Lecture 8: Risk Management
Identifying and Assessing Risk

EECS711 Security Management & Audit

Objectives

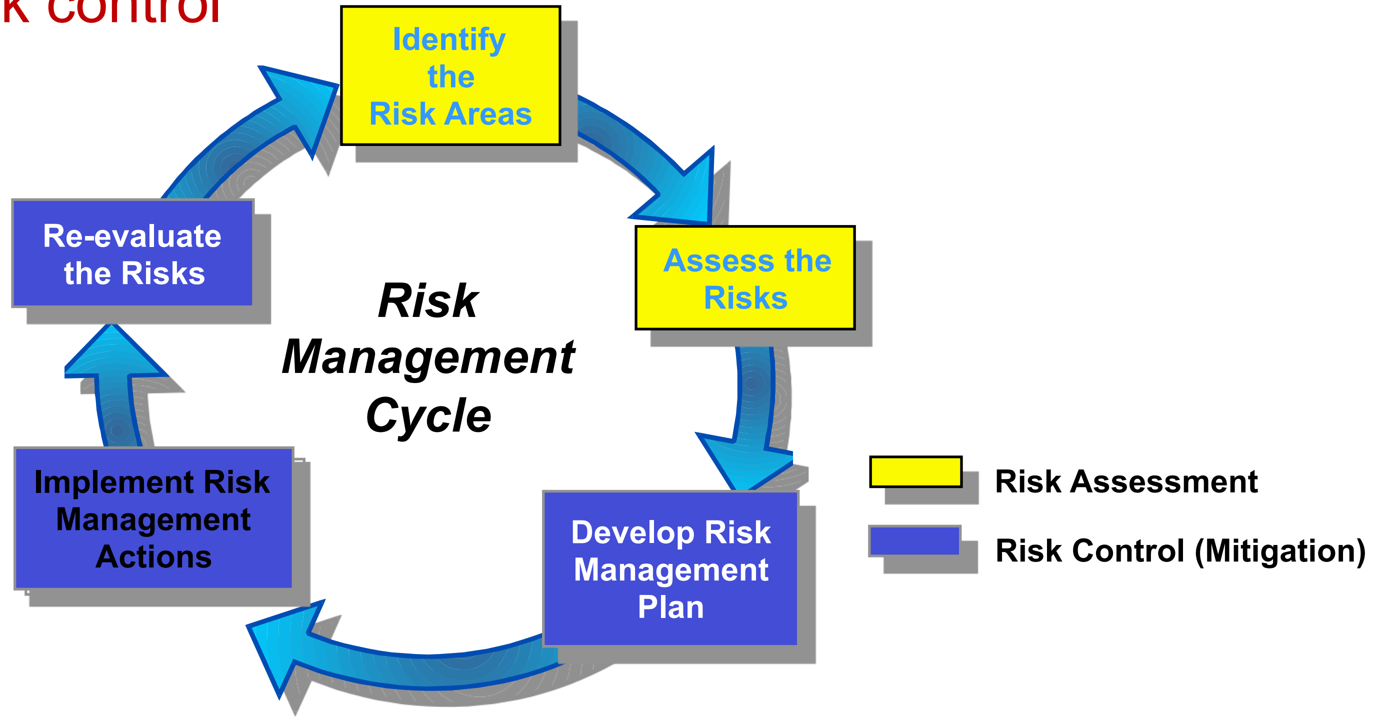
- Define risk management and its role in the organization
- Describe risk management techniques to identify and prioritize risk factors for information assets
- Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur
- Discuss the use of the results of the risk identification process

Risk Management

- Managing risk is one of the key responsibilities of every manager within the organization
- InfoSec program is created primarily to manage **IT risk**
  - Locate the weaknesses of their organization’s operations
  - Understand how the organization’s information is processed, stored, and transmitted
  - Identify what resources are available
- **Risk management** is a process of
  - discovering & assessing the risks to an organization’s operations
  - determining how those risks can be controlled or mitigated

Risk Management

- A well-developed risk management program should have **two** formal processes
  - Risk identification and assessment
  - Risk control



Identify the Risk Areas

Assess the Risks

Develop Risk Management Plan

Implement Risk Management Actions

Re-evaluate the Risks

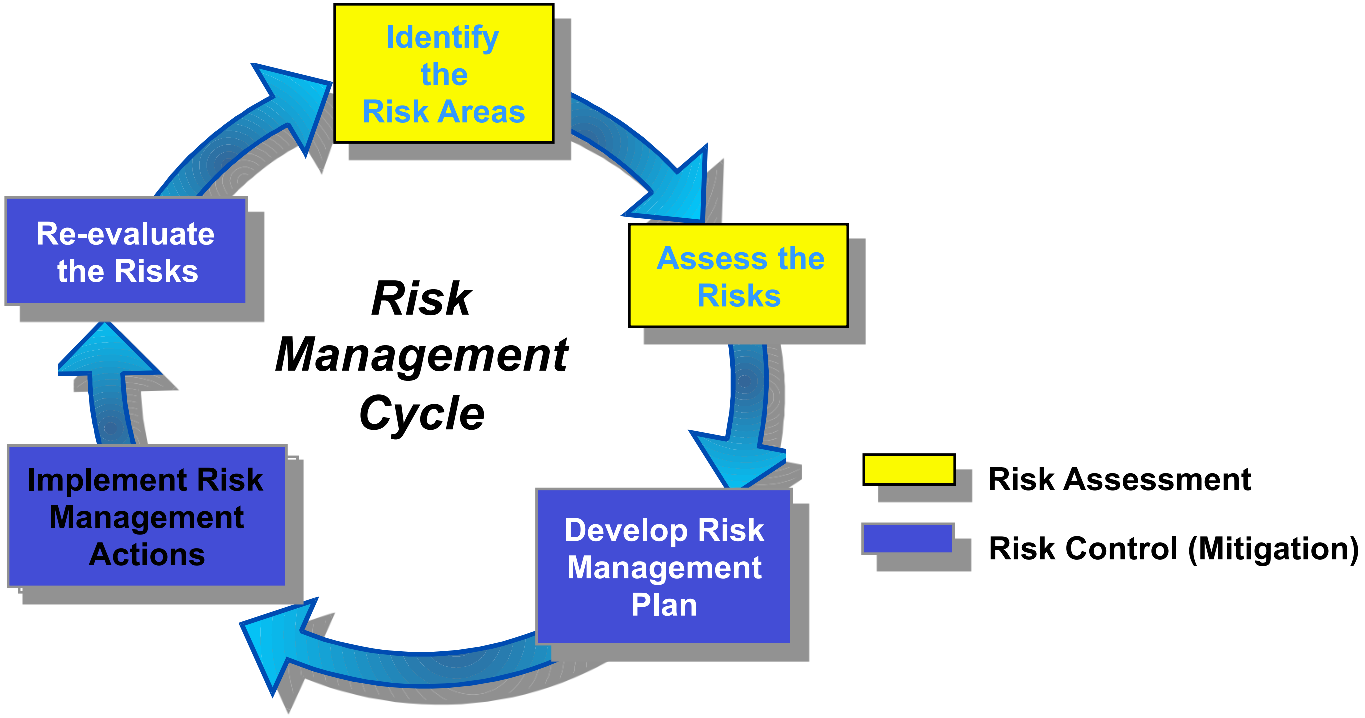
Risk Management Cycle

🟨 Risk Assessment

🟦 Risk Control (Mitigation)

Risk Management

- Risk management is a process
  - Safeguards and controls that are devised and implemented are not install-and-forget devices



Identify the Risk Areas

Assess the Risks

Develop Risk Management Plan

Implement Risk Management Actions

Re-evaluate the Risks

Risk Management Cycle

🟨 Risk Assessment

🟦 Risk Control (Mitigation)

Risk Management

- For any organization, risk management is about
  (1) knowing itself: ***Vulnerability Identification***
  (2) know its enemy
- **“Knowing Yourself”**
  – How information is processed, stored, and transmitted?
  – Which information assets are valuable?
    - Identifying, categorizing, and classifying those assets
  – How they are currently being protected?

