Open Group Guide

Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at www.opengroup.org/library.

Open Group Guide

Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation

ISBN: 1-947754-07-2

Document Number: G181

Published by The Open Group, January 2018.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 550 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The Open Group aims to:

- Capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Open Group Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

This Document

This document is The Open Group Guide to Open FAIR™ Tool with SIPmath™ Distributions. It has been developed and approved by The Open Group.

This document defines the algorithms that can be used to produce an acceptable implementation of the Open FAIR™ Risk Analysis (O-RA) standard, a standard of The Open Group. The Open FAIR Risk Analysis Tool is the basis for developing this document.

Trademarks

ArchiMate®, DirecNet®, Making Standards Work®, OpenPegasus®, Platform 3.0®, The Open Group®, TOGAF®, UNIX®, UNIXWARE®, X/Open®, and the Open Brand X® logo are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, EMMM™, FACE™, the FACE™ logo, IT4IT™, the IT4IT™ logo, O-DEF™, O-PAS™, Open FAIR™, Open Platform 3.0™, Open Process Automation™, Open Trusted Technology Provider™, SOSA™, the Open O™ logo, and The Open Group Certification logo (Open O and check™) are trademarks of The Open Group.

Microsoft® and Excel® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

SIPmath™ is a trademark of ProbabilityManagement.org.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this Guide:

- Christopher Carlson, Lead Author
- Sam Savage, Danny O'Neil, and Mike Jerbic for creating the model
- Members of The Open Group Security Forum for their review
- John “Jay” Spaulding, Director of The Open Group Security Forum

Referenced Documents

The following documents are referenced in this Guide.

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- Calculating Uncertainty: Probability Management with SIP Math, John Mark Thibault (ISBN: 1490947310), February 2013
- Risk Analysis (O-RA), an Open Group Standard (C13G), October 2013, published by The Open Group; refer to: www.opengroup.org/library/c13g
- Risk Taxonomy (O-RT), Version 2.0, an Open Group Standard (C13K), October 2013, published by The Open Group; refer to: www.opengroup.org/library/c13k

The following sources provide additional information:

- ProbabilityManagement.org (see probabilitymanagement.org)
- The Metalog Distributions (see www.metalogdistributions.com)

1 Introduction

This document defines the algorithms that can be used to produce an acceptable implementation of the Open FAIR™ Risk Analysis (O-RA) standard, a standard of The Open Group. The Open FAIR Risk Analysis Tool is the basis for developing this document.

The function of the Open FAIR Tool is to perform a quantitative Open FAIR risk analysis as defined in The Open Group Risk Analysis (O-RA) and Risk Taxonomy (O-RT) standards. It leverages the SIPmath™ tools developed by ProbabilityManagment.org[1] and described in the referenced "Calculating Uncertainty: Probability Management with SIP Math".

The Open FAIR Tool has the following characteristics:

- Runs two quantitative risk analyses at a time, based on input for current and proposed state
- Works with data input at any level of the Open FAIR taxonomy
- Uses SIPmath distribution generation tools based on Microsoft® Excel® that produce auditable results: a given set of input always returns the same distribution for every simulation
- Performs analysis for 100 trials (years), with higher values allowed for low-frequency events
- Produces graphs depicting the two results for total risk and chance of exceeding
- Allows user input for currency and units

1.1 Spreadsheet Purpose and Target Audience

The goals of the Open FAIR Tool are:

- Broadly available, low-cost quantitative risk analysis tool
- Supports teaching the Open FAIR model to students and career professionals
- Supports initial, small-scale analyses that can be used by newcomers
- Aimed at:

  — Teachers, students

  — Corporate trainers and their students

  — New analysts, analysts who are performing their first analyses

[1] Refer to probabilitymanagement.org.

1.2 What the Tool Is and Does

The capabilities of the Open FAIR Tool are:

- Quantitative Open FAIR analysis tool implemented in an Excel spreadsheet
- Inputs taken as ranges/distributions:
  - Specified as a distribution and relevant parameters; e.g., normal distribution parameterized as a mean and standard deviation
  - Poisson distribution parameterized as a mean
  - Triangular distribution parameterized as a minimum, most likely, and maximum value
- Outputs taken as simulated outcomes:
  - Monte Carlo analysis
- Performs before/after comparison between a current and proposed project state
- Interactive, standalone – requires no external server/infrastructure in addition to Excel
- Built upon a known, proven statistical engine, SIPmath from ProbabilityManagment.org

1.3 Distributions

The Open FAIR Tool makes extensive use of distributions produced from direct user inputs or calculated from lower-risk factors. These distributions are produced using the SIPmath tools initialized for 100 trials (for example, each trial represents one year). The distribution produced by SIPmath is stored as a column of data – the Stochastic Information Packet (SIP). This data can be used to calculate a summary value, such as an average, and can be used to produce charts such as sparklines. Basic math functions can be performed on SIPs such as multiplying the SIP by a single value, or adding two SIPs producing the sums in each row of the output SIP.

More importantly, however, multiplying two SIPs will produce another SIP based on the lower-level factors, by multiplying each row of the SIP with the other.

2 Algorithms

2.1 Open FAIR Tool Overview

This section describes the quantitative algorithms used to derive factors of risk based on calibrated input or input from lower-level factors. Calculations rely on the use of SIPmath. The algorithm is based on the use of a minimum of 100 trial periods (e.g., years); larger values are needed in cases of low TEF such as natural disasters.

Figure 1 is the Open FAIR risk taxonomy referenced throughout this document.

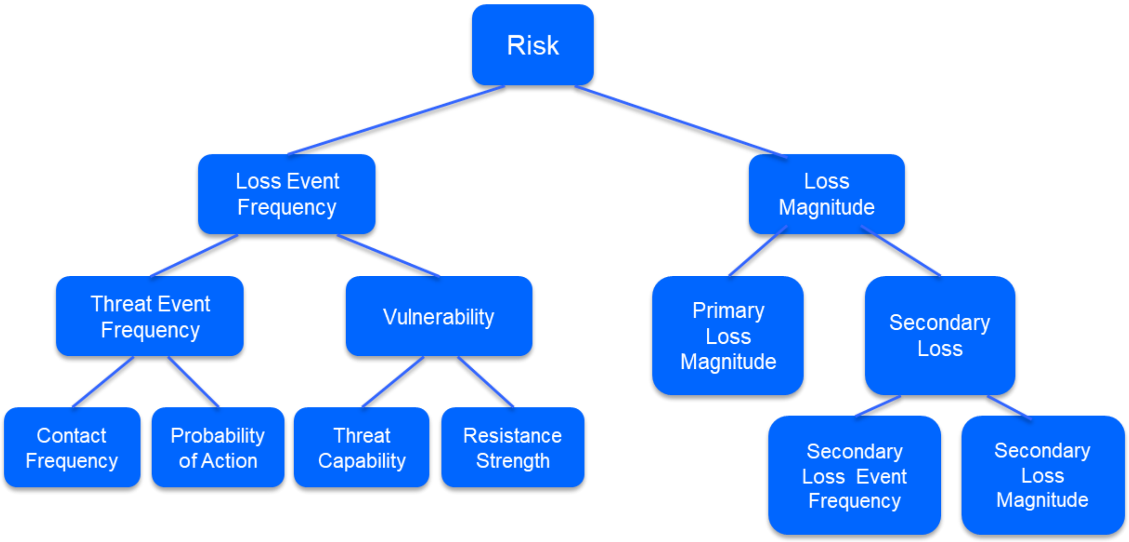


Figure 1: Open FAIR Risk Taxonomy

Data may be input at any level in the taxonomy tree. Data input at a higher level overrides data input at lower levels. For example, data input at TEF overrides a calculated TEF derived from data input into CF and PoA.

