

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 threatsource'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/js p/publications/PublicationDetails.jsp?c atalogno=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



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
 - $\,\circ\,$ How much skill is needed to over come them?
 - $\circ\,$ 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
 - o 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
 - $\,\circ\,$ How easy is it to encounter the method of egress
 - Probability of Acting
 - $\,\circ\,$ 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
 - o July 2, 1776
 - $\,\circ\,$ It was ratified on July 4, 1776
 - Experts often over estimate their level of confidence
 - $\circ~$ Until they learn to calibrate
 - $\circ~$ 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





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

File F	(? ~ ↓ Home Insert	Page Layout	Formulas Data	Review Vie	w Add-Ins		ISO 27005 Risk	Measureme	nt Matrix against BITS I	threat catal	og - Micros	soft Excel	-	-	-					-		-		a x
fx Insert Function	LtoSum Recently Fir Used *	ancial Logical Te	A pate & Looku r Time ▼ Referer orany	p & Math Mo nce + & Trig + Functi	re Dons + Manager E	Define Name	声 Trace Precedents 発 Trace Dependent 会 Remove Arrows Fi	Show s 🚸 Error @ Evalua ormula Audi	Formulas Checking * ate Formula ting	Calculation Options	Calcu Calculation	ulate Now ulate Sheet n												
G14	4 👻 💿	<i>f</i> _x Rep	utation																					~
- 4	А	В	С	D	E	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W)_
1 Probable	e 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																				_
8		lvioderate	\$ 10,000.00	s 99,999.00																				
9		Verv Low	\$ 1,000.00	\$ 999.00																				
10		,																						
11 12 Probable	Loce Magnitudo																							
13	coso magnitude		Loss Forms																					
14 Threat A	ction	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 Disclosu	ire	\$10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00																	
18 Modificat	tion	\$10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00	\$ 10,000.00																	
20 Worst Ca	ase Loss Magnitu	te \$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																	=
23																								
24																								
25																								
27																								
28																								
29																								
30																								
32																								
33																								
34																								
35																								
36																								
3/																								
39																								
40																								
41																								
42																								
43																								
44																								
45																								-
неры	Key Risk Measeme	nt Tool Proba	ble Loss Magnitu	ide / ISO Domain	/ ISO and Basel	Categories / Scoring	Threat Categori	es 🖉 Vuln	erability 🧹 Threat E	vent Frequ	ency 🖉 La	oss I 🖣 📃												▶ [
Ready 🎦																					Ⅲ□Ⅲ	100% —		+



Expand Each Category

	⊡ • • • 				Table Tools	ISO 27005 Risi	k Measurement Matrix	against BITS threat catal	og - Microsoft Excel							
	ile Home In	sert Page Layout	Formulas D	ata Review View	Add-Ins Design			d Ded	D and	Mandad	Colorianiani		Σ Auto	Sum • 🗛 🚓		
Pas	Copy -				Wrap lext Number	• €.0 .00 Condition	nal Format Check	Cell Explanate	Good	Linked Cell	Note	Insert Delete	Format	Zr mil	a Share WebE) ×
Ť	Format Painter Clipboard	Fon		Alignme	nt G Numb	Formattin	ig * as Table *	Explanat	Styles			Cells	- 🖉 Clear	 Filter Select Editing 	This File WebEx	
•	AI4	▼ (=INDEX('Loss Ever	nt Frequency'!\$J\$11:\$T	\$21,(AH4+1),(W4+1))				,					;		~
1						·				-	+		+	+		^
2	A	В	С	D	E	J	K	L	M	N	Т	W	AB	AG	AH	A
1	KEY RISK	MEASURI	EMENT T	OOL FOR SI	ECURITY OPERA	TIONAL RI	ISKS									
2	ISO Domain Reference 🔽	Basel Loss Category for Operational Risk	Threat Even	Vulnerability	Security Control	Minimum Skills/Resources needed	Mode Skills/Resource needed	Maximum s Skills/Resource needed	My Confidence in s Skills/Resources needed	Threat Capabilit <mark>e</mark>	Control Strengt <mark>-</mark>	Vulnerability (Capacity of the threat to overcome control)	Contact Frequenc	Probability of Action <mark>-</mark>	Event Frequency (Agregate of Frequency of Contact with Probabilit	Loss I Frequ (Agreg Vulner and T Eve Frequ
3																
4	Compliance	Business Disruption and System Failures	Viruses	Failure to review standard security configurations for networks, operating	l Standard security configurations for networks, operating systems, applications, desktons and other	70	2	85 9	0	84%	83%	3	82%	82%	7	3
5	Systems Development	Business Discuption 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 5	10 :	82%	82%	3	82%	82%	7	3
6	Access Control	External Fraud	Computer mime	System access logs are not created and erviewed to identify use or attempted use and modification or attempted modification of of citical systems components (files, registry entice, 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 caibeal systems components (files, seguity entries, configurations, security settings/parameters, audit logs).	1 70		85 5	0	82%	83%	3	82%	82%	7	3
7	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.	a70		85 9	10	83%	83%	3	82%	82%	7	3
8	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	10	83%	83%	3	82%	82%	7	3
Rea	Key Risk Me	easement Tool	Probable Loss Magni	itude 🖉 ISO Domain 🦼	ISO and Basel Categories Sco	oring / Threat Catego	ries / Vulnerability	/ Threat Event Frequ	ency Loss I 4						100% 🕞	
																÷ 0