Risk Management

- For any organization, risk management is about

  (1) knowing itself: ***Vulnerability Identification***

  (2) know its enemy: ***Threat Identification***

- **"Knowing the Enemy"**
  - Identifying, examining, and understanding the threats facing the organization's information assets
  - Managers must be prepared to identify those threats
    - Risks posed to the organization and the security of its information assets

Accountability for Risk Management

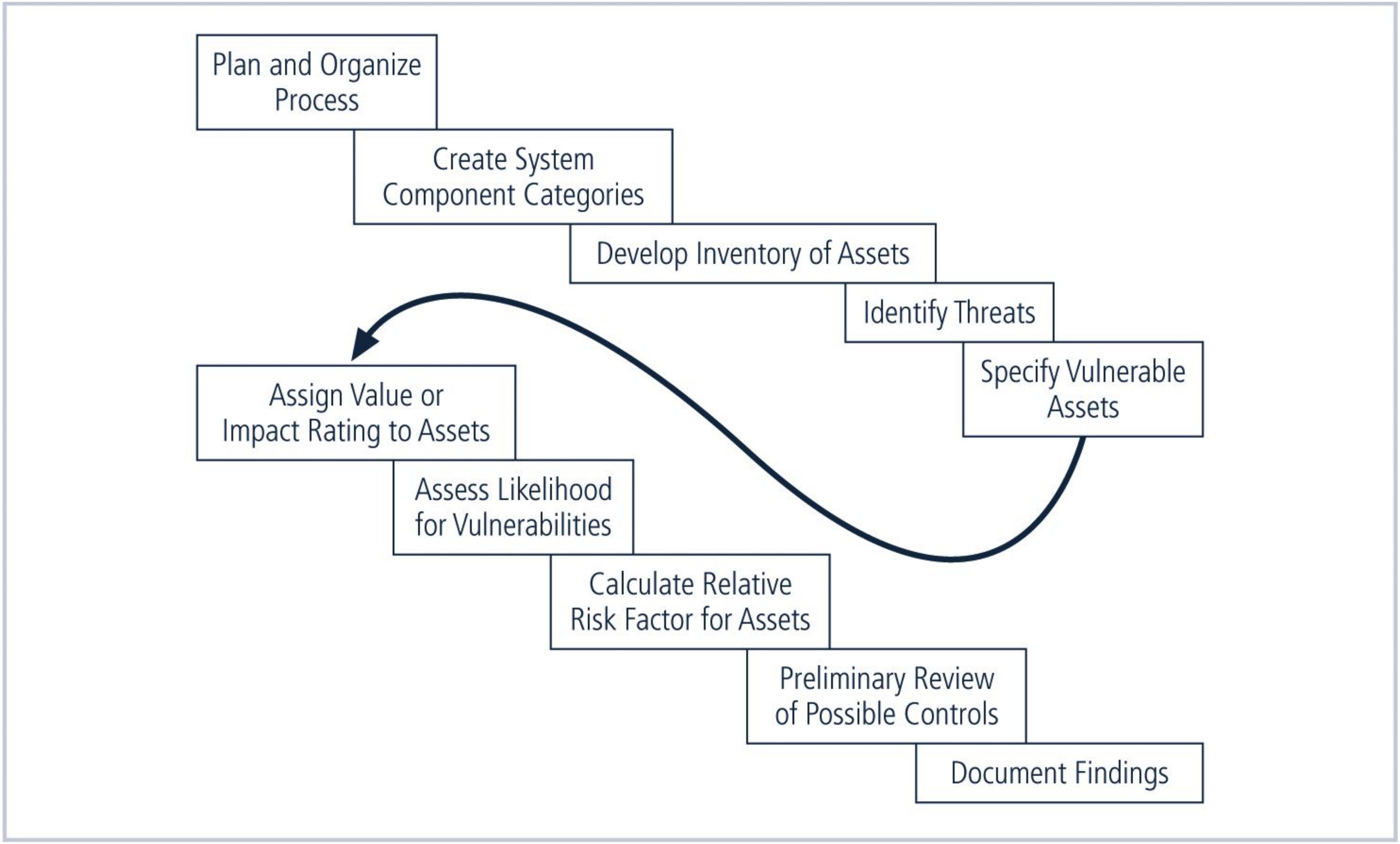
- **All** communities of interest are responsible for the management of risks
- Each has a particular strategic role to play
  - **InfoSec**
    - Understand the threats and attacks that introduce risk best
    - Usually take a leadership role in addressing risk
  - **IT**
    - Help build the secure systems and ensure safe operation
  - **Management** and **users**
    - Ensure sufficient resources are allocated to InfoSec and IT groups
    - Play a part in the early detection and response process

Accountability for Risk Management

- **All** community of interests must be actively involved in:
  - Evaluating risk controls
  - Determining which control options are cost effective
  - Acquiring or installing the appropriate controls
  - Overseeing processes to ensure that the controls remain effective
  - Identifying risks
  - Assessing risks
  - Summarizing the finding

TOPIC 8.1 RISK IDENTIFICATION

Risk Identification and Assessment Process



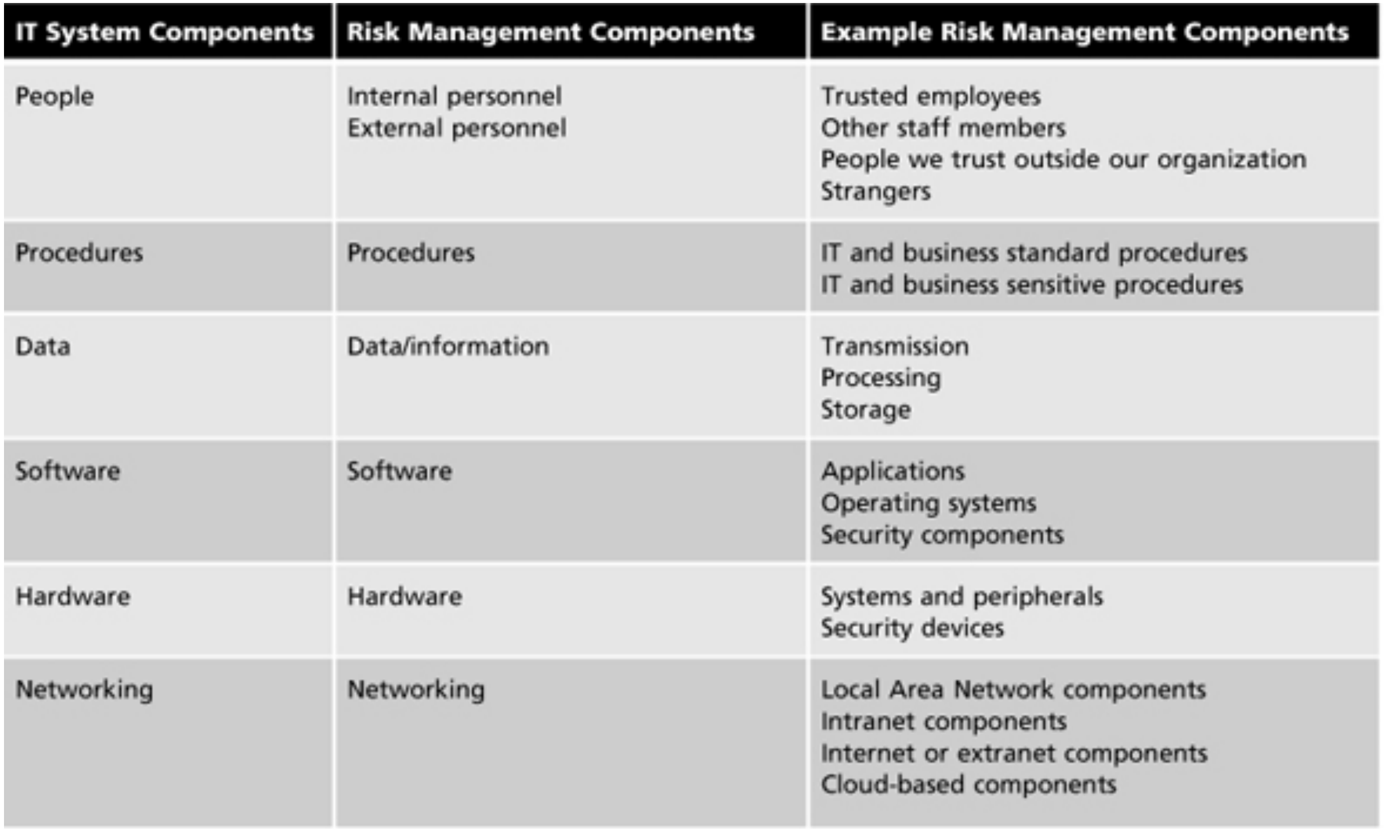
Plan and Organize Process
Create System Component Categories
Develop Inventory of Assets
Identify Threats
Specify Vulnerable Assets
Assign Value or Impact Rating to Assets
Assess Likelihood for Vulnerabilities
Calculate Relative Risk Factor for Assets
Preliminary Review of Possible Controls
Document Findings

Risk Identification

- Risk identification begins with the process of self-examination
- Managers
  - ***Identify*** the organization’s information assets
  - ***Classify*** and ***categorize*** them into useful groups
  - ***Prioritize*** them by their overall importance

Creating an Inventory of Information Assets

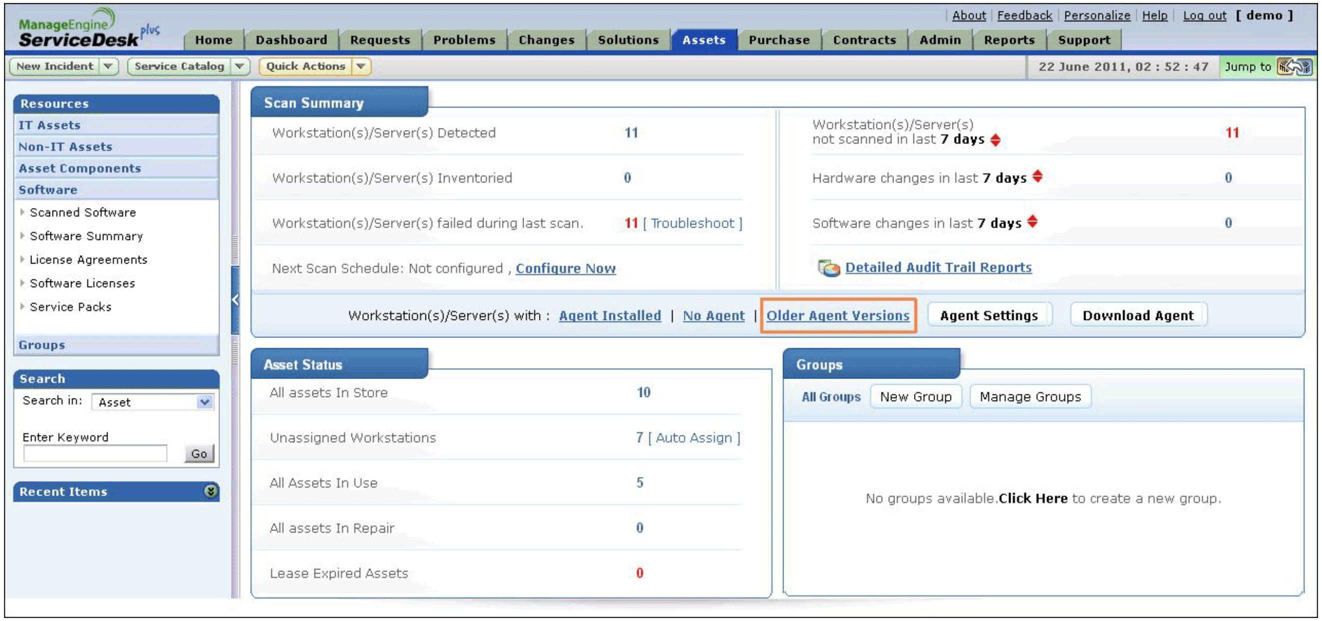
- Information assets includes *people*, *procedures*, *data*, *software*, *hardware* and *networking* components



