

STANDARDIZATION OF RETURN ON RISK INVESTMENT COMPUTATION

Brett Tucker

October 2025

DOI: 10.1184/R1/30299998

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Introduction

Return on Security Investment (ROSI) can be a sophisticated and challenging endeavor for most organizations as they understand how to quantitatively make risk-based decisions related to resource allocation for risk response [Boehm 2019]. The National Academies of Science recently published the book, *Cyber Hard Problems: Focused Steps Toward a Resilient Future* [NASEM 2025]. Among the many strategic and operational challenges it covers, the Committee on Cyber Hard Problems cites pronounced challenges in overcoming the uncertainty involved in determining and applying return on investment (ROI) to enhancing security resilience.¹ Therefore, the SEI's CERT Division proposes standardizing the computation of ROI in practice and methodology to establish consistent measurement and standardized practice across organizations and communities.

This paper explores the benefits of standardizing methodologies and introduces some novel solutions to consider for adoption. More importantly, CERT proposes these ideas while aspiring to establish enduring partnerships across academia, private industry, and the public sector to advance risk-based decision making based on comprehensive quantitative analysis. CERT's depth of expertise in cybersecurity, risk management, modeling, and measurement would complement the expertise of many other organizations that have similar interests in collaborating to better the greater community.

CERT's research has uncovered unique challenges in computing ROI related to the current state of the practice, including the following:

- Improving calculations for ROI does not come with one simple revelation. Rather, the factors that influence ROI (e.g., risk impacts, total cost of control implementation, control efficacy) must each be defined and systematically addressed independently and then in concert.

¹ For more information, see *Cyber Hard Problems: Focused Steps Toward a Resilient Digital Future*, page 63 [NASEM 2025].

- Although tools exist for computing risk impacts, there is no consistent methodology or standard that can be used to gain the necessary consistency needed for community consideration.
- Even if ROI calculations had a standardized dataset and methodology, the risk appetite of each organization influences the course of risk-based decision making.
- Aside from calculations, there are few known datasets that provide comprehensive measurements that demonstrate effective ROI calculations. This shortage may be a result of organizations not wanting to share critical information or a general lack of collecting the data.
- Some organizations, while not having enough data to do so, seek an ROI calculation or estimate before starting a program or selecting a specific cyber control. This practice can be good for gaining a gross understanding of the scope of investment, but revised ROI estimates made after investments are complete, and the data collected can erode the confidence that senior management has in organizational processes. Assumptions must be asserted and clear while considering the risks of error.

Ultimately, the larger cybersecurity community would benefit from a standard calculation of ROI, so that risk-based decisions can unify all responses and create a reduced surface of risk exposure across critical infrastructure sectors as well as in individual organizations.

Background

ROI is not a novel concept, especially for financial analysis and application. The Financial Industry Regulatory Authority (FINRA) defines ROI as the “Level of risk associated with a particular investment or asset class [that] typically correlates with the level of return the investment might achieve” [FINRA]. This definition supports the notion that investors should be willing to invest in a certain level of risk with expectation of reward for taking that risk.

This same concept can be applied to cybersecurity, sometimes called Return on Security Investment (ROSI). Specifically, organizations accept a certain amount of risk to operate their systems. To accept that risk, organizations must establish technical, administrative, and physical controls to limit the amount of exposure to threat-actor actions.

Technical, administrative, and physical controls cost money to implement. Procurement costs of controls, development and implementation costs of policy, and the general burden related to users’ efforts to comply with these controls and policies must be offset by the notion that a realized risk incident outweighs the cost of these mitigations. Put another way, the lack of these mitigating actions may result in a realized incident that would, in turn, result in higher impact losses.

