Bringing British
Education to You
www.nccedu.com

Professional Issues in IT

Topic 7:
IT Risk Management

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.2

Scope and Coverage

This topic will cover:

- What is risk?
- Risk management in IT projects
  - Stages of risk management
    - Risk planning
    - Risk identification
    - Risk analysis
    - Risk response
    - Risk action

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.3

Learning Outcomes

By the end of this topic, students will be able to:

- Define risk
- Name stages of risk management
- Describe each stage's purpose
- Discuss the difference between proactive and reactive approaches to IT risk management
- Generate risk identification lists

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.4

Risk Management

- To understand risk management, first you must understand risk!

- What does risk mean to you?
  - Personal risk?
  - Environmental risk?
  - Work related risk?

- Can you define risk?

NCC Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.5

What is Risk?

- Risk is:

  "a situation involving exposure to danger"

  Oxford English Dictionary

- Examples of possible 'risk'
  - Is it safe to walk home in the dark?
  - Is it safe to use a mobile phone?
  - Is it safe to skydive?

NCC Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.6

Risk in IT Projects

- All projects involve risk

- Eliminating risk
  - Not practical
  - Not desirable

- Risk must be acknowledged
  - Not a sign of weakness
  - Actually a strength!

- Can you identify any possible IT project risks?

NCC Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.7

Possible IT Project Risks

- Not taking risk seriously

- Inexperienced project team

- Lack of specialist software

- Management lack understanding

- No previous experience of project type

- Client mentality

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.8

Potential Consequences - 1

- There are many potential consequences of not taking risk and its impact seriously
  - Strategic
  - Operational

Strategic
  - Abandonment of project
  - Over-run/over-spend
  - Loss of client confidence
  - Loss of future business

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.9

Potential Consequences - 2

Operational

  - Constant change & need for re-planning
  - Inefficiency
  - Over-run/ over-spend
  - Low staff morale/ high staff turnover
  - Unacceptable work conditions

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.10

Risk Tolerance - 1

- Every organisation/project manager has a *risk tolerance*
  - How much risk are they willing to take?
  - How much risk are you willing to take?
- Categories of risk tolerance:
  - Risk averse
  - Risk neutral
  - Risk seeking

V1.0 · © NCC Education Limited

IT Risk Management Lecture 7 - 7.11

Risk Tolerance - 2

- Risk Averse
  - An organisation/project manager that is risk averse is:
    - Unwilling to take risk
    - Uncomfortable taking risks
    - Has greater work satisfaction 'playing safe'
- Risk Neutral
  - An organisation/project manager that is risk neutral is:
    - Balanced in risk vs. payoff

V1.0 · © NCC Education Limited

IT Risk Management Lecture 7 - 7.12

Risk Tolerance (3)

- Risk Seeking
  - An organisation/project manager that is risk seeking has:
    - High risk tolerance
    - Greater satisfaction in risk for payoff
- Consider your own personality. If you were a project manager, how much risk tolerance would you have?

V1.0 · © NCC Education Limited

IT Risk Management Lecture 7 - 7.13

What is Risk Management?

• Risk Management is:

"to avoid or minimize the adverse effects of unforeseen events"

(Hughes & Cotterell 1999:135)

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.14

Risk Management - 1

• Increasingly important
  - Project complexity levels are increasing
  - Projects are becoming increasingly interdependent
  - Projects are varying vastly in skill & technology

• Should always be pro-active, not re-active

• Should always be part of the 'project office'
  - Its scope should be wider than the 'project team'

• Should be a standard procedure for all projects

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.15

Risk Management - 2

• Should be applied to all projects
• There are many variations on how to approach risk management
  - All essentially the same – variations on a theme!
• Include a risk database
  - Feed forward information
  - Compile actual vs. forecasted information
• Link to quality procedures
• Link to monitoring procedures

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.16

Risk Management Process - 1

- Cadle & Yeates Risk Management Process:
  - One approach to mapping the process of risk management
  - Chosen for its simple approach to essential risk management
- Other approaches include:
  - Boehm Software Risk Engineering Tasks
    - Boehm separates risk management & risk analysis under the heading 'risk engineering'
  - Dalcher & Brodie Risk Management Process

NCC Bringing British Education to You www.nccedu.com
V1.0   © NCC Education Limited
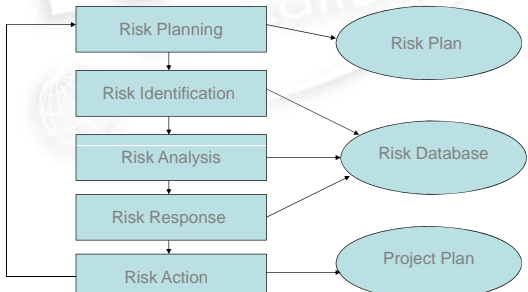
IT Risk Management Lecture 7 - 7.17

