# Section 1: Week 2: Risk Management Frameworks

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 14, 2020

North Central University

# Risk Management Frameworks

Organizations can choose between multiple risk management frameworks to meet the needs of their specific industry or business practices. While differences exist across these frameworks, they generally follow a similar feedback loop of plan-do-check-act (Radhakrishnan, 2015). Where they differ is in terms of their specific focuses and attempts to create consistency or provide general guidance. For instance, ISO 27000 optimizes for rigid consistency over flexibility, making it practical for highly regulated environments and smaller enterprises (Gillies, 2011). In contrast, the NIST Cybersecurity Framework fits the current maturity level of a business by providing a path to mature processes where necessary (Grohmann, 2018). COBIT v5 might provide an ideal middle ground, as it has prescriptive guidance that comes from industry best practices (Devos & Van de Ginste, 2015).

However, each business has specific risks that are most concerning to their continuity and ability to deliver its core mission. If those companies have a simple network topology, like mom-and-pop stops, then simplicity is more desirable than even flexibility. For instance, if a local doctor’s office consists of three workstations, then the VAR framework accurately models the loss at catastrophic failure such as ransomware infecting compromising these machines (Kenton, 2019). The small business owner might purchase backup software, establish a retainer for computer repair service, or purchase insurance to hedge the risk adequately. While they could gain more coverage from additional investments, those protections might negatively detract from the core mission and not provide significant returns.

For other businesses, a need risk management solution might require adopting multiple frameworks. Consider an eCommerce site that operates within a private data center. This organization might need SABRE to manage the physical assets and NIST Risk Framework to cover digital artifacts for industry compliance. When integrating multiple frameworks, there are additional challenges, such as needing to choose the stricter requirement when expectations contradict. Ideally, these scenarios sufficiently overlap; however, specific scenarios can encounter unique issues.

Table 1: Risk Framework Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Model/Framework | Strengths | Limitations | Comments |
| NIST Risk management framework (SP-800-37 R2) | Focuses on checklists of controls and risk categories (Combass & Shilling, 2016) | A more rigid process that is appropriate for military purchases | Seems to be more of an acquisition checklist based on usage |
| ISACA Risk IT management framework | Collection of industry best practices that apply to many scenarios | Not based on academic research (Devos & Van de Ginste, 2015)  Prescriptive guidance might be difficult for every scenario (Chabrow, 2013) | Rebranded to COBIT v5 around 2009 |
| Value at Risk (VAR) framework | A statistical measure of the loss given the probability of an event (Kenton, 2019) | Businesses consistently make more assessments of a security risk (Eling & Wirfs, 2019) | Many technology decisions are not pure black/white (a) will cost (b) if (c) |
| Financial, economic theory | Models time, risk, and uncertainty to make economically sound decisions (Liberto, 2019) | Makes extensive use of hedging, which might not apply to information technology systems |  |
| SABRE security risk management model for asset management | The high-quality standard for physical structures (BRE, 2020) | Only focuses on physical structures | Appropriate for industrial complex through residential housing |
| NIST Cybersecurity Framework | Adapts to various maturity levels through a good-better-best mindset (Grohmann, 2018) | External audiences cannot gauge security posture at a simple glance (are they ok or excellent on aspect 1234) | The right solution for many large and decentralized businesses that lack any formal process |

# References

BRE. (2020, June 14). *What is SABRE*? Retrieved June 14, 2020, from BRE Group: https://www.bregroup.com/sabre/

Chabrow, E. (2013, September 26). *ISACA Unveils New Risk Mgt. Framework*. Retrieved June 14, 2020, from Bank Info Security: https://www.bankinfosecurity.com/isaca-unveils-new-risk-management-framework-a-6098

Combass, T., & Shilling, A. (2016). Integrating cybersecurity into NAVAIR OTPS acquisition. *Institute of Electrical and Electronics Engineering AUTOTESTCON*, (pp. 1-5). Anaheim, CA. doi:https://doi-org.proxy1.ncu.edu/10.1109/AUTEST.2016.7589632

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA.* Black Hat. Retrieved May 2020, from https://www.youtube.com/watch?v=8armE3Wz0jk

Devos, J., & Van de Ginste, K. (2015). Towards a Theoretical Foundation of IT Governance - The COBIT 5 case. *Electronic Journal of Information Systems Evaluation, 18*(2). Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=edb&AN=109261833&site=eds-live

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(1), 1109-1119. doi:https://doi.org/10.1016/j.ejor.2018.07.021

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:http://dx.doi.org.proxy1.ncu.edu/10.1108/17542731111139455

Grohmann, A. (2018). Evolution of the cybersecurity framework. *ISSA Journal, 16*(7), 14-18. Retrieved May 2, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=130572679&site=eds-live

Kenton, W. (2019, April 18). *Value at Risk (VAR)*. Retrieved June 14, 2020, from Investopedia: https://www.investopedia.com/terms/v/var.asp

Liberto, D. (2019, June 26). *Financial Economics*. Retrieved June 14, 2020, from Investopedia: https://www.investopedia.com/terms/f/financial-economics.asp

Radhakrishnan, S. (2015). COBIT Helps Organizations Meet Performance and Compliance Requirements. *COBIT Focus, 5*, 1-5. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=bth&AN=102026122&site=eds-live