IT System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking	Local Area Network components Intranet components Internet or extranet components Cloud-based components

Identifying Hardware, Software, and Network Assets

- **Asset inventory systems**
  - Automated systems to keep track of hardware, network, software components
  - Or create an equivalent manual process



22 June 2011, 02 : 52 : 47

Search in: Asset

Enter Keyword Go

Scan Summary

Workstation(s)/Server(s) Detected	11	Workstation(s)/Server(s) not scanned in last **7 days**	11
Workstation(s)/Server(s) Inventoried	0	Hardware changes in last **7 days**	0
Workstation(s)/Server(s) failed during last scan.	11 [Troubleshoot]	Software changes in last **7 days**	0
Next Scan Schedule: Not configured , Configure Now		Detailed Audit Trail Reports	

Workstation(s)/Server(s) with : Agent Installed | No Agent | Older Agent Versions

Asset Status

All assets In Store	10
Unassigned Workstations	7 [Auto Assign]
All Assets In Use	5
All assets In Repair	0
Lease Expired Assets	0

Groups

No groups available.**Click Here** to create a new group.

Mange Engine AssetExplorer

Identifying Hardware, Software, and Network Assets

- **Asset inventory systems**
  - Automated systems to keep track of hardware, network, software components
  - Or create an equivalent manual process
- The inventory process requires a lot of planning
  - Determine which *attributes* of each information asset should be tracked
    - Depends on the needs of the organization
    - Depends on the risk management efforts
    - Also, the preferences of InfoSec and IT

Identifying Hardware, Software, and Network Assets

- Potential **attributes**
  - Name
  - Asset tag
  - IP address
  - MAC address
  - Asset type
  - Serial number
  - Manufacturer name, model or part number
  - Software version, update revision, FCO number
  - Physical and logical location
  - Controlling entity

Identifying People, Procedures, and Data Assets

- Identify and evaluate human resources, documentation, and data information assets
- Whose Responsibility ?
  - Managers who possess the necessary knowledge, experience, and judgment
- Recording
  - Use reliable data-handling process
  - The record-keeping system should be flexible, allowing you to link assets to attributes based on the nature of the information asset being tracked

Suggested Attributes: People

- **People**
  - Position name/number/ID
  - Supervisor name/number/ID
  - Security clearance level
  - Special skills

Suggested Attributes: Procedures

- **Procedures**
  - Description
  - Intended purpose
  - Software/hardware/networking elements to which the procedure is tied
  - Location where procedure documents are stored
  - Location where it is stored for update purposes

Suggested Attributes: Data

- **Data**
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used
  - Online or offline
  - Location
  - Backup procedures

Classifying and Categorizing Assets

- After initial inventory is assembled
  - Determine whether asset categories are meaningful
    - **Example:** if the category *Internet components* is too general, manager should divide it into subcategories of *servers*, *networking devices*, *protection devices* and *cabling*
  - Categorizes information assets based on the sensitivity and security needs
    - **Ex.:** confidential, internal, and public for info assets
    - **Ex.:** security clearance levels for personnel assets
  - Classification categories must be comprehensive and mutually exclusive

Assessing Values for Assets

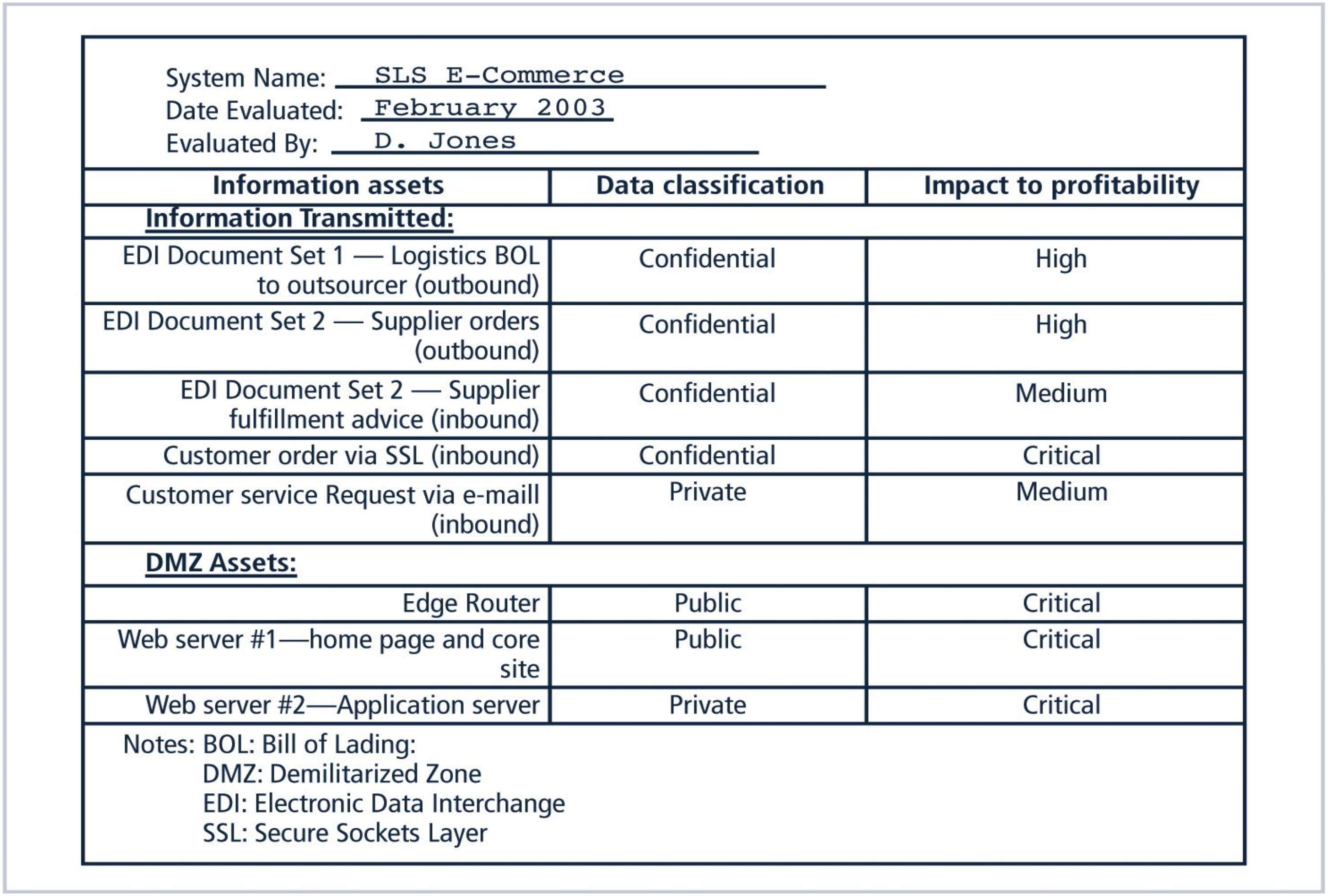
- After each information asset is identified, categorized, and classified
  - Assign a relative value to it
  - Relative values are comparative judgments
  - Ensure that the most valuable information assets are given the highest priority
  - Ensure that higher value assets are protected first

Assessing Values for Information Assets

- Develop the weighting criteria for asset or impact valuation:
  - Which asset is the most critical to the success of the organization?
  - Which asset generates the most revenue?
  - Which asset generates the highest profitability?
  - Which asset is the most expensive to replace?
  - Which asset is the most expensive to protect?
  - Which asset's loss or compromise would be the most embarrassing or cause the greatest liability?

