A Hacker's Guide to Risk

Bruce Potter

DefCon

gdead@shmoo.com || bpotter@keywcorp.com

Don’t believe anything I Say

- Also, hold those around you accountable

Failures in Understanding Risk

- Fukushima
- BP Oil Spill

The other side of the coin…

- Takata airbag recall
  - Airbag inflator may rupture shoot shrapnel onto passengers during deployment
  - Takata knew about the defects in 2004 and attempted to test bags in off-hours to avoid disclosure
  - NHTSA has been criticized for their “slow roll” on the problem
  - 34 million cars effected in North America. Largest single recall in the history of automobiles

MATH!

The Math Behind the Takata Recall

- Number of cars on the roads per year in the US: 250,000,000
- Number of accidents in US per year: 5,500,000 (2009)
- Number of accidents involving airbag deployment: Let's say 30%... Hard to find but 70% of reported crashes are property damage only)
  - (let's assume 100% of these involve a Takata airbag.. And it deploys. In reality 94% of effected cars have 1 Takata airbag… 6% have 2. None have more)
  - (also in reality, airbags only deploy about 80% of the time in serious crashes)

- So the number of Takata airbags deployed is on the order of
  - (# affected[[]] cars / # cars on road) * # of airbag deployments/year = 224,400 crashes / year where a Takata airbag deploys

- “Airbag inflator **may** rupture shoot shrapnel onto passengers during deployment”
- Ballistic testing indicates failure rates up to .084%
  - Some samples were ~.04%

- That’s brings us to ~188 people/year potentially injured by Takata airbags
  - Some of those people would died regardless
  - My assumptions to this point have been worse case
  - Let’s say in reality we’re talking about 100 people/year

LARGEST RECALL IN US AUTOMOTIVE HISTORY

- Takata - $500 million
- Honda - $340 million
- Others haven’t reported

- Easily over $1 billion

Is preventing 100 injuries a year worth $1 billion?

Death Statistics

- ~500 people/year die from TB
- ~500 people/year die from accidental gunshot wounds
  - What would a billion do for them?
- 40,000 people/year die from suicide
  - What would a billion do for them?

What is Risk?

- Like really.. What the hell is “risk”?

What is Risk?

- Risk to a bank – Situations that can lead to loss of funds or profit
- Risk to a manufacturing org – situations that lead to loss of IP and pricing data
- Risk to an ISP – Situations that can lead to service disruption or lost of customer data
- In general, risk is a situation where something you value can be put in harms way

Risk vs. Threat vs. Vulnerability

- Risk Syntax
  - $LIKELIHOOD that $CAUSE results in $IMPACT
- Threat Syntax
  - $ACTOR does $ACTION to $ASSET for $OUTCOME because $MOTIVATION
- Vulnerability
  - A weakness in a system that can be exploited

- Risk tends to be bigger/more general than threat. Multiple threats can role up in to a single risk
- Threats rely on vulnerabilities to be realized

An example

- Risk
  - It is highly likely that an attacker will gain access to our database server leading to loss of all personal information in database and heavily damaging our brand

An example

- Risk – Likelihood
  - It is highly likely that an attacker will gain access to our database server leading to loss of all personal information in database and heavily damaging our brand

An example

- Risk – Likelihood, Cause
  - It is highly likely that an attacker will gain access to our database server leading to loss of all personal information in database and heavily damaging our brand

An example

- Risk – Likelihood, Cause, Impact
  - It is highly likely that an attacker will gain access to our database server leading to loss of all personal information in database and heavily damaging our brand

