Realistic and Affordable Quantitative Information Security Risk Management

Effective risk management for small/medium businesses

Walter Williams

Who am I

- Walt Williams, CISSP, SSCP, CEH, CPT, MCP
- Director of Security and Compliance at Lattice Engines
- Done everything from PKI, meta directory, LDAP, IAM, vulnerability assessment, penetration testing, risk analysis, security architecture and design, business continuity, disaster recovery, incident response……
- wwilliams@lattice-engines.com
- walt.williams@gmail.com
- @LESecurity
- https://infosecuritymetrics.wordpress.com
- **Security for Service Oriented Architectures CRC Press ISBN 978-1-4665-8402-0 due out in 2014**

Thanks, many and manifold

- Dr. Mike Lloyd
- Jeff Bardin
- Donn Parker
- The folks at FAiR
- The Open Group
- Karen P. Stopford
- Matt Truenow
- Everyone at The Society of Information Risk Analysts
- Kevin Riggins
- ISSA
- And a special thanks to the good folks at l0pht who got me into this to begin with

What is Risk so we can measure it?

- First, information security risk is a subset of business risk
  - While important, it does not drive the business
  - It should inform business people in making business decisions
- There are many different definitions for information security risk

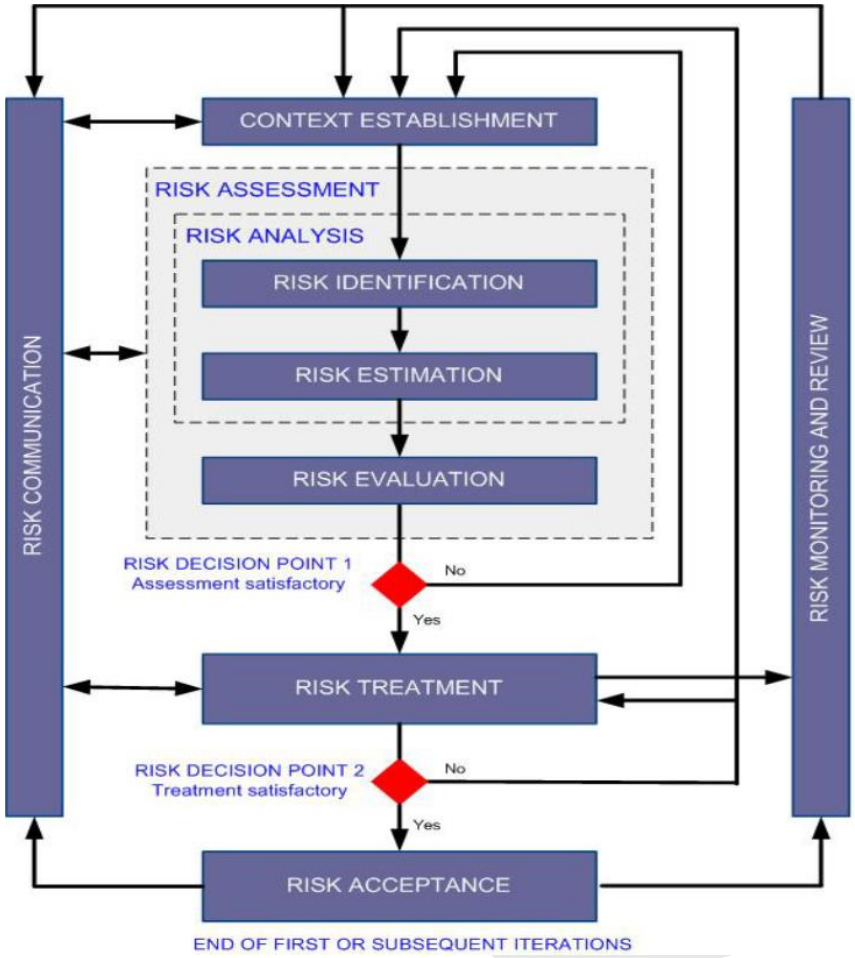
The ‘classic’ definition

- Classic definition (best expressed by NIST):
  - Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.
- Expressed as the formula:
  - Risk = probability of an event * impact of same event
  - You’re multiplying apples * oranges
  - Not a good basis to make a decision

So, what is risk already?

- Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
  - Comes from ISO 27005
  - Implies a metric: Harm
  - No requirement to calculate quantitatively
  - In fact, ISO 27005 allows you to use any method to analyze risk
- To understand (measure) risk involves understanding:
  - Threat
  - Vulnerability
  - Asset
  - Impact/Harm

What ISO 27005 does is define a process for managing risk



Context/Scope

- Risk to what?
  - Defining context allows you to specify the object of concern and where it is found and leveraged
  - The what is defined by the business
  - The where is defined by the business
    - But must include all locations of what and all locations where the what is used.

Assets

- Different people have different definitions of assets
  - They are all right
- Assets have value
  - This is sometimes hard to determine
  - This value helps identify how much you want to spend preventing incidents
  - You don’t put all of your staplers in a bank vault to prevent their theft
- Most important asset: likely is your data

Value is more than just money

- This is where we find a meaningful metric for risk
  - What is Criticality of system?
  - What is Cost of System?
  - What is Sensitivity of System?
  - What is the loss of productivity?
  - What is the cost of incident response?
  - What fines will be incurred?
  - What is the impact to our reputation?
  - What is the impact to our investors?
- Many of these can be estimated using a monte carlo simulation. More on this later
- This provides us with Impact/Harm

Assessing Risk

- This is the step where you identify your threat vectors and your controls
- Octave
  - Very customizable
- RiskIT
  - Excellent if you're using CobIT
- NIST SP 800-30
  - Uses classic definition of risk
- TARA
  - Looks at attack risk only

Risk Analysis

- How effective are your controls at preventing an event for each threat?
- This is where qualitative analysis with mathematical models help

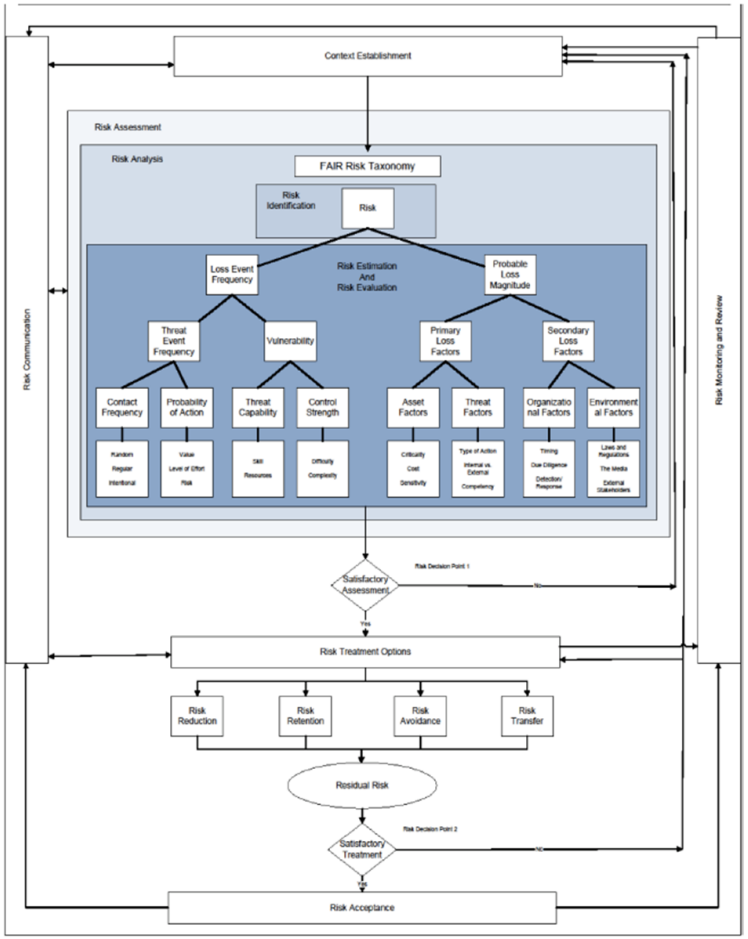
The risk management cookbook

FAIR: A methodology for Risk Analysis

The OpenGroup took ISO 27005 & inserted FAIR into these assessment methodologies to a means for analysis based upon precise terminology

The Risk Cookbook: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=c103

The OpenGroup modified FAIR just enough to make it more useful



Threats

- How frequently do they act/happen?
- How frequently do they have the potential to do harm to an asset?
  - The aggregate of this is your measurement of threat

- Many kinds of threats have the same impact
  - Bomb = earthquake = tornado = tsunami = etc.
  - Therefor you protect against the impact
  - Not the threat
- But not all threats with similar impacts have the same modus apparatus
  - Therefor you protect all points of egress for threats
  - If no threat can act on something, there is no need to protect it
  - It already is protected….