Filter on domain, BASIL & Threat event

XII	∛ • (→ - ÷					Table Tools	ISO	27005 Risk	Measuremen	t Matrix agair	st BITS threat cat	alog - Microsoft Excel									
File	e Home In	nsert Page Layout	Formulas Di	ata Review	/iew Add-In	ns Design											Louise La	5	A 00	۵ (? - d ×
	Copy →	Garamond	• 14 • A A	= = »	Wrap T	Number	*	5 5		Normal	Bad	Good	Neutral	Calculation	n 🔶	÷ *	لي	J Autos	um 🕺 📶	i 🍑 📑	1
Paste	e 🛷 Format Painte	r B I <u>U</u> - E	🛛 • 🌺 • <u>A</u> •		Merge	& Center 🔹 💲 👻 %	• .0 .00 .00 →.0	Conditional Formatting	al Format I™ as Table ▼	Check Cell	Explana	tory Input	Linked Cell	Note	7	Insert Delete	Format	2 Clear	Sort & Find Filter T Selec	& Share WebB	x
	Clipboard	S Font	t G	Ali	Inment	5 Nur	nber 🗔					Styles				Cells			Editing	WebEx	
	AI4	\bullet (f_x =	=INDEX('Loss Even	nt Frequency'!\$J\$:	1:\$T\$21,(AH4+	+1),(W4+1))															*
1											•	•		+				+	+		
	А	В	С	D		E	J		K		L	M	N	Т		W		AB	AG	AH	A
1	KEY RISK	MEASURE	EMENT T	OOL FOR	SECUR	ITY OPER	ATIONA	L RIS	SKS												
2	ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Even	Vulnerabili	v S	ecurity Control	Minimum Skills/Res needed	ources	Mode Skills/Res needed	M sources Si	aximum tills/Resource eeded	My Confidence in s Skills/Resources needed	5 Threat Capability	Control Strengt	Vulne (Capac thro over cor	erability ity of the eat to rcome ntrol)	Co	ntact	Probability of Action	Event Frequency (Agregate of Frequency of Contact with Probabilit	Loss I Frequ (Agreg Vulner and T Eve Frequ
2 A	Ccess Control	Clients, Products and	Web defacements	No processes in pla	e to Default us	er ids are renamed or	-	70		85		90		ourcingt					· · · · ·	· · · · · ·	The
201		Business Practices		ensure default user	ds are disabled.								82%	83%		3	8	2%	82%	7	3
A	Access Control	Clients, Products and	Web defacements	Temporary, generic,	guest Temporar	y, generic, guest or		70		85		90	1								
		Business Practices		or anonymous user are not tightly	IDs anonymou use and tis	us user IDs are limited ir: phtly controlled.							82%	83%		3	8	2%	82%	7	#R]
205				controlled/monitor	ed.																
A 209	Access Control	Clients, Products and Business Practices	Web defacements	Policies / procedures addressing security « stored passwords h not been establishes Systems features to stored passwords (« encryption) have no been enabled.	Appropria of for the sec ive maintenan I. secure g., t	te controls are establishe use storage and see of password lists.	d	70		85		90	82%	83%		3	8	2%	82%	7	3
A	Access Control	Clients, Products and	Web defacements	Systems features (fo	roed The system	n is configured to require		70		85		90	1								
213		Business Practices		password change) h not been enabled or not exist. In abseno systems controls, m processes/procedur	ave the user to do during firs of anual is	o change initial password st logon.							82%	83%		3	8	2%	82%	7	3
A	Access Control	Clients, Products and	Web defacements	System timeout feat	ures The system	n is configured to		70		85		90	1								
047		Dusiness Practices		do not exist.	of users af	t or torre re-authenticatio fter a specified period of	n						82%	83%		3	8	2%	82%	7	3
217	Access Control	Clients, Products and	Web defacements	System unsuccessfu	inactivity. The system	n is configured to disable	•	70		85		90	1				+				
		Business Practices		logon attempt featu are not enabled or d	res or suspend o not number of	d user IDs after a fixed f unsuccessful logon							82%	83%		3	8	2%	82%	7	3
623				exist.	attempts.																
624																					
625 626																					
627	h N Kou Dich M	ansament Tool	robable Loss Marai	tuda / 100 D	in ICO and	Pagel Categories	coring / These	t Catagori	on / Multa-	philty / T	broat Event Free										
Read	y 6 of 620 records	found	Propable Loss Magni	icude / ISO Dom	in / ISO and	Basel Categories 2 S	coming / Threa	at Categori	es / vulne		nreat Event Freq	uency / Loss II 4								100% 😑	· · · ·