Risk Management Process - 2

Risk Planning → Risk Plan

Risk Identification

Risk Analysis → Risk Database

Risk Response

Risk Action → Project Plan

NCC Bringing British Education to You www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.18

Risk Planning

- Also known as risk policy
- Responsibility for risk planning usually dependant on Project size
  - Small projects = Project Manager
  - Large projects = Risk Manager
- Why?
  - To make the decision on how a project is going to approach risk before it starts
    - Pro-active/Decisive
- To finalise which risk management approach is being taken

NCC Bringing British Education to You www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.19

Risk Plan Content

- Statement of scope
- Description of risk management process
  - Method of assessment
  - When/how monitoring will take place
- Assumption list
- Roles & responsibilities
  - Who is responsible for risk management process
  - Structure of reporting
- Description of risk management deliverables

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.20

Risk Identification

- Not as easy as it sounds!
  - Potentially hundreds of risks!
- Stage where all risks are listed
- Virtually impossible to ensure full risk identification
  - Secondary risks & more
- Essential that risk manager/project manager is honest regarding risks
- Must highlight all risks regardless of any repercussions

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.21

Identifying Risks

- How to Identify Risks:
  - Consult all available information/data
    - Customer contracts
    - Previous project plans
    - Known users
    - Project acceptance criteria
    - Functionality requirements
    - Technical requirements
    - Project team skills
    - Development environment
    - Tools, methods, hardware & software availability

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.22

Identifying Risk

- To be a risk
  - Must be defined precisely
    - If necessary, an identified risk must be broken down further into yet more specific risks
  - Must be capable of measurement
    - Must be able to compare risks to prioritise resources/time
  - Must have a measurable impact
    - Must be able to measure the impact of the risk on the project

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.23

Risk List Example

- Lack of experienced project staff
  - Employing contract staff (secondary associated risk)
- Inappropriate budget
- Unrealistic client expectations
- Reliance on 'off the shelf' software

  - Note: this list contains primary risks and an example of a secondary risk

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.24

Risk Analysis/Assessment - 1

- Why risk analysis exists
  - To focus attention where it is needed
    - On risks with higher occurrence probability
    - On risks with higher impact effect

- There are a variety of formal assessments available
  - Decision on which assessment(s) to be used is stated in risk plan

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.25

Risk Analysis/Assessment - 2

- Whichever approach is taken to analysing risk, the following factors must be considered:
  - Quantitative in its approach
  - Vulnerable to opinion and/or skill level of analyst

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.26

Risk Analysis

- One approach to analysing the risks identified in the risk identification step is *Risk Assessment Mapping*
  - Chosen for its simple approach to risk analysis
  - Enables you to see clearly where your issues may lie
  - Enables risks to be assessed according to the potential impact and chance of occurrence

V1.0   © NCC Education Limited
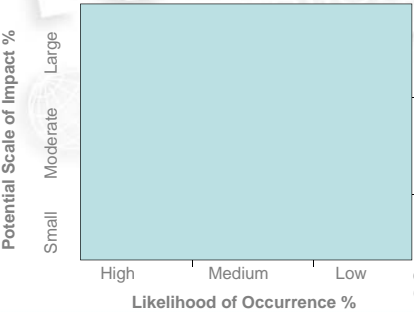
IT Risk Management Lecture 7 - 7.27

Risk Assessment Map - 1

Potential Scale of Impact %

Large

Moderate

Small

High   Medium   Low   Cadle & Yeates (2001)

Likelihood of Occurrence %

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.28

Risk Assessment Map - 2

- Likelihood of risk occurrence as a probability
  - High   >30%
  - Medium   10%-30%
  - Low   <10%

- Probable scale of impact on project as a probability
  - Large   >30% or abandonment
  - Moderate   10%-30%
  - Small   <10%

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.29

Risk Assessment Map Example - 1

- Before plotting risks on the map, each risk must be assessed
  - Estimation process should consider:
    - Risk manager/project manager expertise
    - Knowledge of current situation
      - Existing software
      - Budget
  - Can you name any other factors which could influence the estimation process?

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.30

Risk Assessment Map Example - 2

Risk	Occurrence %	Impact %
1. Availability of software required	5%	90%
2. Inexperienced project team	40%	90%
3. Project budget unrealistic	30%	70%
4. Customer initial requirements unrealistic	10%	20%

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.31

Risk Assessment Map Example - 3

- Having estimated each risk's impact and occurrence, the next step is to plot each risk on to the map

- Note: how accurately the risks are plotted on to the map is again down to the manager
  - If not accurately plotted, does the process hold any value?
  - Without the initial table containing the percentage estimates, is the map of use?

