# Risk Management Frameworks

The

# 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 ridge 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 |