FISMACS FAIR™ Compliant Model

Contents

CONVENTIONS

TAB Names and **Field Names** are **BOLD.**

Ideas or suggestions on use or implementation have the bulb icon.

Warning use this symbol.

INTRODUCTION

THE STANDARD

The FAIR™ standard is an international model for quantifying cyber risk focused on financial impact. It's widely adopted but the tools needed to use it can be expensive. The difficulty has been sourcing affordable tools for analysts to perform FAIR™ analysis.

That's all changed with the FISMACS FAIR™ Compliant model. It's an Excel-based model that's easy to understand and use, and it's completely FAIR™ compliant.

MEASURING RISK

Risk is a range of possibilities of an event with a negative outcome.

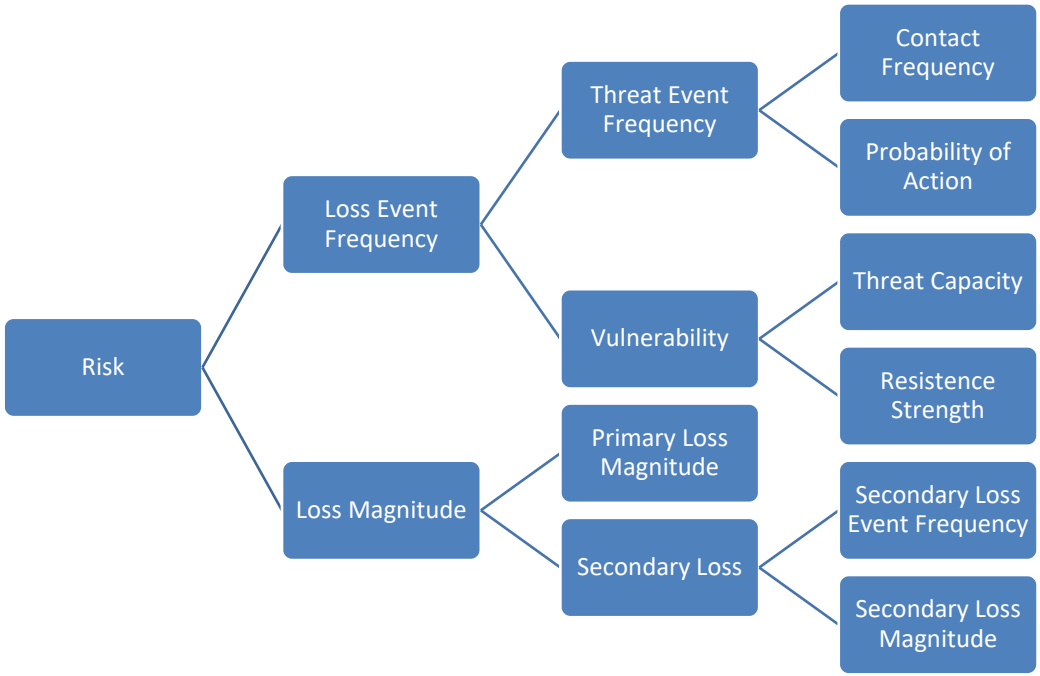
The range is derived from estimating three values; worst-case, most likely, and best-case scenarios.

Multiple factors are considered in development of the risk estimate.

FAIR ™

THE FAIR STANDARD

Fair™ seeks to establish a standard language for describing risk. Here are key terms you need to know.



DEFINITIONS

Risk is the frequency and magnitude of future loss.

Loss Event Frequency is the probable frequency, within a given timeframe, that a threat action will result in a loss.

Contact Frequency is the probable frequency, within a given timeframe, that a threat will come into contact with an asset.

Probability of Action is the probability that a threat will act against an asset once contact has occurred.

Vulnerability is the probability that a threat event will become a loss event.

Threat Capacity is the probable level of force that a threat is capable of applying against an asset.

Resistance Strength is the degree of difficulty faced by the threat agent.

Loss Magnitude is the probable magnitude of a loss resulting from an event.

Primary Loss Magnitude is a primary stakeholder loss that occurs directly as a result of the event.