The risk analysis result, a SIP containing currency values of total annual loss, can be displayed as a chart. A bar chart of total risk represents bins of annual loss, with height representing probability of occurrence. An exceedance chart shows a declining curve of the probability for annual loss. Similar charts can be used for a single Primary or Secondary Loss, or single total risk (i.e., LEF is set to 1 so that only LM is used in the calculation).

Each of the following sections describes one factor, using the following naming convention:

- Estimate – produce output based on direct user input
- Derive – produce output based only on data in the model

Each section begins with a description in *italics* derived from the risk taxonomy.

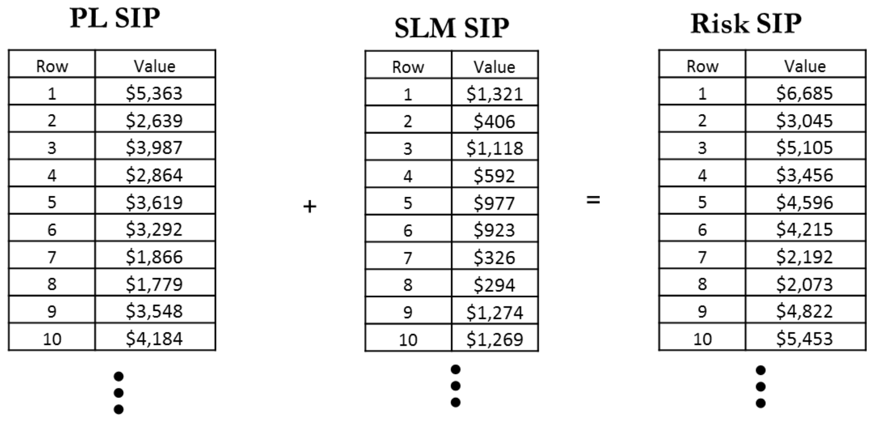
2.2 Derive Risk

Risk estimates the probable frequency and magnitude of future loss (also known as "loss exposure").

Objective Risk for a trial period is the sum of the LMs for all loss events.

The calculation of risk for a trial period (e.g., one year) may represent multiple loss events identified in the LEF SIP. Each loss event has a unique LM.

Risk is calculated as the sum of Primary Loss and Secondary Loss Magnitude. Note that the calculation of Primary Loss and Secondary Loss Magnitude, described below, has already incorporated the values for LEF.



PL SIP

Row	Value
1	$5,363
2	$2,639
3	$3,987
4	$2,864
5	$3,619
6	$3,292
7	$1,866
8	$1,779
9	$3,548
10	$4,184

⋮

+

SLM SIP

Row	Value
1	$1,321
2	$406
3	$1,118
4	$592
5	$977
6	$923
7	$326
8	$294
9	$1,274
10	$1,269

⋮

=

Risk SIP

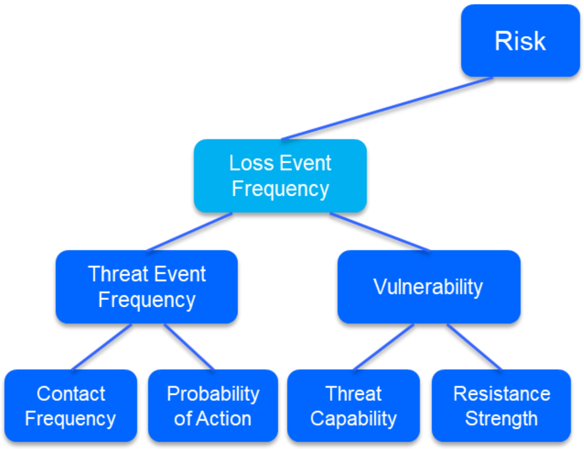
Row	Value
1	$6,685
2	$3,045
3	$5,105
4	$3,456
5	$4,596
6	$4,215
7	$2,192
8	$2,073
9	$4,822
10	$5,453

⋮

2.3 Loss Event Frequency (LEF)

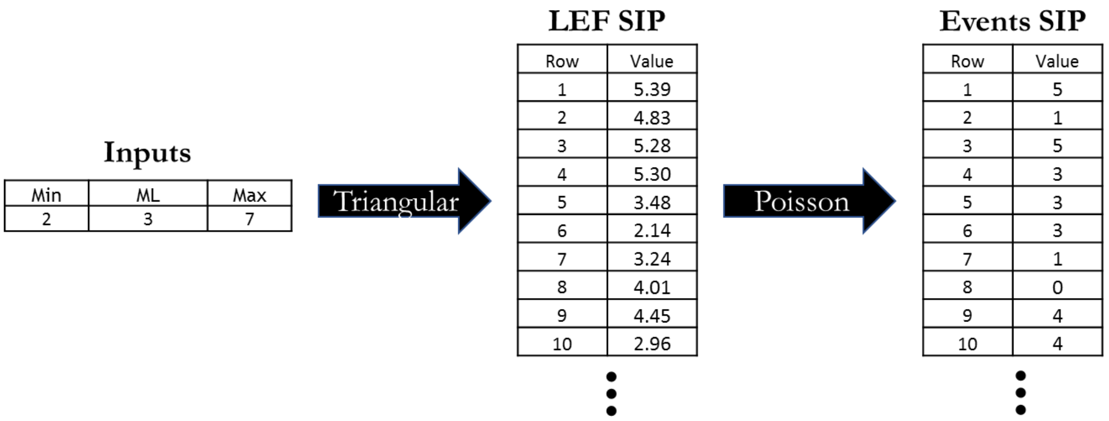
Loss Event Frequency (LEF) is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset. In order for a loss event to occur, a threat agent has to act upon an asset, such that loss results. Probability is always based on a timeframe (event X is 10% likely to occur over the next Y).

Objective Loss Event Frequency is the count of events for the trial period.



2.3.1 Estimate LEF

Develop a calibrated estimated range of LEF values with a 90% confidence interval, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the LEF SIP containing real numbers. The LEF SIP is input to a Poisson distribution to produce the loss events SIP containing integers.



Inputs

Min	ML	Max
2	3	7

LEF SIP

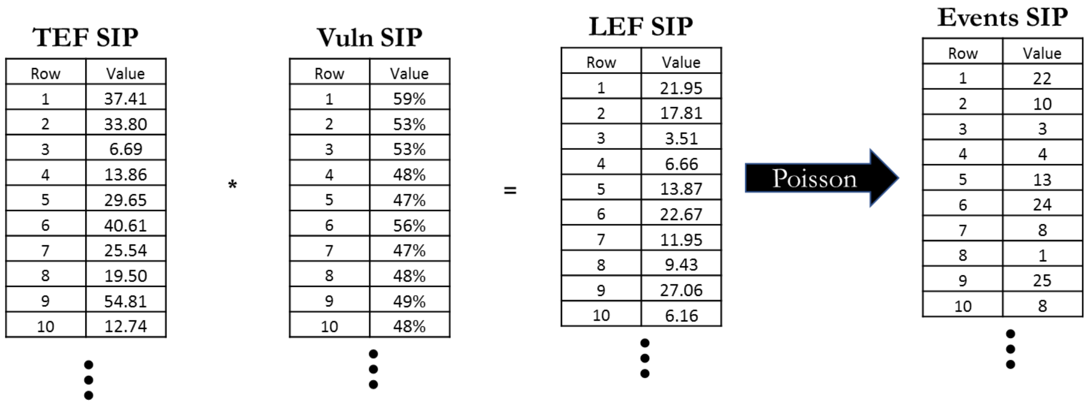
Row	Value
1	5.39
2	4.83
3	5.28
4	5.30
5	3.48
6	2.14
7	3.24
8	4.01
9	4.45
10	2.96

Events SIP

Row	Value
1	5
2	1
3	5
4	3
5	3
6	3
7	1
8	0
9	4
10	4

2.3.2 Derive LEF

The LEF SIP is produced by multiplying the TEF SIP by the value of Vuln – if estimated – or by the value of Vuln from the simulator. The LEF SIP is input to a Poisson distribution to produce the Loss Events SIP containing integers.



