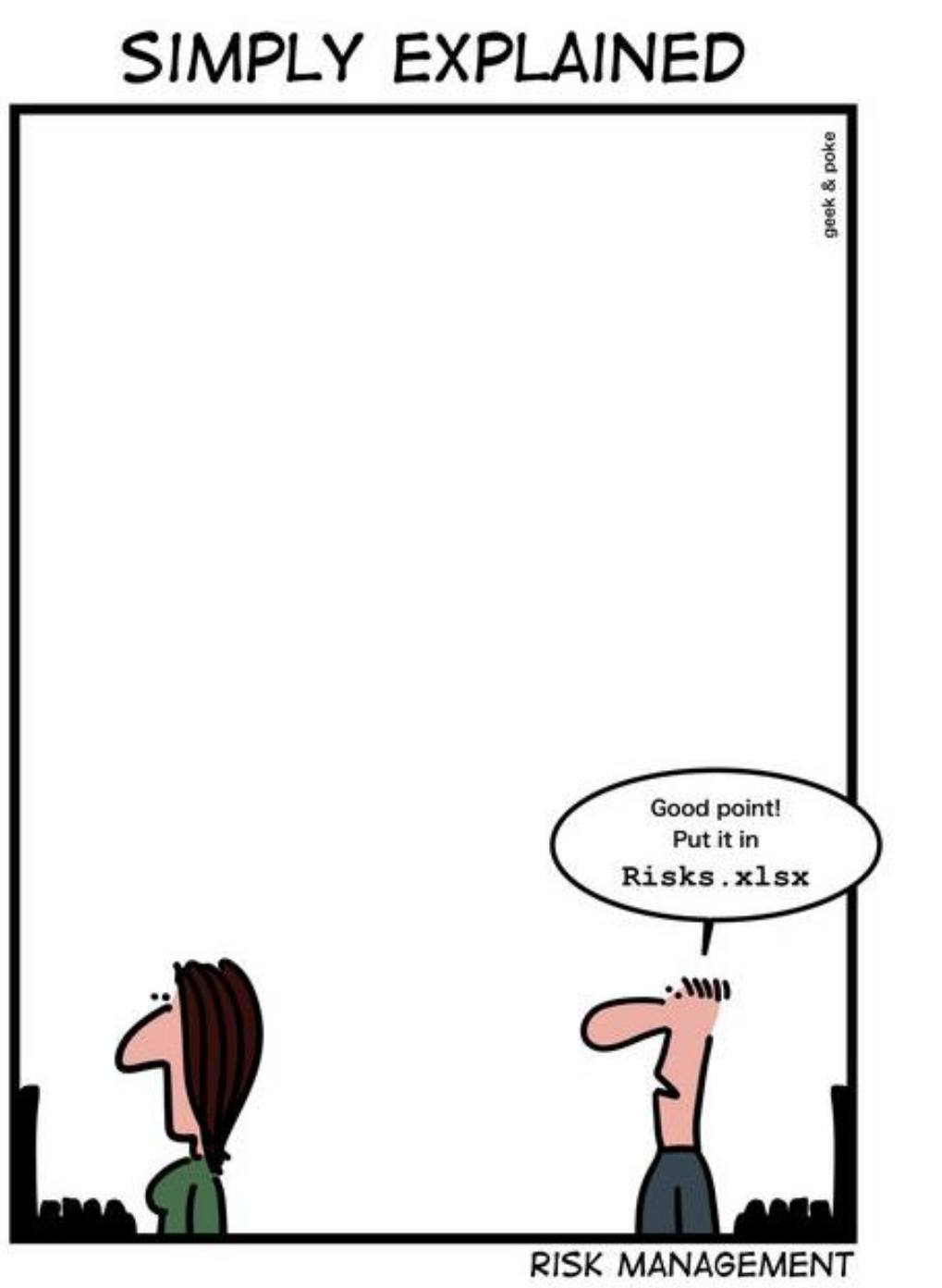
7. **Monitor & Review**
   - Continuously identify new risks as things progress, monitor implementation of controls and communicate risk to stakeholders