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/



OpenPERT

OpenPERT Simulation	ि २
Enter Minimum Estimate 100000	
ОК	Cancel
OpenPERT Simulation	१ X
Enter Most Likely Estimate 500000	
OK	Cancel
OpenPERT Simulation	१ ×
Enter Maximum Estimate	
ОК	Cancel

A1 OpenPert Function Percentite Value Image: Second	A1 A more function imum Estimate t Likely Estimate imum Estimate scriptive Stat an dard Error fian dard Error fian andard Deviation nple Variance tosis	<i>B</i>	C DeenPert C D aFERT Distrib Percentile 19% 10% 20% 25% 30% 35% 40% 40% 50%	E Function E Jution Value 199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 406775.034 406775.034 406775.034 406789.891 473983.994	F	G bins ######## ######## ######## ######## ####	H freq 3 5 15 45 42 96 110 160 203	I 0.0% 0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	J 500 - 400 - 300 -	K	Histogr	M am & Cun	N nulative P	o ercentage	P Chart	Q	10.0%
A B C D E F G H I J K L M N O P Q I Minimum Estimate 100000 Mainum Estimate 100000 Percentile Value 31.01% 100000 1	A enPert Function imum Estimate ti Likely Estimate imum Estimate ecriptive Stat an ndard Error filan ndard Deviation nple Variance tosis wmess	B 3 Parameter bel 100000 500000 750000 Value 473704.1864 12.12240556 14695274077 -0.601288447 -0.19706222	C D aPERT Distrib Percentile 1% 5% 10% 25% 20% 25% 30% 35% 40% 40% 50%	E Value 199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 479983.994	F	G bins ######## ######## ######## ######## ####	H freq 3 5 15 45 42 96 110 160 203	I cuml 0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	J 500 - 400 - 300 -	K	Histog	M am & Cun	N nulative P	0 ercentage	P Chart	Q	10.0%
OpenPert Function 3 Parameter betaPERT Distribution Minimum Estimate 500000 Maximum Estimate 500000 19% 29831.659 Weestimate 500000 19% 29831.659 Weestimate 500000 19% 20729.439 Weestimate 150.050 19% 307279.439 Weestimate 150.050 19% 307279.439 Weestimate 150.050 19% 3056674.245 Weestimate 100.05% Standard Error 127224.056 100006 40675.024 Weestimate 100.05% Standard Deviation 17222.40656 0.019706222 55% 20% 55% Stewness 0.019706222 50% 686830.01 Weestimate 10000 85% 686830.01 Weestimate 10000 85% 686830.01 Weestimate 561 99%% <td>enPert Function imum Estimate imum Estimate imum Estimate ecriptive Stat in ndard Error ifian ndard Deviation nple Variance tosis wmess</td> <td>3 Parameter bet 100000 500000 750000 473704.1864 12.12240656 478983.9944 12.1224.0656 14695274077 -0.601288447 -0.19706222</td> <td>aPERT Distrib Percentile 196 5% 10% 20% 20% 25% 30% 40% 40% 5% 5% 5% 5% 40% 5% 5% 5% 5% 5% 40% 5% 5% 5% 5% 5% 5% 5% 5% 5% 5</td> <td>ution Value 199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994</td> <td></td> <td>bins ####### ####### ####### ####### ######</td> <td>freq 3 5 15 45 42 96 110 160 203</td> <td>cuml 0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%</td> <td>500 - 400 - 300 -</td> <td></td> <td>Histog</td> <td>am & Cun</td> <td>ulative P</td> <td>ercentage</td> <td>2 Chart</td> <td>- 10 - 90 - 80</td> <td>10.0%</td>	enPert Function imum Estimate imum Estimate imum Estimate ecriptive Stat in ndard Error ifian ndard Deviation nple Variance tosis wmess	3 Parameter bet 100000 500000 750000 473704.1864 12.12240656 478983.9944 12.1224.0656 14695274077 -0.601288447 -0.19706222	aPERT Distrib Percentile 196 5% 10% 20% 20% 25% 30% 40% 40% 5% 5% 5% 5% 40% 5% 5% 5% 5% 5% 40% 5% 5% 5% 5% 5% 5% 5% 5% 5% 5	ution Value 199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994		bins ####### ####### ####### ####### ######	freq 3 5 15 45 42 96 110 160 203	cuml 0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	500 - 400 - 300 -		Histog	am & Cun	ulative P	ercentage	2 Chart	- 10 - 90 - 80	10.0%
Minimum Estimate 100000 Percentite Value bins freq cumit Miximum Estimate 750000 5% 256554.975 ######## 50.0%6 Maximum Estimate 750000 5% 256554.975 ######## 50.0%6 Descriptive Stat Value 90.9% 90.784 ######## 45.0.0%6 Standard Error 127.9240565 305657.442 ######## 42.0.0%6 Standard Deviation 127.9240565 305657.442 ######## 100.0% 90.0% Standard Deviation 127.9240565 40538.418 ######## 100.7% 90.0% 90.0% Standard Deviation 127.9240565 478083.984 ######## 308 152.5% 466398.801 ######## 308 152.5% Standard Deviation 1010766222 55%6 466398.8101 ######## 308 152.5% 400.5% 50.05% 0.05% 50.05% 0.05% 50.05% 0.05% 50.05% 0.05% 50.05% 0.05% 0.05% 0.05% 0.05%	imum Estimate st Likely Estimate imum Estimate an ndard Error dian ndard Deviation nple Variance tosis	100000 500000 750000 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	Percentile 1% 5% 10% 20% 25% 30% 35% 40% 45% 50% 50%	Value 199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 4267721.899 443848.61 460998.801 479983.994	9 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	bins ####################################	freq 3 5 15 45 42 96 110 160 203	cuml 0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	500 400 300		Histog	am & Cun	ulative P	ercentage	chart	- 10	10.0%