TEF SIP

Row	Value
1	37.41
2	33.80
3	6.69
4	13.86
5	29.65
6	40.61
7	25.54
8	19.50
9	54.81
10	12.74

Vuln SIP

Row	Value
1	59%
2	53%
3	53%
4	48%
5	47%
6	56%
7	47%
8	48%
9	49%
10	48%

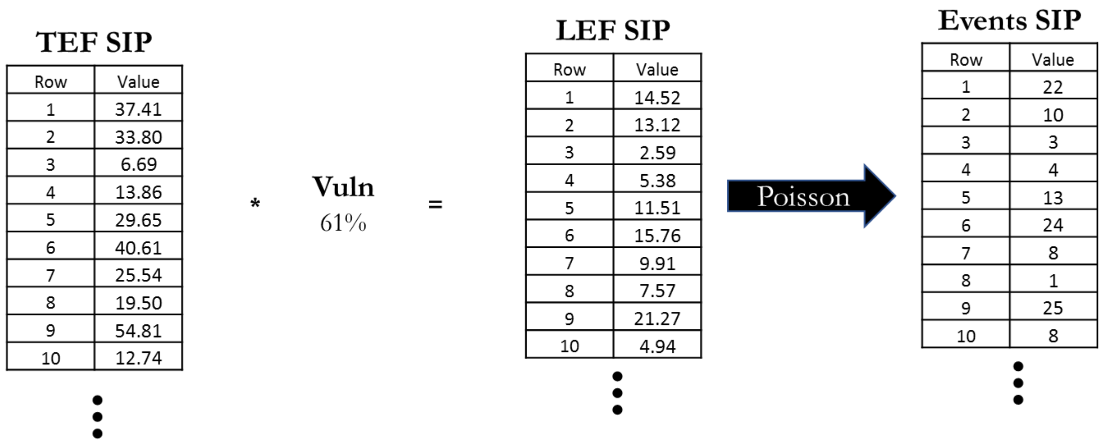
LEF SIP

Row	Value
1	21.95
2	17.81
3	3.51
4	6.66
5	13.87
6	22.67
7	11.95
8	9.43
9	27.06
10	6.16

Events SIP

Row	Value
1	22
2	10
3	3
4	4
5	13
6	24
7	8
8	1
9	25
10	8

Or:



TEF SIP

Row	Value
1	37.41
2	33.80
3	6.69
4	13.86
5	29.65
6	40.61
7	25.54
8	19.50
9	54.81
10	12.74

LEF SIP

Row	Value
1	14.52
2	13.12
3	2.59
4	5.38
5	11.51
6	15.76
7	9.91
8	7.57
9	21.27
10	4.94

Events SIP

Row	Value
1	22
2	10
3	3
4	4
5	13
6	24
7	8
8	1
9	25
10	8

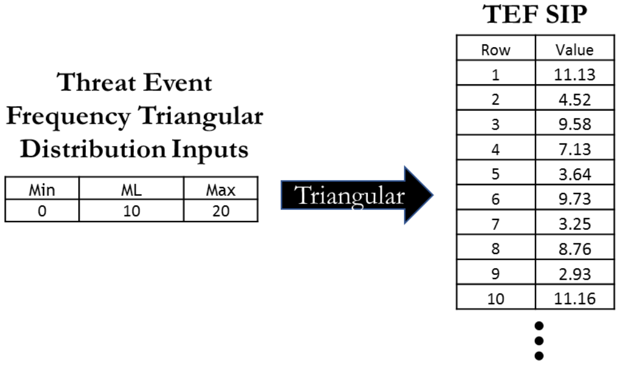
2.4 Threat Event Frequency (TEF)

Threat Event Frequency (TEF) is the probable frequency, within a given timeframe, that a threat agent will act against an asset. Once contact occurs between a threat agent and an asset, action against the asset may or may not take place.

Objective Threat Event Frequency is the count of events for the trial period based on the number of contact events and the chance of success.

2.4.1 Estimate TEF

Develop a calibrated estimated range of TEF values with a 90% confidence interval, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the TEF SIP containing real numbers.



Threat Event Frequency Triangular Distribution Inputs

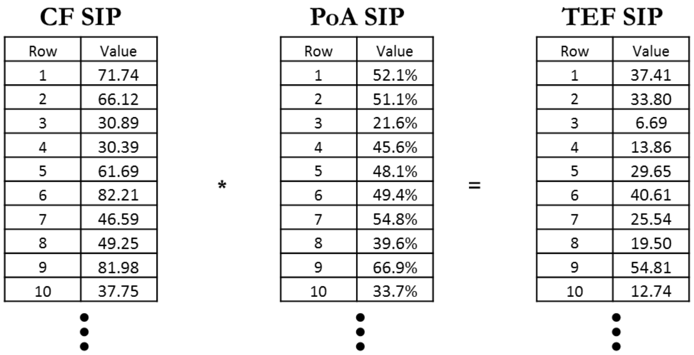
Min	ML	Max
0	10	20

TEF SIP

Row	Value
1	11.13
2	4.52
3	9.58
4	7.13
5	3.64
6	9.73
7	3.25
8	8.76
9	2.93
10	11.16

2.4.2 Derive TEF

The TEF is produced by multiplying the CF SIP by the PoA SIP containing real values.



CF SIP

Row	Value
1	71.74
2	66.12
3	30.89
4	30.39
5	61.69
6	82.21
7	46.59
8	49.25
9	81.98
10	37.75

*

PoA SIP

Row	Value
1	52.1%
2	51.1%
3	21.6%
4	45.6%
5	48.1%
6	49.4%
7	54.8%
8	39.6%
9	66.9%
10	33.7%

=

TEF SIP

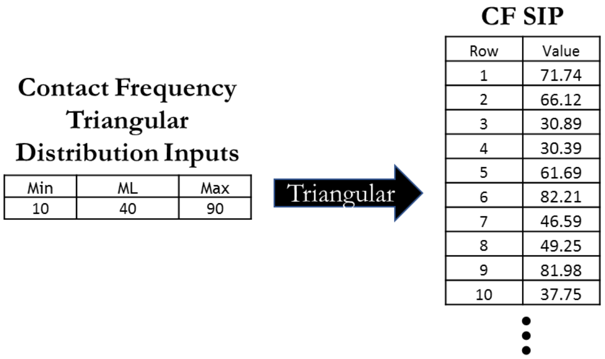
Row	Value
1	37.41
2	33.80
3	6.69
4	13.86
5	29.65
6	40.61
7	25.54
8	19.50
9	54.81
10	12.74

2.4.3 Estimate Contact Frequency (CF)

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

Objective Contact Frequency is the number of contact events in the trial period.

Develop a calibrated estimated range of CF values with a 90% confidence interval for each applicable loss type, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the CF SIP containing real numbers.



Contact Frequency Triangular Distribution Inputs

Min	ML	Max
10	40	90

CF SIP

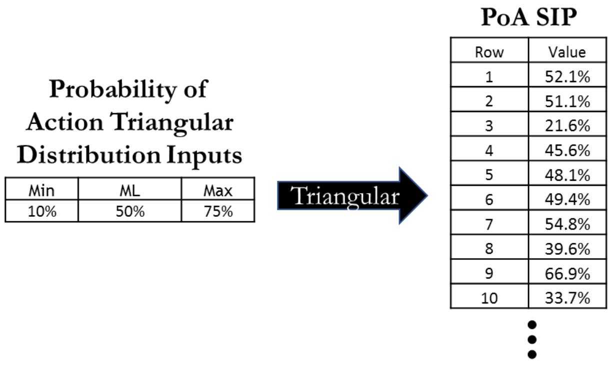
Row	Value
1	71.74
2	66.12
3	30.89
4	30.39
5	61.69
6	82.21
7	46.59
8	49.25
9	81.98
10	37.75

2.4.4 Estimate Probability of Action (PoA)

Probability of Action (PoA) is the probability that a threat agent will act against an asset once contact occurs.