Assessing Values for Information Assets

- Use a worksheet to collect answers



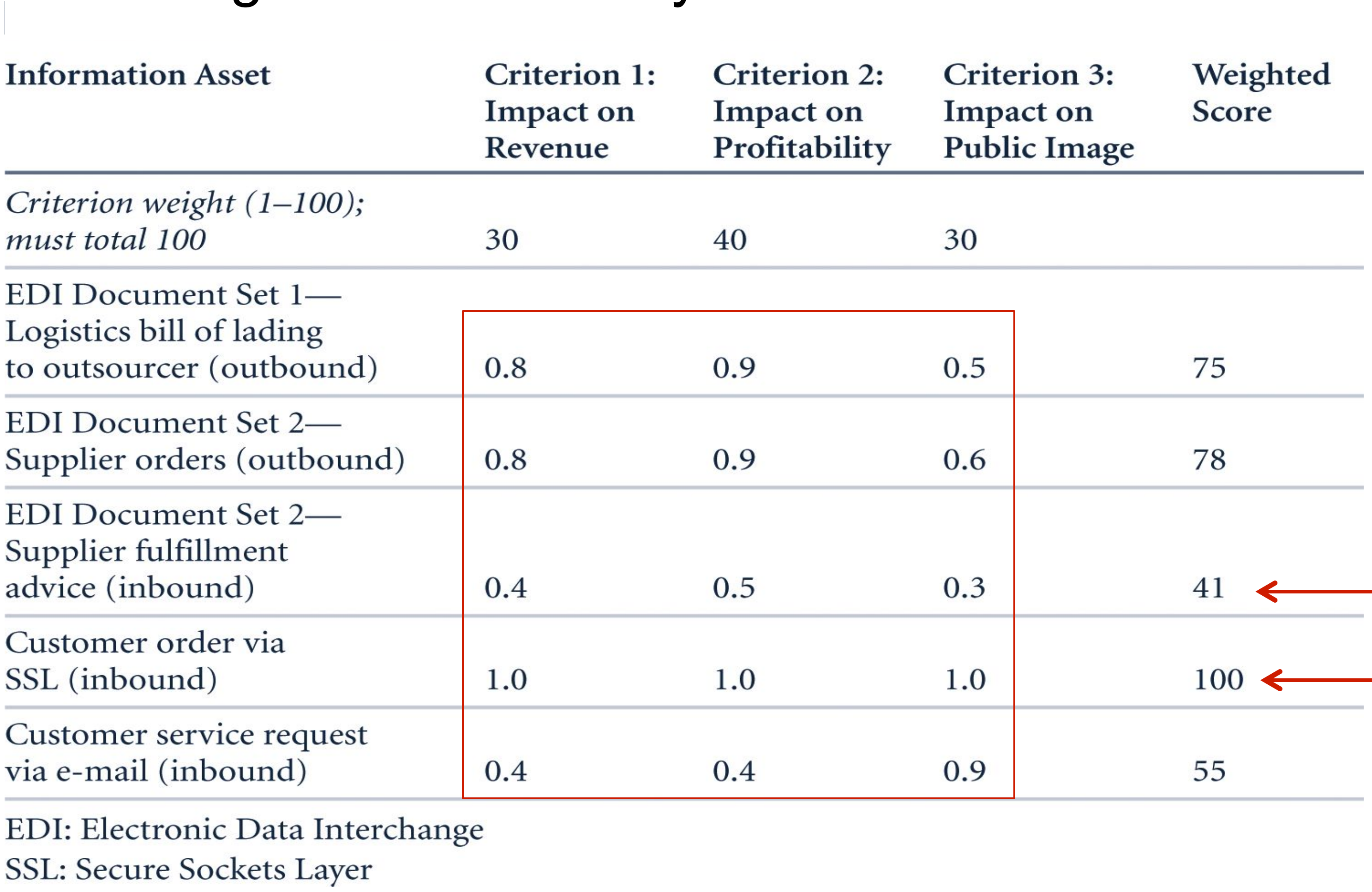
System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-maill (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Listing Assets in Order of Importance

- Use a weighted factor analysis worksheet



Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

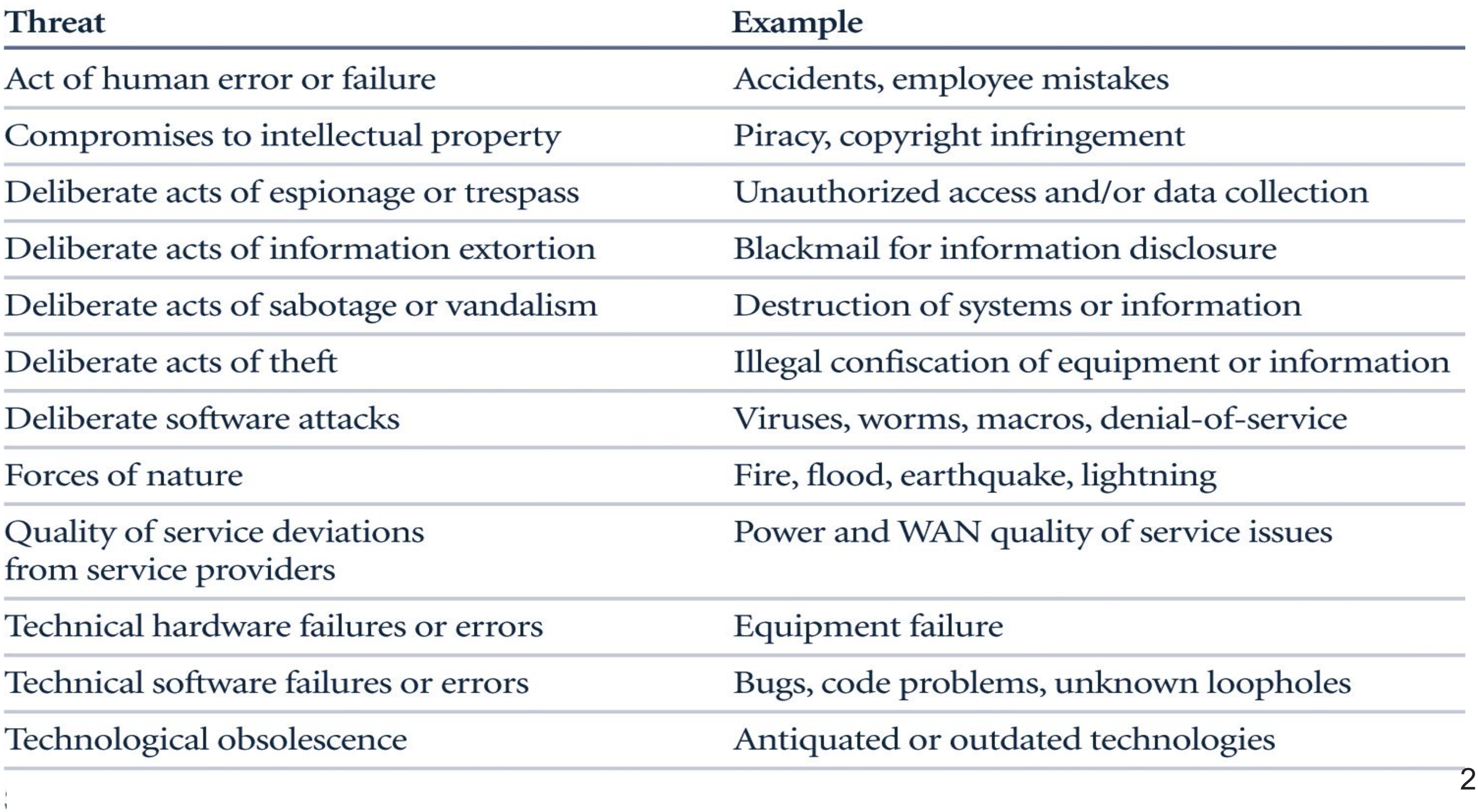
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Threat Identification

- **Threat identification**
  - A process of assessing potential weaknesses in each information asset
- Do not assume every threat can and will attack every information asset
  - Otherwise project scope will become too complex
- Each step in the threat and vulnerability identification process should be
  - Managed separately
  - Coordinated at the end

