

Frequently Asked Questions (FAQ)

Contents

Introduction	1
General.....	2
Mergers and Acquisition (M&A).....	4
Federal Contractors.....	5

Introduction

This is a list of Frequently Asked Questions (FAQ) about SecuriThink Step Zero, a field-tested cyber tool for business decision-makers which provides a financial estimate of the cost to achieve a cybersecurity stance reasonable for both risk management and most compliance requirements.

For publicly held companies, most of the inputs are publicly available data. The report can often be generated in 72 hours rather than weeks or months for typical methods.

Forged in Mergers and Acquisitions (M&A), this report is wielded by Compliance for data-driven decisions with a verified level of accuracy.



- Shift Cybersecurity estimate left
- Avoid buyer’s remorse
- Know spend and schedule
- Minimal sunk costs



Early schedule and estimates support a faster, data-driven decision

General

Q: Why is the Report called “Step Zero”?

A: The typical approach to develop a cost estimate for a cybersecurity project begins with a Gap Analysis. This is traditionally Step One.

The report is called “Step Zero” because it happens before Step One.

It delivers an early financial estimate with a verified level of accuracy to support a data-driven business decision.

Q: What is included in a Step Zero report?

A: Estimates

- One time spend and recurring costs
- Spend detail by timing intervals to support financial forecasts
- Spend detail to support expense versus capital cost forecasts
- Spend detail by typical project milestones
- Project duration

Verified Accuracy

- Based on 12 Fortune 500 deals estimated over 8 years
- Several deals were tracked to completion (14-36 months later) to verify the range of accuracy of the original estimate

Q: What costs does a Step Zero report cover?

A: Step Zero includes all the costs for Step 1 (Gap Analysis), Step 2 (Design & Plan), Step 3 (Execute), and recurring costs.

Step Zero is a rapid estimate of the cost to achieve and maintain a foundational level of cybersecurity.

It assumes a pragmatic level of cybersecurity which:

- Meets the requirements currently in many customers’ contracts
- Satisfies most regulations
- Demonstrates sound practices to satisfy cyber insurance policy underwriters
- Includes just enough policies and procedures to support repeatable processes and fundamental technical controls
- Gives a level of overall business risk reduction that buys time to decide if even more security has enough value for business goals or if that’s hitting diminishing returns

Q: What is not included in a Step Zero report?

A: Step Zero is specifically engineered to accomplish three things: speed, verified accuracy, and cybersecurity estimates for both cost and schedule. It does not include advanced protections (e.g., protection against Advanced Persistent Threats (APT), zero trust architecture, secure by design culture).

Since scoping is a critical success factor, further details are part of the Step Zero report which can be previewed by qualified clients under our confidentiality agreement.

Q: The Step Zero process focuses on bringing the target organization to a pragmatic level of cybersecurity. How is that measured?

A: A 5-point maturity scale is widely used; an organization can pick a framework and apply it. The SecuriThink team has experience with the Gartner IT Score which is based on the Capability Maturity Model Integration (CMMI) framework.

[Read more about the Step Zero cybersecurity maturity target here.](#)

Q: How is the accuracy of a Step Zero Report verified?

A: Step Zero was forged by a Chief Information Security Officer (CISO) who had ultimate accountability for the cybersecurity gap no matter what the estimate said; he was highly motivated to be accurate.

Verification is based on 12 Fortune 500 Mergers and Acquisitions (M&A) deals over a period of 8 years with several deals closely tracked to completion 14-36 months later. Having tracked the results over a long period and leveraging our insider's access to real data to get past the post-deal tendency to over- or under-report costs, this judicious follow through to verify accuracy is a unique dimension of the Step Zero capability.

With more information, or "Black Box Plus" option for inputs, we expect higher accuracy but do not offer a specific confidence interval. Meticulous data collection over long duration projects is difficult to impossible without insider access to time and cost-tracking systems.

Q: How can you know what the schedule is going to be when we don't know when we can begin?

A: The estimate is of project duration. For M&A the start date is usually when the deal closes. In general, the start date is when the gap analysis (Step One) begins.

Q. How does the accuracy of the Step Zero Report compare to what the typical process provides?

A: In our experience accuracy of the resource estimate improves with progressive phases. Accuracy can be expected to improve as shown in the table below. We share the verified accuracy of Step Zero with qualified customers under a Non-Disclosure Agreement

Phase	Activity	Rough Order of Magnitude (ROM) Accuracy
Step One	Gap Analysis	No budget information
Step Two	Plan & Design	+/- 20 %
Step Three	Execute	+/- 10 - 15 %

Q: For what kinds of companies does Step Zero apply?