NEGATIVE RISK RESPONSE STRATEGIES
(PROJECT CONTROLS EXPO, 2011)

Response	Strategy	Examples
Avoid	**Risk avoidance** is a strategy where the project team takes action to remove the threat of the risk or protect from the impact	• Extending the schedule • Reducing/removing the scope • Changing the execution strategy
Transfer	**Risk transference** involves shifting or transferring the risk threat and impact to a 3rd party. This does not eliminate the risk, rather transfers the responsibility and ownership.	• Purchasing insurance • Performance bonds • Warranties • Contract issuance (lump sum)
Mitigate	**Risk mitigation** is the strategy whereby the project team takes action to reduce the probability of the risk occurring. This does not remove the risk or the potential impact, but rather reduces the likelihood of it becoming real.	• Increasing testing • Changing suppliers to a more stable one • Reducing process complexity
Accept	**Risk acceptance** means the team acknowledges the risk and its potential impact, but decides not to take any preemptive action to prevent it. It is dealt with only if it occurs.	• Contingency reserve budgets • Management schedule float • Event contingency

POSITIVE RISK RESPONSE STRATEGIES
(PROJECT CONTROLS EXPO, 2014)

Response	Strategy	Examples
Exploit	**Risk exploitation** is used when the team wants to ensure that the risk opportunity is realized and any uncertainty is removed	• Developing a project team with the most talented resources • Upgrading technology to reduce cost and project duration
Enhance	**Risk enhancement** is used to increase the probability or impact of a positive risk occurring. The strategy requires identifying and maximizing the key drivers.	• Fast tracking an activity or overall schedule by adding additional resources or shifts to achieve an incentive
Share	**Sharing a positive risk** involves allocating some or all of the ownership of the risk and opportunity to a 3rd party who has the best chance of meeting the objective.	• Risk sharing partnerships • Subcontracting a firm with technical expertise and adding incentive targets
Accept	**Accepting a positive risk** means you intend to take advantage of the opportunity if it becomes available, but not actively pursuing it.	• Meeting incentive dates naturally • Discounted equipment or material costs


SIMPLY EXPLAINED
geek & poke
Good point!
Put it in
Risks.xlsx
RISK MANAGEMENT

22 TYPES OF PROJECT RISK

PROJECT RISK MANAGEMENT

- A project management activity that involves identifying, assessing, measuring, documenting, communicating, avoiding, mitigating, transferring, accepting, controlling and managing risk

- The process of identifying risks is intuitive for experienced project managers

TYPES OF RISK
(RISK CATEGORIES)

- **Executive Support**
  - Wavering, inconsistent or weak executive commitment is often a project's biggest risk
  - This can be difficult (but not impossible) to document
  - Ask for specific commitments
  - Where you are denied you can document it as a risk
  - **Executives fail to support project**
    Executives become disengaged with project
    Conflict between executive stakeholders disrupts project
    Executive turnover disrupts project

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Scope**
  - The quality of your estimates, dependencies and scope management. If an estimate is just a guess, that's a risk. Be sensitive to the comfort level of estimates. If your team is unsure about a particular estimate, you can document this as a risk
  - **Scope is ill defined**
    Scope creep inflates scope (Uncontrolled changes and continuous growth of scope)
    Gold plating inflates scope (The project team add their own product features that aren't in requirements or change requests)
    Estimates are inaccurate
    Dependencies are inaccurate
    Activities are missing from scope

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Cost Management**
  - Inaccurate cost estimates and forecasts or when costs are incurred in foreign currencies exchange rates can have a dramatic impact
  - **Cost forecasts are inaccurate**
    Exchange rate variability
    .