Basel I Threat Categories

- Originated with financial industry
  - Provided free tool for risk measurement
  - http://www.bits.org/publications/doc/bitskalculatorspreadsht.xls
- I have a modified version of this tool
- Reasonable categories
  - Internal Fraud
  - External Fraud
  - Employee Practices and Workplace Safety
  - Clients, Products and Business Practices
  - Damage to Physical Assets
  - Business Disruption and System Failures
  - Execution , Delivery and Process Management

The details

Airplane crash
Application software failure
Automobile crash
Biological agent attack
Bomb attacks
Bomb threats
Chemical spill
Civil disorder
Computer crime
CPU malfunction/failure
DDoS or DoS attacks
Discussing sensitive matters in open
DNS failure
Dumpster diving
Dust/sand
Embezzlement
Epidemic
Extortion
Fire
Floods
Gas leaks
Hardware failure
Hazardous waste exposure
Heat
High winds
Human error
Hurricane
HVAC failure
Lawsuits/ litigation
Leaving computer screen exposed or unlocked
Leaving doors unlocked
Leaving sensitive documents exposed
Lightning
Lost or stolen laptops
Malicious code
Network spoofing
Network/application backdoor
Network/application time bomb
Power failure
Power fluctuation
Radiation contamination
Robbery
Sabotage
Seismic activity
Shoulder surfing
Snow/ice storms
Social engineering
Software defects
Solar flares
System software failure
Tailgating to gain unauthorized access
Terrorist attack
Telecommunications failure
Tidal Wave
Tornados
Trojans
Typhoon
Unauthorized network or system access
Unauthorized scans
Unintentional DDoS
Unintentionally bad legislation
Vandalism
Virus hoaxes
Viruses
Volcanic eruption
War
War dialing
Web defacements
Work stoppage/ strike
Worms

Lattice

Controls

- You have to know what your controls are
  - You have to know why you have those controls
  - You have to know how effective are your controls
    - How much skill is needed to over come them?
    - How easy is it to acquire this skill?
      - Is there an app for that?
- How do you get to this knowledge?
  - Ask
  - Audit
  - Test

Control Categories

- I like to use the ISO 27002 catalog (still on version 2005)
  - Not perfect but more comprehensive than PCI
  - Leveraged in the BITS provided tool
  - Known and understood internationally
  - If you prefer, use CobIT which is another excellent controls catalog
- Access Control
- Asset Classification & Control
- Business Continuity Management
- Communications & Operations Management
- Compliance
- Organizational Security
- Personnel Security
- Physical and Environmental Security
- Security Policy
- Systems Development

Vulnerability

- This is the method through with a threat can act on an asset.
  - Think of it as a malicious user story where the threat is human in origin
- Or, a gap in a control.
  - Sometimes this is the same method through which authorized action takes place
  - Sometimes it is through a method that no one knew existed until it is found and used against you
  - You can only protect what you know.
  - Which is why we protect assets not protect against vulnerabilities

Impact

- This a statement of the harm done by the threat acting on the vulnerability to the asset
  - Not all impacts compromise the entire value of an asset
  - Some impacts will compromise the value of multiple assets.
  - The value of an asset is the aggregate of:
    - Loss of Productivity
    - Cost of Response
    - Cost of Replacement
    - Loss of Competitive Advantage
    - Fines/Judgments
    - Reputation
  - The value of the protection should always be less than the value of the asset
- Again a real metric we can estimate using a monte carlo scenario

Impact: The dilema

- How much is it really worth?
  - Your CEO says X
  - Your CFO says Y (next year Z)
  - Your CTO says A
  - How confident are you in any of their numbers?
- They're all correct! Aggregate!

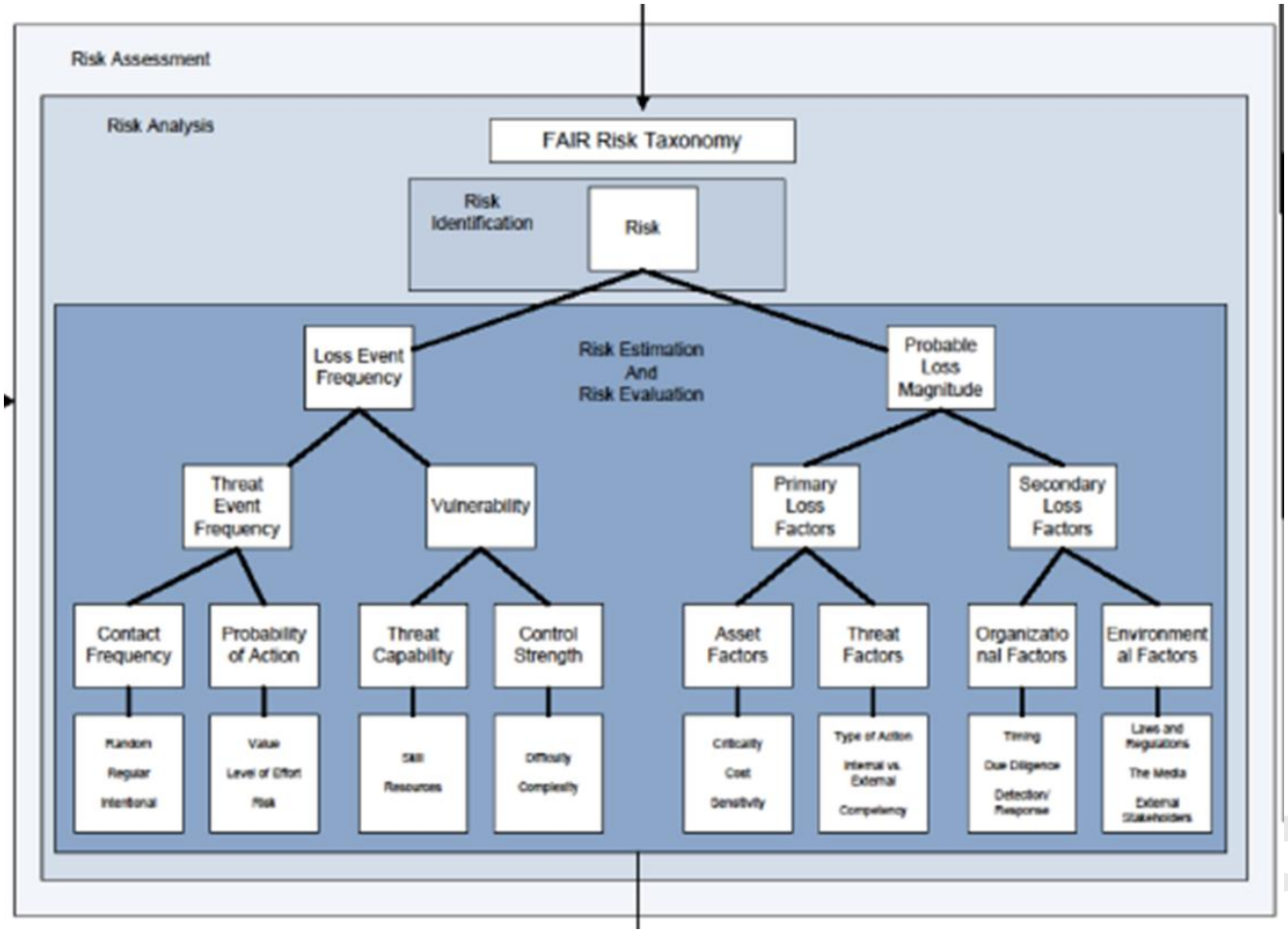
Getting towards analysis

- Understand the impact to each asset
  - Where multiple assets are impacted, aggregate the impacts
- Establish a scale
  - Scale should be proportional to impact
  - Scale should be proportional to the frequency of an event
  - Scale should be proportional to the capability of the threat agent
  - Scale should be proportional to the strength of existing controls
  - Scale should be proportional to the strength of existing vulnerabilities
- Remember: This is a model not reality