Most Likely Estimate 500000 1% [19831.659 ####### 3 0.0% Maximum Estimate 75000 50% [25656.434] 5 0.0% 109% J07279.439 ######## 16 0.2% 109% J07279.439 ######## 16 0.2% 109% J07279.439 ######## 16 0.2% 100% J07279.439 ######## 16 0.2% 100% J07279.439 ######## 16 0.2% 10000 4458404 ######## 10 16% 258andard Error 121224.0556 30% 405775.034 ######## 100 17% 358anderd Variance 14686274077 45% 460398.801 ######## 100 15% 358anderd Variance 14696274077 45% 460398.801 ######## 100 15.2% Maximum 1164640.0022 55% 496339.418 ######## 100 15.2% Sum 4737041864 75% 566647.294 ######## 100 10.0%	st Likely Estimate imum Estimate an ndard Error dian ndard Deviation nple Variance tosis	 500000 750000 Value 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222 	1% 5% 10% 20% 25% 30% 35% 40% 45% 50%	199831.659 265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994			3 5 45 42 96 110 160 203	0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	500 400 300		Histogi	am & Cun	iulative P	ercentage	e Chart	- 90	10.0%
Maximum Estimate 750000 55% 265654.975 ######## 5 0.0% Descriptive Stat Value 15% 340319.038 ######## 15 0.2% Standard Error 12% 240656 305874.45 ######## 96 0.0% Standard Error 12% 1240656 305% 406775 100.0% 90.0% 90.0% Standard Error 12% 1240656 305% 406775 100.0% 90.0% 90.0% Standard Error 12% 1240656 305% 406775 100.0% 90.0% 90.0% Standard Error 100.0% 43888.91 ######## 100.1% 90.0% 90.0% Standard Error 100.0% 43888.91 ######## 100.1% 90.0%	imum Estimate an indard Error dian ndard Deviation nple Variance tosis wness	750000 Value 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	5% 10% 20% 25% 30% 35% 40% 45% 50%	265654.975 307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994	5 3 5 5 1 1		5 15 45 42 96 110 160 203	0.0% 0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	500 400 300					IIII		90	0.0%
10% 307279.439 ######## 15 0.2% Descriptive Stat Value 20% 365874.645 ######## 45 0.6% Standard Eror 12.12240656 30% 406775.034 ######## 100.7% 500 Standard Deviation 121224.0856 40% 443.84.81 ######## 100.7% 500 Standard Deviation 121224.0856 40% 443.84.81 ######## 100.7% 400% 500% Standard Deviation 121224.0856 40% 443.84.81 ######## 200.8 500 Starules -0.019706222 65% 496.833.8418 ######## 303 15.2% Sum 473704.1864 75% 566647.294 ######## 315.2% 30.6% 56.15.2% 30.6% Sum 473704.1864 75% 566647.294 ####### 471 22.5% 42.7% ####### 471 22.5% Sum 473704.1864 75% 568647.294 ######### 471 42	an an an dard Error dian dard Deviation nple Variance tosis wness	Value 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	10% 15% 20% 25% 30% 35% 40% 45% 50%	307279.439 340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994	9 3 5 2 1 1	######## ####################################	15 45 42 96 110 160 203	0.2% 0.6% 1.0% 2.0% 3.1% 4.7%	500 400 300					HH,		90	0.0%
Descriptive Stat Value 15% 340319.038 ######## 42 0.6% Mean 473704.1864 25% 385658.742 ######## 96 20% Standard Error 12 1204056 39% 42671.189 ######## 96 20% Standard Error 12 1204056 39% 42671.189 ######## 96 20% Standard Error 10 30% 40% ######## 100 11% 40.0% 40	in and and Error dian ndard Deviation nple Variance tosis wness	Value 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	15% 20% 25% 30% 35% 40% 45% 50%	340319.038 365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994	3 5 2 1 1	**************************************	45 42 96 110 160 203	0.6% 1.0% 2.0% 3.1% 4.7%	500							- 80	1.070
Descriptive Stat Value 20% 356574.645 Immemmed 42 10% Standard Error 12.122.40656 30% 406775.034 Immemmed 96 20% 300 50.05% Standard Error 12.122.40656 30% 406775.034 Immemmed 203 67% 40% 50.05%	an an andard Error dian ndard Deviation nple Variance tosis wness	Value 473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	20% 25% 30% 35% 40% 45% 50%	365874.645 385658.742 406775.034 426721.899 443848.61 460998.801 478983.994	5 2 4 9 1	**************************************	42 96 110 160 203	1.0% 2.0% 3.1% 4.7%	400 -								1.0%