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Change Management**
  - A continuous flow of complex change requests can escalate the complexity of your project and throw it off course
  - Change requests may lead to a perception that a project has failed because they continually add budget and time to the project
  - If requirements are missing items that are expected to come later, that is a risk
  - **Change management overload**
    Stakeholder conflict over proposed changes
    Perceptions that a project failed because of changes
    Lack of a change management system
    Lack of a change management process
    Lack of a change control board
    Inaccurate change priorities
    Low quality of change requests
    Change request conflicts with requirements

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Stakeholders**
  - Stakeholders with a negative attitude towards a project may intentionally throw up roadblocks every step of the way
  - If you anticipate conflict or a lack of cooperation between stakeholders, document it as a risk
  - **Stakeholders become disengaged**
    Stakeholders have inaccurate expectations
    Stakeholder turnover
    Stakeholders fail to support project
    Stakeholder conflict
    Process inputs are low quality

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Resources and Team**
  - Resource issues such as turnover and learning curves are common project risks
  - *For example:* your key experts will leave, if your team are inexperienced or need to acquire new skills
  - **Resource shortfalls**
    Learning curves lead to delays and cost overrun
    Training isn't available
    Training is inadequate
    Resources are inexperienced
    Resource performance issues
    Team members with negative attitudes towards the project
    Resource turnover
    Low team motivation
    Lack of commitment from functional managers

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Architecture**
  - Architectural issues such as inflexibility to support change requests or is impossible to implement
  - **Architecture fails to pass governance processes**
    Architecture lacks flexibility
    Architecture is not fit for purpose
    Architecture is infeasible

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Design**
  - The feasibility and flexibility of architecture and design are key to your project's success
  - Low quality design is a risk
  - You might want to highlight the design of complex or experimental components as separate risks
  - **Design is infeasible**
    Design lacks flexibility
    Design is not fit for purpose
    Design fails peer review

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Technical**
  - The risk that components of your technology stack will be low quality
  - There are dozens of quality factors for technical components (e.g. stability, availability, scalability, usability, security, extensibility)
  - It is a good idea to identify specific risks in components
  - *For example:* the risk that a component will have a security flaw
  - **Technology components aren't fit for purpose**
    Technology components aren't scalable
    Technology components aren't interoperable
    Technology components aren't compliant with standards and best practices

TYPES OF RISK (RISK CATEGORIES) (CONT.)

Technology components have security vulnerabilities
Technology components are over-engineered
Technology components lack stability
Technology components aren't extensible
Technology components aren't reliable
Information security incidents
System outages
Legacy components lack documentation
Legacy components are out of support
Components or products aren't maintainable
Components or products can't be operationalized
Project management tool problems & issues

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Integration**
  - Whatever you are delivering needs to integrate with the processes, systems, organizations, culture and knowledge of the environment
  - Integration risks are common
  - If you need to integrate your project into a business process there is a risk that the process will be disrupted
  - **Delays to required infrastructure**
    Failure to integrate with business processes
    Failure to integrate with systems
    Integration testing environments aren't available
    Failure to integration with the organization
    Failure to integrate components
    Project disrupts operations
    Project disrupts sales
    Project disrupts compliance

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Communication**
  - Invalid stakeholder expectations are a fundamental project risk. If the stakeholders think you're building an orange but you're building an apple — your project will fail
  - *For example:* if stakeholders become disengaged (e.g. ignore project communications)
  - **Project team misunderstand requirements**
    Communication overhead
    Under communication
    Users have inaccurate expectations
    Impacted individuals aren't kept informed

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Requirements**
  - Garbage in, garbage out. If requirements aren't feasible or are detached from business realities, your project may fail
  - Look at the feasibility, quality and completeness of requirements to identify risk
  - Look at whether requirements are possible to integrate with organizations, processes and systems
  - **Requirements fail to align with strategy**
    Requirements fail to align with business processes
    Requirements fail to align with systems
    Requirements have compliance issues
    Requirements are ambiguous
    Requirements are low quality
    Requirements are incomplete

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Decision Quality and Issue Resolution**
  - Slow, low quality or ambiguous decisions are common risks
  - **Decision delays impact project**
    Decisions are ambiguous
    Decisions are low quality
    Decisions are incomplete