Objective Probability of Action is a probability value for the trial.

Develop a calibrated estimated range of loss values with a 90% confidence interval for each applicable loss type, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the PoA SIP containing real numbers.



Probability of Action Triangular Distribution Inputs

Min	ML	Max
10%	50%	75%

PoA SIP

Row	Value
1	52.1%
2	51.1%
3	21.6%
4	45.6%
5	48.1%
6	49.4%
7	54.8%
8	39.6%
9	66.9%
10	33.7%

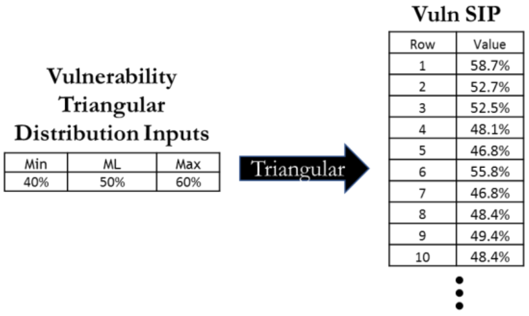
2.5 Vulnerability (Vuln)

Vulnerability (Vuln) is the probability that a threat event will become a loss event. Vuln is determined by comparing RS against the capability of the specific threat … under analysis.

Objective Vulnerability represents the success or failure for a trial based on the comparison of CF and PoA.

2.5.1 Estimate Vulnerability

Develop a calibrated estimated range of Vuln values with a 90% confidence, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the Vuln SIP containing real numbers.



Vulnerability Triangular Distribution Inputs

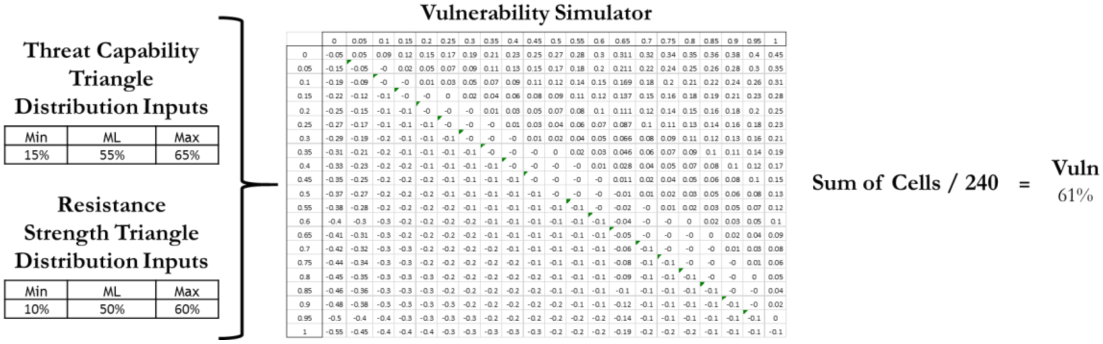
Min	ML	Max
40%	50%	60%

Vuln SIP

Row	Value
1	58.7%
2	52.7%
3	52.5%
4	48.1%
5	46.8%
6	55.8%
7	46.8%
8	48.4%
9	49.4%
10	48.4%

2.5.2 Derive Vulnerability

Produce the value of Vuln by providing the TCap and RS values to the Vulnerability simulator.



Threat Capability Triangle Distribution Inputs

Min	ML	Max
15%	55%	65%

Resistance Strength Triangle Distribution Inputs

Min	ML	Max
10%	50%	60%

Vulnerability Simulator

	0	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95	1
0	-0.05	0.05	0.09	0.12	0.15	0.17	0.19	0.21	0.23	0.25	0.27	0.28	0.3	0.311	0.32	0.34	0.35	0.36	0.38	0.4	0.45
0.05	-0.15	-0.05	-0	0.02	0.05	0.07	0.09	0.11	0.13	0.15	0.17	0.18	0.2	0.211	0.22	0.24	0.25	0.26	0.28	0.3	0.35
0.1	-0.19	-0.09	-0	-0	0.01	0.03	0.05	0.07	0.09	0.11	0.12	0.14	0.15	0.169	0.18	0.2	0.21	0.22	0.24	0.26	0.31
0.15	-0.22	-0.12	-0.1	-0	-0	0	0.02	0.04	0.06	0.08	0.09	0.11	0.12	0.137	0.15	0.16	0.18	0.19	0.21	0.23	0.28
0.2	-0.25	-0.15	-0.1	-0.1	-0	-0	-0	0.01	0.03	0.05	0.07	0.08	0.1	0.111	0.12	0.14	0.15	0.16	0.18	0.2	0.25
0.25	-0.27	-0.17	-0.1	-0.1	-0.1	-0	-0	-0	0.01	0.03	0.04	0.06	0.07	0.087	0.1	0.11	0.13	0.14	0.16	0.18	0.23
0.3	-0.29	-0.19	-0.2	-0.1	-0.1	-0.1	-0	-0	-0	0.01	0.02	0.04	0.05	0.066	0.08	0.09	0.11	0.12	0.13	0.16	0.21
0.35	-0.31	-0.21	-0.2	-0.1	-0.1	-0.1	-0.1	-0	-0	-0	0	0.02	0.03	0.046	0.06	0.07	0.09	0.1	0.11	0.14	0.19
0.4	-0.33	-0.23	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0	-0	-0	-0	0.01	0.028	0.04	0.05	0.07	0.08	0.1	0.12	0.17
0.45	-0.35	-0.25	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0	-0	-0	-0	0.011	0.02	0.04	0.05	0.06	0.08	0.1	0.15
0.5	-0.37	-0.27	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0	-0	-0	-0.01	0.01	0.02	0.03	0.05	0.06	0.08	0.13
0.55	-0.38	-0.28	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0	-0.02	-0	0.01	0.02	0.03	0.05	0.07	0.12
0.6	-0.4	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.04	-0	-0	0	0.02	0.03	0.05	0.1
0.65	-0.41	-0.31	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.05	-0	-0	-0	0	0.02	0.04	0.09
0.7	-0.42	-0.32	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.06	-0.1	-0	-0	-0	0.01	0.03	0.08
0.75	-0.44	-0.34	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.08	-0.1	-0.1	-0	-0	-0	0.01	0.06
0.8	-0.45	-0.35	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.09	-0.1	-0.1	-0.1	-0	-0	0	0.05
0.85	-0.46	-0.36	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0	-0	0.04
0.9	-0.48	-0.38	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.12	-0.1	-0.1	-0.1	-0.1	-0.1	-0	0.02
0.95	-0.5	-0.4	-0.4	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.14	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	0
1	-0.55	-0.45	-0.4	-0.4	-0.4	-0.3	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.19	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1

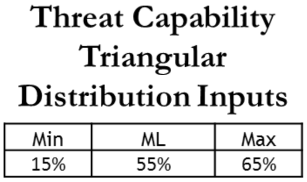
Sum of Cells / 240 = Vuln 61%

2.5.3 Estimate Threat Capability (TCap)

Threat Capability (TCap) is the probable level of force that a threat agent is capable of applying against an asset.

Objective Threat Capability is a percentage value for a trial.

Estimate the minimum, most likely, and maximum values for the probable level of force for the threat agent.



Threat Capability Triangular Distribution Inputs

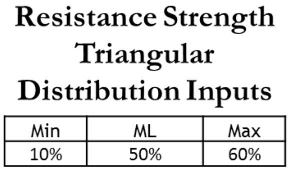
Min	ML	Max
15%	55%	65%

2.5.4 Estimate Resistance Strength (RS)

Resistance Strength (RS) is the strength of a control as compared to a baseline measure of force.

Objective Resistance Strength is a percentage value for a trial.

Estimate the minimum, most likely, and maximum values for the strength of a control.

