[All] Unit Readings Compilation

Unit 1 Reading

The reading this week focusses on various definitions of Risk, plus the basic concepts of Security and Risk Management (SRM) including threats and vulnerabilities. It also introduces the risk management process (RMP) and various risk management process standards and approaches.

Required Reading

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

- Chapter 1.

Stoneburner, G., Goguen, A. & Feringa, A. (2002) SP 800-30: *Risk Management Guide for Information Technology Systems*

Sørensen, B.T. (2018) Digitalisation: An Opportunity or a Risk? *Journal of European Competition Law & Practice*, 9(6). 349–350.

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.

Additional Reading

Campbell, T. (2016) *Practical Information Security Management*. 1st ed. APRESS.

- Chapters 1 and 2.

Hubbard (2020). T*he Failure of Risk Management : why it's broken and how to fix it*, 1st ed. Wiley and Sons.

- Chapter 6.

Blakley, B., McDermott, E. & Geer, D. (2001) Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms* 1(1): 97-104.

Unit 2 Reading

The reading this week focusses on a study by Spears & Barki (2010) that looks at both the effect of user participation on the Risk Management Process, as well as spending significant time discussing the different approaches to assessment – that is Qualitative vs. Quantitative.

Required Reading

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

Renn, O., Beier, G. and Schweizer, P.-J. (2021) The opportunities and risks of digitalisation for sustainable development: a systemic perspective. GAIA - Ecological Perspectives for Science and Society, 30(1), pp.23–28.

Josey, A., Hietala, J. & Jones, J. (2014) Introducing The Open Group Open FAIR™ Risk Analysis Tool.

AIRMIC (2010) A structured approach to enterprise risk management.

Additional Reading

Wang, J., Neil, M. and Fenton, N. (2020) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security. 89.101659.

Unit 3 Reading

The reading this week focusses on a survey of a range of threat modelling tools, frameworks and techniques.

Required Reading

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: a summary of available methods*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

NIST (2022) IT Laboratory Computer Security Resource Center.

Shostack et al (2020) *The Threat Modelling Manifesto.*

Additional Reading

Shostack, A. (2014). *Threat modeling : designing for security*. Wiley & sons ltd.

- Chapters 1 and 2.

Unit 4 Reading

The reading this week focusses on examples of various modelling tools and techniques and their use including attack trees, STRIDE, DREAD and CVSS.

Required Reading

Shostack, A. (2014). *Threat modeling : designing for security*. Wiley & sons ltd.

- Chapters 3 - 6.

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: a summary of available methods*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Meier, J. Mackman, A. Dunner, M. Vasireddy, S. Escamilla, R. & Murukan, A. (2003) *Improving Web Application Security: Threats and Countermeasures.*

Ross, R., McEvilley, M. & Oren, J. (2016) *Systems Security Engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems.*

Threat Modelling CookBook (OWASP).

Additional Reading

Hijazi, H., Alqrainy, S., Muaidi, H. & Khdour, T. (2014) Identifying Causality Relation between Software Projects Risk Factors. *International Journal of Software Engineering and its Applications*, 8(2): 51-58.

Salter, C., Saydjari, O., Schneier, B., & Wallner, J. (1998) Toward a secure system engineering methodology. In: *Proceedings of the 1998 Workshop on New Security Paradigms* (NSPW '98). Charlottesville, Virginia, United States, pp. 2–10.

Unit 5 Reading

The reading this week focusses on a selection of papers and blogs in order to support the selection of evaluation and scanning tools to use in the assessment as well as create an informational wiki.

Required Reading

Barafort, B., Mesquida, A.-L. & Mas, A. (2018) ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, 31(1), p.e1984.

Additional Reading

Campbell, T. (2016) *Practical Information Security Management*. 1st ed. APRESS.

- Chapter 7.

Unit 6 Reading

The reading this week focuses on security standards and recommendations, including GDPR. The reading will consist of chapters from a supplementary text (Campbell (2016)), as well as suppliers and government sources including the GDPR, PCI-DSS and the ISO 27000 web sites. There is also a case study based on data available.

Required Reading

Kirvan, P. (2021) *Top 10 IT security frameworks and standards explained.*

Additional Reading

Campbell, T. (2016) *Practical Information Security Management.* 1st ed. APRESS.

- Chapter 6.

Unit 7 Reading

The reading this week focuses on the theory behind the Monte Carlo method and Bayes theorem as a background to creating quantitative risk models. In addition, you should read the course text (Olsen & Desheng, 2020) and study the case studies provided.

Required Reading

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

- Chapters 2 - 9.