Closer to Analysis

- In order to measure information security risk, one must first measure
  - Impact
  - Frequency
  - Capability of threat
  - Strength of controls
  - Degree of vulnerability
- Some of these measurements can inform others
  - Loss Event frequency can be expressed as a factor of Vulnerability and Threat Event Frequency
    - If it is hard to exploit, hard to come across, frequency of loss is low
    - If vulnerability is easy to exploit or easy to come across, frequency of loss is high
  - Loss Magnitude can be expressed as a factor of Asset, Threat, Organizational and Environmental issues

Some times you need to estimate



Estimation may be done at any point on the tree where no data below that point is available or reliable.

Vulnerability

- Vulnerability is a factor of
  - Threat capability
  - Or how knowledgeable do you have to be to exploit the vulnerability
- Control strength
  - If the vulnerability exists, but there is no way to get to that method of egress, the strength of the control may eliminate the threat
- CVSS 3.0 numbers can provide a point of comparison
  - But ONLY if they are the complete CVSS 3.0 number

Completing CVSS

- CVSS provided with each vulnerability is a generic statement of vulnerability
- To complete:
- http://nvd.nist.gov/cvss.cfm?calculator&version=2
  - This completes the calculation by providing a relative measurement of vulnerability within the context of your environment

Why Probability by itself is almost Useless

- You have a 100% chance of dying.

How to make it useful

- But your chance of dying right now is much less than 1%
- Probability is not useful unless you time box it.
- You need understand the chance of something happening now

Frequency

- Event Frequency can be derived from historical data BUT
  - Past performance is no guarantee of future results
  - See Sony the day before the first compromise
- Event Frequency can be estimated as a factor of:
  - Contact Frequency
    - How easy is it to encounter the method of egress
  - Probability of Acting
    - How likely is it that some one would exploit the vulnerability
  - Both can be estimated using a BETA Pert distribution
  - This gets better when you calibrate

What do I mean by Calibrated?

- Calibration is a measure of what is your level of confidence in the numbers you provide
  - On what day was the Declaration of Independence voted on by Congress:

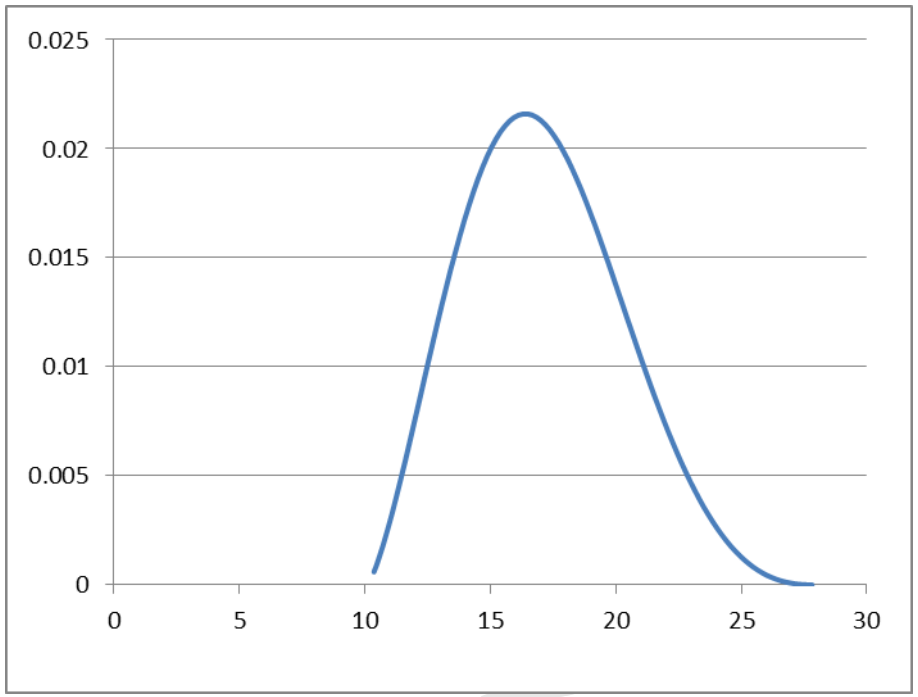
Calibration

- The day the Declaration of Independence voted on by Congress
  - July 2, 1776
  - It was ratified on July 4, 1776
- Experts often over estimate their level of confidence
  - Until they learn to calibrate
  - The best calibration comes from research
- Event frequency data available
  - Verizon data breach report, Poneman data breach report, CSI Annual report, dataloss.org, etc.
  - These reports have issues, take them with a grain of salt

BETA Pert Distribution

- Provides a reliable way to estimate probability
- Mean =(Optimistic Estimate + (g times Most Likely Estimate) + Pessimistic Estimate) divided by g+2 is the estimate of likelihood (where g=4)
- David Vose proposed that if you replaced g with a value indicating confidence, you could get a more realistic estimate of frequency:
  - Mean=(Optimistic + (Confidence * most likely) + Pessimistic) divided by confidence + 2
- This is very useful for gaging event frequency
- Does *not* need random number inputs (though some think it is improved with random numbers)

What a BETAPert distribution looks like

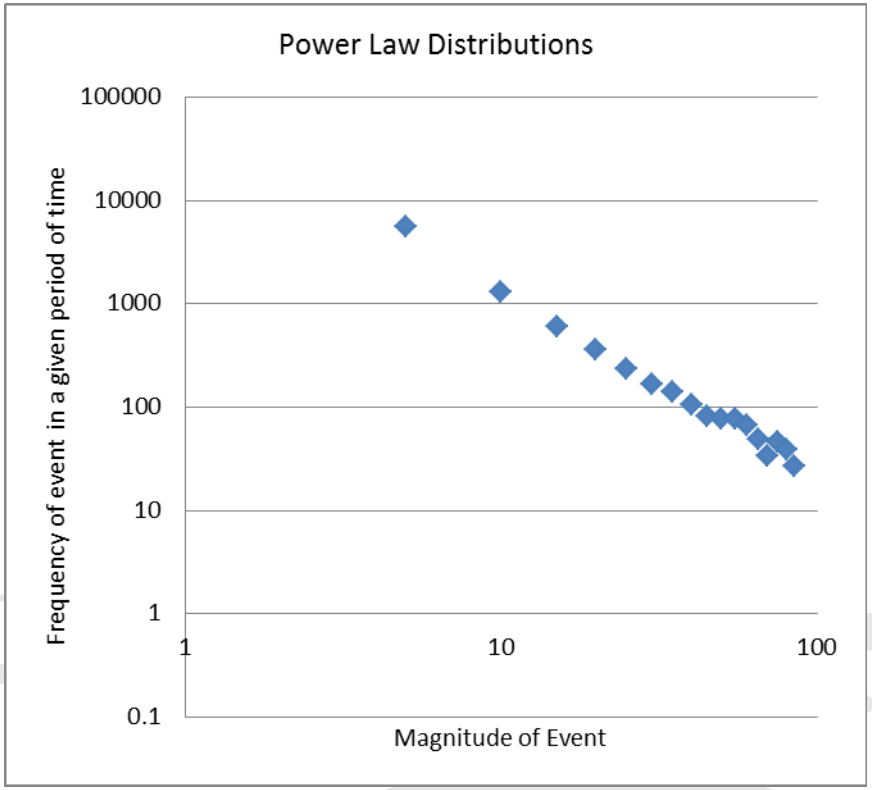


Lattice

Alternative Models

- The Power law distribution has been shown to be rather useful to relate the frequency and magnitude of disasters

