30th Annual Minnesota Government IT Symposium

Why take the risk?
Doing risk assessments right.

December 7, 2011

Matthew J. Harmon
IT Risk LTD., LLC
Owner & Security Researcher
matthew@itriskltd.com

GSEC, GCIH, CISSP, CISA, ISO 27001 Lead Auditor
ISO JTC 1 / SC 31 / US TAG 7 "Security" Chairman
ISO JTC 1 / SC27 "IT Security Techniques" Liaison
SANS Mentor Instructor

What is an IT Risk Assessment?

- "An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures (*controls*) are adequate to reduce the probability of loss or the impact of loss to an acceptable level."
  Department of the Navy (OPNAVINST 5239. 1 A) 1980

- Overall process of risk identification, risk analysis, risk evaluation
  ISO Guide 73:2009

What does an IT Risk Assessment accomplish?

- IT Risk Assessments identify areas of potential loss and their impact on the organizations mission
- They put an organizations IT infrastructure into context with the organizations objectives
- They give senior management crucial information including threats, vulnerabilities and they identify where controls are lacking
- IT Risk Assessments help prevent loss, increase value and increase organizational resiliency.

Terms and Definitions

- Threat (or threat agent):
  Anything that is capable of acting against an asset in a manner that can result in harm. [FAIR]
  The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. [NIATEC]
  A threat agent has Capability, Intent and History [OWASP]

- Vulnerability:
  A weakness that could be exploited by a threat. The presence of a vulnerability does not in itself cause harm [NIATEC]

National Information Assurance Training and Education Center (NIATEC) niatec.info
Factor Analysis of Information Risk (FAIR) fairwiki.riskmanagementinsight.com
Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Category:Threat_Agent

Notice some new terminology? Threats, vulnerabilities, impact and our over arching term: RISK

Terms and Definitions

- Impact:
  To have an effect upon the confidentiality, integrity or availability of an asset
- Risk:
  Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. [NIST 800-30]
  ... or how long can you get away without patching before something bad happens. [MJH]

Reference: Federal Information Processing Standard (FIPS) 199. 2004. http://csrc.nist.gov/publications/fips
Source: NIST Special Publication 800-30 "Risk Management Guide for Information Technology Systems"

These two terms, Impact and Risk have a bit of debate surrounding them. For the purposes of this

IT Risk Assessments

Let’s get down to business, shal we?

Getting into the mindset for IT Risk Assessments

- Threats, vulnerabilities, likelihood and controls
- Prevent loss, generate value
- Can be applied to anything and should be
- Every project, activity, product, investment should have a risk assessment
- It is a key component of decision making
- Think of a big decision that was made recently as we move through this process

We're going to focus today on threats and controls
Risk Assessments, when properly used, help prevent loss and generate value
Prevent Loss - Direct: prevent data breach due to a lost laptop because the confidentiality control of whole disk encryption was in use or Indirectly

Popular Frameworks

- NIST 800-30: "Risk Management Guide for IT"
- ISO 27005: Security Techniques - Information Security Risk Management
- ISO 31010: Risk Management - Risk Assessment Techniques
- FAIR "Factor Analysis of Information Risk"
- CERT at CarnegieMellon University's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Risk Assessment Process