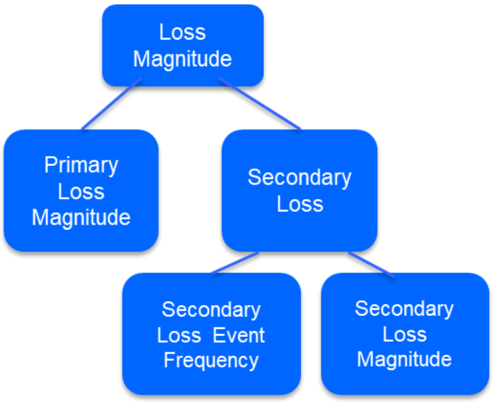


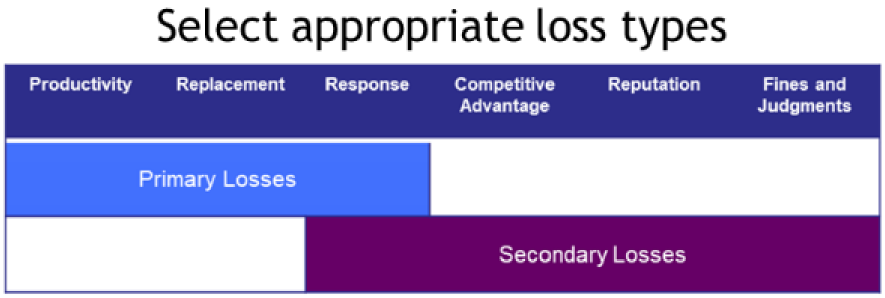
Resistance Strength Triangular Distribution Inputs

Min	ML	Max
10%	50%	60%

2.6 Loss Magnitude (LM)

Loss Magnitude (LM) is the probable magnitude of loss resulting from a loss event.





Objective Loss Magnitude is a currency value of the sum of Primary Loss Magnitude and Secondary Loss for a trial.

Risk is calculated as the sum of Primary Loss and Secondary Loss; there is no need for a separate calculation of LM.

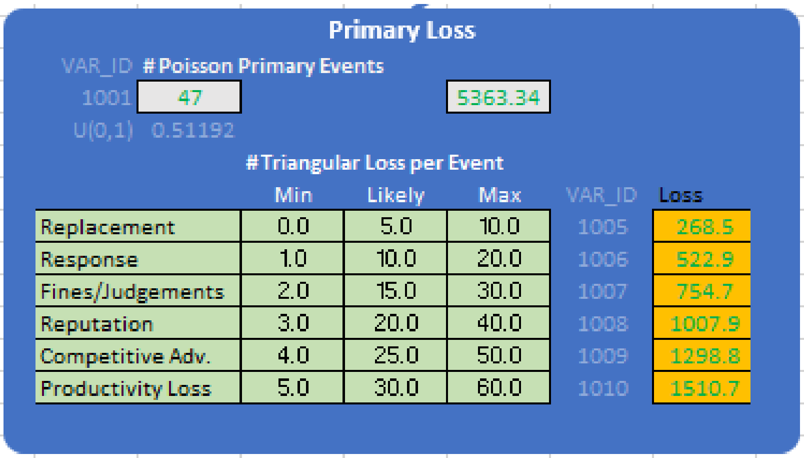
2.6.1 Estimate Primary Loss

Primary Loss occurs directly as a result of the threat agent's action upon the asset based on the probable magnitude of loss resulting from a loss event.

Objective Primary Loss Magnitude is a currency value of all probable losses for a trial.

Develop a calibrated estimated range of loss per event values with a 90% confidence interval for each applicable loss type, defining the minimum, most likely, and maximum values. These values are used along with the LEF SIP by a metalog distribution to produce the PLM SIP containing real numbers.

PLM is the sum of the six calculations of loss.



Primary Loss

VAR_ID # Poisson Primary Events

1001 47 5363.34

U(0,1) 0.51192

Triangular Loss per Event

	Min	Likely	Max	VAR_ID	Loss
Replacement	0.0	5.0	10.0	1005	268.5
Response	1.0	10.0	20.0	1006	522.9
Fines/Judgements	2.0	15.0	30.0	1007	754.7
Reputation	3.0	20.0	40.0	1008	1007.9
Competitive Adv.	4.0	25.0	50.0	1009	1298.8
Productivity Loss	5.0	30.0	60.0	1010	1510.7

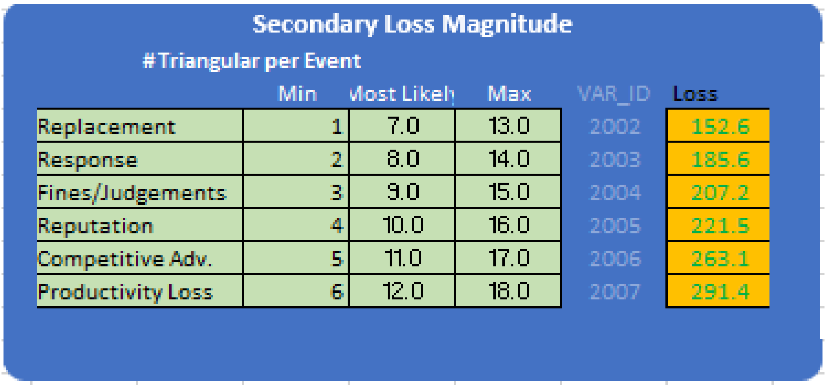
2.6.2 Estimate Secondary Loss

Secondary Loss, occurs as a result of secondary stakeholders (e.g., customers, stockholders, regulators, etc.) reacting negatively to the primary event. Secondary Losses are always predicated upon a Primary Loss.

Objective Secondary Loss is a currency value of all Secondary Loss Magnitudes (SLM) for a Secondary Loss Event for a trial.

Develop a calibrated estimated range of loss per event values with a 90% confidence interval for each applicable loss type, defining the minimum, most likely, and maximum values. These values are used along with the SLEF SIP by a metalog distribution to produce the SLM SIP containing real numbers.

SLM is the sum of the six calculations of loss.



Secondary Loss Magnitude

Triangular per Event

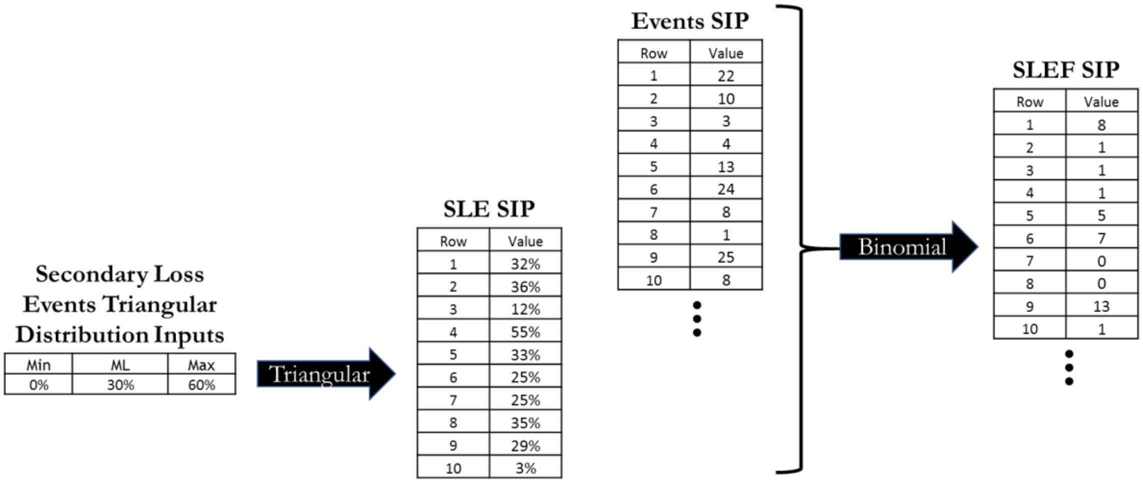
	Min	Most Likel	Max	VAR_ID	Loss
Replacement	1	7.0	13.0	2002	152.6
Response	2	8.0	14.0	2003	185.6
Fines/Judgements	3	9.0	15.0	2004	207.2
Reputation	4	10.0	16.0	2005	221.5
Competitive Adv.	5	11.0	17.0	2006	263.1
Productivity Loss	6	12.0	18.0	2007	291.4

2.6.3 Estimate Secondary Loss Event Frequency (SLEF)

Secondary Loss Event Frequency (SLEF) allows the analyst to estimate the percentage of time a scenario is expected to have secondary effects. Note that even though this variable is called a "frequency", it actually is estimated as a percentage to reflect that it represents the percentage of primary events that have secondary effects.