Mean 4737041864 25% 385658.742 ######## 96 20% Standard Error 12:1240666 39% 40675.54 ######## 100.31% 300 Standard Error 12:1240666 39% 40675.24 ######## 100.31% 300 Standard Error 14595274077 40% 4388480 ######## 203.67% 40.0% Standard Error 0.60128447 55% 406332.418 ######## 223.67% 40.0% Stewness -0.10708222 55% 406332.418 ######## 274.121% 10.0% 0.0% Stewness -0.10708222 55% 40617.752 ######## 129.21% 10.0% 0.0% Maimum 746564.8081 70% 5676.17.22 ######## 1472.22.87% ######## 1472.23.87% ######## 100.0% 10.0% 0.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0% 10.0%	an ndard Error dian ndard Deviation nple Variance tosis wness	473704.1864 12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	25% 30% 35% 40% 45%	385658.742 406775.034 426721.899 443848.61 460998.801 478983.994		######## ####################################	96 110 160 203	2.0% 3.1% 4.7%	300 -							- 70	0.0%
Standard Error 12:12240656 30% 406775.034 ######## 110 31% Median 478983.9944 45% 46998.4861 ######## 100 37% Sample Variance 14682274077 45% 46998.8944 100.7% 50% Sample Variance 14682274077 55% 496338.418 ######## 203 67% 10.0% Kurtosis -0.19706226 55% 496338.418 ######## 203 15.2% ######## 203 15.2% Mairmum 114640.0022 65% 530161.795 ######## 477 22.3 % 4.0% 5.0% Sum 4737041864 75% 566647.294 ######## 561 30.9% 5.05% 9.0% 5.0% Sum 4737041864 75% 566647.294 ######## 561 50.2% ######## 561 50.2% Sum 4737041864 75% 568647.294 ######## 561 50.2% ######## 561 50.6% Sum 4737041864 75% 568647.294 ######## 478 25.7% ####### 561 50.2% Sum 4737041864 75% 568647.294 ######## 478 25.6% ######## 561 50.2% #########################	ndard Error dian ndard Deviation nple Variance tosis wness	12.12240656 478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	30% 35% 40% 45% 50%	406775.034 426721.899 443848.61 460998.801 478983.994		######## ######## ####################################	110 160 203	3.1%	300 -							- 60	0.0%
Median 478983.9944 55% 426721.899 ####### 160 47% Standard Dvizto 10 12120.0666 49% 438.461 ######## 203 67% Sample Variance 14696274077 45% 460998.801 ######## 203 67% Stewness -0.10706222 55% 49633.9418 ######## 302 15.2% Mainmum 114540.0022 65% 530161.795 ######## 302 15.2% Mainmum 746664.8081 70% 547671.202 ######## 177 23.9% Sum 47375 566647.294 ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ######## 561 50.2% ####################################	dian ndard Deviation nple Variance tosis wness	478983.9944 121224.0656 14695274077 -0.601288447 -0.19706222	35% 40% 45% 50%	426721.899 443848.61 460998.801 478983.994		####### ######## ########	160 203	4.7%								- 50	1.0%
Standard Deviation 121224.0656 40% 443848.61 ######## 203 67% Sample Variance 1468624077 55% 469393.934 ######## 223 0.6% Kurtosis -0.601284477 55% 46933.948 ######## 220 12.9% Marimum 114640.0022 65% 530161.786 ######## 477 23.9% Marimum 114640.0022 65% 530161.786 ######## 471 23.9% Sum 4737041864 75% 566647.294 ######## 561 30.9% Sum 4737041864 75% 568637.041 ######## 561 30.9% 00% 85% 60838.533 ######## 561 58.9% 59.9% 58.5% 59.9% 58.5% 59.9% 58.5% 58.5% 59.9% 58.5% 58.5% 59.9% 58.5% 58.5% 59.9% 58.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% 59.5% </td <td>ndard Deviation nple Variance tosis wness</td> <td>121224.0656 14695274077 -0.601288447 -0.19706222</td> <td>40% 45% 50%</td> <td>443848.61 460998.801 478983.994</td> <td></td> <td>######## #########</td> <td>203</td> <td></td> <td>200</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>- 40</td> <td>1.0%</td>	ndard Deviation nple Variance tosis wness	121224.0656 14695274077 -0.601288447 -0.19706222	40% 45% 50%	443848.61 460998.801 478983.994		######## #########	203		200							- 40	1.0%
Sample Variance 14595274077 4595 460998.801 Immemer 282 9.4% Stewness -0.01706222 55% 496339.418 Immemer 324 12.1% 10.0% 0.03% Minimum 114440.0022 65% 530151.795 Immemer 477 12.3% Immemer 477 13.0% Immemer 561 14.7% Immemer 561 14.7% Immemer 561 14.7% Immemer 561 14.7% Immemer 561 150.2%	nple Variance tosis wness	14695274077 -0.601288447 -0.19706222	45% 50%	460998.801 478983.994		########		6.7%	200 -							- 30	1.0%
Kurtosis 0-0601288447 50% 478983.994 ######## 2741 12.1% Range 632024.8059 60% 513648.437 ######## 2001 12.0% Mairmum 114640.0022 65% 530161.795 ######## 477 22.7% Sum 4737041864 75% 566647.294 ######## 477 23.4% Minimum 110000 85% 65386.5331 ######## 561 30.0% Sum 4737041864 75% 566647.294 ######## 561 50.2% 99%% 65386.5331 ######## 561 50.2% 95% 95% 95% 99.6% 719257.755 ######## 581 70.5% 95%	tosis wness	-0.601288447 -0.19706222	50%	478983.994			262	9.4%	100 -		╺╺┠╢╢		T III I		\mathbf{T}		1.0%