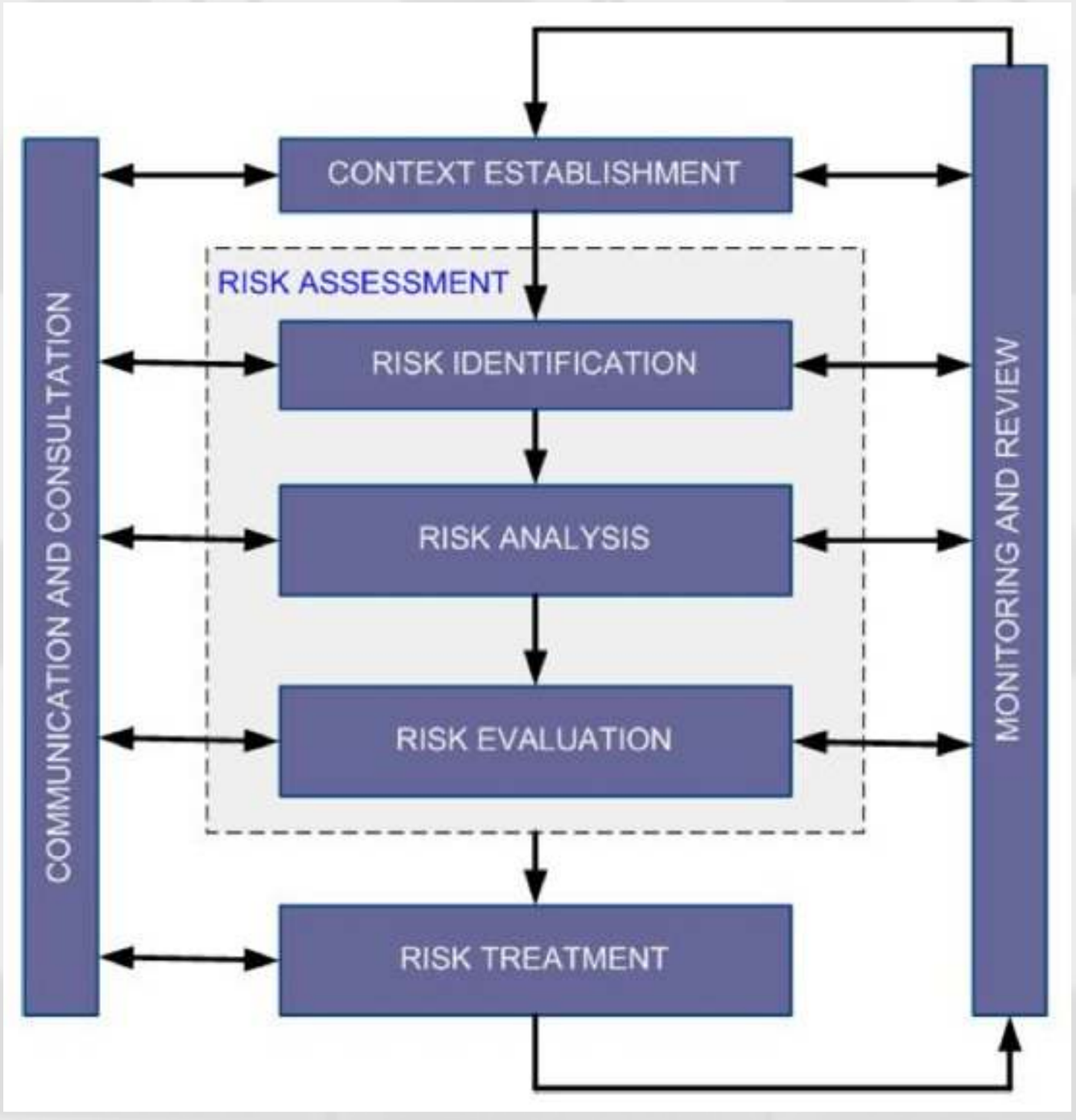
- **Plan**
  - Establishing Context, Risk Assessment
  - Develop risk treatment plan, Risk Acceptance
- **Do** - Implement the risk treatment plan
- **Check** - Monitor and review risks
- **Act** - Maintain and improve

Reference: ISO/IEC 27001 Security Techniques - Information Security Management System
Reference: Julia H. Allen, Software Engineering Institute, 2006/2008 "Plan, Do, Check, Act"
https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/574-BSI.html