Secondary Loo is loss that exists due to the potential reaction by secondary stakeholder to the event.

Secondary Loss Event Frequency is the probability that secondary losses will materialize.

Secondary Loss Magnitude is the loss that occurs as a result of secondary stakeholder reaction to the primary event.

THE SIX FORMS OF LOSS

Productivity (primary) reduces an organization's ability to generate its primary value.

Response (primary & secondary) are expenses associated with managing or responding to a loss event.

Replacement (primary) is a capital expense associated with replacing or repairing lost or damaged tangible assets.

Competitive Advantage (secondary) is the loss associated with competitors obtaining and using trade secrets.

Fines & Judgements (secondary) are losses from legal or regulatory actions.

Reputation (secondary) is the loss associated with an external perception of the organization's value or competency dimished..

THE FOUR TYPES OF CONTROLS

The same controls can play different roles across scenarios, or even within a single scenario.

Avoidance Controls seek to prevent threats from coming into contact with assets.

Deterrence Controls seek to deter threats from launching threat events once contact with an asset has been established.

Resistance Controls seek to keep threat events from becoming loss events by hardening assets against the attack.

Responsive Controls limit loss magnitude by detecting or breaking threat actor's contact.

THE FAIR CONCEPTS

FAIR™ utilizes several concepts within the standard and practice. First, risk is a range. That range is worst-case, most likely, and best-case. You could create three estimates, one for each. Or, you could use a Monte-Carlo model with 3-point input generating a probability distribution that covers the full risk range. The three input values are the estimated values of worst-case, most likely, and best-case.

The work that we do with FAIR is an estimate, also referred to as a forecast. Estimates are based on the data available and subject to change as new data is made available. As an analyst you are interested in being accurate, not precise. You cannot be precise when discussing the unknown or uncertainty. You can, however, provide accurate estimates of that uncertainty.

Each module of the FAIR model is a Monte-Carlo simulation producing a probability distribution representing the range of our estimate. Some probabilities are numbers, some are percentages, and some are monetary representations. Probability distributions are mathematically acted upon in accordance with the mathematics of probability.

MODEL OVERVIEW

THE FISMACS FAIR MODEL PROCESS

The FISMACS FAIR model goes beyond the constraints of the FAIR standard and provides additional worksheets to assist in collecting and documenting data in preparation for generating a FAIR compliant analysis.

MODEL COMPONENTS

TABS

There are eleven tabs in the model. Nine are involved in the analysis, one is informational only, and one is for your use in editing results.

The **AboutThisModel** tab is informational only. It presents an image of the main data entry screen and highlights some of the model's capabilities.

There are 11 tabs which are used for data input, analysis, and presenting results.

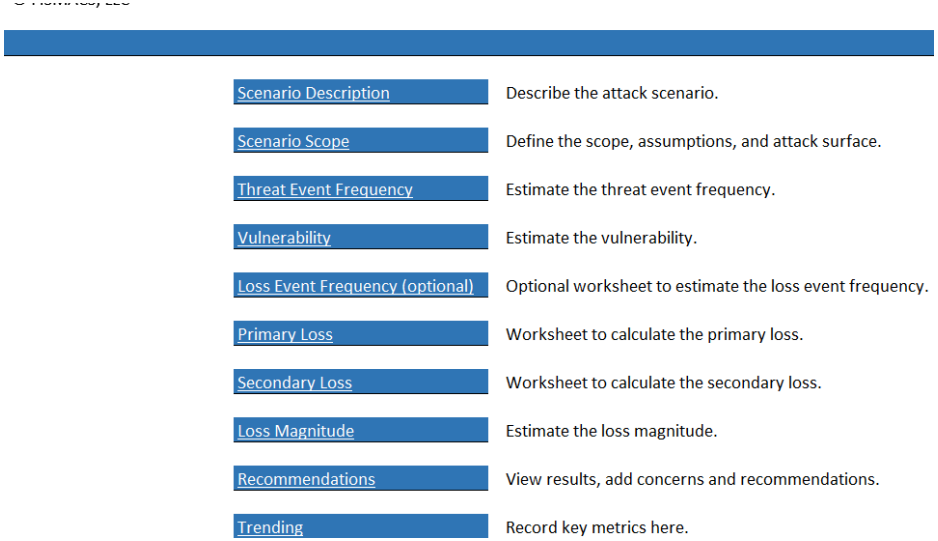
- **Scenario Description**
- **Scenario Scope**
- **Threat Event Frequency**
- **Vulnerability**
- **Loss Event Frequency (Optional)**
- **Primary Loss**
- **Secondary Loss**
- **Loss Magnitude**
- **Recommendations**
- **Trending**
- **Scratchpad**