Mathematically, the definition of ROI can be expressed this way:

$$\text{ROI} = [(\text{Benefits} - \text{Costs})/\text{Costs}] \times 100\%.$$

This definition points to the quantification of the expected impacts realized by a given set of cyber risks for an organization. The SEI has written about risk impact quantification, for example, in the report, *Loss Magnitude Estimation in Support of Business Impact Analysis* [Kambic 2020]. However, there are a host of other generally accepted frameworks to assist organizations in risk quantification, such as Factored Analysis for Information Risk (FAIR) [FAIR 2025].

Although robust, these frameworks rely on a significant amount of data and analysis to gain an answer. Organizations must be aware of the analytical investment required to gain an understanding of ROSI and risk prioritization to avoid the over investment of resources to attain “perfect” estimates over just “good” assessments.

That said, risk impact quantification should be considered in terms of a range of values that reflect the best case, worst case, and most likely outcomes. The benefits of the ROSI calculation refer to the primary savings of preventing or alleviating risk events. These benefit values are usually based on specific application functions. For example, an integrated firewall solution may report a number of threat-actor signatures that are then identified and blocked from system access. Said another way to be more applicable to cybersecurity measurement, the calculation may be expressed mathematically this way:

$$\text{ROSI} = (\text{Annual Loss Expectancy} - \text{Cost of Controls}) / \text{Cost of Controls} \text{ [ENISA 2012].}$$

In this computation, data analytics may be applied to cyber incident datasets to develop Annual Loss Expectancy (ALE), which can be made equivalent to the “benefits” of ROSI when assuming that controls are effectively mitigating incidents. A historical review of Single Loss Expectancies (SLE) multiplied by the Annual Rate of Occurrence (ARO) delivers the ALE calculation. However, improving data standards for collection and analysis may provide greater efficiency and fidelity in calculation.

Similar research must be conducted to develop methodologies that determine the efficacy of defensive controls. As discussed, some of those measurements exist on an application-by-application basis. However, currently there are no consistent standards to enable a universal understanding of the benefit calculations. Historically, the ROSI calculation provides insights for making strategic decisions, such as justifying the purchase of new controls or the implementation of new processes.

The ROSI calculation may enhance risk-based decisions by also relating the specific value of a decision, where technological results can be translated to dollars saved. At best, organizations must be trained to recognize that these calculations suffer diminishing returns proportionate with greater fidelity based on the cost of conducting the analysis. Therefore, these metrics are best applied as part of prioritizing potential solutions.

Varied Applications of ROSI Calculations

CERT researchers have worked to develop novel means of measuring the efficacy of controls to determine their direct ROI for owners. Over time, several observations have become representative of the challenges related to making these calculations:

- **Context matters in determining ROSI.** Organizations may use different risk tools, interpret information differently, identify new alternative and varied data sources, and make different risk decisions related to control selection and implementation.
- **Control implementation influences ROSI.** Organizations implement risk and cyber controls in varied ways with diverse policies. This principle, in turn, impacts the efficacy of the controls in mitigating threat actor actions and potential risk impacts.
- **Risk appetite influences ROSI.** Organizations perceive their tolerance to risk based on their risk strategy matched with their belief that they can “beat the odds.” As a result, risk-based decisions related to control prioritization and selection vary from organization to organization. Likewise, ROSI may influence risk appetite, where improved certainty may narrow ranges of risk tolerance. Regardless, risk appetite and ROSI both play roles in influencing risk-based decision making.

Given these observations, CERT recognizes the need to standardize methodologies for calculating ROSI. The following examples demonstrate the context of applying ROSI in making risk-based decisions.

Example 1: Calculating Business Impact

Fundamentally, organizations must identify consistent ways to aggregate data related to risk incidents. Business Impact Analysis (BIA) methods typically focus on adding primary and secondary impacts. According to the FAIR model, primary impacts cause direct financial impacts to the organization from a loss event, while secondary impacts typically occur later from the reactions of outside parties [Maze 2020].

An example of these impacts is when several organizations compiled the impact of the CrowdStrike Falcon incident from July 2024 to be approximately \$5 Billion [Parametrix 2024]. Unfortunately, the secondary effects related to subsequent litigation, claims, loss of reputation, and other unforeseen outcomes may not be known entirely for years to come. However unfortunate, significant events such as this one provide use cases and an appreciation of the costs related to addressing cyber disruptions.