An example

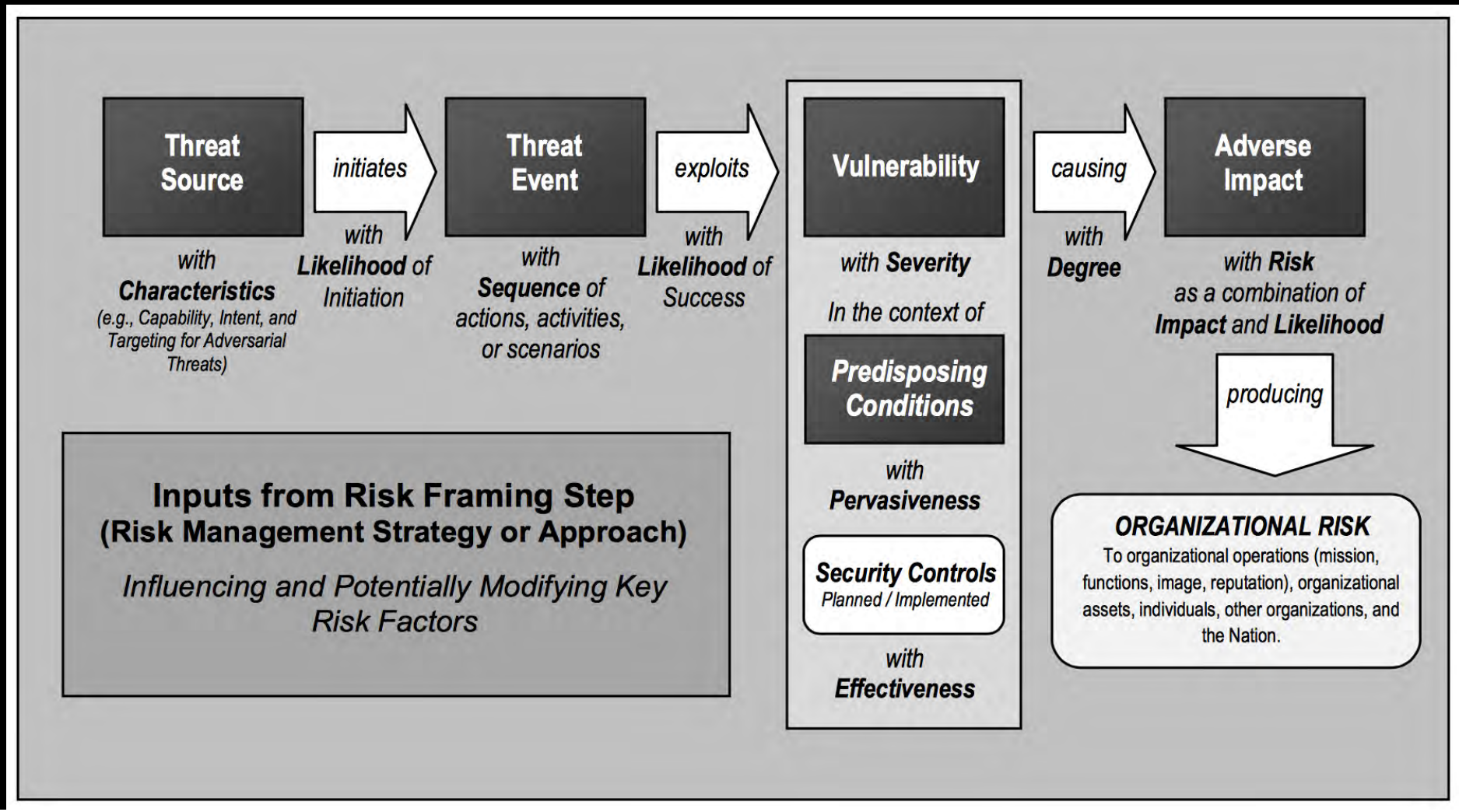
- Risk
  - It is highly likely that an attacker will gain access to our database server leading to loss of all personal information in database and heavily damaging our brand
- Threats
  - External attackers can execute SQL injection attack against our webservers
  - Insiders will inappropriately log in to the database server via shared credentials
  - Nation states will backdoor our database server hardware
- Vulnerabilities
  - Our website has SQLi weaknesses
  - We use shared creds for database access
  - We buy our servers from an Iranian on eBay

How Do We Measure Risk?

- NIST 800-30 (2002 publication)
  - Vulnerability X Likelihood X Impact

How Do We Measure Risk?