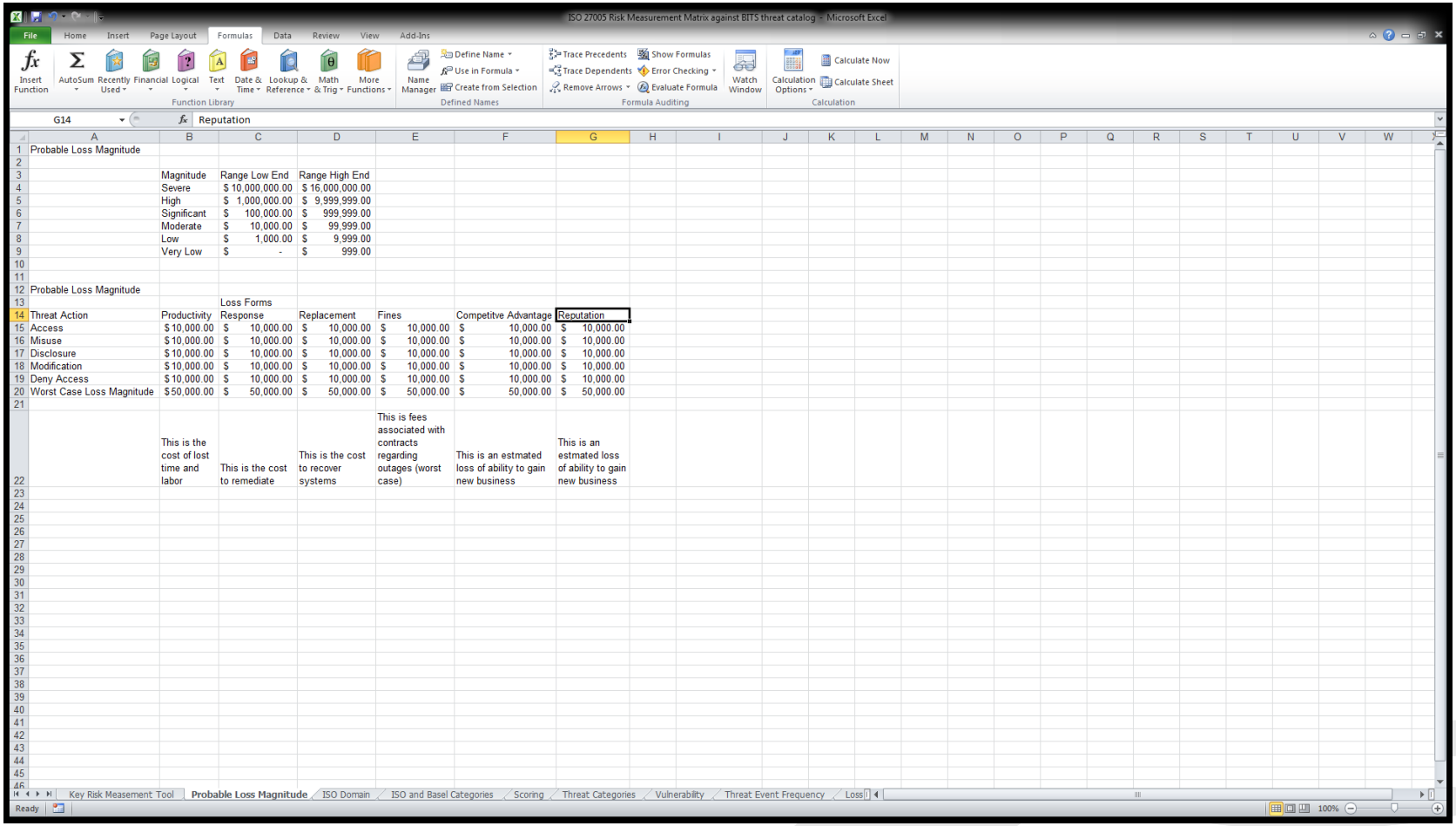
To calculate, you need the slope and intercept, a random generator, size of the event, and event frequency



Tools

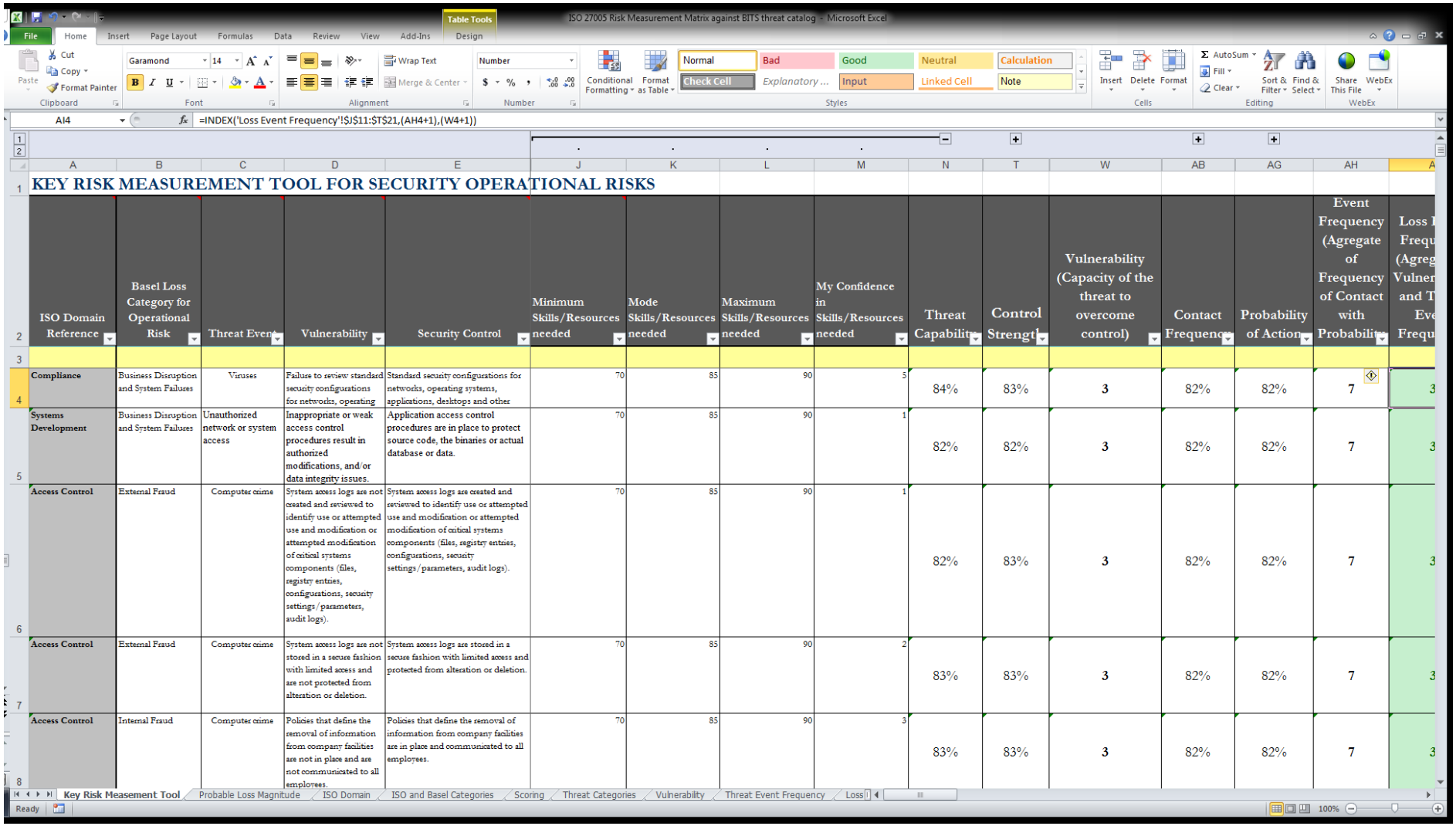
- Free
  - http://code.google.com/p/openpert/
    - Requires Excel
  - OpenOffice
- Commercial Tools
  - http://www.vosesoftware.com
  - http://www.riskamp.com/library/pertdistribution.php
  - Excel