Threat Identification

- Each threat presents a unique challenge
  - 12 threats to InfoSec



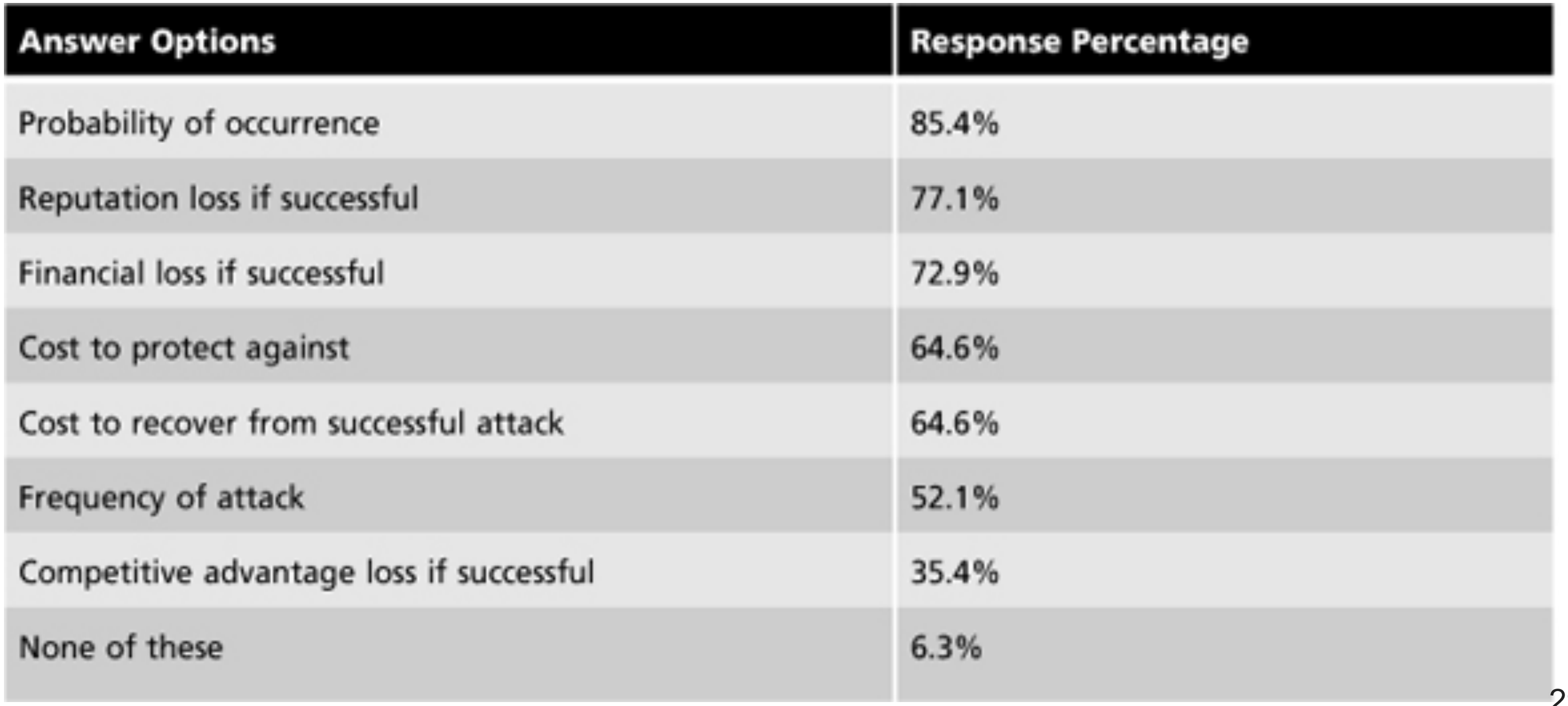
Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Identify and Prioritize Threats and Threat Agents

- **Threat assessment**
  - Each threat must be handled with specific controls that directly address threat and threat agent’s attack strategy
  - A process to determine the potential of each identified threat to affect the targeted information asset
- To understand threats and their potential effects
  - Which threats present a danger to this organization’s information assets in its current environment?
    - Not all threats endanger every organization
  - Which threats represent the gravest danger to the organization’s information assets?
    - Probability, amount of damage, and frequency

Methods of Assessing Threats

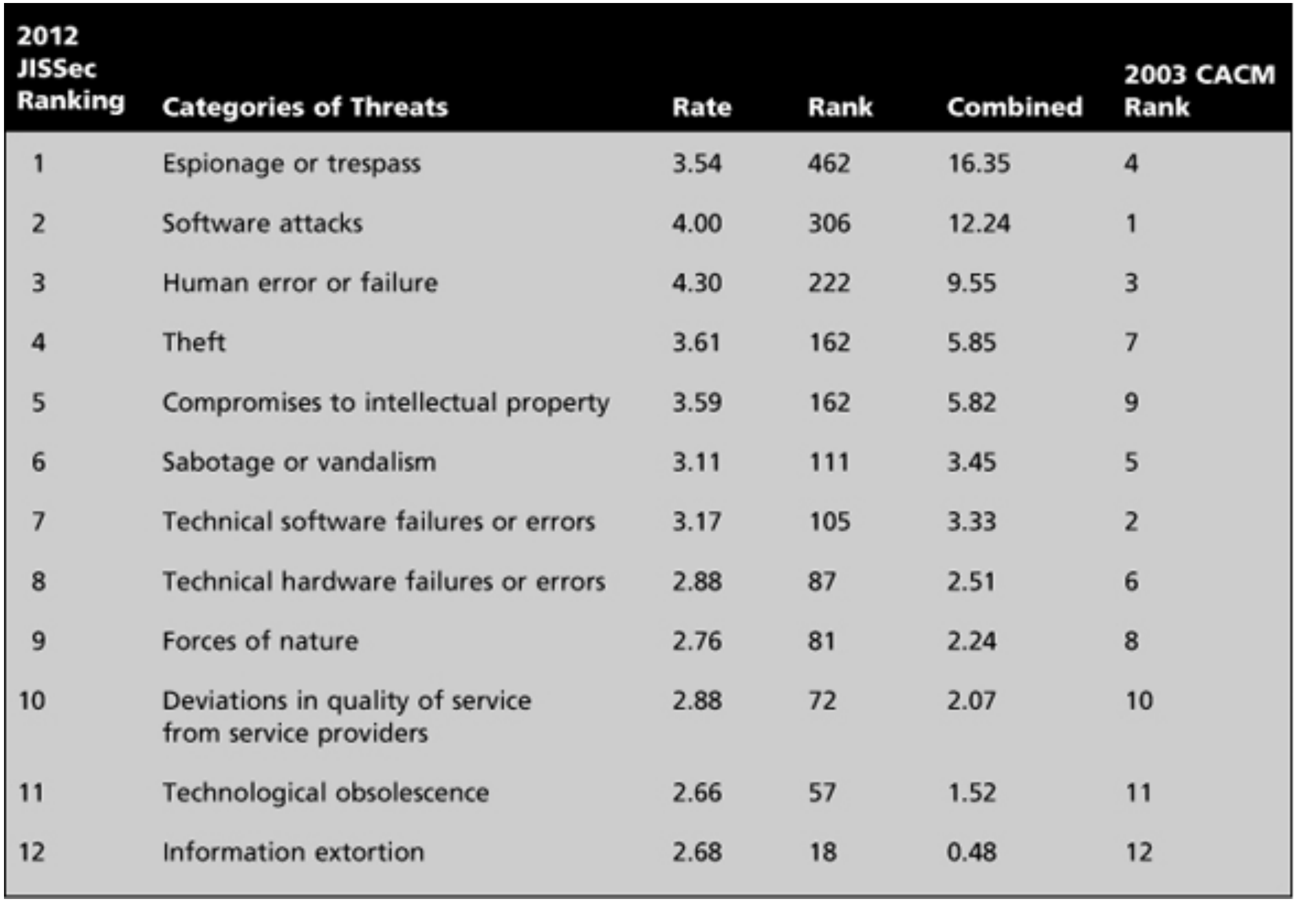
- “In your organization’s risk management efforts, what basis do you use to assess threats?”
  - A 2012 survey of 1000 computing executives



Answer Options	Response Percentage
Probability of occurrence	85.4%
Reputation loss if successful	77.1%
Financial loss if successful	72.9%
Cost to protect against	64.6%
Cost to recover from successful attack	64.6%
Frequency of attack	52.1%
Competitive advantage loss if successful	35.4%
None of these	6.3%

Threats to InfoSec

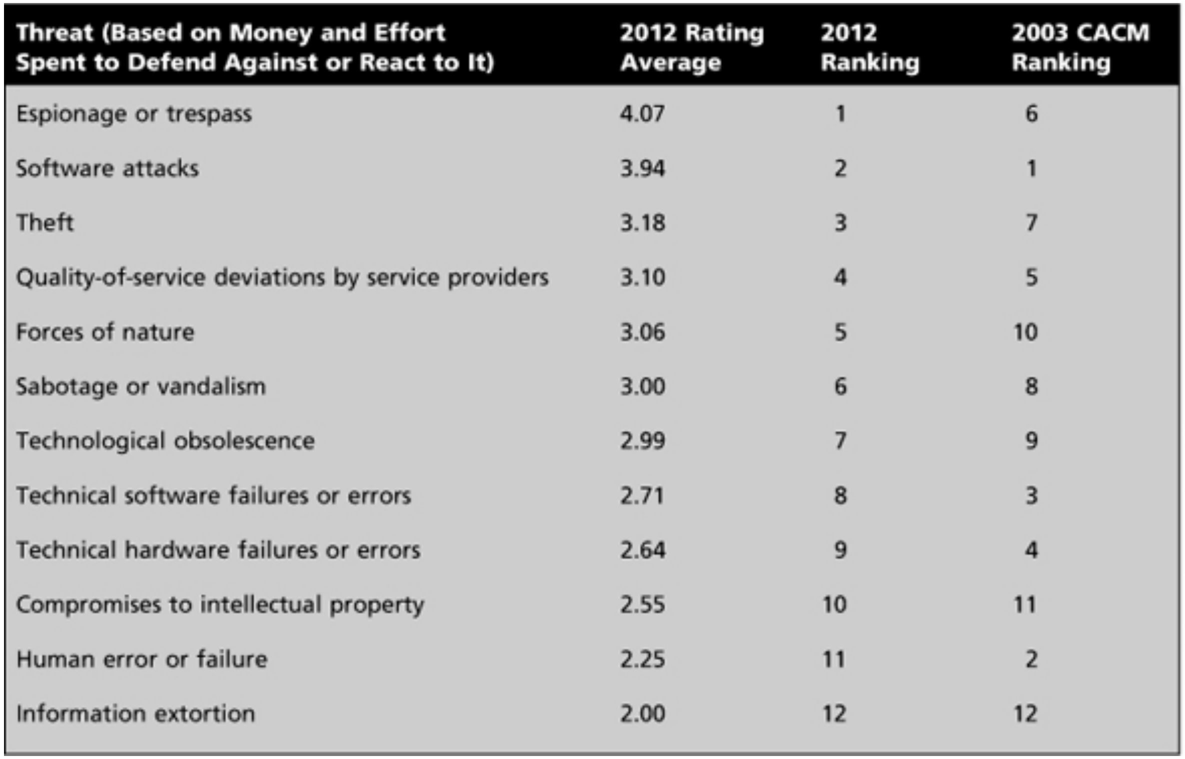
- Weighted ranks of threats to InfoSec
  - 5-point scale rating; rank top 5 threats



2012 JISSec Ranking	Categories of Threats	Rate	Rank	Combined	2003 CACM Rank
1	Espionage or trespass	3.54	462	16.35	4
2	Software attacks	4.00	306	12.24	1
3	Human error or failure	4.30	222	9.55	3
4	Theft	3.61	162	5.85	7
5	Compromises to intellectual property	3.59	162	5.82	9
6	Sabotage or vandalism	3.11	111	3.45	5
7	Technical software failures or errors	3.17	105	3.33	2
8	Technical hardware failures or errors	2.88	87	2.51	6
9	Forces of nature	2.76	81	2.24	8
10	Deviations in quality of service from service providers	2.88	72	2.07	10
11	Technological obsolescence	2.66	57	1.52	11
12	Information extortion	2.68	18	0.48	12

Expenditures for Threats to InfoSec

- Assess the recovery cost – *a rough assessment*
  - How much would it cost to recover from a successful attack?
  - Which threats would require the greatest expenditure to prevent?