- NIST 800-30 (2012 publication)



Likelihood

- Choose a scale and stick with it
  - NIST 800-30r1 is a good starting point
- Another model that has served me well

Likelihood	Description
Very High	Almost Certain
High	Highly Likely
Medium	Somewhat Likely
Low	Unlikely
Very Low	Highly Unlikely

Likelihood	Description
High	Is happening to us or to others in our vertical
Medium	Happening to orgs not in our vertical
Low	Not happening

Impact

- Again, NIST 800-30r1 is probably the easiest place to start

Impact	Description
Very High	Multiple Severe or Catastrophic
High	Severe or Catastrophic
Medium	Serious
Low	Limited
Very Low	Negligible

Types of Risk

- Technical Risk vs. Business Risk
  - Technical – Risk that impacts IT, engineering, development, or other “technical” operations
  - Business – Risk that impacts business operations
  - In my experience, the security industry is good at identifying technical risks and lousy at identifying business risks
- Inherent Risk vs. Residual Risk
  - Inherent – Risk in the “as is” system or system without compensating controls
  - Residual – Risk that’s left over after you’ve implemented controls/remediation activities

Understanding Threats?

- Google “Bruce Potter Derbycon Threat”.

Risk Frameworks

- NIST 800-30r1 – Guide for Conducting Risk Assessments
  - A process you can work through. Attempting to make Risk Assessments uniform throughout USG
- NIST Cyber Security Framework
  - Not something you "do". It's a common taxonomy of security controls and how you can measure "as is", "to be" and maturity
- Cyber VAR – Cyber Value At Risk
  - A structured way to put a concrete dollar amount around the impact of risk and a roll-up risk number to represent cyber risk
- HITRUST Risk Management Framework
  - Healthcare specific RMF
- If you squint, you can turn NIST 800-53, COBIT, ISO 27k, etc in to risk frameworks. This is the "control" view of the world and is quite common.

Why is Risk Important to Hackers?

- That was a lot of acronyms… and seems far removed from what most hackers care about
- Turns out, when we measure risk incorrectly, we lose credibility and traction
  - May even cause harm. Certainly cause wasted time
- Examples…

Imagine a vulnerability that…

- Requires you to be actively man-in-the-middle the victim (so you're a nation state or on the same LAN)
- The attack requires you to MiTM each individual TCP connection
- The attack requires $100 post processing to look inside the data just to see if there's anything of interest

- How would you rate this?

Imagine a vulnerability that…

Likelihood	Description
Very High	Almost Certain
High	Highly Likely
Medium	Somewhat Likely
Low	Unlikely
Very Low	Highly Unlikely

…Must actively MiTM…

Impact	Description
Very High	Multiple Severe or Catastrophic
High	Severe or Catastrophic
Medium	Serious
Low	Limited
Very Low	Negligible

…Must MiTM each TCP session…
…Have non-trivial amount of post processing…

Know what it is?

FREAK Out: Yet Another New SSL/TLS Bug Found

Old-school, export-grade crypto standard used until the 1990s can be triggered to downgrade security of client, servers, researchers find.

Turns out the old US government restriction of exporting strong encryption that led to the shipping of weaker 512-bit crypto products overseas didn't actually disappear with the outdated policy in the late 1990s. A group of researchers from Microsoft Research, INRIA and IMDEA, has found that some SSL/TLS client and server implementations--such as OpenSSL versions 1.01k and earlier and Apple Safari--can be forced to employ the weaker cipher suite.

The weaker SSL/TLS encryption key can be easily cracked, researchers say, and used to wage man-in-the-middle attacks on the secured connections in order to sniff passwords or other sensitive information.

FREAK New SS

Old-school, ex the 1990s can client, servers,

Turns out the ol strong encryptic crypto products outdated policy from Microsoft F some SSL/TLS OpenSSL versi be forced to em

The weaker SS researchers say attacks on the s passwords or ot

National Cyber Awareness Systen

Vulnerability Summary for CVE-2015-0204

Original release date: 01/08/2015

Last revised: 07/05/2015

Source: US-CERT/NIST

Overview

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0 remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-fo ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of t OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized modification

Up next… PCI

groans

Seriously, how specifically does PCI incorrectly deal with risk

- HUGE number of requirements levied on individual webservers… in particular on cipher types, key size, etc
  - At the time of PCI standard's creation, VERY little evidence that weak crypto configurations were being attacked
  - Fast forward to today, that's still the case
- The real issue are the backend systems and the integrity front-line systems like POS machines
  - These were being attacked before, and they're being attacked now

Has PCI incorrectly managed risk?