Establish value of Asset



	A	B	C	D	E	F	G
1	Probable Loss Magnitude						
2							
3		Magnitude	Range Low End	Range High End			
4		Severe	$ 10,000,000.00	$ 16,000,000.00			
5		High	$ 1,000,000.00	$ 9,999,999.00			
6		Significant	$ 100,000.00	$ 999,999.00			
7		Moderate	$ 10,000.00	$ 99,999.00			
8		Low	$ 1,000.00	$ 9,999.00			
9		Very Low	$ -	$ 999.00			
10							
11							
12	Probable Loss Magnitude						
13			Loss Forms				
14	Threat Action	Productivity	Response	Replacement	Fines	Competitve Advantage	Reputation
15	Access	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
16	Misuse	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
17	Disclosure	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
18	Modification	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
19	Deny Access	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00	$ 10,000.00
20	Worst Case Loss Magnitude	$ 50,000.00	$ 50,000.00	$ 50,000.00	$ 50,000.00	$ 50,000.00	$ 50,000.00
21							
22		This is the cost of lost time and labor	This is the cost to remediate	This is the cost to recover systems	This is fees associated with contracts regarding outages (worst case)	This is an estmated loss of ability to gain new business	This is an estmated loss of ability to gain new business

Expand Each Category



ISO 27005 Risk Measurement Matrix against BITS threat catalog - Microsoft Excel

=INDEX('Loss Event Frequency'!$J$11:$T$21,(AH4+1),(W4+1))

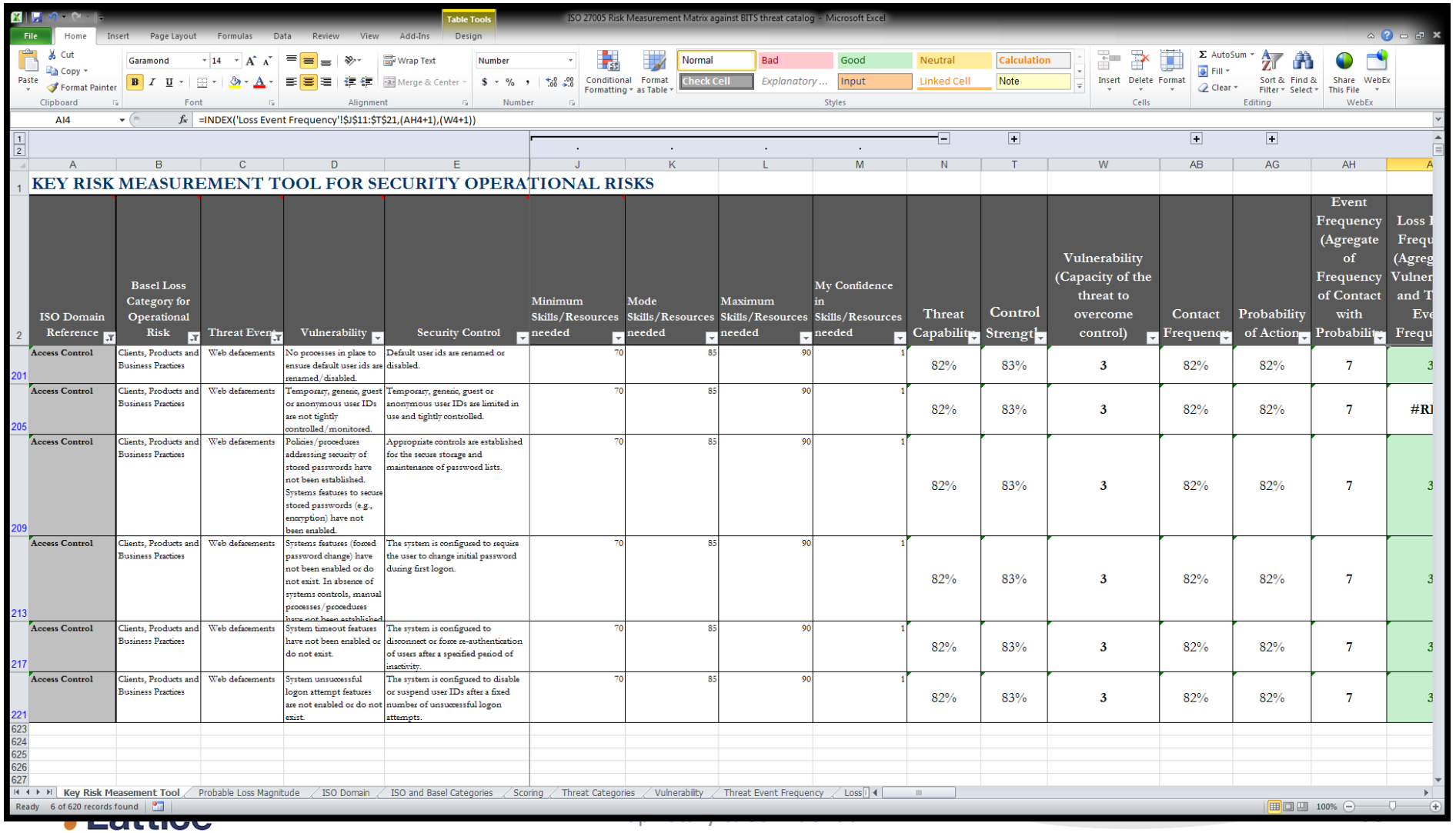
KEY RISK MEASUREMENT TOOL FOR SECURITY OPERATIONAL RISKS

ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Minimum Skills/Resources needed	Mode Skills/Resources needed	Maximum Skills/Resources needed	My Confidence in Skills/Resources needed	Threat Capability	Control Strength	Vulnerability (Capacity of the threat to overcome control)	Contact Frequency	Probability of Action	Event Frequency (Agregate of Frequency of Contact with Probability	Loss Frequ (Agreg Vulner and T Eve Frequ
Compliance	Business Disruption and System Failures	Viruses	Failure to review standard security configurations for networks, operating	Standard security configurations for networks, operating systems, applications, desktops and other	70	85	90	5	84%	83%	3	82%	82%	7	3
Systems Development	Business Disruption and System Failures	Unauthorized network or system access	Inappropriate or weak access control procedures result in authorized modifications, and/or data integrity issues.	Application access control procedures are in place to protect source code, the binaries or actual database or data.	70	85	90	1	82%	82%	3	82%	82%	7	3
Access Control	External Fraud	Computer crime	System access logs are not created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).	System access logs are created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).	70	85	90	1	82%	83%	3	82%	82%	7	3
Access Control	External Fraud	Computer crime	System access logs are not stored in a secure fashion with limited access and are not protected from alteration or deletion.	System access logs are stored in a secure fashion with limited access and protected from alteration or deletion.	70	85	90	2	83%	83%	3	82%	82%	7	3
Access Control	Internal Fraud	Computer crime	Policies that define the removal of information from company facilities are not in place and are not communicated to all employees.	Policies that define the removal of information from company facilities are in place and communicated to all employees.	70	85	90	3	83%	83%	3	82%	82%	7	3

