

Bringing British
Education to You
www.nccedu.com

Professional Issues in IT

Topic 8:
Applying, Evaluating & Managing Risk Analysis

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.2

Scope and Coverage

This topic will cover:

- The development of a practical risk analysis skill base
- An introduction to international standards for risk management
- An introduction to international institutes for risk management



Bringing British
Education to You
www.nccedu.com

V1.0


© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.3

Learning Outcomes

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

- Generate risk assessment maps and tables;
- Analyse findings;
- Create risk responses;
- Evaluate actions proposed;
- Create risk databases;
- Report conclusions;
- Provide reasoned recommendations;
- Name and discuss examples of risk management international standards;
- Name examples of international institutes concerned with risk management.



Bringing British
Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.4

International Standards

- Few industry recognised standards for risk management exist
- Three risk management standards:
 - ISO 31000
 - Risk Management Standard
 - COSO2
- Focus on the first two standards

Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.5

ISO 31000 - 1

- International organisation for standardisation
- Official name ISO 31000:2009
 - Launched 2009
 - Has own terminology guide: 73
- Replaces AS/NZS 4360 from 2004
 - Australian standard
- Aim:
 - Provide a best practice structure for risk management

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.6

ISO 31000 - 2

- Objectives:
 - To replace all existing standards, methodologies and approaches to risk management
 - To provide one generic standardisation across all industries regardless of subject area
- Not a certifiable standard
 - More of a benchmark

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.7

ISO 31000 - 3

- Potential benefits:
 - Increased likelihood of achieving objectives
 - Encourages proactive management
 - Increases awareness of risks
 - International norm
 - Establishes reliable decision making and planning basis
 - Encourages effective resource allocation and use

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.8

ISO 31000 - 4

- Risk management (RM) framework
 - Actually three frameworks:
 - Developing a RM framework
 - Implementing a RM framework
 - Monitoring and reviewing a RM framework
 - Series of checklist questions
 - Provide benchmark for organisations to generate own approach to risk management
 - Organisations encouraged to adapt language to fit
 - Intention is that nothing obvious is missed by an organisation and all organisations are understanding risk management in the same way

Bringing British Education to You
www.nccedu.com

V1.0


© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.9

Framework Checklist Examples

| | Section | Requirement | Essential/ Advanced | In Place (Yes/No) |
|----|-----------------------|---|------------------------|----------------------|
| 14 | Communicate & consult | Has Risk committee & board reviewed & approved Risk Policy? | Essential | |
| 32 | Risk assessment | Has Risk brainstorming been conducted? | Essential | |
| 55 | Monitor & review | Has Risk Policy been reviewed & approved in last year? | Essential | |

Adapted from: riskmanagementtemplates.com

Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.10

Risk Management Standard -1

- Created by:
 - Institute of Risk Management (IRM)
 - The Association of Insurance & Risk Managers (AIRMIC)
 - The Public Risk Management Association (ALARM)
- Published 2002
- Later adopted by Federation of European Risk Management Associations (FERMA)
- Developed in United Kingdom
- Non certifiable standard
- Organisations aim to be 'in compliance'

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.11

Risk Management Standard - 2

- Objectives of standard is to agree:
 - Terminology
 - Risk management process
 - Risk management organisation structure
 - Risk management objective
- Acknowledges the many approaches available to achieving objectives

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.12

Risk Management Standard - 3

- A 'best practice' standard
- Updated when ISO 31000 launched in 2009
 - 'A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000'.
- IRM, AIRMIC & ALARM still remain loyal to original Risk Management Standard
- Own risk management process

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.13

Risk Management Standard - 4

- 7 step process with sub steps:
 1. Organisation's strategic objectives
 2. Risk Assessment
 - Risk Analysis
 - Risk identification
 - Risk description
 - Risk estimation
 - Risk evaluation
 3. Risk reporting
 4. Decision
 5. Risk treatment
 6. Residual risk reporting
 7. Monitoring

Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.14

International Institutes

- Many risk management institutes worldwide, such as:
 - Institute of Risk Management (IRM)
 - Federation of European Risk Management Associations (FERMA)
 - International Federation of Risk & Insurance Management Associations (IFRIMA)
 - The Association of Insurance & Risk Managers (AIRMIC)
 - Public Risk Management Association (ALARM)
- There are also other organisations that have special interest groups (SIG) in risk management, such as:
 - Project Management Institute (PMI)
 - Chartered Institute for IT (BCS).

Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.15

International Federation of Risk & Insurance Management Associations

- Known as IFRIMA
- Founded 1984
- An 'Association of Associations'
 - International umbrella organisation for RM Institutes
- Operates as a forum for RM Institutes
- Members from over 30 countries
- Supports ISO 31000
 - Agrees with benchmarking approach
 - Did not support Certification

Bringing British Education to You
www.nccedu.com

V1.0


© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.16

IFRIMA - 2

- Goals
 - Improve the 'value' of risk managers
 - Encourage and assist in creation of new risk management organisations globally
 - Promote organisation cooperation
 - Specifically the exchange of ideas
- Focus
 - Risk management education

V1.0

Bringing British Education to You
www.nccedu.com


© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.17

Project Management Institute

- Known as PMI
- Published own standard named project management book of knowledge (PMBOK)
- Risk management is one of nine recognised knowledge areas

V1.0

Bringing British Education to You
www.nccedu.com


© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.18

Project Management Institute
PMBOK

- Breaks risk management down into six processes:
 1. Plan risk management
 2. Identify risks
 3. Perform qualitative risk analysis
 4. Perform quantitative risk analysis
 5. Plan risk responses
 6. Monitor and control risks

V1.0


Bringing British Education to You
www.nccedu.com

© NCC Education Limited

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.19

BCS Chartered Institute for IT


- Known as BCS
- Previous name British Computer Society
- “Mission is to enable the Information Society”
- Special Interest Group (SIG)
 - Information Risk Management & Assurance Group (IRMA)

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

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.20

BCS IRMA


- Information Risk Management & Assurance Group (IRMA)
- Established 1965
- Objectives:
 - Encourage research and promote development
 - Provide a forum
 - Promote efficiency, effectiveness and economics
 - Represent information risk management to other organisations

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

Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.21

References


- Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 4th Edition. Project Management Institute.
- www.ifrima.org
- www.theirm.org
- www.pmi.org
- www.bcs.org

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


Applying, Evaluating & Managing Risk Analysis Topic 8 - 8.22

Topic 8 – Applying, Evaluating & Managing Risk Analysis

Any Questions?



Bringing British Education to You
www.nccedu.com



V1.0 © NCC Education Limited