Risk Assessment Plan

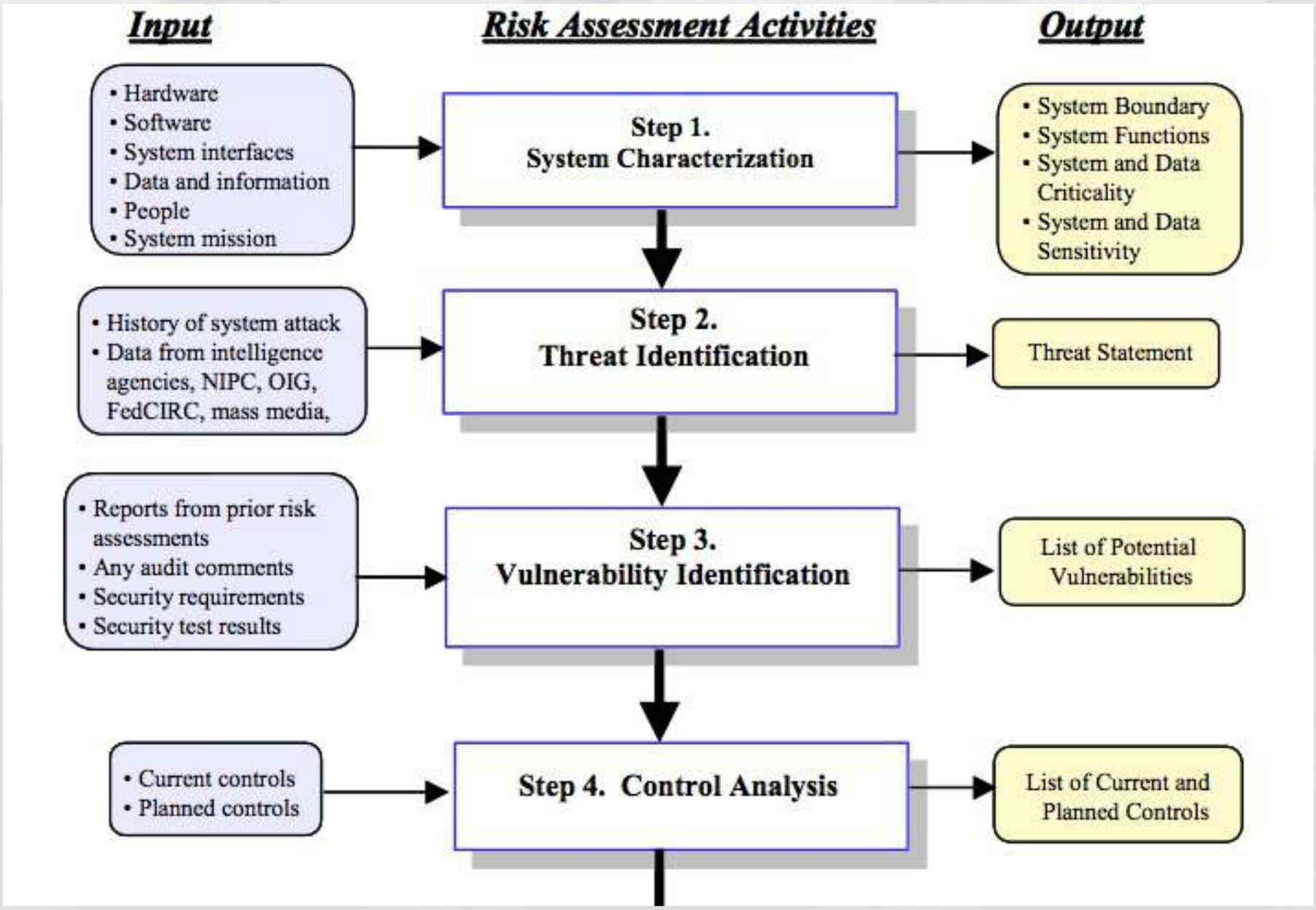
- Identify critical assets and business processes
- Identify threat agents and attack surface
- Identify vulnerabilities and exposure
- Identify scenarios where critical assets are vulnerable to threat agents and what would be necessary to stop the attacks
- How likely are the identified scenarios? Does the cost to stop the attack cost more than the loss?
- Compare what is necessary to the current state

Risk Management Process



Source: ISO/IEC 27005 "Information Security Risk Management" Figure 1 "The risk management process"