A: Step Zero was created and its accuracy verified in Engineering and Manufacturing organizations ranging in headcount from 50 to 12,000

Q: What are the inputs to a Step Zero Report

A: Black Box option – is a handful of parameters which, for a public company are usually publicly available
Black Box Plus option – adds another handful of parameters

Q: What is the client level of effort to gather the inputs for Step Zero?

A: Black Box option – 1 hour or less
Black Box Plus option – 1-3 hours

Q: How can you generate a Step Zero Report with so few inputs?

A: Our decades of extensive experience with Steps 1, 2, and 3 coupled with judicious tracking of 12 M&A deals from transaction to transformation allows us to provide estimates with a known range of accuracy.

Q. Why do business decision-makers need a cyber tool?

A. Cybersecurity risk has new and costly implications for a growing number of business decisions as both regulations and customer contractual requirements for cybersecurity are rapidly increasing in addition to the ever-changing criminal threat landscape.

Some of the greatest urgency is driven by the U.S. Department of Justice (DOJ) Civil Cyber Fraud Initiative (CCFI) to prosecute gaps with existing requirements and the strong resolve signaled by Department of Defense (DoD) rulemaking

to certify compliance with their existing contractual requirements (Cybersecurity Maturity Model Certification or CMMC). The DoD is taking the lead while many other federal agencies are watching closely; the mandate to protect Controlled Unclassified Information (CUI) is government-wide.

An example of a broader trend is the Securities Exchange Commission (SEC) adoption of new rules effective September 2023 for cybersecurity risk management, strategy, and governance in public companies.

Q: How is a Step Zero Report used?

A:

Business decision for cybersecurity	Where does the Step Zero Report offer leverage?
Mergers and Acquisitions (M&A)	Screening targets, the negotiation process, and planning integration
Protecting company value	Data-driven decisions for resource allocation relative to threats, regulations, or customer-driven contractual requirements
Owner exit planning	Timing the harvest of current value or investments to protect future value
Accepting customer contract terms	Balance cost of increasing cyber requirements versus profit
Compliance decisions	Data-driven basis to choose the standards worth investment
Insurance & Risk management	Balance insurance (i.e., risk transfer) vs. cost of risk mitigation
Underwriting Representations and Warranty Insurance (RWI)	Quantify cyber business and compliance risk in financial terms
Lending, especially highly regulated, highly threatened organizations	Quantify cyber business and compliance risk in financial terms

Q: What materials are publicly available about Step Zero?

What’s available if a Non-Disclosure Agreement (NDA) is in place?

A: Step Zero™ Publicly Available Materials

- SecuriThink.com website
- Value Proposition one pager
- Frequently Asked Questions (FAQ) = this document
- Presentation from / discussion with a SecuriThink advisor

Step Zero™ Materials under NDA

- Guided tour of NDA materials
- Input description
- Report Template
- Report Authorization Form

Q: Why has Step Zero not been available until now?

A: Step Zero originated as the solution to a problem confronting a Fortune 500 company. The approach was initially used only inside that company until all Step Zero practitioners became free agents.

Mergers and Acquisition (M&A)

Q: How does Step Zero address the buyer risks associated with M&A?

A:

- *Prepare to hit the ground running as soon as the deal closes.* An honest gap analysis (Step One) is nearly impossible before the close date, making the known accuracy and advance delivery of the Step Zero report an ultimate edge.

Step Zero identifies the resources needed on day one and for all that follow so all the business and technology stakeholders can align. Avoid losing time to close the inevitable gaps a smaller, less mature company brings because this is also a jump start for Step One toward execution.

- *Engage business decision-makers with the big picture.* Step Zero provides a top-down outline to avoid the drip, drip, drip water-torture business leaders complain about when resource requirements are built from the bottom up during Steps 1, 3 and then 3. With one report, you can address the costs for closing the security gaps at the same time as regulatory and customer contract gaps to avoid penalties or lost contract opportunities
- *Avoid being a day late and a dollar short.* Without Step Zero, you start justifying the resources to begin after the deal closes

Q: How often has the Step Zero cost estimate killed a Mergers and Acquisitions (M&A) deal?