Through its work with organizations in the financial sector, CERT has developed novel methods to assess organizations, and facilitate and glean relevant information for FAIR assessments. CERT encourages risk managers to use related event data to inform their risk analyses and decision making. Further, organizations that have not suffered similar events may leverage use-case impact data to calculate their potential losses compared to their security stack costs to determine a reasonable ROSI.

Example 2: Dynamically Calculating Risk Exposure

As a strategic example, an organization may want to dynamically measure and calculate risk exposure on a given computer or communications network. In this example, the organization may want to make network connections across various assets from allied countries as well as third-party providers. The application of an ROSI calculation in that environment may inform mission planners so that they may optimize mission effectiveness given specific security considerations. The benefit calculation in this example may not specifically link back to a monetary return as a benefit. This points to another research consideration in weighing the use of ROSI.

Example 3: Prioritizing CPGs within an Organization

CERT recognizes the value of good cyber hygiene practices suggested by United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Specifically, CISA published the *Cross-Sector Cybersecurity Performance Goals (CPGs)* [CISA 2025]. The CISA CPG checklist does not directly point to ROSI within its structure.

However, CISA utilizes three specific rating measures: cost, impact, and complexity [CISA 2023]. At this point, those measurements adequately conceptualize the value and ranking of implementing each performance goal. An organization implementing those goals could use those ratings as a qualitative means of prioritizing one set of controls or practices over others. For example, if one CPG has a four dollar sign rating of cost and a low rating for impact, then an organization may prioritize the implementation of other CPGs with fewer dollar signs and higher impact.

Example 4: Prioritizing CPGs Across Organizations

CERT has partnered with CISA and other organizations to develop specific definitions for qualification and some quantification of three measurements (i.e., cost, impact, complexity) so that they may provide greater fidelity in risk-based decision making. Suppose that “impact” is the value realized through proper deterrence, avoidance, or resistivity from cyber attacks affected by a CPG, and “cost” is defined as the total sum of resources invested in implementing that CPG. The ratio of the impact and cost would yield a ROSI for that CPG.

Organizations could leverage the cost-benefit analysis of many controls to quantitatively identify their best options and priorities for resource allocation in CPG implementation. Not to be forgotten, complexity measurements could serve as a “tiebreaker” if cost and impact values are too close for proper judgement.

CERT aspires and has been working to develop the ideal means to quantify these measures in a standardized and consistent manner. If standardized to a satisfactory degree, then CPGs could be prioritized across entire sectors. Organizations may vary in their decisions based on their risk appetite. However, the benchmarking could be beneficial for smaller organizations that struggle with limited resources.

Furthermore, CERT has considered utilizing specific quantitative measures for ROSI to understand the compound benefits of using multiple CPGs at one time as opposed to others.

Finally, this same principle of establishing a standardized ROSI calculation may be extended across other control regimes and standards. For example, Defense Industrial Base organizations may use standardized ROSI calculations to prioritize Cybersecurity Maturity Model Certification (CMMC) requirements for protecting Controlled Unclassified Information (CUI) [DoW 2025].

Example 5: Calculating Risks to Assets

Traditionally, some programs may struggle with not being a revenue-generating function. To deal with this challenge, security teams must focus on the value of information assets targeted by threat actors by reviewing, for example, intellectual property assets recovered. Some other programs may reflect on and collect data about program effectiveness related to the number of security events compared to those that manifest as incidents that require action.

Similarly, costs may gain greater fidelity as asset evaluations improve. Marketing teams and industry surveys may support these estimates. Costs may include employee wages combined with benefits and overhead. Tool purchases and maintenance costs should be carefully tracked throughout the lifecycle of a security asset. Finally, reliance on third-party providers should be monitored and reviewed regularly to determine whether contract terms and conditions are met in accordance with spending.