1 Main Menu

Main Menu Tab contains an easy-to-use menu for navigating the model. It is organized in sequence of typical use.

The menu options are:

- **Scenario Description**
- **Scenario Scope**
- **Threat Event Frequency**
- **Vulnerability**
- **Loss Event Frequency (Optional)**
- **Primary Loss**
- **Secondary Loss**
- **Loss Magnitude**
- **Recommendations**
- **Trending**
- **Scratchpad**



2 Scenario Description

FISMACS, LLC
Modeling Cyber Risk

Scenario Description

Steps:

1. Enter the name of this analysis in row 7.
2. Enter the description of the analysis in rows 11-17.
3. Click Next.

Home | Next

Analysis Name
Software Risk Analysis

Analysis Description
We are most concerned with a data breach. Our product manages client data including network management and vulnerability data. We employ industry best practices.

3 Scenario Scope

FISMACS, LLC
Modeling Cyber Risk

Scenario Scope

Steps:
1. Enter the analysis scope in lines 7-8.
2. Enter your assumptions and dependencies in rows 12-16.
3. Enter the attack surface in rows 20-26.
4. Click Next.

Previous | Home | Next

Analysis Scope

Our target client base includes government agencies, defense contractors and mid-size businesses.

Assumptions and Dependencies

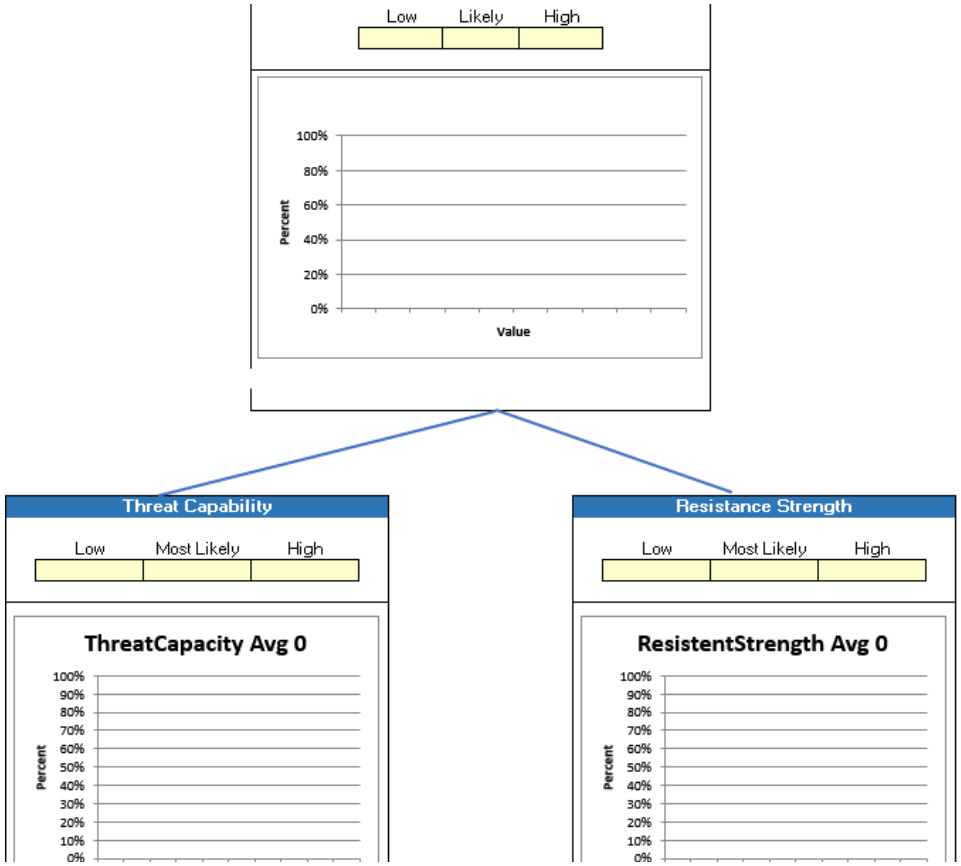
1 Web-facing server operating systems are Microsoft.	6	11
2 Vendor provides frequent updates and patches.	7	12
3 Web-facing server interface utilizes popular components.	8	13
4 Two factor authentication is available for clients.	9	14
5	10	15