V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.32

Risk Assessment Map Example - 4

Potential Scale of Impact	Large	2	3	1
	Moderate			
				4
	Small			
		High	Medium	Low

Likelihood of Occurrence

V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.33

Risk Assessment Map Example - 5

- Remember the % estimates in the example are based on the manager's prior knowledge, therefore you may assess the situation very differently

- Example % based on:
  - Knowing the customer
  - Having already been allocated a project team
    - Contains one new employee with unproven skill base
  - Prior experience of similar projects

V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.34

Downfalls of the Risk Assessment Map

- Does not take into account urgency
  - How quickly a particular risk is likely to occur
  - How quickly action must be taken
    - To avoid risk occurring
    - To resolve situation if risk occurs

NCC Bringing British Education to You
www.nccedu.com
V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.35

Risk Response

- After identifying and analysing risk, the next stage is to plan how to respond should a risk become live

- Four basic strategies
  - Prevention
  - Reduction
  - Acceptance
  - Transference

NCC Bringing British Education to You
www.nccedu.com
V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.36

Prevention

- To eliminate the risk from occurring
  - Very difficult

- Risk prevention can only occur if risk management is very pro-active

- Example of risk prevention:
  - Revisiting original client requirements and negotiating out unrealistic goals

NCC Bringing British Education to You
www.nccedu.com
V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.37

Reduction

- Risk reduction can be achieved through pro-active planning
  - Risks that through analysis are recognised as being able to be reduced, either in impact or chance of occurrence

- Examples of risk reduction:
  - Scheduling in advance availability of specialised programmers for specific code development
  - Using 'off the shelf' proven software where possible rather than creating bespoke for the sake of it

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.38

Acceptance

- Risk acceptance is exactly that:
  - Acceptance of any consequences arising from an occurring risk, no matter how large or small the impact
  - No action taken
  - Usually restricted to smaller, lower impact risks

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.39

Transference

- Risk transference or transfer
  - Could be described as 'passing the buck' – passing on the responsibility/blame to someone else

- Involves handing over to a third party the consequences and management of a risk
  - E.g. An insurance policy with another company against software failure - if software fails the other company is required to find a solution!

NCC Bringing British Education to You
www.nccedu.com
V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.40

Risk Response

- During risk response, the identification of additional secondary risks will almost certainly occur

    - Requiring the update of the risk Identification list
    - Requiring the analysis of each newly identified risk
    - Requiring a risk response to be generated for each new risk

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.41

Risk Database - 1

- The result of risk identification, risk analysis and risk response is the generation of a risk database

- A central location for all risk information
    - Note: Database does not necessarily mean a computerised database

- Variety of formats
    - Database
    - Paper based
    - Word processing file

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.42

Risk Database - 2

- Format often dependant on
    - Size of organisation
    - Project scale

- The risk manager/ project manager's responsibility to ensure database is up-to-date

- The whole project team are responsible for updating the database throughout the project lifetime

V1.0

© NCC Education Limited

IT Risk Management Lecture 7 - 7.43

Risk Database Content - 1

- Risk ID number
  - Unique identifying number
- Risk ranking number
  - how highly ranked is the risk e.g. R1, R2 etc
- Name
  - Clear, concise name for each risk
- Description
  - Clear and concise, avoiding exact repetition
- Triggers
  - Any identifiable event or occurrence that will trigger risk

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.44

Risk Database Content - 2

- Risk status
  - Live or inactive

- Potential impact(s)
  - In quantifiable terms
    - time/cost/quality
  - Multiple impacts?
  - Record description
    - Including likelihood/scale

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.45

Risk Database Content - 3

- Risk owner
  - Who is responsible for tracking risk?
  - Who is responsible for implementing risk actions?

- Risk action(s)
  - What to do?
    - Avoidance/acceptance

- Action log
  - Record of action taken
    - When/where/by whom?

V1.0   © NCC Education Limited

IT Risk Management Lecture 7 - 7.46

Risk Action

- Actually acting on all the identification, analysis and response planning
  - if previous stages are completed with integrity, balance and knowledge, the Project Manager and team should be as prepared as possible in their response to any actual risk that occurs (goes live)
- Any action taken must be documented so the flow of information links back to the risk planning stage
- ...and the whole cycle of Risk Management flows on

V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.47

References

- Cadle, J. and Yeates, D. (2001). *Project Management for Information Systems*. FT Prentice Hall.
- Dalcher, D. & Brodi, L. (2007). *Successful IT Projects*. Thomson.
- Hall, P. and Fernandez-Ramil, J. (2007). *Managing the Software Enterprise*. Thomson.
- Hughes, B. and Cotterell, M. (1999). *Software Project Management*. McGraw Hill.
- Schwalbe, K. (2010). *Managing Information Technology Projects*. Course Technology CENGAGE Learning

V1.0
© NCC Education Limited

IT Risk Management Lecture 7 - 7.48

Topic 7 – IT Risk Management

Any Questions?

NCC Bringing British Education to You www.nccedu.com

V1.0
© NCC Education Limited