[Unit 2] Seminar 1: User Participation in the Risk Management Process

A. Risk Management Process

1. Context Establishment
    - [Scoping exercise] Standards (e.g. transactions -> payment card industry), risk appetite
    - Main stakeholders
    - Cost-benefit analysis
2. Risk Identification
    - BIA: Business Impact Assessment
        - [Scoping exercise cont.] Financial, reputational, legal damage
        - Interviews, focus groups, workshops, email, risk suggestion box submit anonymously
3. Risk Analysis
    - Modelling
4. Risk Evaluation
    - Quantitative – objective
        - Based on historical data, numerical, probability curves, algorithm, relationship between data and outcomes
    - Qualitative - subjective
        - [Matrix] Scorecards & Registers - responses of different roles may differ
        - New risks, new process
        - No historical data, not enough info for algorithm

- Subjective data, behavioural
- Tacit/classic knowledge, preconceptions, bias

5. Risk Treatment
   - Avoid - preventive measures (e.g. security cameras, guards)
   - Transfer - insurance policy, transfer to another company department
   - Reduce - technical measures/physical measures (e.g. access controls), security education/training (e.g. phishing campaigns)
   - Accept
6. [Reporting] Communication and Consultation
   - RAG Reports: Red, Amber, Green
7. Monitoring and Review
   - PDCA (iterative): Plan Do Check (Change what doesn't work) Act

B. Spears & Barki (2010)

1. Qualitative Approaches

To find variables to test for the qualitative component of the study, the authors adopted several qualitative approaches:

- Semi-structured interviews with the users
- SOX Experience

2. Quantitative Approaches

- Partial Least Squares (PLS), Average Variable Extracted (AVE)
- Correlation matrix, composite, manifest constructs (formative, reflective, latent)

3. **Both Approaches**
    - Used both approaches because triangulation of different data points
4. **Advantages of involving users in the risk management process**
    - Data verifies that there is actual statistical weight to the hypotheses that they found
    - User participation in SRM raises organisational awareness of security risks & controls, their role in security, who has access to what info
    - Compliance standards
    - Better buy-in when people feel involved, better collaboration, cooperation

C. ACM Guidelines - Empirical Standards

SSM: Soft Systems Methodology

References

Kovaitė, K. and Stankevičienė, J. (2019) Risks of digitalisation of business models. Proceedings of 6th International Scientific Conference Contemporary Issues in Business, *Management and Economics Engineering* ‘2019.

Olson, D.L. & Desheng D.W (2020) *Enterprise risk management models.* Berlin, Germany: Springer.

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly* 34(3): 503.