Objective Secondary Loss Event Frequency is the count of events for the trial period based on the number of loss events and the chance of Secondary Loss.

Develop a calibrated estimated range of probability values with a 90% confidence, defining the minimum, most likely, and maximum values. These are used by a triangular distribution to produce the Secondary Loss Event (SLE) SIP containing percentages. The number of events in the LEF SIP and the probability of success in the SLE SIP are input to a binomial distribution to produce the SLEF SIP containing integers.



Secondary Loss Events Triangular Distribution Inputs

Min	ML	Max
0%	30%	60%

SLE SIP

Row	Value
1	32%
2	36%
3	12%
4	55%
5	33%
6	25%
7	25%
8	35%
9	29%
10	3%

Events SIP

Row	Value
1	22
2	10
3	3
4	4
5	13
6	24
7	8
8	1
9	25
10	8

⋮

SLEF SIP

Row	Value
1	8
2	1
3	1
4	1
5	5
6	7
7	0
8	0
9	13
10	1

⋮

3 Distribution Modeling Methods

This chapter provides a general explanation of the mathematical methods for generating distributions, and suggests when each is appropriate to use. The reader is assumed to have some knowledge of probability and statistics.

The following elements will be included in each method's description:

- When is it appropriate to use this method?
- What is this method?
- How is the output generated and stored?

3.1 Triangular Distribution

A triangular distribution is used to model the number of events that take place within an interval defined by a minimum and maximum value when a most likely outcome is also known. The output is real numbers.

The triangular distribution is a continuous probability distribution with lower limit (*min)*, upper limit *(max)*, and mode *(ml)*, where $min < max$ and $min \leq ml \leq max$.

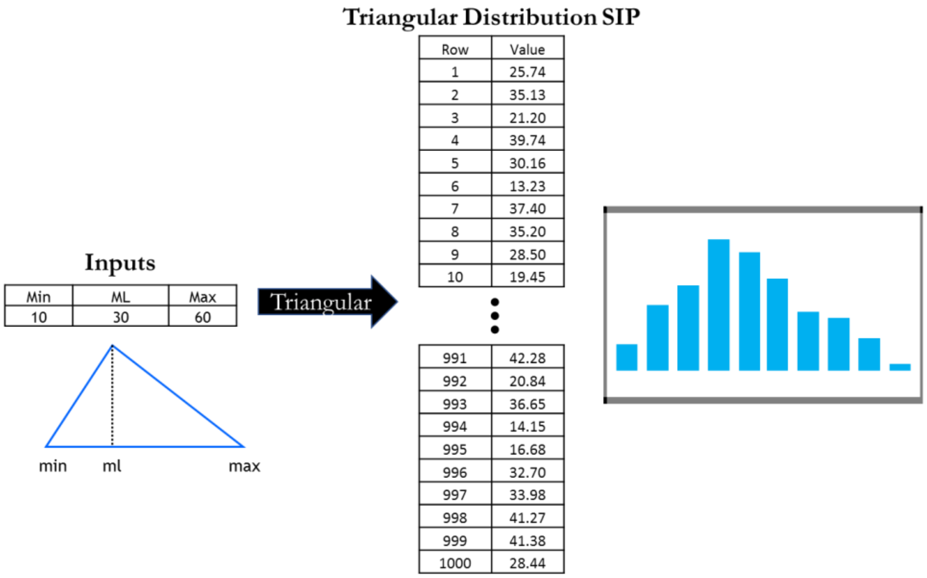
A calibrated estimate for a risk factor with a 90% confidence interval can be used to create a triangular distribution of real numbers:

```
riskFactor() = triangularDistribution(min, ML, max)
```

where:

- min = minimum likely value
- ML = most likely value
- max = maximum likely value

produces *riskFactor*(), a SIP of triangular distribution values as shown below.



Min	ML	Max
10	30	60

Row	Value
1	25.74
2	35.13
3	21.20
4	39.74
5	30.16
6	13.23
7	37.40
8	35.20
9	28.50
10	19.45
⋮	
991	42.28
992	20.84
993	36.65
994	14.15
995	16.68
996	32.70
997	33.98
998	41.27
999	41.38
1000	28.44

3.2 Poisson Distribution

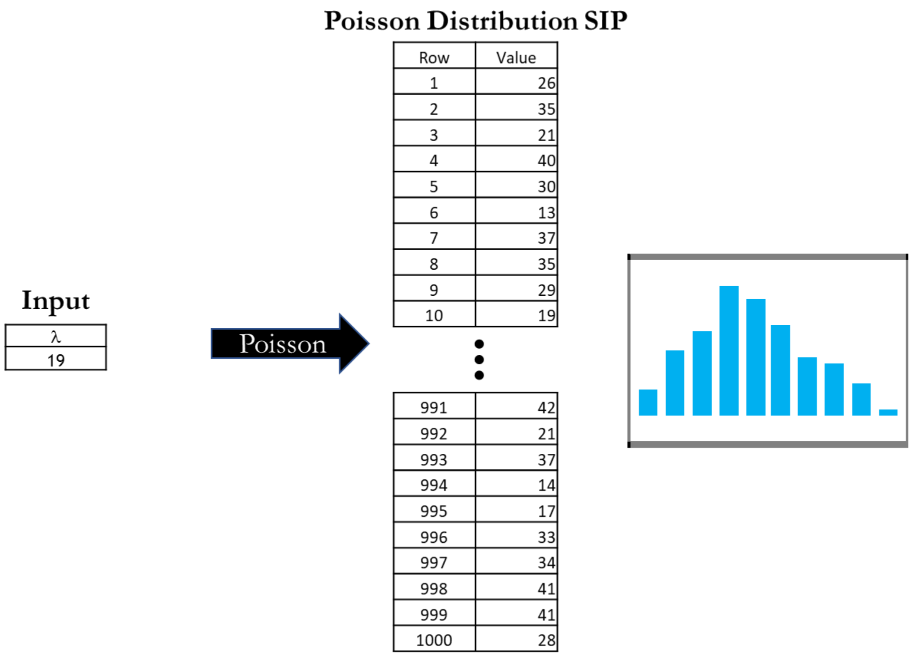
A Poisson distribution is used to model the number of events that take place, where λ (Lamba) is the average number of events per interval. The output is integers.

The Poisson distribution is a discrete probability distribution that expresses the probability of a given number of events occurring within a discrete time interval, if these events occur with a known average rate independent of the time since the last event. The Poisson distribution will provide a simulated number of events based on this average value.

A SIP containing a distribution of real values can be used to produce a Poisson distribution of integer values:

```
temp() = riskFactor1() * riskFactor2()
λ = Average(temp() )
riskFactor12() = poissonDistribution(temp(), λ )
```

produces *riskFactor12*(), a SIP of distribution values as shown below.



Poisson Distribution SIP

Input

λ
19

Row	Value
1	26
2	35
3	21
4	40
5	30
6	13
7	37
8	35
9	29
10	19
⋮	
991	42
992	21
993	37
994	14
995	17
996	33
997	34
998	41
999	41
1000	28

3.3 Binomial Distribution

A binomial distribution is used to model situations where an event may or may not occur, where the output is the number of events that occurred.