Skewness -0.19706222 55% 496339.412 ######## 300 115.2% Minimum 7148648.0059 65% 530161.795 ######## 477 23.9% Maximum 746664.8061 65% 530161.795 ######## 477 23.9% Maximum 746664.8061 75% 566647.224 ######## 477 23.9% ######## 611 30.0% 58560.031 ######## 561 30.0% 00% 58560.041 ######## 561 50.2% ######## 561 50.2% 99% 705579.55 ######## 561 50.2% ######## 478 586 ######## 561 50.2% ######## 479 30.0% ######## 561 50.2% ######## 561 50.2% ######## ######## 561 50.2% ######## ######## ######## ######## ####################################	wness	-0.19706222	CCA.			########	274	12.1%									0%
Range 632024.8059 60% 513648.437 ######## 192 19156 Minimum 114540.0022 65% 530181.795 ######## 177 23.956 Maimum 746664.8081 77% 566647.224 ######## 179 25.756 Sum 4737041864 75% 566647.234 ######## 476 33.4% Count 10000 85% 606350.411 ######## 561 30.9% 99.9% 70557755 ####### 556 50.2% 99.9% 99.9% 99.9% ######## 561 50.2% 99.9% 99.9% 99.9% 778.97.66 ######## 561 50.9% 99.9% 99.9% 778.97.66 99.9% 99.9% 778.97.66 99.9% 99.9% 778.97.66 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% 99.9% <t< td=""><td></td><td></td><td>1 55%</td><td>496339.418</td><td>3</td><td>#######</td><td>309</td><td>15.2%</td><td>1 "!</td><td></td><td></td><td></td><td></td><td>0.0</td><td>0.0</td><td>0. 6</td><td>070</td></t<>			1 55%	496339.418	3	#######	309	15.2%	1 "!					0.0	0.0	0. 6	070
Minimum 1148400022 65% 530161785 ######## 477 22.9% 4x84 yes 4x84 yes	nge	632024.80591	60%	513648.437	1	########	392	19.1%	53	~	0.08 1.5%	N. 6, N.	1.1° 23.3°	0° 1 M-2	9,55 19	ઙૼૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢૢ	- F
Maximum 746664.8081 70% 647671.202 ######## 476 28.7% % <td>imum</td> <td>114640.0022</td> <td>65%</td> <td>530161.795</td> <td>5</td> <td>########</td> <td>477</td> <td>23.9%</td> <td>2452</td> <td>A02-352,301</td> <td>251 202</td> <td>and apply a</td> <td>54.002.95</td> <td>2000000</td> <td>2802 153</td> <td>102</td> <td>-</td>	imum	114640.0022	65%	530161.795	5	########	477	23.9%	2452	A02-352,301	251 202	and apply a	54.002.95	2000000	2802 153	102	-
Sum 4737041864 75% 56647.294 ######## 476 33.4% Count 10000 85% 66647.294 ######## 476 33.4% 00% 63304.799 ######## 561 30.4% 90% 00% 63304.799 ######## 561 50.2% ######## 00% 63304.799 ######## 561 50.2% ######## 00% 63304.799 ######## 561 50.2% ######## 00% 63306.7505 ######## 561 50.2% ######## 99% 70507.555 ######## 561 7.7% ######## 561 7.3% 99.97% 739786.68 ######## 561 7.3% ######## 561 5.3% ####### 401 72.7% #9.9% 739786.68 ######## 561 5.3% ####### 408 72.2% ######## 561 5.3% ######### ####################################	imum	746664.8081	70%	547671.202	2	########	479	28,7%	Nº Nº	20 24	2 36	20 NO. No.	Nº 55	5 5 6	0 6 1	*	- F
Count 10000 80% 585600.023 ######## 561 39.0% ######## 561 39.0% ######## 561 39.0% 90% 631807.33 ######## 561 52.0% 99% 705577.56 ######## 561 52.0% 99.0% 719257.756 ######## 561 72.0% 99.97% 739786.88 ######## 561 72.5% ######## 541 73.1% ######## 561 52.5% 99.97% 739786.88 ######## 561 72.5% ######## 561 52.5% ######## 561 52.5% 56.5% 56.5% 56.5% 56.5% 56.5% 99.97% 739786.88 ######## 561 72.5% ######## 561 72.5% ######## 561 57.5% ####### 561 72.5% ####### 561 56.5% ####### 561 56.5% ####################################	n	4737041864	75%	566647,294		########	476	33.4%									
05% 06835.041 ######## 551 44.7% 00% 60386.330 ######## 551 50.2% 09% 703579.55 ######## 561 55.6% 99% 703579.55 ######## 561 55.6% 99% 703579.55 ######## 561 57.6% 99.97% 73978.68 ######## 561 77.5% ######## 561 57.3% ######## ######## 561 73.3% ######## ######## 561 73.3% ######## ######## 561 73.3% ######## ######## 561 56.5% ####################################	unt	10000	80%	585690.003	3	########	561	39.0%									
90% 631947.90 ######## 556 50.2% 95% 60386.383 ######## 561 55.8% 99% 70557756 ######## 561 55.8% 99.97% 739786.68 ######## 561 77.9% 99.97% 739786.68 ######## 541 73.1% ######## 428 72.3% ######## 427 ######## 427 90.2% ######## 541 73.1% ######## 428 72.5% ######## 542 73.1% ######## 427 80.2% ######## 541 73.1% ######## 427 50.2% ######## 541 73.1% ######## 427 50.2% ######## 541 73.1% ######## 428 57.2% ####### 541 73.1% ######## 428 57.2% ######## 541 73.1% ######### 140.8 87.2% ############			85%	606635.041		########	561	44.7%									