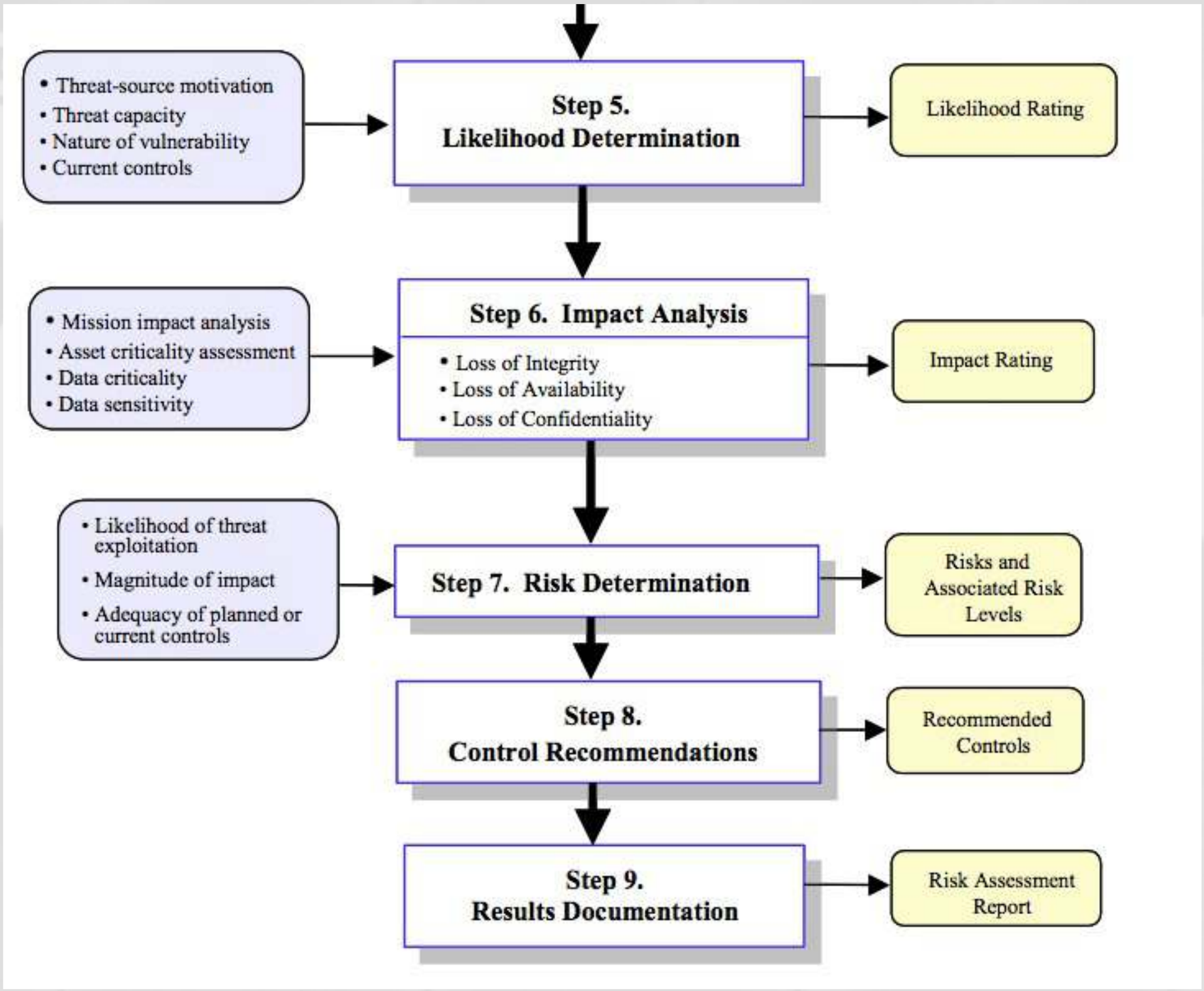
Risk Assessment Activities



Source: NIST Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Figure 3-1

Data Criticality, Data Sensitivity == Data Classification

Risk Assessment Activities



Source: NIST Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Figure 3-1

The Value of an Risk Assessment

Your best assurance and confidence booster is to actually implement the controls you identified as necessary during the assessment:

Confidence in Risk Assessments comes from the knowledge that your findings result in actions that help support the organizational mission.

Establish context

- Scope and Boundaries
- What is the organizational mission and values?
- Assemble your team:
  Senior Management
  Chief Information Officer (CIO)
  Information Systems Security Officer (ISSO)
  Business and Functional Managers
  IT Security Practitioners
  System and Information Owners

How to identify and characterize assets

- Your critical assets are those things which support your core mission.
- Data assets: names, identifiers, location, demographic, medical, employment, education, criminal history, trade secrets, deliberative process, intellectual property
- What processes would stop without IT?
  Look at Disaster Recovery efforts.
- Where does IT support business?
  Look at Sarbanes-Oxley IT processes, work flows and procedures

Reference: Ortwin Renn, A Model for an Analytic-Delibèrative Process in Risk Management, Center of Technology Assessment, Industriestrasse, Stuttgart, Germany. 1999 http://pubs.acs.org/doi/abs/10.1021/es981283m

Deliberative process, decision making

Threat Identification

- Scenarios: who, what, where, why, when, how?
- Intel's Threat Agent (TARA) Library 22 Attributes
  - Intent: **Non-Hostile**, Reckless behavior or Untrained employee. **Hostile,** such as Competitor, Government Spy, Disgruntled Employee, Activist, Thief, Vandal, Vendor
  - **Access**: Internal or External. **Outcome**: Theft, Business Advantage, Damage, Embarrassment, Technical Advantage, etc.
  - Capability: Resources, Experience and more...