The binomial distribution is used where there are two discrete outcomes of an event. It is used to obtain the probability of observing *x* successes in *n* trials, with the probability of success for a single event denoted by *p*.

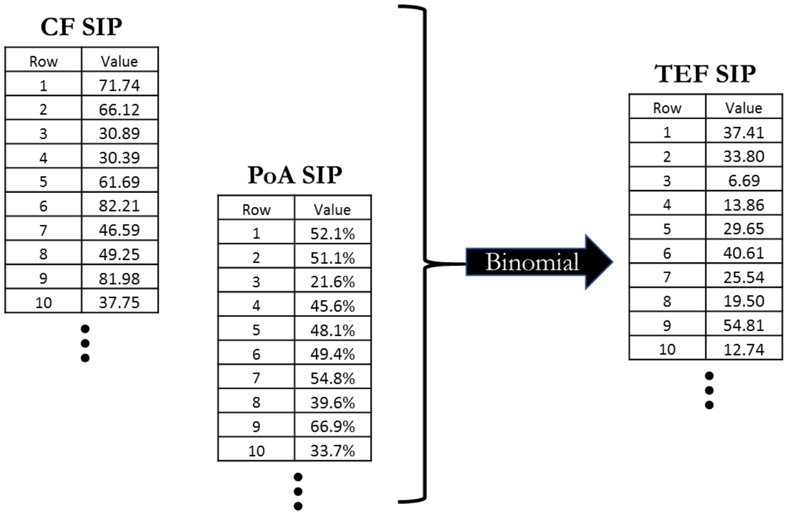
A binomial distribution is created based on input of SIPs:

```
riskFactor() = binomialDistribution(n, p))
```

where:

- n = number of events (integer)
- p = chance of success for an event (percent)

produces *riskFactor*(), a SIP of binomial distribution values as shown below.



CF SIP

Row	Value
1	71.74
2	66.12
3	30.89
4	30.39
5	61.69
6	82.21
7	46.59
8	49.25
9	81.98
10	37.75

PoA SIP

Row	Value
1	52.1%
2	51.1%
3	21.6%
4	45.6%
5	48.1%
6	49.4%
7	54.8%
8	39.6%
9	66.9%
10	33.7%

TEF SIP

Row	Value
1	37.41
2	33.80
3	6.69
4	13.86
5	29.65
6	40.61
7	25.54
8	19.50
9	54.81
10	12.74

3.4 Metalog Distribution

A metalog distribution is used to provide more accuracy, when needed, than can be achieved by using other standard distribution methods, such as normal or triangular.

Metalog distributions allow modeling for any combination of skewness and kurtosis (the peakedness or flatness of the graph of a frequency distribution especially with respect to the concentration of values near the mean as compared with the normal distribution). The system is comprised of unbounded, semi-bounded, and bounded distributions, each of which offers nearly unlimited shape flexibility. Applications in decision analysis (such as risk analysis) can use the metalog system by specifying three assessed quantiles. A "quantile" is a point on the Cumulative Probability Distribution (CDF), or, depending on context, just the *x*-coordinate of that a point.

The Open FAIR Tool uses the metalog distribution to replace the triangular distribution to produce a continuous probability distribution curve. Inputs include lower bound, mode, and upper bound of the distribution, and the number of events being modeled. The Open FAIR Tool identifies these inputs as *min*, *ml*, and *max* respectively, where $min < max$ and $min \leq ml \leq max$. The metalog is used in the Open FAIR Tool to represent sums of Independent and Identically Distributed (IID) variables.

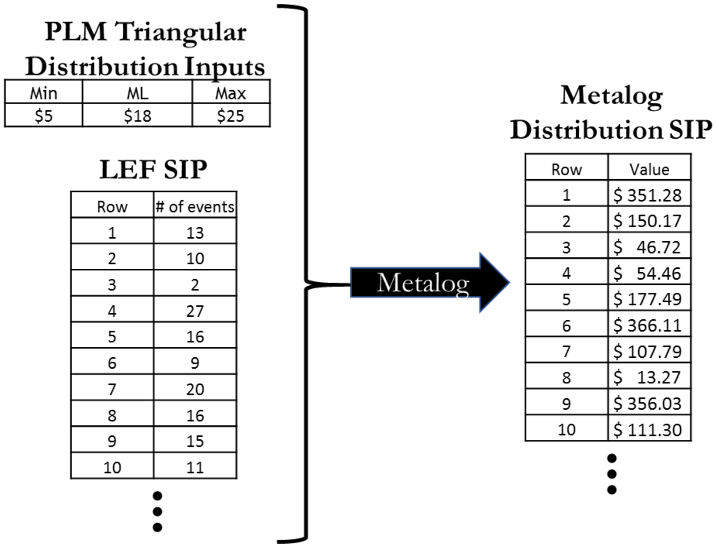
A calibrated estimate with a 90% confidence interval for an LM factor can be used as a metalog input, along with the associated frequency:

```
riskFactor() = metalog(min, ML, max, n, y)
```

where:

- min = minimum likely value
- ML = most likely value
- max = maximum likely value
- n = frequency
- *y* = random value

to produce *riskFactor*(), a SIP of metalog distribution values as shown below.



PLM Triangular Distribution Inputs

Min	ML	Max
$5	$18	$25

LEF SIP

Row	# of events
1	13
2	10
3	2
4	27
5	16
6	9
7	20
8	16
9	15
10	11

Metalog Distribution SIP

Row	Value
1	$ 351.28
2	$ 150.17
3	$ 46.72
4	$ 54.46
5	$ 177.49
6	$ 366.11
7	$ 107.79
8	$ 13.27
9	$ 356.03
10	$ 111.30

3.5 Vulnerability Simulator

The Vulnerability simulator is used to calculate Vulnerability (Vuln) based on the TCap and RS triangular distribution input values (minimum, most likely, and maximum). This algorithm replaces the need to generate and compare values for the TCap and RS SIPs with no adverse effect on desired randomness.

A triangular distribution is simulated for both TCap and RS, where the differences max-ML and ML-min represent the sides of a triangle, and max-min is the hypotenuse. The algorithm incrementally compares RS to TCap (subtracts the TCap calculation from the RS calculation), where a negative result indicates a loss event. The resultant Vuln (i.e., the probability of a loss event occurring for a threat event) is the sum of the table cells divided by 240 (the number of cells).

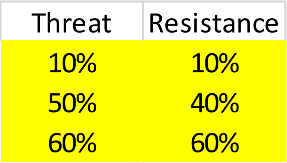
Each cell in the 21 x 21 table contains the following formula (indentation to ease readability):

```
= IF( RS_Min_0 > RS_ML_0, NA(),
  IF( RS_ML_0 > RS_Max_0, NA(),
    IF( RS_Min_0 = RS_Max_0, RS_ML_0,
      IF( Col_0 < (( RS_ML_0 - RS_Min_0 ) / ( RS_Max_0 - RS_Min_0 )),
        RS_Min_0 + SQRT( Col_0 * ( RS_ML_0 - RS_Min_0 ) * ( RS_Max_0 -
          RS_Min_0 )),
        RS_Max_0 - SQRT(( 1 - Col_0 ) * ( RS_Max_0 - RS_Min_0 ) * ( RS_Max_0 -
          RS_ML_0 ))))))
- IF( TCap_Min_0 > TCap_ML_0, NA(),
  IF( TCap_ML_0 > TCap_Max_0, NA(),
    IF( TCap_Min_0 = TCap_Max_0, TCap_ML_0,
      IF( Row_0 < (( TCap_ML_0 - TCap_Min_0 ) / ( TCap_Max_0 - TCap_Min_0 )),
        TCap_Min_0 + SQRT( Row_0 * ( TCap_ML_0 - TCap_Min_0 ) * ( TCap_Max_0 -
          TCap_Min_0 )),
        TCap_Max_0 - SQRT(( 1 - Row_0 ) * ( TCap_Max_0 - TCap_Min_0 ) * (
          TCap_Max_0 - TCap_ML_0 ))))))
```