- Heartland was PCI compliant at the time they were breached
- Target was PCI compliant at the time they were breached
- Home Depot was PCI compliant at the time they were breached

- YES!

Does that stop people from bitching about SSL “misconfiguations”?

- Nope
- If you run VA tools against your network, you live this dream every day

Other Examples…

- DNSSec (/me looks around room for DT)
- EMET
- Shift to the Cloud

Operationalizing Risk (aka: So What?)

- Pick a framework and run with it
- Me? I like NIST 800-30 and the CSF
  - 800-provides the process, the CSF provides the structure

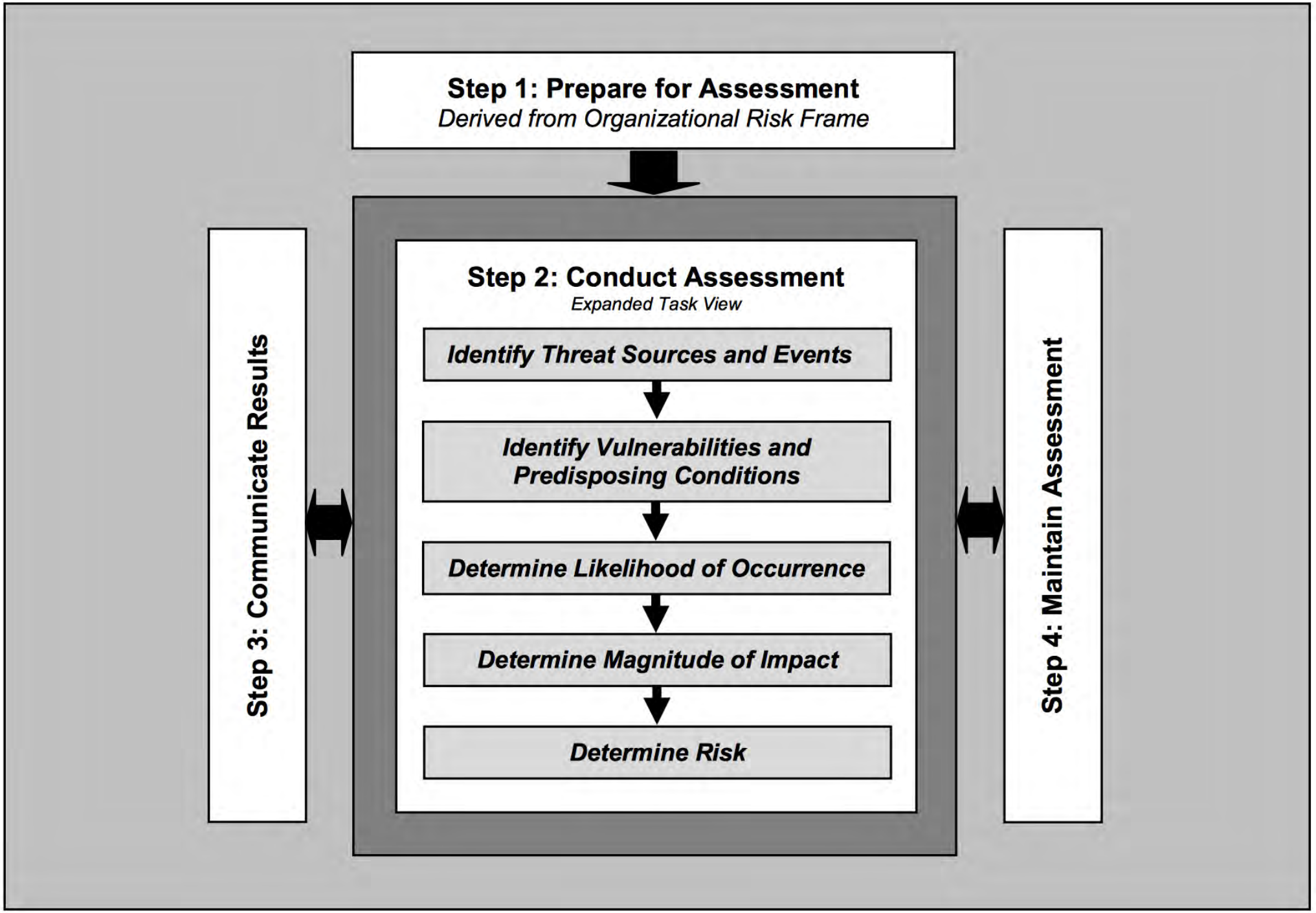


FIGURE 5: RISK ASSESSMENT PROCESS

Threat Modeling
- MS Style
- Mine
- Others?