Attack Surface

Typical perimeter security is provided including firewalls, intrusion detection systems, application firewalls and proxies, and more. Once authenticated clients have access to their application suite and data which is on a shared infrastructure with best practices in place for security.

4 Threat Event Frequency

5 Vulnerability



6 Loss Event Frequency (Optional)

7 Primary Loss

Response	Replacement	Productivity
$0.00	$0.00	$0.00

Response Cost Calculation						
Title/Role	Hrs #	Wage $	Total	Notes		
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
			$0.00			
				Min -15%	ML	Max +15
	TOTAL		$0.00	$0.00	$0.00	$0.00

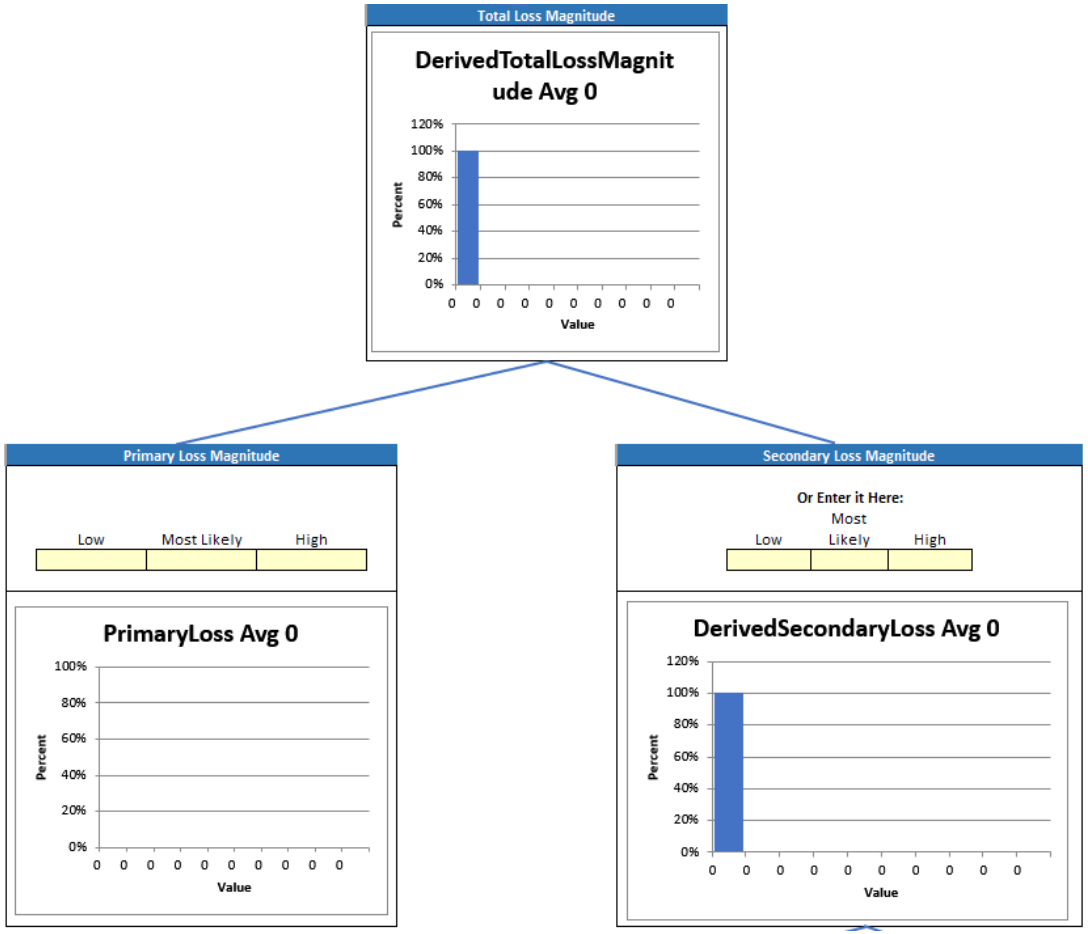
8 Secondary Loss

ines & Fees	Reputation	Competitiveness
$0.00	$0.00	$0.00

