An Introduction to Security and Risk Management

In unit 1, There are various definition of security risk, and it depends on context and situation of the events. Below are various definitions of risk by different authors.

- Blakely et al (2002) define risk as the possibility that an event would reduce the value of the business and it can be measure as Annualised Loss Expectation (ALE).
- Stoneburner et al (2002) define risk as the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.
- Hubbard (2009) define risk a state of uncertainty with an undesirable outcome.
- NIST define risk as a measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of adverse impacts that would arise if the circumstances or event occurs.
- Sutton (2016) states that Information risk is a subset of business risk and relates to the confidentiality, Integrity and Availability of business information assets and the information management.
- Josey et al (2014) “The OPEN Fair Body of Knowledge defines risk as the probable frequency and magnitude of future loss”.

The summarize of the various risk definitions is that risk is associated with uncertainty of event that result to adverse outcome. This is better summarized by the OPEN Fair basic equation for risk calculation which equal Threat *Vulnerability *Asset. This shows that risk is a combination of threat event, vulnerability, asset value and liability characteristic.

Information Risk can be assessed using either quantitative or qualitative methodologies or both in some cases. The differentiating factors on the two-assessment methodologies are as follows:

S/N	Quantitative Assessment	Qualitative Assessment
1	Mathematical Calculation	It is based on individual perception or judgement
2	Probabilities and game theory are used to in ranking matrix	Risk impact is categorized into Low, Medium & High
3	Contain measurable variables	Associated with lower asset value
4	It used when there is large number of data	Low availability of data
5	Ability to predict outcome	

It is advised to start risk assessment with qualitative methodology and further applied quantitative assessment to get a more reliable assessment.

Upon ascertaining the associated risk, it can be classified under the following categories:

- Risk to avoid completely (Eliminate).

- Tolerate (the cost-benefit of risk impact is low).
- Reduce (the impact of risk can be minimized by preventive measures)
- Transfer (the impact or cost of mitigation is shared among the stakeholders).

Next step is what are the mitigation for the identified Risk. The mitigation can be group as follows:

S/N	Group	Mitigation Type
1	Physical Control	Security guard, Alarms system, CCTV, Biometric devices
2	Technical Control	Firewall applications, IDS system, SIEM (Security Information &Event Management)
3	Procedural Control	Annual training to keep abreast with new or existing technology, Induction of staff on new assignment or new hirer.

The above mitigation Mechanism can be used as preventative control, Directive control, Detective control and Corrective control.

Risk Assessment Standards and Best Industry Practices includes but are not limited to;

- Open Fair (F-Factor, A-Analysis, I-Information R-Risk). This involves Open Risk Taxonomy(0-R-T) and Open Risk Analysis9O-RA) and according to Open Group (Josey et, al 2024) the rational for the Open Fair is based on its emphasis on risk, Logical & rational framework nature, Quantitative application, Flexibility and Rigorous to avoid gaps and errors.
- Also, other alternative framework are ISO 31000, ISO27001, ISO27005
- COBIT (Control Objective for Information Technology).
- OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)
- NIST800-30

Reference:

Kovaitė, K. & Stankevičienė, J. (2019). Risks of Digitalisation of Business Models. Available from: **https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models** DOI:10.3846/cibmee.2019.039 [Accessed 20 August 2023]

Regoniel.P. (2015). Simplyeducate.me ,Quantitative Research Methods: Meaning and Characteristics. Available from :https://simplyeducate.me/2015/01/03/quantitative-methods-meaning-and-characteristics/?expand_article=1&_gl=1*70w9ce*_up*MQ..*_ga*NzQ3NTg5MjkyLjE2OTYyODYzMDU.*_ga_TWKB5R2G2M*MTY5NjI4NjMyNS4xLjAuMTY5NjI4NjMyNS4wLjAuMA. [Accessed 20 August 2023].

University of Essex Online Lecturecast 1 (2023) Risk & The Risk Management Process. Available from: https://www.my-

course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%201/content/index.html#/ [Accessed 15 August 2023].