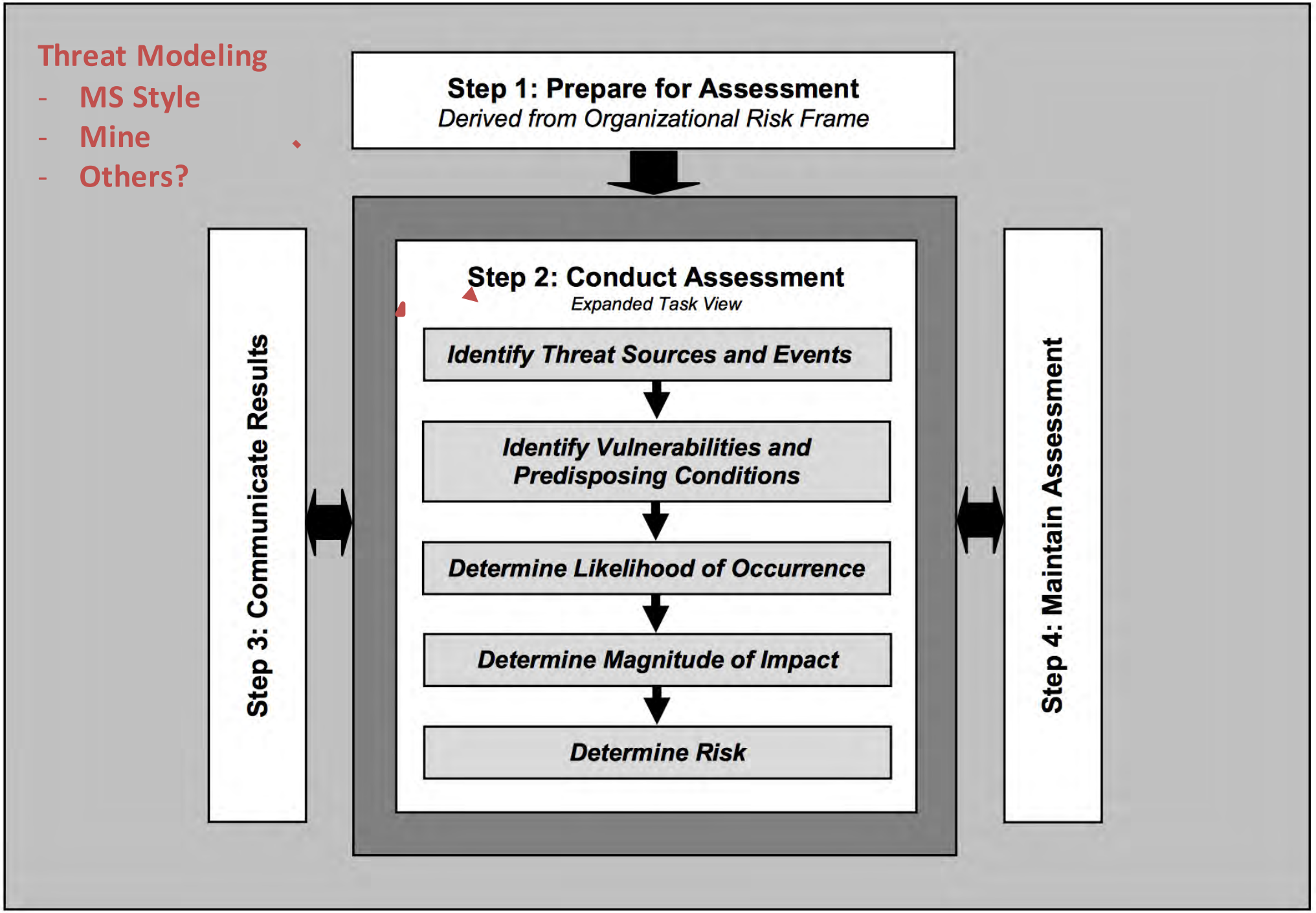


FIGURE 5: RISK ASSESSMENT PROCESS

Architectural assessment
Code Review
Pen testing / VA
Etc…

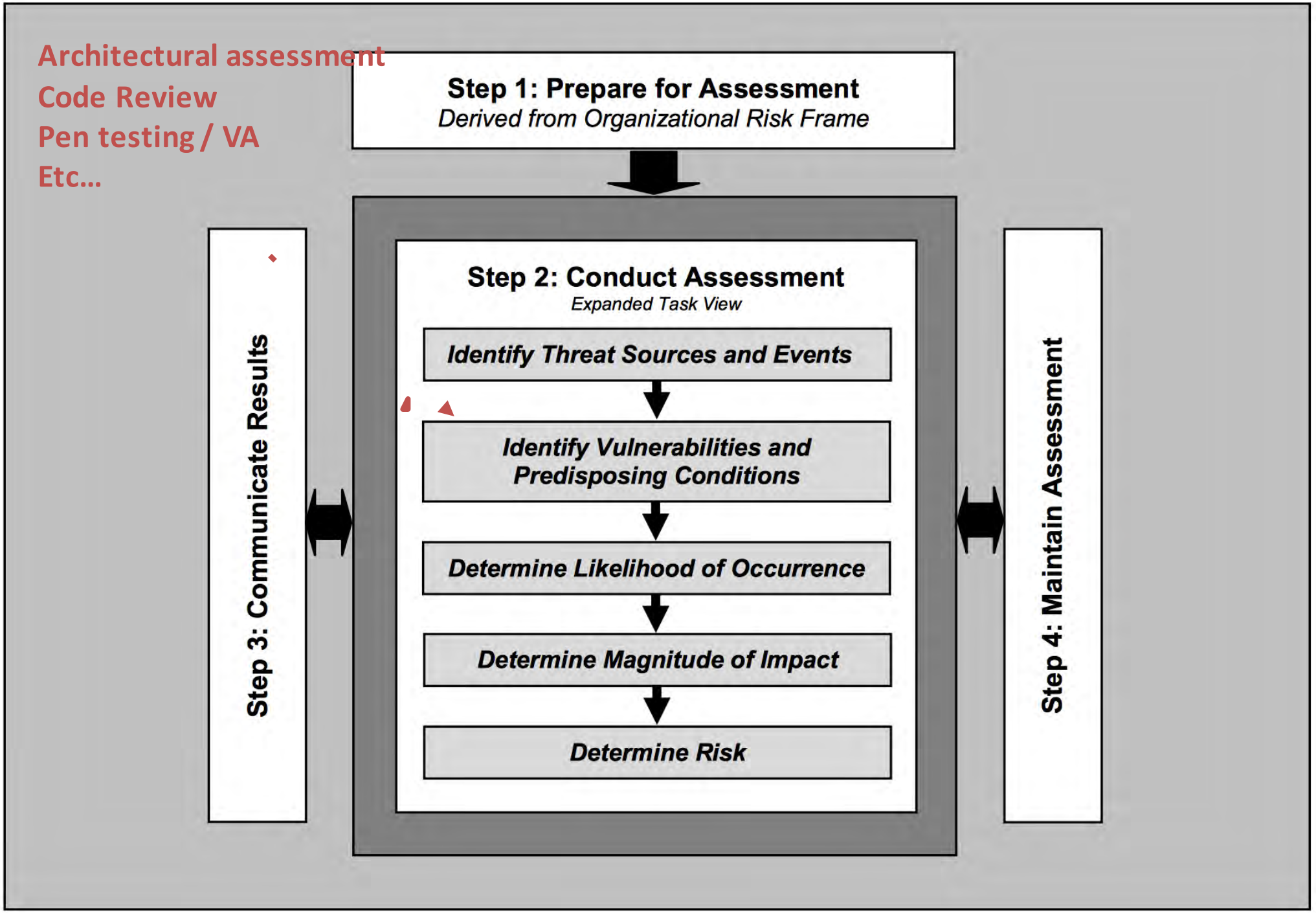


FIGURE 5: RISK ASSESSMENT PROCESS

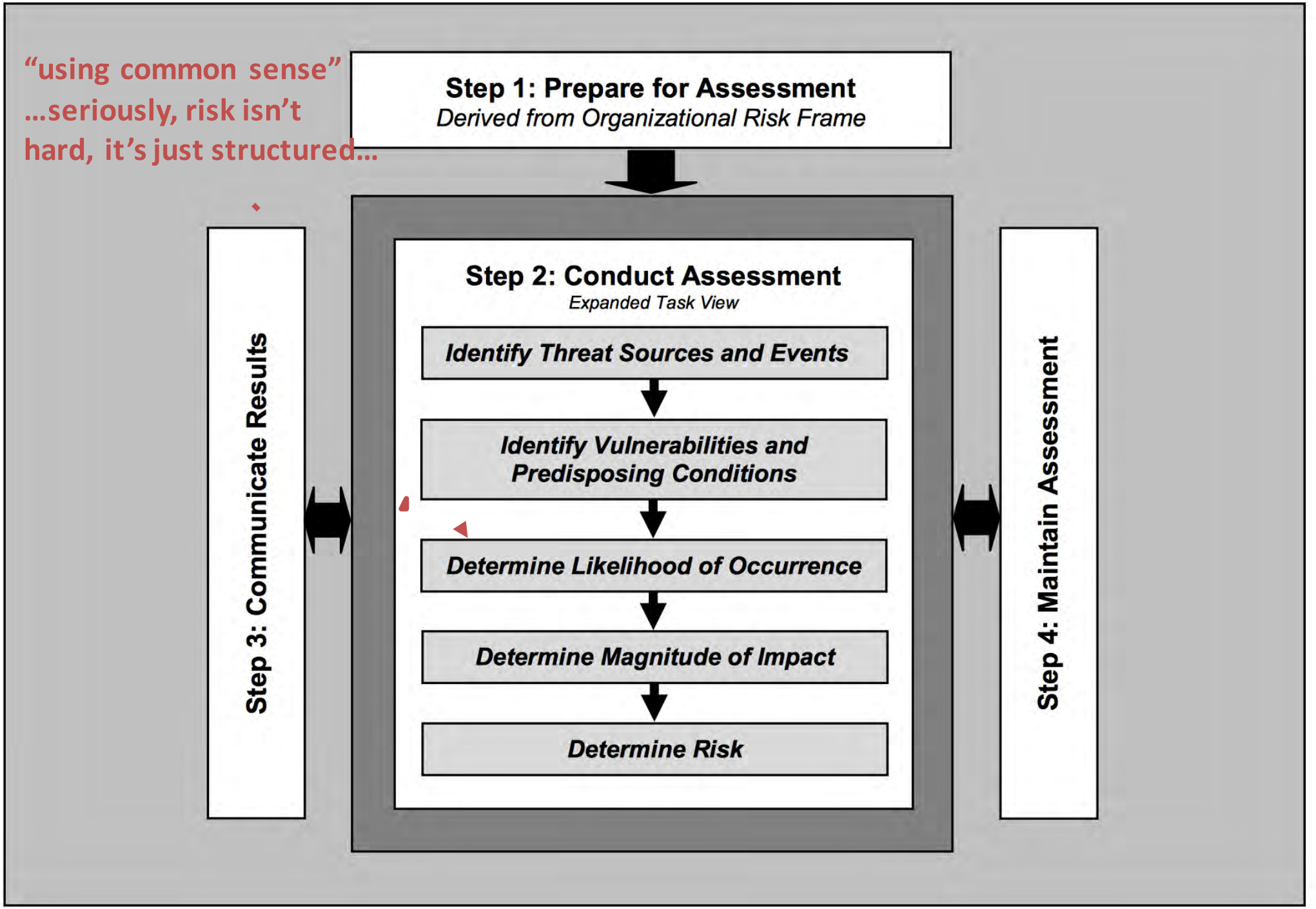


FIGURE 5: RISK ASSESSMENT PROCESS

The Core… aka: All Things Security

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS,MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

And in general

- Banks are big risk management machines
- So are cyber security orgs
- Apply risk concepts for
  - Vulnerability release and analysis
  - New defenses
  - New attack methods
  - New threat actors, campaigns, etc..
  - You know.. All the time, every day

Questions