Reference: Intel's "Threat Agent Library" http://www.intel.com/it/pdf/threat-agent-library.pdf

Threat Identification

- Physical Damage
- Natural Events
- Loss of essential services
- Compromise of information
- Technical failure

Make sure to include “real world” threats, such as physical damage (server dropped while being moved and power supply broke), natural events (Tornado, Collapsed Roof from Snow in the case of our Stadium), loss of essential services (extended power outage,

Vulnerability Identification

- Vulnerabilities are exposed areas with ineffective controls to prevent damage by a threat agent
- Software vulnerabilities left unpatched allow bypassing computer controls
- Security badges left on a restaurant table allow bypassing single-factor physical security controls
- Building a data center in a flood plain allows environmental conditions to impact availability

Vulnerability Identification

- Many tools exist in order to check for vulnerabilities:

  Nessus (by Tenable) will check for operating system vulnerabilities,
  Nipper (by Titania) to check firewalls rules,
  Netsparker (by mavituna security) to check web applications

- Software vulnerabilities are well documented:
  National Vulnerability Database: nvd.nist.gov
  Open Source Vulnerability Database: osvdb.org

Disclaimer: **Never run security tools on a production network without appropriate permission and training**

Nessus: tenable.com/products/nessus - Nipper: titania-security.com/nipperstudio - Netsparker: mavitunasecurity.com/netsparker/

Vulnerability Identification

- Penetration Test's simulate real attacks and should use a standard such as the Penetration Testing Execution Standard
- IT Audit evaluates the effectiveness and coverage of process, procedure, standards such as the Federal Information Security Management Act (FISMA), Payment Card Industry (PCI), DPA
- Start with a good known good configuration such as the United States Government Configuration Baseline (USGCB) and then add features

Reference: Penetration Testing Execution Standard. www.pentest-standard.org
Reference: Federal Information Security Management Act (FISMA) Controls. csrc.nist.gov/groups/SMA/fisma/
Reference: United States Government Configuration Baseline (USGCB). usgcb.nist.gov

DPA, Data Protection Act

Identifying Impact

- **Direct Impacts** include:
  - Replacement cost and operationalizing an asset
  - Cost of suspended operations
  - A security breach
- **Indirect Impacts** include:
  - Reallotment of resources (opportunity cost)
  - Potential misuse of information (data) obtained
  - Violations of regulatory obligations

Replacement cost, operationalizing, bringing something back into production

Impact Analysis

- What is harmed or lost?
- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- Availability - Ensuring timely and reliable access to and use of information
- Other losses: life, income, property

Reference: Federal Information Processing Standard (FIPS) 199. 2004. http://csrc.nist.gov/publications/fips

Identifying Controls

- Control groups include:
- **People** - Policies and Procedures, Training and Awareness, Physical Security
- **Technology** - Firewalls, Intrusion Detection Systems, Configuration Management
- **Operations** - Security Policies, System Certification and Accreditation

Identifying Controls

- Five major types of controls exist, a control may include multiple types

Type of Control	Purpose	Example
Directive	Provides Guidance	Policies and Procedures, login banner warnings
Preventive	Discourage or pre-empt errors	Configuration Management, encrypting data, backups
Detective	Uncover undesirable actions	Intrusion Detection, reporting account lockouts
Compensating	Makes up for a missing control elsewhere	"Creative controls"
Corrective	Corrects problems after discovery	Training, restoring from backups, account lockouts

Reference: Carolyn L. Lousteau, Mark E. Reid, The CPA Journal. 2006. http://www.nysscpa.org/cpajournal/2003/0103/features/f013603.htm
Reference: SANS IT Audit Blog, David Hoelzer. http://it-audit.sans.org/blog/2009/09/15/fundamental-it-audit-controls/comment-page-1/

David Hoelzer of SANS has a great example. No Smoking signs. The objective of this policy is to prevent smoke from cigarette smokers from impacting the health of others. So, we have a directive (guidance) and preventive control (discourage) – the signs, that's it. A detective control in this case would be a very sensitive smoke detector – but that only detects the presence of smoke, add triggering the sprinkler to put out the cigarette or draw the attention of physical security to remove the offender by lighting up a security board which is the (corrective) control. However, the smoke is still present in the air (or the floor if the sprinklers went off), so you would need to add an air evacuation system or cleaning crew to compensate.