Key Risk Measement Tool | Probable Loss Magnitude | ISO Domain | ISO and Basel Categories | Scoring | Threat Categories | Vulnerability | Threat Event Frequency | Loss

Ready

Filter on domain, BASIL & Threat event



ISO 27005 Risk Measurement Matrix against BITS threat catalog - Microsoft Excel

=INDEX('Loss Event Frequency'!$J$11:$T$21,(AH4+1),(W4+1))

KEY RISK MEASUREMENT TOOL FOR SECURITY OPERATIONAL RISKS

	ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Minimum Skills/Resources needed	Mode Skills/Resources needed	Maximum Skills/Resources needed	My Confidence in Skills/Resources needed	Threat Capability	Control Strength	Vulnerability (Capacity of the threat to overcome control)	Contact Frequency	Probability of Action	Event Frequency (Agregate of Frequency of Contact with Probability	Loss Frequ (Agreg Vulner and T Eve Frequ
201	Access Control	Clients, Products and Business Practices	Web defacements	No processes in place to ensure default user ids are renamed/disabled.	Default user ids are renamed or disabled.	70	85	90	1	82%	83%	3	82%	82%	7	3
205	Access Control	Clients, Products and Business Practices	Web defacements	Temporary, generic, guest or anonymous user IDs are not tightly controlled/monitored.	Temporary, generic, guest or anonymous user IDs are limited in use and tightly controlled.	70	85	90	1	82%	83%	3	82%	82%	7	#RI
209	Access Control	Clients, Products and Business Practices	Web defacements	Policies/procedures addressing security of stored passwords have not been established. Systems features to secure stored passwords (e.g., encryption) have not been enabled.	Appropriate controls are established for the secure storage and maintenance of password lists.	70	85	90	1	82%	83%	3	82%	82%	7	3
213	Access Control	Clients, Products and Business Practices	Web defacements	Systems features (forced password change) have not been enabled or do not exist. In absence of systems controls, manual processes/procedures have not been established	The system is configured to require the user to change initial password during first logon.	70	85	90	1	82%	83%	3	82%	82%	7	3
217	Access Control	Clients, Products and Business Practices	Web defacements	System timeout features have not been enabled or do not exist.	The system is configured to disconnect or force re-authentication of users after a specified period of inactivity.	70	85	90	1	82%	83%	3	82%	82%	7	3
221	Access Control	Clients, Products and Business Practices	Web defacements	System unsuccessful logon attempt features are not enabled or do not exist.	The system is configured to disable or suspend user IDs after a fixed number of unsuccessful logon attempts.	70	85	90	1	82%	83%	3	82%	82%	7	3

Key Risk Measement Tool | Probable Loss Magnitude | ISO Domain | ISO and Basel Categories | Scoring | Threat Categories | Vulnerability | Threat Event Frequency | Loss

Ready 6 of 620 records found

Enter assessment

- Minimum % of attackers who would know how to exploit vulnerability
- Mode % of attackers who would know how to exploit vulnerability
- Maximum % of attackers who would know how to exploit vulnerability
- Your confidence in your estimates
  - 4 is most confident
  - Lower than 4: your estimates are likely low
  - Higher than 4: your estimates are likely high

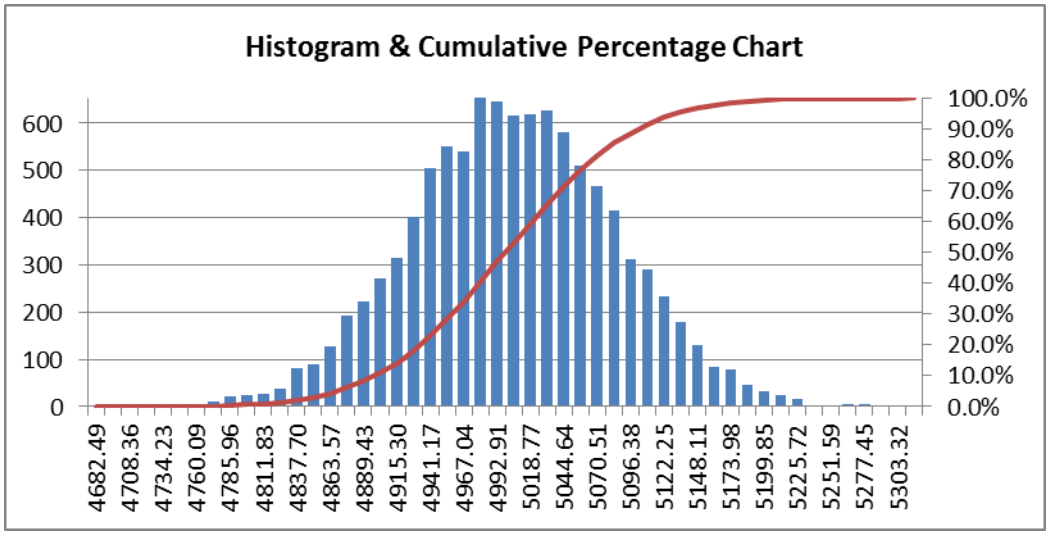
Calculating Risk

- Asset Catalog
  - Derived from interviews
  - Impact to organization from event by a threat regarding asset is key metric
  - This considers the vulnerability and controls context of your organization
- Threat Catalog
  - BITS or other
- Controls Catalog
  - ISO 27002, CobIT or other
- Vulnerability/Gap analysis
  - Your CVSS numbers can help here IF put in context using environmentally calibrated CVSS 2 scoring
- Frequency Estimation and Calibration
  - Frequency is best used to determine priority between two different risks of the same impact to the same asset
- Impact
  - Your best metric

Impact through a Monte Carlo Simulation

- Simply put, this is a methodology of estimating reality
  - Used by the Manhattan Project
  - You need domain of possible inputs
  - Generate them randomly from a probability distribution over the domain
    - good use for beta-pert
    - Need uniform distribution with large number of inputs
  - Perform a deterministic computation
  - Aggregate the results
    - Determine probability of each result
  - Perfect tool to estimate impact
  - Provides a good metric