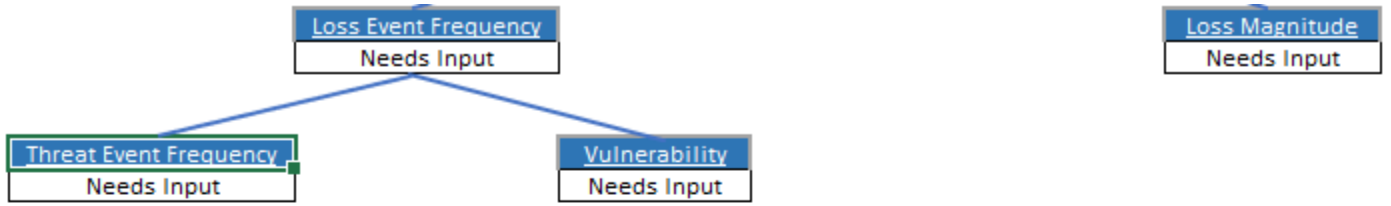
Fines & Fees Calculation				
Title/Role	Hrs #	Wage $	Total	Notes
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	
			$0.00	

		Min -15%	ML	Max
TOTAL	$0.00	$0.00	$0.00	$0

9 Loss Magnitude



10 Recommendations



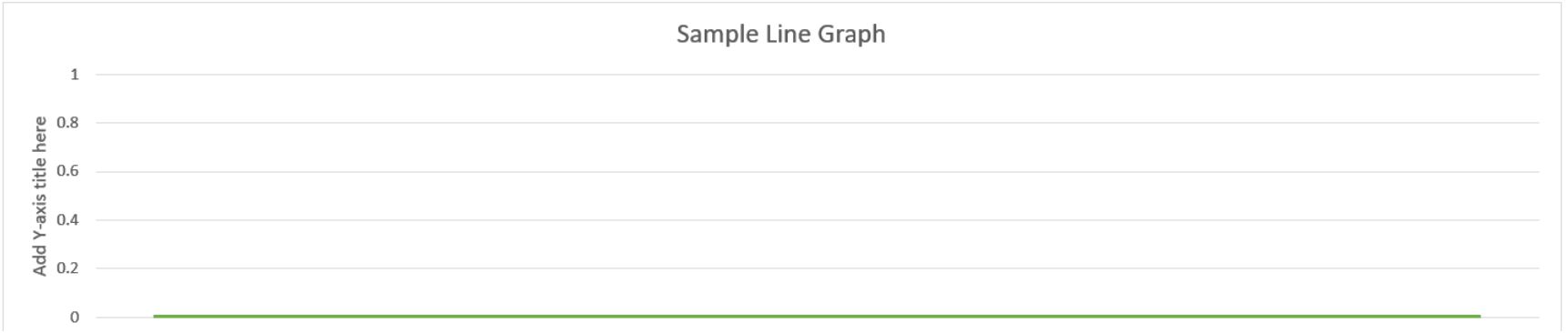
Concerns

Recommendations

1
2
3
4
5

11 Trending

Metric												



12 Scratchpad

The Scratchpad is a flexible work area provided to support editing charts and graphs. It is recommended to copy charts and graphs, whether edited or not, and save each as an image for use in reports and briefings. Charts and graphs are dynamic and will change each time data is updated, or tag categories are selected. Saving charts and graphs as images allows you to capture each iteration in a series.