Identifying Controls

- Industry and government experts have identified **20 Critical Security Controls** every organization should deploy broken into four areas:
- Quick Wins - Fundamental aspects of information security
- Improved Visibility - These sub-controls focus on improving monitoring
- Hardened Configuration / Hygiene - Reducing the attack surface
- Advanced - Further improve IT above and beyond

Reference: 20 Critical Security Controls, The SANS Institute. 2011. http://www.sans.org/critical-security-controls/guidelines.php

and all 20 map back to NIST 800-53 (FISMA)

Identifying Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on the Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Reference: 20 Critical Security Controls, The SANS Institute. 2011. http://www.sans.org/critical-security-controls/guidelines.php

Measuring Risk

- Constants:
  Threats, Vulnerabilities and Controls
- Risk = Threat x Vulnerability x Cost (or Impact)
- Risk = Threat x Vulnerability x Data Classification
- Still coming out of alchemy and into science
- The formulas frequently described are not meant to be used literally but instead to describe multipliers.

There are two main formulas used in the Risk Management industry, Threat x Vulnerabilities x Cost (or Impact) and substituting Impact for Data Classification
It is assumed that Data Classification has taken care of both the Cost and Impact values
However, there is a missing component, the control applied to the risk.
Some industries, such as Insurance, Environmental, Credit, and Fraud have a significantly more matured approach to risk management.

Quantitative Risk Analysis

- Uses numerical values for both consequence and likelihood
- Assumes everything can be measured
- Risks are treated because of their value and need of a sound basis for decisions
- Data points and historical data is limited but growing. Historical breach data is not as extensive as finance, insurance and fraud.

How to Measure Anything: Finding the Value of "Intangibles" in Business
by Douglas W. Hubbard, ISBN 0470539399 howtomeasureanything.com

Quantitative Risk Analysis

ARO (Annualized Rate of Occurrence)
x SLE (Single Loss Expectancy)
= ALE (Annualized Loss Expectancy)

- The Society of Actuaries have many advanced formulas for calculating risk.
- Don't use numbers when assigning risk where you don't have solid data. Use good sources, such as:
  DataLossDB.org OpenSecurityFoundation.org
  US-CERT.gov (US Computer Emergency Response Team)
  Multi-State Information Sharing & Analysis Center
- Verizon Business Breach Investigations Report

Society of Actuaries: www.soa.org
2011 Verizon Business Breach Report: http://www.verizonbusiness.com/go/2011dbir
Multi-State Information Sharing & Analysis Center http://msisac.cisecurity.org/

Qualitative Risk Analysis

- Prioritization and ranking of risks based on qualifying attributes to describe magnitude: Low, Medium, High
- Frequently, risks are treated because of the imperative to accomplish a mission
- Factual data should be used where available
- May build into a quantitative analysis where numerical data or resources are available

Qualitative Calculations

	Likelihood
Low	0-24% chance of threat agent exploiting a given vulnerability in a year
Moderate	25-74% chance of threat agent exploiting a given vulnerability in a year
High	75-100% chance of threat agent exploiting a given vulnerability in a year

Reference: National Information Assurance Training and Education Center (NIATEC) niatec.info
Reference: Federal Information Processing Standard (FIPS) 199. 2004. http://csrc.nist.gov/publications/fips

Qualitative Calculations

	Potential Impact	
Low	loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals	Causes degradation and effectiveness is noticeably reduced
Moderate	loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals	Causes *significant* degradation and effectiveness is *significantly* reduced
High	loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect on organizational operations, organizational assets, or individuals	Causes *severe* degradation and effectiveness is *severely* reduced

Reference: National Information Assurance Training and Education Center (NIATEC) niatec.info
Reference: Federal Information Processing Standard (FIPS) 199. 2004. http://csrc.nist.gov/publications/fips

Risk Determination

Regardless of the formula, there are constants: threat agents and vulnerabilities exist, controls should be effective at preventing damage and losses.