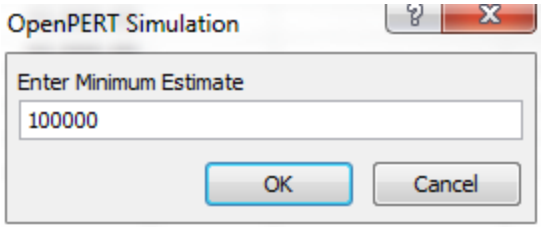
Graph of Monte Carlo simulation results

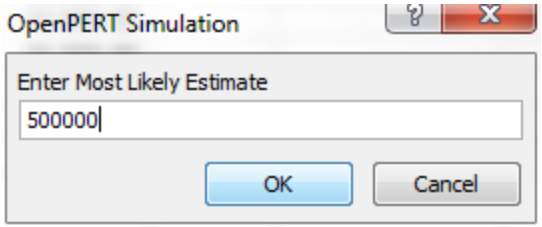


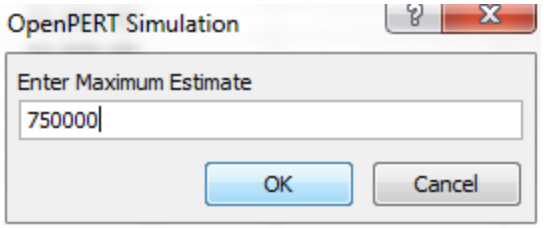
http://code.google.com/p/openpert/

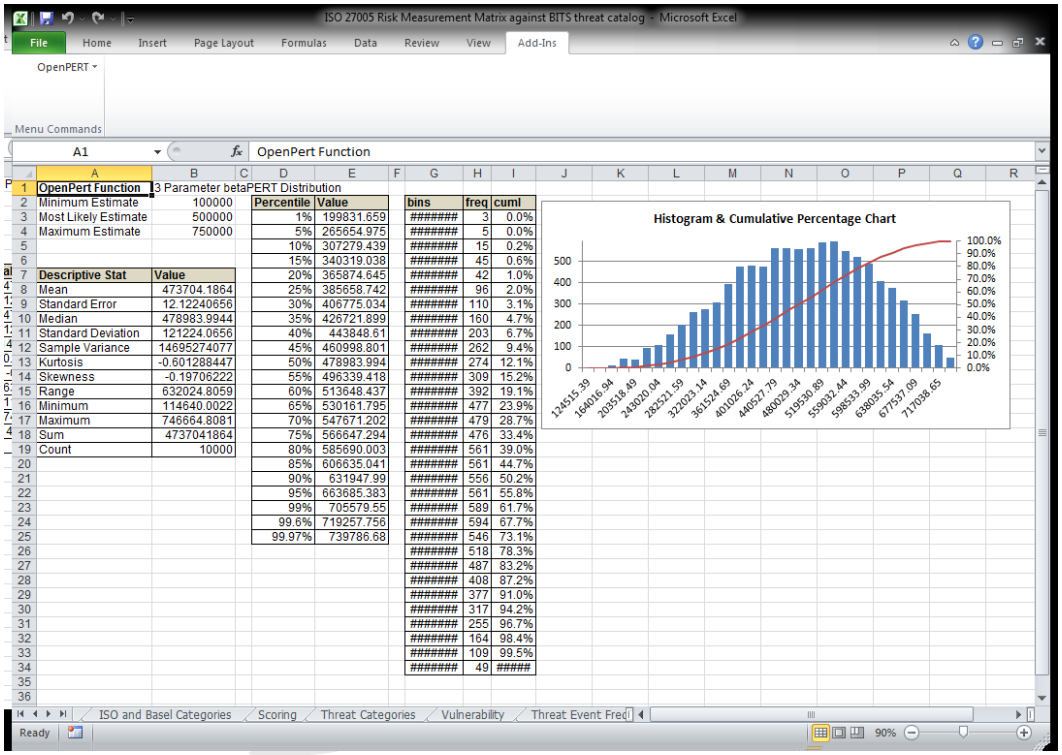
Lattice

OpenPERT


OpenPERT Simulation
Enter Minimum Estimate
100000
OK
Cancel


OpenPERT Simulation
Enter Most Likely Estimate
500000
OK
Cancel


OpenPERT Simulation
Enter Maximum Estimate
750000
OK
Cancel


ISO 27005 Risk Measurement Matrix against BITS threat catalog - Microsoft Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Add-Ins
OpenPERT
Menu Commands
A1
OpenPert Function
OpenPert Function
3 Parameter betaPERT Distribution
Minimum Estimate 100000
Most Likely Estimate 500000
Maximum Estimate 750000
Descriptive Stat | Value
Mean 473704.1864
Standard Error 12.12240656
Median 478983.9944
Standard Deviation 121224.0656
Sample Variance 14695274077
Kurtosis -0.601288447
Skewness -0.19706222
Range 632024.8059
Minimum 114640.0022
Maximum 746664.8081
Sum 4737041864
Count 10000
Percentile | Value
1% 199831.659
5% 265654.975
10% 307279.439
15% 340319.038
20% 365874.645
25% 385658.742
30% 406775.034
35% 426721.899
40% 443848.61
45% 460998.801
50% 478983.994
55% 496339.418
60% 513648.437
65% 530161.795
70% 547671.202
75% 566647.294
80% 585690.003
85% 606635.041
90% 631947.99
95% 663685.383
99% 705579.55
99.6% 719257.756
99.97% 739786.68
bins | freq | cuml
######## 3 0.0%
######## 5 0.0%
######## 15 0.2%
######## 45 0.6%
######## 42 1.0%
######## 96 2.0%
######## 110 3.1%
######## 160 4.7%
######## 203 6.7%
######## 262 9.4%
######## 274 12.1%
######## 309 15.2%
######## 392 19.1%
######## 477 23.9%
######## 479 28.7%
######## 476 33.4%
######## 561 39.0%
######## 561 44.7%
######## 556 50.2%
######## 561 55.8%
######## 589 61.7%
######## 594 67.7%
######## 546 73.1%
######## 518 78.3%
######## 487 83.2%
######## 408 87.2%
######## 377 91.0%
######## 317 94.2%
######## 255 96.7%
######## 164 98.4%
######## 109 99.5%
######## 49 #####
Histogram & Cumulative Percentage Chart
ISO and Basel Categories
Scoring
Threat Categories
Vulnerability
Threat Event Fre
Ready
90%

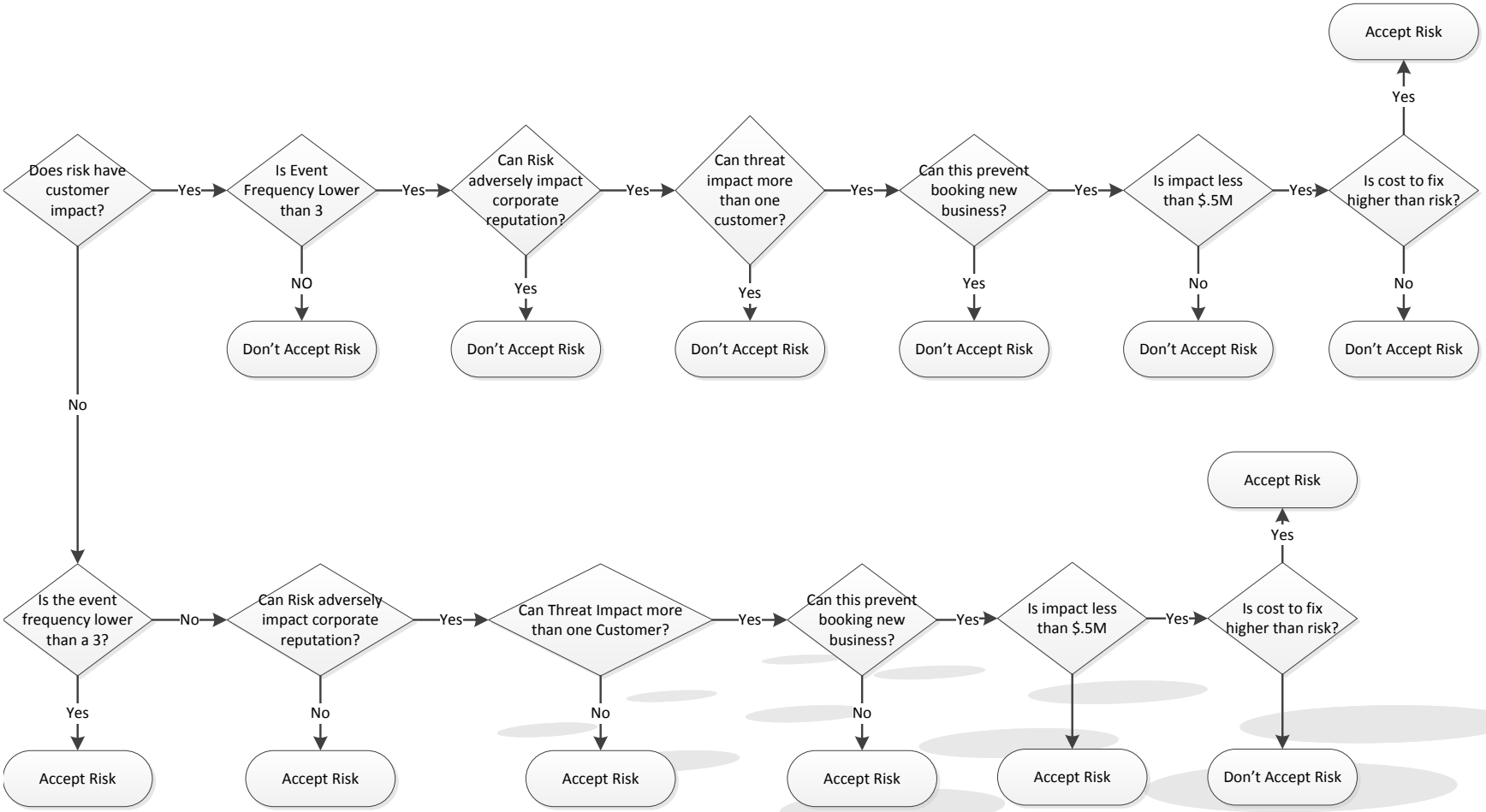
After the Analysis

- Document and communicate risk
- Determine how to manage
  - Remediate, Transfer, Avoid, Accept
- Determine what is residual risk from management strategy
- Implement risk management strategy

