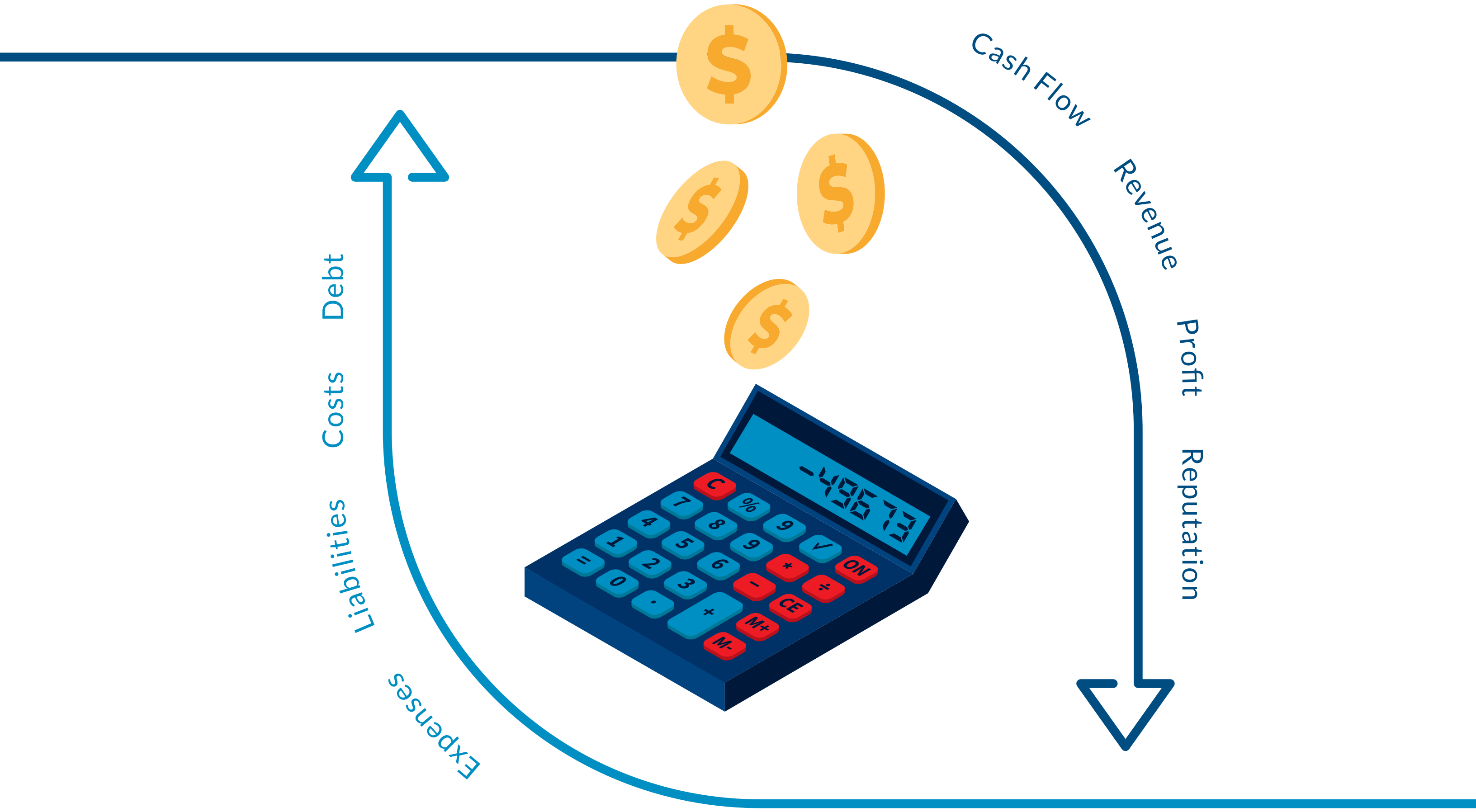
THE NEED TO CONTAIN

Protect your business and reputation during uncertainty, as you see cybersecurity risk differently.

Your template-guided collaboration process to reduce the cost and duration of future loss events.