Impact		Minimal	Moderate	Significant
Likelihood	Unlikely	Low	Low	Mod
	Possible	Low	Mod	High
	Likely	Mod	High	High

Risk Treatment Plan

- Engage senior management and align threats identified with strategic organization objectives
- Focus efforts on the threats most likely and **recommend controls** to counteract those threats
- Low complexity to remediate and large attack surface? Low hanging fruit. Quick wins.
- High complexity to remediate and high asset value? Consider the motivated attackers.
- Some **residual risk** will always exist

Making strategic decisions

- **Accept** the risk?
  - Low value of asset, low probability of occurrence, low impact / damage prediction
- **Mitigate** the risk?
  - Apply appropriate controls and fix the flaw
- **Transfer** the risk?
  - Buy insurance or out-source. Reduces impact.
- **Avoid** the risk.
  - Remove the risk or find alternatives

Making tactical decisions

- If risk is accepted, increase directive and detective controls
- When mitigating a risk with a preventive or corrective control, test the vulnerability before and after applying the control to ensure effectiveness
- When transferring a risk, remember there is no complete transfer, out-sourcing causes control to be limited to contractual agreements and enforcement can be challenging.
- Risk avoidance is frequently the best bet.

Risk Matrix

The result.

Risk	Description	Threat	Vulnerability	Impact	Likelihood	Treatment	Residual
High	Workstations are not regularly patched and are vulnerable to malicious software	Organized crime uses malicious code to exfiltrate confidential data and spread	Workstations are not patched and users browse with local administrator rights	Confidentiality : High Availability: Medium Integrity: High	High Based on vulnerabilities exploited by malicious code [ISC]	Mitigate by: 1. Install anti-virus 2. Patch Systems 3. Harden Workstation Configuration 4. Training	Low

Reference: SANS Internet Storm Center. isc.sans.edu

Plan of Action & Milestones

The action.

Risk	Treatment	Contact	Resources	Completion Date	Milestones	Status
Workstations are not regularly patched and are vulnerable to malicious software	Mitigate by: 1. Install anti-virus 2. Patch Systems 3. Harden Workstation Configuration 4. Admin Training	Matthew J. Harmon	1. $50,000 Licensing 2. 12 Desktop Staff Weeks 3. 1000 hours 4. 8 hours/wk for 30 staff for 2 months	1. 2/10/2012 2. 2/21/2012 3.	1. Licenses acquisition, Deployment Schedule 2. Software inventory, Patch identification, Deployment Schedule 3. Apply USGCB controls to template image, tweak as needed, test with business units, deploy 4. Call SANS	Ongoing

Template: http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/POAM_template_01052007.xls

Take Away

- Risk Assessments are crucial to decision making
- Focus on threats and controls
- Use good data
- Regardless of how you measure it, Risk Assessments identify weaknesses that can impact organizational resiliency that should be acted on.

A unique point of view
Matthew J. Harmon

SANS Mentor Instructor for:
SEC 504 “Hacker Techniques, Exploits and Incident Handling” (GCIH)
SEC 464 “Hacker Detection for Systems Administrators”
SEC 401 “Security Essentials” (GSEC)

ISO JTC 1 / SC 31 / US TAG 7 "Security" Chairman
International Organization for Standardization Joint Technical Committee 1 / Sub-Committee 31 / US Technical Advisory Group 7 "Security for Item Identification" Chairman

ISO JTC 1 / SC27 "IT Security Techniques" Liaison
International Organization for Standardization Joint Technical Committee 1 / Sub-Committee 27 "IT Security Techniques" Liaison from SC 31

Member of the ISO Technical Management Board Steering Committee for Privacy

Elected Board Member for the Whittier Alliance and Whittier Business Association
Published: Plugging the Gaps in RFID Security (ISO Focus+, April 2010)

GIAC Security Essentials Certification (GSEC)
GIAC Certified Incident Handler (GCIH)
$(ISC)^2$ Certified Information Systems Security Professional (CISSP)
ISACA Certified Information Systems Auditor (CISA)
ISO 27001 "Information Security Management Systems" Auditor (ISO 27001 Auditor)

IT Risk LTD., LLC

matthew@itriskltd.com

IT Risk Ltd. performs IT risk assessments, advanced security testing, incident response, leads security research and participates in international standards development, and if you couldn't tell, we are passionate about what we do.

Thank you!

Questions?

I hope you enjoyed this presentation, it can be downloaded after the Symposium from:

https://github.com/itriskltd/ or
http://itriskltd.com/MNGTS2011-ITRisk.pdf