Threat (Based on Money and Effort Spent to Defend Against or React to It)	2012 Rating Average	2012 Ranking	2003 CACM Ranking
Espionage or trespass	4.07	1	6
Software attacks	3.94	2	1
Theft	3.18	3	7
Quality-of-service deviations by service providers	3.10	4	5
Forces of nature	3.06	5	10
Sabotage or vandalism	3.00	6	8
Technological obsolescence	2.99	7	9
Technical software failures or errors	2.71	8	3
Technical hardware failures or errors	2.64	9	4
Compromises to intellectual property	2.55	10	11
Human error or failure	2.25	11	2
Information extortion	2.00	12	12

Vulnerability Assessment

- Steps revisited
    1. Identify the information assets of the organization
    2. Document some threat assessment criteria
    3. Review every information asset for each threat
        - Leads to a list of vulnerabilities that remain potential risks to organization
- **The goal** is to evaluate relative risk of each listed vulnerability

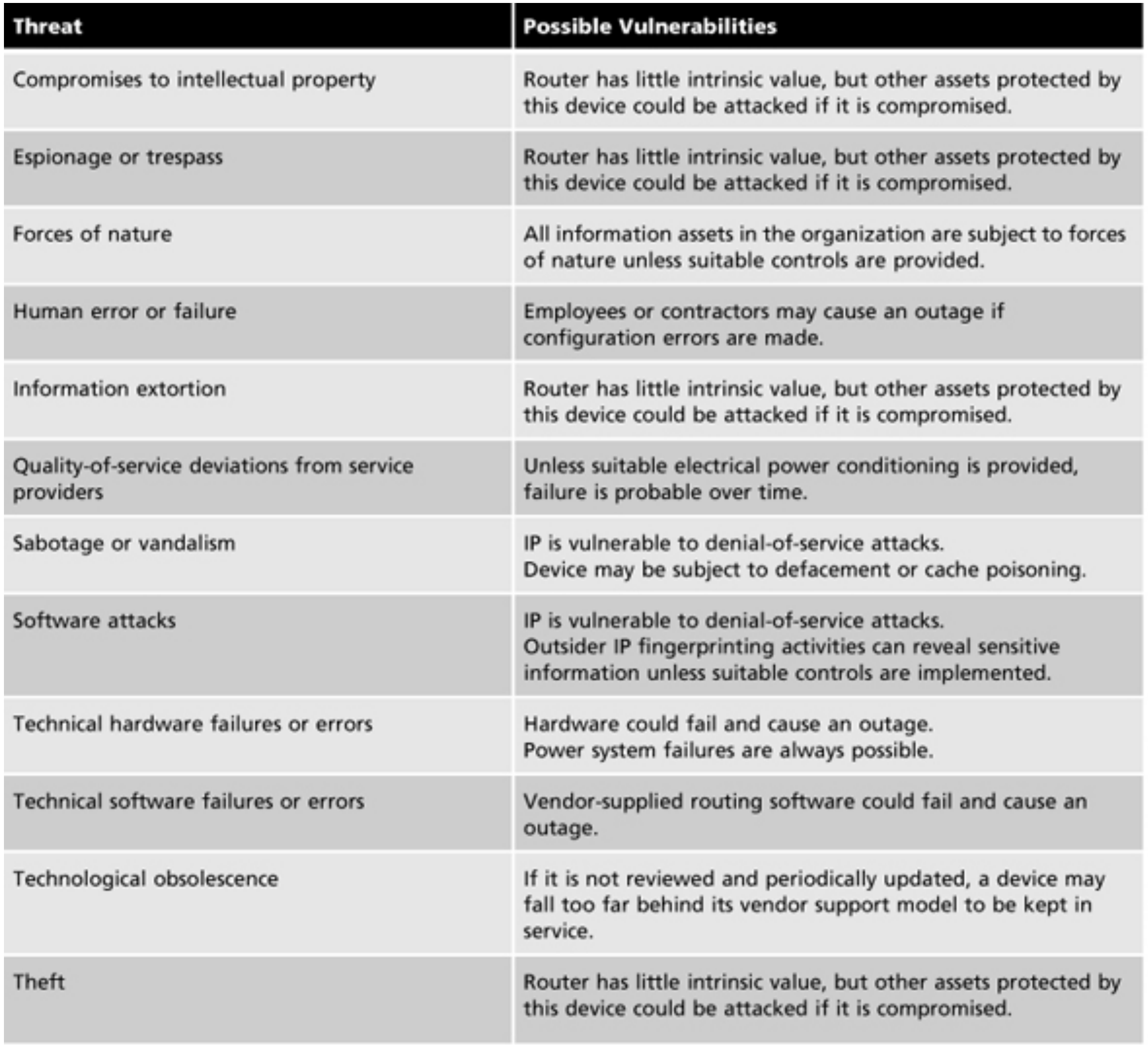
Vulnerability Assessment

- CERT Methodology
  - Setup
    - Begin documentation, secure permission, update and configure tools
  - Test Execution
    - Run tools, document
  - Vulnerability Analysis
    - CVE, CVSS
  - Reporting
    - Summarize vulnerabilities found, prioritize, and suggest remediation
  - Remediation
    - Fix/Accept/Mitigate, automatic vs. manual

Vulnerability Assessment

- **CVE:** The Common Vulnerabilities and Exposures
  - http://cve.mitre.org
  - Can also look up additional vulnerability information from trusted sources
    - US-CERT, NVD, Secunia, or vendors
- **CVSS: Common Vulnerability Scoring System**
  - An industry standard for assessing system vulnerabilities
  - NIST provides a CVSS calculator
    - http://nvd.nist.gov/cvss.cfm?calculator
    - Adjust the value of vulnerability based on its characteristics
    - CVSS score goes up or down depending on the risk presented to your specific environment

Example: VA of a DMZ Router



Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	Employees or contractors may cause an outage if configuration errors are made.
Information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	Hardware could fail and cause an outage. Power system failures are always possible.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.