Future Perspective

Once the definition and quantification of ROI are standardized, CERT plans to take ROI calculations to yet another level of innovation by using them in a model designed for risk-based decision making. Specifically, a future ROI consideration may include utilizing artificial intelligence (AI) and machine learning (ML). Specifically, organizations could use ROI data to train models to properly respond to risk incidents. For example, suppose an incident takes place, the AI or ML system may have a sufficient data repository and training to identify the need for making configuration changes or selecting and implementing a new cybersecurity tool to alleviate current incidents and avoid future events.

Conclusion

CERT aspires to improve measurements of cost and impact to make informed risk-based decisions using ROSI. Research and development are necessary to refine the calculation of risk impacts across the cybersecurity risk community. Methodologies exist; however, improvements must be identified to streamline and standardize the ROSI process as much as drive economy into the computation. CERT aspires to evolve the utility of the ROSI calculation to connect executive direction to technological decisions. Risk appetite statements, for example, could relate the capacity for loss in terms expressed as dollars in revenue.

References

[Boehm 2019]

Boehm, J. et al. The Risk-Based Approach to Cybersecurity. *McKinsey & Company Website*. October 8, 2019. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/>

[CISA 2023]

Cybersecurity and Infrastructure Security Agency (CISA). CISA CPG Checklist Version 1.0.1. *CISA Website*. March 2023. https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

[CISA 2025]

Cybersecurity and Infrastructure Security Agency (CISA). Cross-Sector Cybersecurity Performance Goals. *CISA Website*. October 3, 2025 [accessed]. <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

[DoW 2025]

Department of War (DoW) Chief Information Officer. About CMMC. DoW. October 3, 2025 [accessed]. <https://dodcio.defense.gov/cmmc/About/>

[ENISA 2012]

European Network and Information Security Agency (ENISA). Introduction to Return on Security Investment. ENISA. 2012. <https://www.enisa.europa.eu/sites/default/files/publications/Return%20On%20Security%20Investment.pdf>

[FAIR 2025]

FAIR Institute. Prepare for the Future of Digital Risk. *FAIR Institute Website*. October 3, 2025 [accessed]. <https://www.fairinstitute.org/>

[FINRA 2024]

Financial Industry Regulatory Authority, Inc. (FINRA). Calculating Your Investment Returns. *FINRA Website*. December 4, 2024. <https://www.finra.org/investors/insights/investment-returns>

[Kambic 2020]

Kambic, D. J. et al. Loss Magnitude Estimation in Support of Business Impact Analysis. CMU/SEI-2020-TR-008. Carnegie Mellon University, Software Engineering Institute. 2020. <https://www.sei.cmu.edu/library/loss-magnitude-estimation-in-support-of-business-impact-analysis/>

[Maze 2020]

Maze, T. & Musselwhite, D. Primary vs. Secondary Loss in FAIR™ Analysis: What's the Difference and Why It Matters [blog post]. *FAIR Institute Blog*. May 19, 2020. <https://www.fairinstitute.org/blog/primary-vs.-secondary-loss-in-fair-analysis-whats-the-difference-and-why-it-matters>

[NASEM 2025]

National Academies of Sciences, Engineering, and Medicine (NASEM). *Cyber Hard Problems: Focused Steps Toward a Resilient Digital Future*. National Academies Press. 2025. ISBN: 10.17226/29056. <https://nap.nationalacademies.org/catalog/29056/cyber-hard-problems-focused-steps-toward-a-resilient-digital-future>

[Parametrix 2024]

Parametrix Solutions, Inc. CrowdStrike's Impact on the Fortune 500: An Impact Analysis. Parametrix. 2024. <https://www.parametrixinsurance.com/crowdstrike-outage-impact-on-the-fortune-500>

Legal Markings

Copyright 2025 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Requests for permission for non-licensed uses should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM25-0785

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479

Web: www.sei.cmu.edu

Email: info@sei.cmu.edu