A: Never. It has informed a new price point in some cases. When deals have fallen through, it has never been due to the cost of cybersecurity.

Q: How does Step Zero address due diligence?

A: Step Zero estimates the cost of both due diligence and mitigation.
Step Zero is not a substitute for due diligence; it plans for and increases the likelihood of proper due diligence

Q: How is Step Zero different from Bitsight, Black Kite, UpGuard, etc.?

A: These services provide a cybersecurity risk score based on the security posture (e.g., vulnerabilities, misconfigurations) of the company's Internet-facing systems and dark web data. They provide a gauge of how "hackable" are the Internet facing systems of a company.

In comparison, Step Zero gives a financial estimate of what investments are needed to bring the company's overall security posture, not just the Internet-facing systems, to a practical level.

Federal Contractors

Q: Is the DoD SPRS* Score a deliverable of Step Zero?

A: The calculation of this score is not actually performed during Step Zero; the Step Zero estimate includes this task, if required, to be done during Step One, the Gap Analysis Phase

*A Supplier Performance and Risk System (SPRS) score must be calculated using Department of Defense Assessment Methodology (DoDAM) as required by federal contracts with a DFARS 252.204-7012 and -7019 clause

Q: How does Step Zero apply to CMMC* Level 3?

A:

- Step Zero answers the question: "How much will it cost my organization to meet CMMC Level 2 requirements?"
- It focuses on the cost of implementation of the requirements. It does not include the cost of preparing for a CMMC assessment such as gathering evidence and doing dress rehearsals with relevant staff, nor the cost of the assessment by a CMMC Third Party Assessment Organization (C3PAO)

*CMMC = Cybersecurity Maturity Model Certification

Q. Step Zero was created for Mergers and Acquisitions (M&A); why is it relevant to CMMC*?

Step Zero was forged in an environment where the Department of Defense (DoD) was the primary customer driving cybersecurity contract requirements. While the Fortune 500 organization which inspired this approach was itself meeting DoD requirements, as it continued to acquire new companies that were less prepared, Step Zero was forged specifically to measure the costs to close the cybersecurity gap of each new acquisition target. Step Zero was forged by M&A yet it's a powerful tool to be wielded by compliance.

*CMMC = Cybersecurity Maturity Model Certification

Q: How is a Step Zero Report different from a vendor proposal, such as one from a Managed Services Provider (MSP)?

A: Even the most comprehensive MSP has a Shared Responsibility Matrix (SRM). There are some responsibilities that always fall to your organization.

Step Zero was created to address *all* the costs your organization incurs during Steps 1, 2, 3 *and* recurring costs; that's both sides of the SRM, not just the part a vendor proposes to do.

Q: What does SecuriThink experience say about the timeline to implement CMMC?

- Across 12 M&A* deals over 8 years, our shortest time to fully implement was 14 months, and some took nearly 36 months
- We have already seen DoD* contracts that specify once CMMC is fully authorized, the existing contract will be subject to the requirement
- The DoD is demonstrating strong resolve by CMMC rulemaking in both part 32 and part 48 of the CFR*
- Given DoD statements of intent combined with research available on typical time intervals for rulemaking, we believe organizations that do not want to risk losing DoD contracts due to CMMC should already be seriously engaged in implementation

Q: How does Step Zero address CMMC* Level 3?

A: The Step Zero report covers the investment to achieve CMMC Level 2 then SecuriThink advisors have worked with clients on a consulting basis to describe and estimate the work to go beyond Level 2 and achieve Level 3. [While our experience at achieving a level of security maturity comparable to Level 3](#) gives us more background than most consultants to address this question, we make a clear distinction between the verified accuracy of a Step Zero report and our best effort at accuracy as consultants.

*CMMC = Cybersecurity Maturity Model Certification

Q: How does Step Zero address Department of Energy (DOE) cybersecurity requirements?

A: Our experience writing DOE plans for clients has been they have guidance on the general direction and content but are not accountable to implement specific controls; it is up to the organization to decide how much is enough. Step Zero assumes a pragmatic level of cybersecurity which shows due diligence to the DOE while giving a level of overall business risk reduction that [buys time to decide if even more security has enough value for business goals](#) or if that's hitting diminishing returns.



Rapid Cybersecurity Cost Estimates

Forged by M&A, Wielded by Compliance