Asadabadi, M. Chang & Saberi, M. (2019) Are MCDM methods useful? A critical review of Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP), *Cogent Engineering*, 6:1, 162315.

Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS? *IEEE Security & Privacy*, 19(2), pp.74–78.

Winston, W. Introduction to Monte Carlo Simulation in Excel.

Downey, A. (2021) *Think Bayes 2.*

Unit 8 Reading

The reading this week focusses on case studies of the use of QR models, as well as studies that critically evaluate the use of such techniques.

Required Reading

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

- Chapters 2 - 9.

Downey, A. (2016) *Think Bayes*. Sebastopol, Ca:O'Reilly.

- Chapters 1 - 3.

Goerlandt, F., Khakzad, N. and Reniers, G. (2017). Validity and validation of safety-related quantitative risk analysis: A review. *Safety Science*, 99, pp.127–139.

Hugo, F.D., Pretorius, L. & Benade, S.J. (2018) Some Aspects of the use and Usefulness of Quantitative Risk Analysis Tools in Project Management. *South African Journal of Industrial Engineering*, 29(4).

Çelikbilek,Y. & Tüysüz, F. (2020) An in-depth review of theory of the TOPSIS method: An experimental analysis, *Journal of Management Analytics*, 7:2, 281-300.

Eckstein, J. and Riedmueller, S.T. (2002) YASAI: Yet Another Add-in for Teaching Elementary Monte Carlo Simulation in Excel. *INFORMS Transactions on Education*, 2(2), pp.12–26.

Karen, T. (2021) *Monte Carlo Simulation and Variants with Python*.

NB: YASAI - easier alternative to crystal ball

Unit 9 Reading

The reading this week focuses on background material around BC and DR planning. Alhazmi & Malaiya (2013) provide a review of various evaluation strategies and terminology related to disaster recovery strategies (DR). Andrade et al (2017) provide a mathematical evaluation of strategies that can be used for probabilistic or statistical predictions. Finally, the course text, chapter 13 (Olsen & Desheng, 2020) provides a review of natural disaster risk management strategies and probabilities.

Required Reading

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

- Chapter 13.

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing*, 99(10), pp.929–954.

Unit 10 Reading

The reading this week focuses on the practical implementation of DR strategies and some of the issues and challenges of implementation – including around solutions such as DRaaS.

Required Reading

Morrow, T., LaPiana, V., Faatz, D., Hueca, A. & Richmond, N. (2021) *Cloud Security Best Practices Derived from Mission Thread Analysis.* Carnegie-Mellon Univ Pittsburgh PA.

Opara-Martins, J., Sahandi, R., & Tian, F. (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing. *In International Conference on Information Society* (i-Society 2014) (pp. 92-97). IEEE.

Alhazmi, O. & Malaiya, Y. (2013) Evaluating Disaster Recovery Plans using the Cloud. *2013 Proceedings Annual Reliability and Maintainability Symposium* (RAMS) 1(1): 1-6.

Unit 11 Reading

The reading this week focuses on emerging trends in the risk science and management based on a paper by Aven (2016). There are additional articles in the reading list that will act as preparation for next week's seminar.

Required Reading

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

- Chapter 12.

Pineiro-Chousa, J., Vizcaíno-González, M., López-Cabarcos, M. & Romero-Castro, N. (2017) Managing Reputational Risk through Environmental Management and Reporting: An Options Theory Approach. *Sustainability* 9(3): 376-391.

Fahimnia, B., Pournader, M., Siemsen, E., Bendoly, E. & Wang, C. (2019) Behavioral Operations and Supply Chain Management–A Review and Literature Mapping. *Decision Sciences* 50(6): 1127-1183.

Ridley, A., McCloskey, J. & Mountain, D. (2018) Machine Learning for Autonomous Cyber Defense. *The Next Wave* 22(1): 7-14.

Varshney, K. & Alemzadeh, H. (2017) On the Safety of Machine Learning: Cyber-Physical Systems, Decision Sciences, and Data Products. *Big Data* 5(3): 246-255.

Fraser, J. & Simkins, B. (2016) The Challenges of and Solutions for Implementing Enterprise Risk Management. *Business Horizons* 59(6): 689-698.

Aven, T. (2016) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research* 253(1): 1-13.

Unit 12 Reading

The reading this week focusses on current and emerging trends as listing in the reading list.

Required Reading

Marks, L. (2019) *The Optimal Risk Management Framework: Identifying the Requirements and Selecting the Framework.*

David M Nicol et al.(2012) "*Science of Security Hard Problems: A Lablet Per- spective*". Illinois.