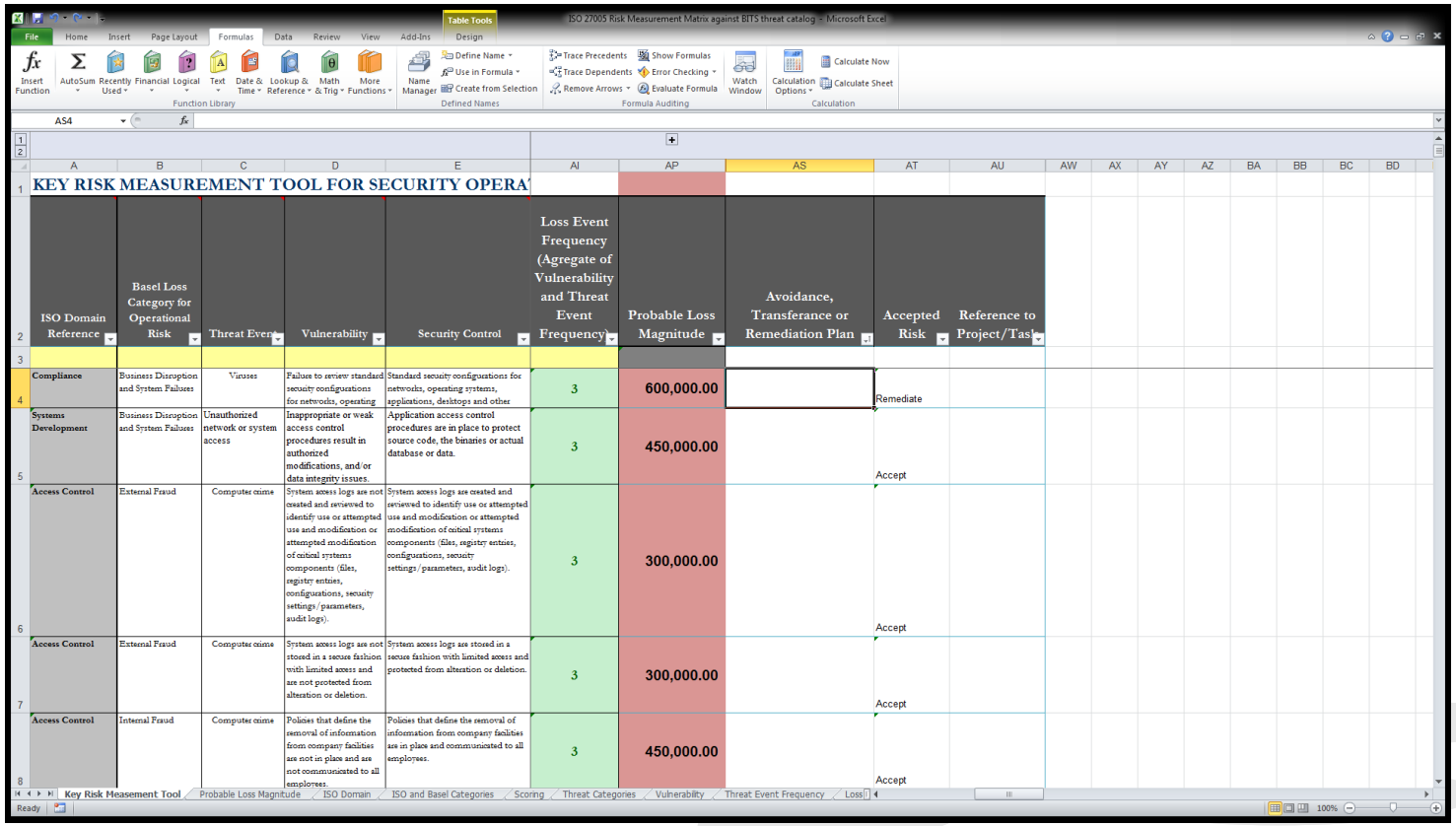
Remediation Strategy

- Does the risk have a impact on a system in scope?
- If no, then this risk is a candidate for acceptance.
- Does the risk have an impact of less than Tolerance in $
- If yes, then this risk is a candidate for acceptance.
- Can this risk adversely impact the public reputation of the company?
- If no, then this risk is a candidate for acceptance.
- Is the estimated event frequency of this risk less than a 3 in the Loss Event Frequency Matrix from the risk analysis?
- If yes, then this risk is a candidate for acceptance.
- Can the identified risk impact more than one customer?
- If no, then this risk is a candidate for acceptance.
- If the risk materialized into a security incident, could publicity impact the company's ability to book new business?
- If no, then this is risk is a candidate for acceptance.
-
- Independent of other criteria, if the cost of remediating, avoiding, or transferring the risk is greater than the impact, then the risk may be considered as a candidate for acceptance.

Or to put it more elegantly



If the recommendation is to remediate, enter your remediation plan, and the project/task to execute



KEY RISK MEASUREMENT TOOL FOR SECURITY OPERA

ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Loss Event Frequency (Agregate of Vulnerability and Threat Event Frequency)	Probable Loss Magnitude	Avoidance, Transferance or Remediation Plan	Accepted Risk	Reference to Project/Task
Compliance	Business Disruption and System Failures	Viruses	Failure to review standard security configurations for networks, operating	Standard security configurations for networks, operating systems, applications, desktops and other	3	600,000.00		Remediate	
Systems Development	Business Disruption and System Failures	Unauthorized network or system access	Inappropriate or weak access control procedures result in authorized modifications, and/or data integrity issues.	Application access control procedures are in place to protect source code, the binaries or actual database or data.	3	450,000.00		Accept	
Access Control	External Fraud	Computer crime	System access logs are not created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).	System access logs are created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).	3	300,000.00		Accept	
Access Control	External Fraud	Computer crime	System access logs are not stored in a secure fashion with limited access and are not protected from alteration or deletion.	System access logs are stored in a secure fashion with limited access and protected from alteration or deletion.	3	300,000.00		Accept	
Access Control	Internal Fraud	Computer crime	Policies that define the removal of information from company facilities are not in place and are not communicated to all employees.	Policies that define the removal of information from company facilities are in place and communicated to all employees.	3	450,000.00		Accept	

If not remediate, then

- Transfer
  - Cyberinsurance policies make a lot of sense for certain risks
- Avoid
  - Sometimes the impact is so bad that the best choice is to not take the chance
- Accept
  - Present the owner of the asset with a “Business Acceptance of Risk Form.”
  - Get a signature
  - Re-examine annually

Remediate

- In the end, this is just strengthening a control
- Controls are never 100% effective, even when implemented well
- That gap is your residual risk.
- The trick is selecting the right control is not easy
  - IE: RSA Breach showed that security awareness is not effective to prevent APT, as a single mistake means a compromise.
  - The control that caught the attack, a tool that does behavior analysis on internal traffic, only works when normative behavior is known.
  - So the residual risk is that you might implement this after the breach, not before, and therefor whitelist the breach as part of normative behavior.

Questions?

- wwilliams@lattice-engines.com
- walt.williams@gmail.com
- @LESecurity
- https://infosecuritymetrics.wordpress.com