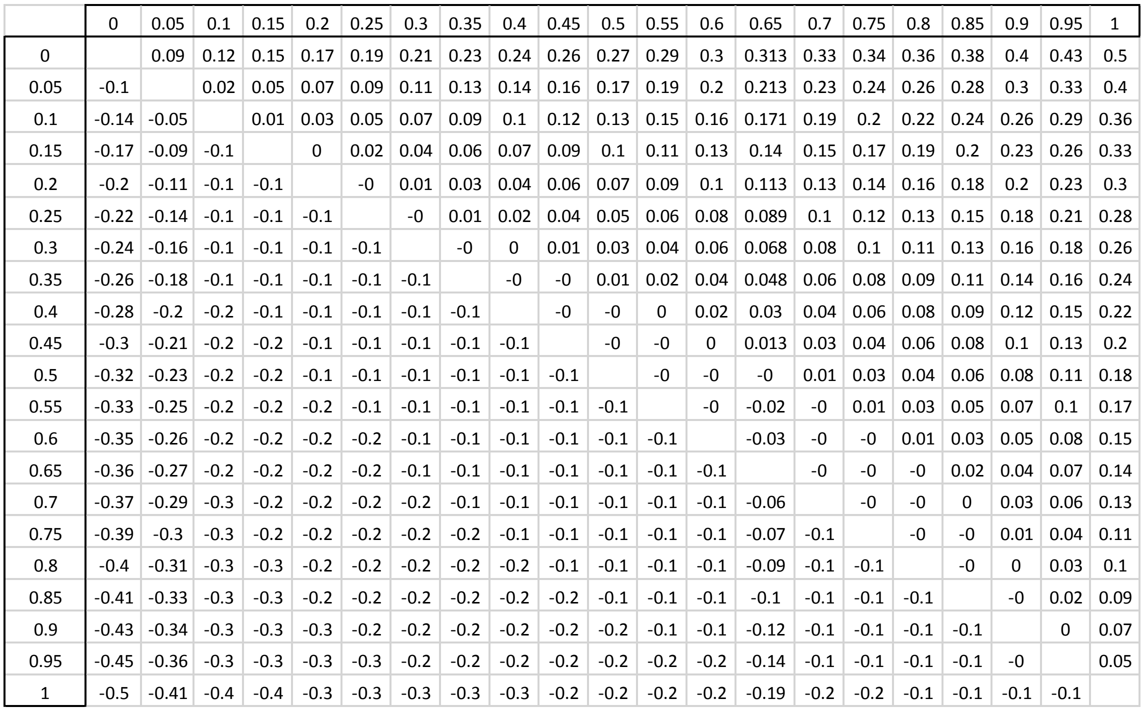
where:

- TCap_x = the minimum, most likely, and maximum input values
- RS_x = the minimum, most likely, and maximum input values
- Col_x and Row_x = the columns’ and rows’ fixed input values ranging from 0 to 1 in .05 increments

No calculation is performed in cells where *Col_x* = *Row_x*. The following shows input values and the resultant table.



Threat	Resistance
10%	10%
50%	40%
60%	60%



	0	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95	1
0		0.09	0.12	0.15	0.17	0.19	0.21	0.23	0.24	0.26	0.27	0.29	0.3	0.313	0.33	0.34	0.36	0.38	0.4	0.43	0.5
0.05	-0.1		0.02	0.05	0.07	0.09	0.11	0.13	0.14	0.16	0.17	0.19	0.2	0.213	0.23	0.24	0.26	0.28	0.3	0.33	0.4
0.1	-0.14	-0.05		0.01	0.03	0.05	0.07	0.09	0.1	0.12	0.13	0.15	0.16	0.171	0.19	0.2	0.22	0.24	0.26	0.29	0.36
0.15	-0.17	-0.09	-0.1		0	0.02	0.04	0.06	0.07	0.09	0.1	0.11	0.13	0.14	0.15	0.17	0.19	0.2	0.23	0.26	0.33
0.2	-0.2	-0.11	-0.1	-0.1		-0	0.01	0.03	0.04	0.06	0.07	0.09	0.1	0.113	0.13	0.14	0.16	0.18	0.2	0.23	0.3
0.25	-0.22	-0.14	-0.1	-0.1	-0.1		-0	0.01	0.02	0.04	0.05	0.06	0.08	0.089	0.1	0.12	0.13	0.15	0.18	0.21	0.28
0.3	-0.24	-0.16	-0.1	-0.1	-0.1	-0.1		-0	0	0.01	0.03	0.04	0.06	0.068	0.08	0.1	0.11	0.13	0.16	0.18	0.26
0.35	-0.26	-0.18	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0	0.01	0.02	0.04	0.048	0.06	0.08	0.09	0.11	0.14	0.16	0.24
0.4	-0.28	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0	0	0.02	0.03	0.04	0.06	0.08	0.09	0.12	0.15	0.22
0.45	-0.3	-0.21	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0	0	0.013	0.03	0.04	0.06	0.08	0.1	0.13	0.2
0.5	-0.32	-0.23	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0	-0	0.01	0.03	0.04	0.06	0.08	0.11	0.18
0.55	-0.33	-0.25	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0.02	-0	0.01	0.03	0.05	0.07	0.1	0.17
0.6	-0.35	-0.26	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1		-0.03	-0	-0	0.01	0.03	0.05	0.08	0.15
0.65	-0.36	-0.27	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1		-0	-0	-0	0.02	0.04	0.07	0.14
0.7	-0.37	-0.29	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.06		-0	-0	0	0.03	0.06	0.13
0.75	-0.39	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.07	-0.1		-0	-0	0.01	0.04	0.11
0.8	-0.4	-0.31	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.09	-0.1	-0.1		-0	0	0.03	0.1
0.85	-0.41	-0.33	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1		-0	0.02	0.09
0.9	-0.43	-0.34	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	-0.12	-0.1	-0.1	-0.1	-0.1		0	0.07
0.95	-0.45	-0.36	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.2	-0.14	-0.1	-0.1	-0.1	-0.1	-0		0.05
1	-0.5	-0.41	-0.4	-0.4	-0.3	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.19	-0.2	-0.2	-0.1	-0.1	-0.1	-0.1	

The values in this 21 x 21 table are counted then divided by 420 to determine the percentage Vuln based on input values. The first row and column contain incremental values that apply to the intersecting cell in the body of the table.

4 Future Directions

Potential enhancements to the baseline Open FAIR Tool are discussed in this section. No priority is implied by the order of this content.

- Import historic data as a SIP for any risk factor of the Open FAIR methodology

Glossary

Term/Acronym	Definition
Contact Frequency (CF)	The probable frequency, within a given timeframe, that a threat agent will come into contact with an asset.
Control Strength (CS)	The strength of a control as compared to a standard measure of force.
FAIR	Factor Analysis of Information Risk
Loss Event Frequency (LEF)	The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.
Loss Magnitude (LM)	The probable magnitude of loss resulting from a loss event.
Probability of Action (PoA)	The probability that a threat agent will act against an asset once contact occurs.
Primary Loss Magnitude (PLM)	The probable magnitude of loss resulting from a loss event.
Resistance Strength (RS)	The strength of a control as compared to a baseline measure of force.
Risk	The probable frequency and probable magnitude of future loss.
Stochastic Information Packet (SIP)	A way of representing an uncertainty as a data array comprised of thousands of possible outcomes. A SIP makes the abstract concept of a probability distribution actionable, additive, and auditable.
Threat Capability (TCap)	The probable level of force that a threat agent is capable of applying against an asset.
Threat Event Frequency (TEF)	The probable frequency, within a given timeframe, that a threat agent will act against an asset.
Vulnerability (Vuln)	The probability that a threat event will become a loss event.

Index