05% 663805383 99% 705579.55 99.67% 705579.55 99.97% 73978568 ######## 544 ######## 544 ######## 548 ####### 377 ####### 377 ####### 378 ######## 377 #########			90%	631947.99		#########	556	50.2%									
09% 708579.55 ######## 580 6.7.% 99.6% 719257.756 ######## 594 6.7.% 99.97% 739786.68 ######## 594 6.7.% ######## 518 7.3.3% ######## 518 7.3.9% ######## 178 546 7.3.1% ######## 407 33.2.% ######## 407 33.2.% ######## 407 33.2.% ######## 137 9.0.% ######## 317 9.4.2% ######## 158 90.5% ######## 109.95% ####### ######### 109.95% ######## 49 #######			95%	663685 383	ì	########	561	55.8%									
99.6% 719257.756 99.97% 739786.68 ######## 544 67.7% ######## 54 67.7% ######## 54 67.7% ######## 54 67.7% ######## 54 67.7% ######## 54 67.7% ######## 54 67.7% ######## 58 73 ######## 487 73 ######## 73 91.9% ######## 109.9% ######## 109.9% ######## 109.9% ######## 109.9% ####### ######## 49 #######			00%	705579.55	1		580	61.7%									
30.00 130786.63 99.97% 739786.63 ######## 546 73.3% ######## 578 78.3% ######## 407 83.2% ######## 407 83.2% ######## 407 83.2% ######## 377 91.0% ######## 377 91.0% ######## 137 94.2% ######## 110 99.5% ######## 109 99.5% ######### 49 #######			20,000	719257 756	í	########	594	67.7%									
35.81 % 1300000 1781000 ######### 151 78.3% ######## 487 83.2% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 191.0% ######## 100.0% ######## 100.0% ####################################			00 0704	730786.60	2		546	73 104									
######## 487 83.2% ######## 487 83.2% ######## 487 83.2% ######## 371 91.0% ######## 377 91.0% ######## 137 94.2% ######## 149 83.4% ######## 109 99.5% ######## 49 ########			59.9770	135700.00	2	#######################################	510	79 304									
1000 1001 <td< td=""><td></td><td></td><td></td><td></td><td></td><td>+++++++++++++++++++++++++++++++++++++++</td><td>107</td><td>02 204</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>						+++++++++++++++++++++++++++++++++++++++	107	02 204									
######## 400 67.2% ######## 377 91.0% ######## 137 94.2% ######## 142 255 ######## 164 84.4% ######## 164 98.5% ######## 109 99.5%						+++++++++++++++++++++++++++++++++++++++	40/	03.2%									
######## 37/ 94.2% ######## 37/ 94.2% ######## 101 98.4% ######### 109 99.5% ######### 49 ######							277	01.2%									
1 1 1 94.2% 1 1 94.2% 1 1 1 1 1 1 1 1 1 1 1 1 1						*****	3/1	91.0%									
######## [25] 90.7% ######## [16] 99.5% ######## 49 ######						****	31/	94.2%									
######## 104 99.5% ######## 49 #######							255	90.7%									
######## 1091 993.5% ######### 49 #######						########	164	98.4%									
######### 49 ######						########	109	99.5%									
						#########	49	#######									
					/ 150 and Bacel Categories - Caroling - Thread Categories	/ ISO and Basel /Stannvise / Scronn / Threat /Stannv	/ ISO and Basel Categories / Scoring / Threat Categories / Vult	150 and Basel Categories Scorpg Threat Categories Vulnerab	####### 408 87.2% ####### 377 91.0% ####### 377 91.0% ####### 357 96.7% ####### 255 96.7% ######## 255 96.7% ######## 255 96.7% ######## 109 93.5% ######## 409 ####### 409 ####### 49	####### 408 87.2% ######## 377 91.0% ######## 371 94.2% ######## 255 96.7% ######## 164 98.4% ######## 109 99.5% ######## 109 99.5% ######## 109 10%	####### 408 87.2% ######## 377 91.0% ######## 377 91.0% ######## 372% 91.0% ######## 144 98.4% ######## 109 99.5% ######## 109 99.5% ######## 49 ####### ISO and Base/ Catenories Scruing Threat Catenories / Universibility Threat Event Fred/1	######## 406 87.2% ######## 377 91.0% ######## 377 91.0% ######## 355 96.7% ######## 108 99.5% ######## 109 99.5% ######## 109 99.5% ######## 49 #######	######## 408 87.2% ######## 377 91.0% ######## 377 91.0% ######## 355 96.7% ######## 144 98.4% ######## 109 99.5% ######## 49 ####### 409 84% ######## ######## 49 ########	######## 408 87.2% ######## 377 91.0% ######## 255 96.7% ######## 255 96.7% ######## 1408 98.4% ######## 109 99.5% ######## 109 99.5% ######## 408 ########	######## 408 37.2% ######## 371 91.0% ######## 255 96.7% ######## 1255 96.7% ######## 1408 39.5% ######## 109 99.5% ######## 109 99.5%	######## 408 87.2% ######## 371 91.0% ######## 255 96.7% ######## 255 96.7% ######## 164 98.4% ######## 164 98.3% ######## 164 98.3% ######## 164 98.3% ######## 49 ########	######## 408 87.2% ######## 317 94.2% ######## 255 67.7% ######## 256 67.7% ######## 256 67.7% ######## 108 99.5% ######## 108 99.5% ######## 43 ########



