Information Risk Management – Seminar 2: User Participation in the Risk Management Process

Outline:

- Announcements
- Reading & Qestions
- ACM guidelines
- Questions & Next Week

Announcements:

- Group Contracts
- → Helps you resolve any issues or problems in the group
- → Clarifies and defines roles, responsibilities and deliverables
- Reflection Deliverable
- → Based on e-portfolio but is not whole portfolio (500 words)
- → Use evidence you have collected throughout the module to support
- Quote references if helps / support your reflection

- Peer Review

- → You are expected to create a peer review for each of your team members and submit it as part of your assessment. If your fellow team members have performed as expected and delivered what is required I would encourage you to give them a rating for three.

- → If someone has performed really well (maybe mentoring you or providing additional advice / input / content) you can award them a four for that specific activity (e.g. running meetings, etc.) Likewise, if someone has not met expectations in a specific area (e.g. meeting attendance) it is acceptable to give them a rating of 2.

- Please do not award individuals a 1 or 5 without any real reason – this will often backfire and I will be following up unusual and difficult to justify ratings. Before awarding a 1 please raise it as an issue with the tutor so I can investigate as there may be extenuating circumstances.

Group Presentation:

Group 1:

-affect of lack of user access to risk assessment:

Design, implementation and performance for security control development:

- ➔ Inferior knowledge of user operation
- ➔ No consideration to user feedback
- ➔ Potentially lower performance as user can support the level of risk exposure understanding

➔ Risk assessment may not be directly relevant for effective use

Business objectives:

➔ Challenge to align security measures to business objectives
➔ Business outcomes may be lower
➔ Lack of organisational awareness with business processes

Expertise:

➔ Lack of user expertise to identify mitigation needs
➔ Limitation of the expression of expertise to the business-oriented goals
➔ Lack of empowerment for the users

- Affect of the choice of Qualitative vs. Quantitative assessment methods:

➔ Quantitative method uses numerical and statistical techniques to calculate the likelihood and impact of risk
➔ Quantitative method is data-driven and produces statistically reliable results
➔ Given the high degree of uncertainty and insufficient knowledge to deduce user participation, a quantitative method will not yield a satisfactory result.
➔ It is not easy to collect data on every process.
➔ Reliable historical data may not be available for analysis to quantify risk.
➔ The cost of quantitative analysis is usually higher than qualitative analysis
➔ Qualitative analysis often reflects inputs of business units more accurately than quantitative analysis, and it also captures 'soft' risk such as moral or repudation.

■ Considering the above, we would use the qualitative assessment method for risk assessment.

- How to mitigate any issues encountered?

Issues	Mitigation
Subjective Assessment: Qualitative assessment does not yield measurements, it is based on the perspective of the individual doing the research instead.	A qualitative risk analysis should involve numerous persons to reduce subjectivity. The accuracy and depth of the analysis are determined by the team's past expertise.
Noisy data: Meaningless data might produce during the assessment when users resist the change or focus on self-interest.	According to the research, it could be robust to noise with regression like Partial Least Squares (PLS), developed from the principal component regression, which helps in building models predicting more than one dependent variable (Lorber et al., 1987)

ISO 27001:

- These ISO standards help organizations maintain the security of their information assets by recommending types of security controls and processes.
- They also help to define a risk strategy based on business needs to mitigate risk across the enterprise and continually monitor and communicate progress in a methodical fashion – as shown in this schematic.

Factor Analysis of Information Risk (FAIR)

- Factor Analysis of Information Risk (FAIR) breaks don risk into separate variables that can be quantified and examined together to describe risk as a range of likely loss in money.
- Unlike risk assessment methodologies that provide qualitative colour chars or numerical weighted scales, the FAIR standard produces financially determined, which can be communicated across the company in normal business terms of loss exposure and return on investment.

Open FAIR vs ISO 27001

Open FAIR is often seen as a preferred risk assessment tool due to the its following benefits:

- ➔ Highly useful during threat assessments and helps to understand the impact of threat mitigation options during the ADM cycle.
- ➔ Identify top risks in financial terms for loss exposure
- ➔ Evaluate the efficacy of risk treatments for risk reduction in terms of probable dollar savings
- ➔ Fulfil the spirit of ISO 27001 by effectively communicating on cyber risk in the language that the enterprise best understands.

Questions & Next Week

- Questions:
- Next Week:
- → First deliverable, Report (proposal – 600 words)
- Needs to include:
- → What will your final report include (assumptions & requirements)
- → How will you deliver it (charts, frameworks, data, references)
- → When will you do the work (plan and milestones)
- → Don't forget – Peer Review form
- No Seminar next unit but office hours are available if required

- ➔ Question Timeline: With your assessment and assumptions maybe think about your kind of proposals, how long will it take for you to implement your idea or implement the things that you've proposed.