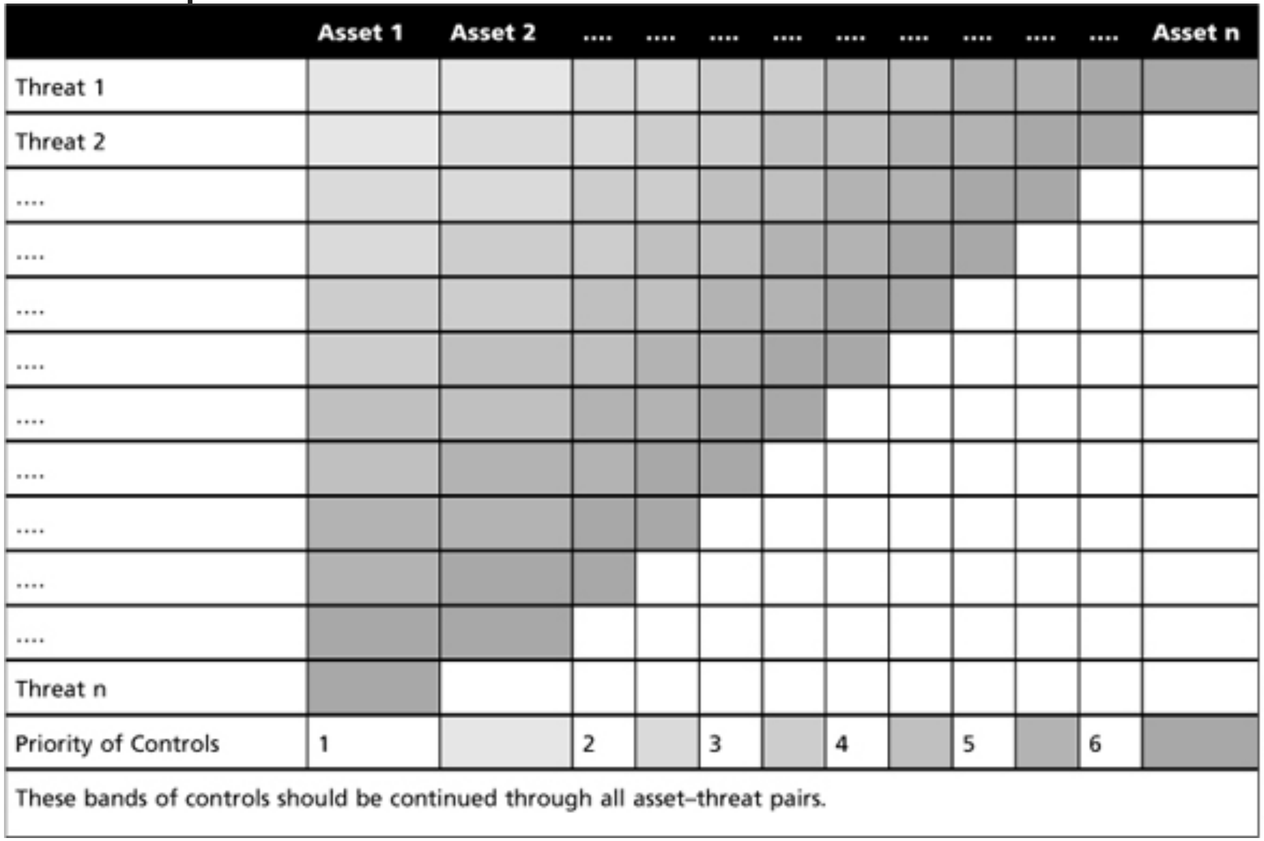
The TVA Worksheet

- The risk identification process should produce two lists:
  - Prioritized list of assets and their vulnerabilities
  - Prioritized list of threats facing the organization based on a weighted table

- Combine the two into a Threats-Vulnerabilities-Assets (TVA) worksheet
  - Columns: prioritized set of assets
  - Rows: prioritized list of threats
    - Analyzes existing controls that protect assets from threats
    - Cataloging and categorizing controls in the next step
  - Cells: vulnerabilities

The TVA Worksheet

- T1V1A1 - Vulnerability 1 that exists between Threat 1 and Asset 1
- T1V2A1 - Vulnerability 2 that exists between Threat 1 and Asset 1
- Not all TVA triples exist



	Asset 1	Asset 2	....	....	....	....	....	....	....	....	....	Asset n
Threat 1	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Threat 2	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
....	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
....	▨	▨	▨	▨	▨	▨	▨	▨	▨			
....	▨	▨	▨	▨	▨	▨	▨	▨				
....	▨	▨	▨	▨	▨	▨	▨					
....	▨	▨	▨	▨	▨	▨						
....	▨	▨	▨	▨	▨							
....	▨	▨	▨	▨								
....	▨	▨	▨									
....	▨	▨										
Threat n	▨											
Priority of Controls	1	▨	2	▨	3	▨	4	▨	5	▨	6	▨
These bands of controls should be continued through all asset–threat pairs.												

Copyright © 2014 Cengage Learning®.

TOPIC 8.2 RISK ASSESSMENT

Risk Assessment

- **Risk assessment**
  - A process that assigns a comparative risk rating or score to each specific information asset
  - Enable the organization to evaluate the relative risk introduced by each vulnerable information asset
  - Support comparative ratings in risk control
- Develop a *repeatable* method to evaluate the *relative* risk of each vulnerability
  - Estimating risk is not an exact science
  - A variety of methods of estimation
  - A simple model: based on estimate factor

Risk Assessment Estimate Factors

Risk is

The ***likelihood*** of the occurrence of a vulnerability

Multiplied by

The ***value*** of the information asset

Minus

The ***percentage*** of risk mitigated by current controls

Plus

The ***uncertainty*** of current knowledge of the vulnerability

Likelihood

- Likelihood – an overall rating of the probability that a specific vulnerability will be exploited
  - NIST recommends likelihood rating between 0.1 and 1.0
  - Use external references for likelihood values
- Examples:
  - The likelihood of an employee or system being struck by a meteorite while indoors would be rated 0.1
  - The likelihood of receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0
  - The likelihood of fire for types of structures
  - The likelihood of network attacks related to network addresses

Assessing Potential Loss

- Use information from risk identification to assign values to information assets:
  - Which threats present a danger to the organization’s assets in its current environment?
  - Which threats represent the gravest danger to the organization’s information assets?
  - How much would it cost to recover from an attack?
  - Which threats would require the greatest expenditure to prevent?
  - Which of the aforementioned questions is the most important to the protection of information from threats within the organization?

Assessing Potential Loss

- Assign weighted scores
  - Use 1-10, or 1-100 scale
  - NIST 800-30 scale
    - All-important assets have a value of 100
    - Low-criticality ones have a value of 1
    - Others have a medium value of 50
  - Low-medium-high scale
    - Values of 1, 3, 5

Percentage of Risk Mitigated by Current Controls

- If a vulnerability is fully managed by an existing control
  - It can be set aside
- If a vulnerability is partially controlled
  - Estimate what percentage of the vulnerability has been controlled
- **Uncertainty**
  - Estimation errors exist
  - An estimate made by the manager using judgment and expertise

Risk Determination Example

Two information assets

- Asset A has a value of 50 and has vulnerability #1,
  - likelihood of 1.0 with no current controls
  - assumptions and data are 90% accurate
- Asset B has a value of 100 and has two vulnerabilities
  - Vulnerability #2
    - likelihood of 0.5 with a current control that addresses 50% of its risk
  - Vulnerability # 3
    - likelihood of 0.1 with no current controls
  - Assumptions and data are 80% accurate

Risk Determination Example

Risk ratings for the three vulnerabilities:

- Asset A: Vulnerability 1 rated as 55

  = (50 × 1.0) × (1 - 0% + 10%)

- Asset B: Vulnerability 2 rated as 35

  = (100 × 0.5) × (1 - 50% + 20%)

- Asset B: Vulnerability 3 rated as 12

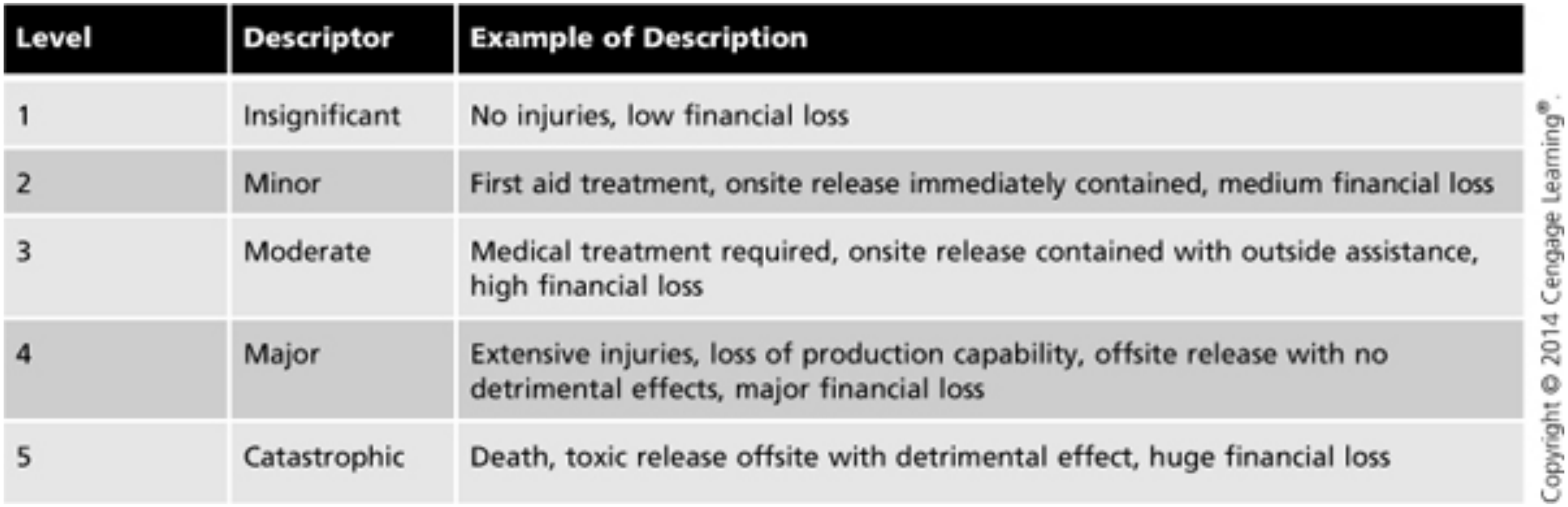
  = (100 × 0.1) × (1 - 0 % + 20%)

Likelihood and Consequences Rating

- A qualitative risk assessment approach
  - Australian and New Zealand Risk Management Standard 4360
  - Use categories instead of specific values to determine risk
    - Likelihood: threat’s probability of occurrence
    - Consequences: expected results of an attack