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Feasibility**
  - Risk identification is a critical time to consider the feasibility of the project
  - Ask the key members of your team to do their own sanity checks
  - List any doubts about feasibility as risks

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Procurement**
  - The procurement process is ripe with risks
  - *For example:* there is a risk that you will not find an acceptable proposal to a Request for Proposal (RFP)
  - There is also a risk that your vendors will not deliver to the terms of their contracts
  - **No response to RFP**
    Low quality responses to RFP
    Failure to negotiation a reasonable price for contracts
    Unacceptable contract terms
    Conflict with vendor leads to project issues
    Conflict between vendors leads to project issues
    Vendors start late
    Vendor components fail to meet requirements
    Vendor components are low quality
    Infrastructure is low quality
    Service quality is low
    Vendor components introduce third party liability
    Loss of intellectual property

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Quality**
  - Quality and risk management are intertwined
  - Expect to have defects in your project
  - There is a risk that quality will not meet basic levels
  - Significant rework may trigger project failure
  - Identify quality related risks for process inputs and outputs
  - Identify quality risks for infrastructure, work packages, components and products

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Authority**
  - Project teams often lack authority to complete project work
  - In many cases, teams are expected to influence to achieve project objectives
  - This reflects business realities
  - For example, your project may cross organizational boundaries
  - **Project team lack authority to complete work**
    Authority is unclear

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Approvals & Red Tape**
  - If you anticipate that red tape (e.g. financial approvals) will slow down your project — add this as a risk
  - **Delays to stakeholder approvals impact the project**
    Delays to financial approvals impact the project
    Delays to procurement processes impact the project
    Delays to recruiting processes impact the project
    Delays to training impact the project

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Organizational**
  - Organizational change (e.g. restructuring, mergers, acquisitions) will throw your project off track
  - Think about the minimum stability that your products require to launch
  - List potential organizational changes as risks
  - **The project fails to match the organization's culture**
    An organizational restructuring throws the project into chaos
    A merger or acquisition disrupts the project

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **External**
  - External forces such as laws, regulations and markets
  - If your project touches compliance-sensitive processes, regulatory change is a risk
  - **Legal & regulatory change impacts project**
    Force Majeure (e.g. act of nature) impacts project
    Market forces impact project
    Technical change impacts project
    Business change impacts project

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Project Management**
  - If your organization asks you to streamline your project management methodology (drop processes and documentation) you can document this as a risk
  - **Failure to follow methodology**
    Lack of management or control
    Errors in key project management processes

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Secondary Risks**
  - Secondary risks are often overlooked aspect of risk
  - They are the result of risk mitigation and transfers
  - For example, you transfer a risk to a vendor with a fixed price contract
  - **Counterparty risk**

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **User Acceptance**
  - There is always a chance that users will reject your product
  - You can build a product that matches requirements (on time and to budget)
  - If users reject the product, the project will be considered a **failure**.
  - **Users reject the prototype**
    User interface doesn't allow users to complete tasks
    User interface is low quality
    User interface isn't accessible
    Project reduces business productivity
    Project reduces innovation
    Product disrupts business metrics (measurements of objectives)
    Users reject the product

TYPES OF RISK (RISK CATEGORIES) (CONT.)

- **Commercial**
  - If you're building a commercial product for market (new product development), there's always a chance the product will be a commercial failure
  - This should be documented as a project risk
  - **Product doesn't sell**
    Product incurs legal liability
    Product negatively affects brand
    Product negatively affects reputation

RISK MANAGEMENT PLAN FORMAT

- Risk identification (based on discussions with key stakeholders)
- Risk categorization
- Risk probability and impact assessment
- Risk prioritization
- Risk response planning
- Risk management strategy
- Risk monitoring
- Risk control
- Assumptions with significant impact on project risk
- Roles and responsibilities unique to the risk function

END OF PRESENTATION