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

🗶 🛃 🎝 - 🗞 - 🔤				Table Tools	ISO 27005 Ris	k Measurement Matrix aga	inst BITS threat catalog - Microsoft E	xcel									
File Home Ir	sert Page Layout	Formulas Da	ata Review View	Add-Ins Design) 🕜 🗆 🗗 👌
fx Insert Function	ently Financial Logical d Functio	Text Date & Loo Time * Refe	okup & Math More erence * & Trig * Function	> Define Name ▼ Name Manager Create from Selection Defined Names	S= Trace Preceden	its ∰ Show Formulas ints ∲Error Checking * s * @ Evaluate Formula Formula Auditing	Watch Window Calculation Options - Calculation	Now									
AS4	▼ (* _ f x																
1						+											ĺ
A	В	С	D	E	Al	AP	AS	AT	AU	AW	AX	AY	AZ	BA	BB	BC	BD
1 KEY RISK	MEASURI	EMENT T	OOL FOR SI	ECURITY OPERA													
ISO Domain 2 Reference	Basel Loss Category for Operational Risk	Threat Even	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/Tas								
3																	
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 zoess logs are not rested and seviewed to identify use or attempted use and modification or attempted modification of caibal systems components (files, registry entities, configurations, security settings/parameters, audit logs).	System seess logs as created and createred to identify use or attempted use and modification or attempted modification of attempted modification of attempted modification or attempted monoponante (list, explort, entries, comfigurations, security settings/parameters, sudit 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									
Key Risk M	easement Tool	Probable Loss Magnit	tude / ISO Domain /	ISO and Basel Categories / Sco	ring / Threat Catego	ories / Vulnerability /	Threat Event Frequency 🖉 Loss 🗌	4									
Ready 🔚															≝[[] [] 1	00% ——	



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