SPOT-Beam™
by CERTITUDE SECURITY®

EMPOWERMENT TEMPLATE SERIES

Table of Contents

SPOT-Beam Contain Summary PAGE 3

How To Use Your SPOT-Beam Contain Template Package PAGE 4

Baseline: Expense Statement Summary of Operating Expenses PAGE 5

Worksheet 1: Loss Measurement Criteria for Productivity PAGE 6

Worksheet 2 : Loss Measurement Criteria for Replacement PAGE 8

Worksheet 3: Loss Measurement Criteria for Response PAGE 9

Worksheet 4 : Loss Measurement Criteria for Reputation PAGE 10

Worksheet 5 : Loss Measurement Criteria for Fines and Legal PAGE 11

Worksheet 6: Loss Measurement Criteria for Competitive Advant. PAGE 12

Worksheet 7 : Loss Measurement Criteria for Safety and Health PAGE 13

Worksheet 8 : Loss Measurement Criteria for Open Category PAGE 14

Worksheet 9: Impact Area Prioritization PAGE 15

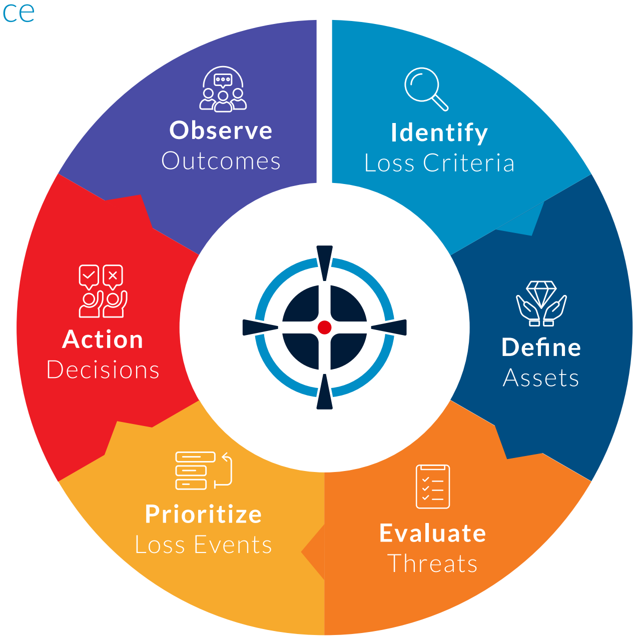
Worksheet 10: Critical Information Asset Profile PAGE 16

Worksheet 11: Information Asset Exposure and Decision PAGE 20

SPOT-Beam™
by CERTITUDE SECURITY®

Protect your business and reputation during uncertainty, as you see cybersecurity risk differently.

Your template-guided collaboration process to reduce the cost and duration of future loss events.



No one takes pride in being second-guessed when criminal attacks cripple your organization. You know security measures need improvement, yet business assets remain exposed. The only way to contain lost revenue and expenses caused by exploited cybersecurity weaknesses is to take decisive action before criminals expose you.

What are the loss implications for you and your company? Misclassified assets and misunderstood threats lead to business disruption events. The effects of cybercrime often spill over from the initial target to stakeholders, magnifying the damage to your business and reputation.

We understand that a useful and practical process is needed to help the team see cyber risk differently. To support your efforts, we created SPOT-Beam Contain to help you. The template process will guide you through steps to make business disruption less severe.

Here's how it works:

1. When you are ready to speak up, purchase and download the PDF pack.
2. Identify and invite the stakeholders into the collaboration process to redefine essential business processes and loss event scenarios.
3. Align team actions with the mission and values of the business to enhance cybersecurity preparedness and customer confidence.

This planning process allows you to quickly write a detailed asset protection plan that you can defend. The fillable built-in PDF templates provide preset structures for stakeholder collaboration and decisive actions. You will improve trust with transparency and shared understanding, and action commitments needed to support your business and customers.

> The CONTAIN process of defining your Specific Points of Truth (SPOT) begins with identifying acceptable loss and ends with observing the outcomes from decisive actions. Decisions include acting on a narrow grouping (Beam) of resource allocations to address asset exposures likely to cause loss events.

This template pack is designed to help you contain lost revenue and expenses from avoidable outages. If your customers will not tolerate your business being offline for weeks or months, then this investment will benefit you.

To protect your business and reputation, implement the template pack. Your aspirations and implications will define your journey and success.

How To Use the SPOT-Beam CONTAIN Template Package

1. Assemble your CONTAIN team.

   Skim through the template pack to identify and invite stakeholders and collaborators into this process. To succeed, your collaboration team must have at minimum five members.

   The number of stakeholders and contributors is essential because larger diverse groups are less prone to groupthink. A five-number summary is helpful in descriptive analyses or during the preliminary investigation of a more extensive data set.

   Significance refers to data sets created not being the result of chance with five or more stakeholders and contributors. The team will evaluate the most extreme values in the data set (the maximum and minimum values), the lower and upper quartiles, and the median decreases the degree of error.

2. Collaboratively complete the Baseline.

3. Initiate the seven or eight loss measurement criteria by completing Worksheets 1-8.

4. Prioritize the forms of loss with Worksheet 9.

5. Begin defining critical information asset profiles with Worksheet 10a-d for each asset.

6. Review the asset profiles and consider the areas of concern, weaknesses, limitations, probability, consequences, and severity using 11a.

   a) Review and prioritize as a group.

   b) Cross-reference the Baseline to identify gaps for weaknesses and areas with duplicate coverage that need reallocating.

7. Provide asset exposure summaries and recommendations for action based on the impact on the business, stakeholders, and customers using associated 11b.

   a) Review and prioritize as a group.

8. The responsible executive will review 11a-b, seek any clarifications, and authorize action of mitigate, accept, defer, or transfer.

When the CONTAIN team completes profiles for all critical assets, the Worksheets become part of your quarterly risk management process to reduce the cost and duration of future loss events.

You will uplevel your actions as you focus on your specific points of truth. Now that you can see how the process fits together, you can create more value. As you implement this repeatable collaboration framework, you will use it to communicate effectively for years.