Consequences Levels

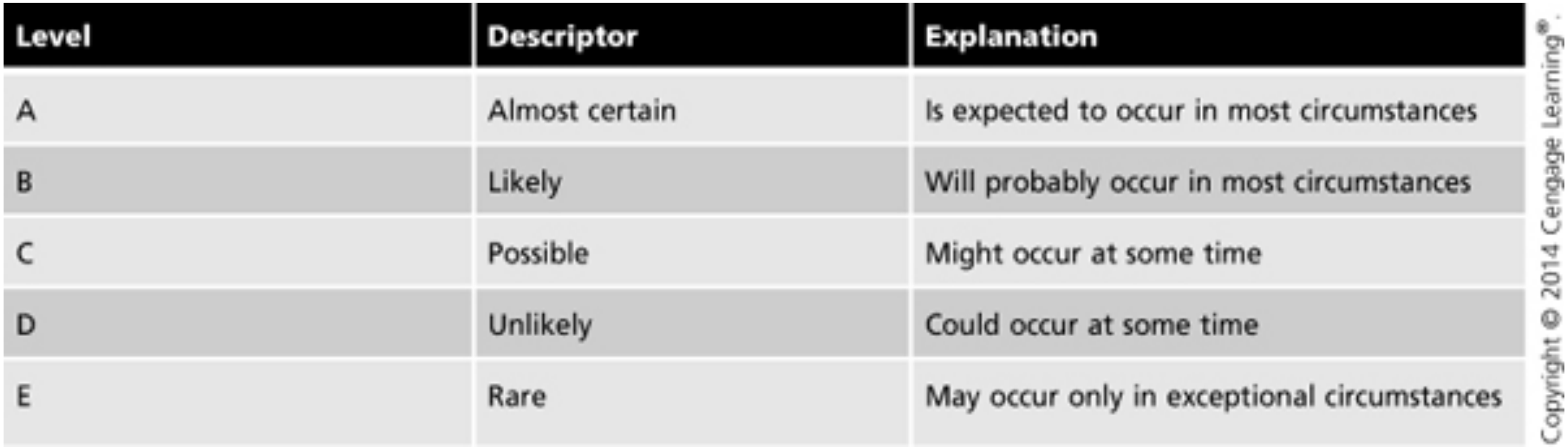
- Consequences evaluated on five levels
  - Determine for each attack from each specific threat category



Level	Descriptor	Example of Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, onsite release immediately contained, medium financial loss
3	Moderate	Medical treatment required, onsite release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, offsite release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release offsite with detrimental effect, huge financial loss

Likelihood Levels

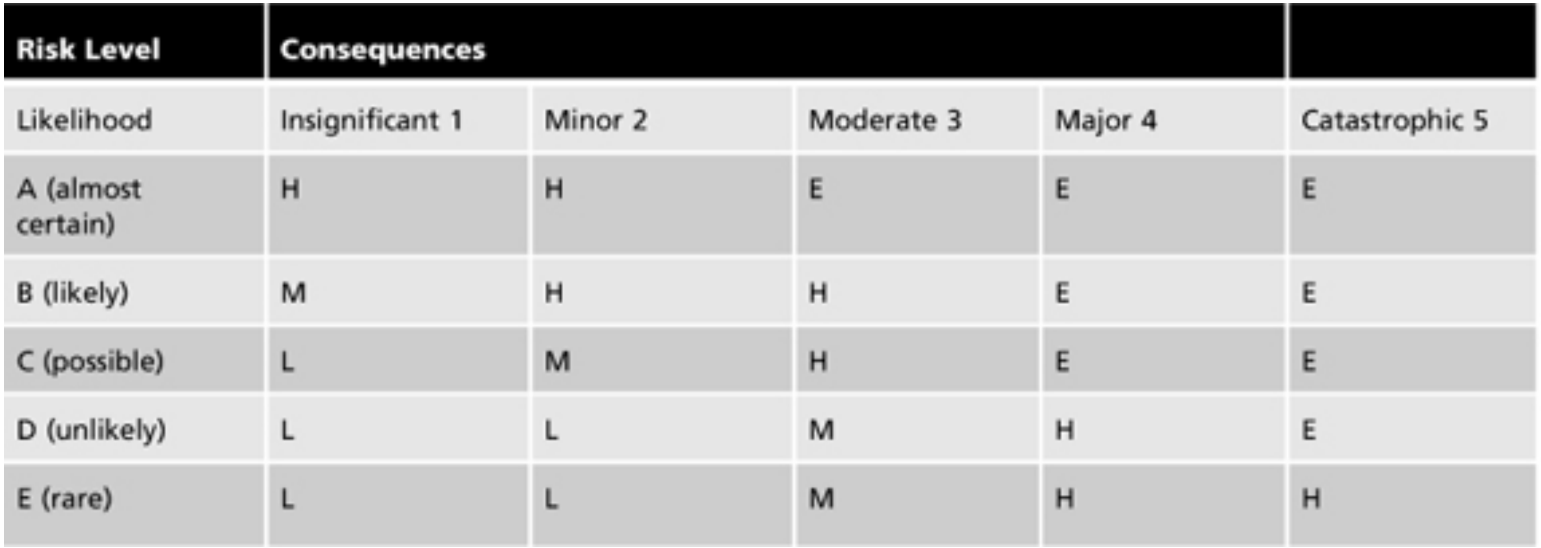
- Qualitative likelihood assessment on five levels
  - Determine for each attack from each specific threat category



Level	Descriptor	Explanation
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

Qualitative Risk Assessment Matrix

- Potential consequences at various risk levels
  - E: extreme risks, immediate action required
  - H: high risks, senior management attention required
  - M: moderate risk, management responsibility specified
  - L: low risk, management by routine procedure required



Risk Level	Consequences				
Likelihood	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

Source: Risk management plan templates and forms from www.treasury.act.gov.au/actia/Risk.htm

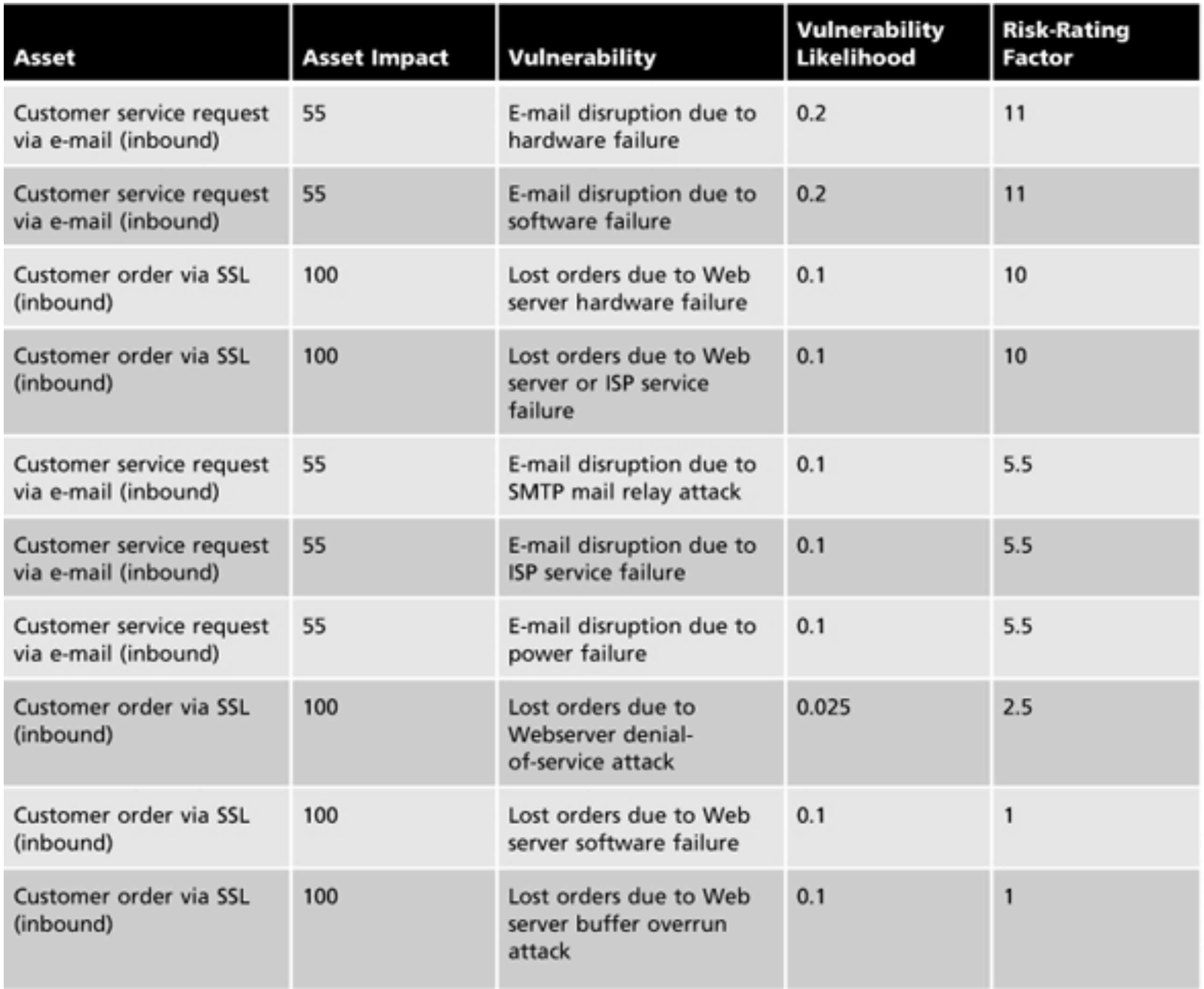
Identify Possible Controls

- **Residual risks**
  - Risk remaining after existing control has been applied
  - “Controls”, “safeguards”, and “countermeasures” are security mechanisms to counter attacks, reduce risk, resolve vulnerabilities, and improve security
  - Three general categories of controls: Policies, Programs, Technical controls
- For each threat and its associated vulnerabilities with residual risk, create a preliminary list of control ideas
  - Identify extant controls
  - Identify areas of residual risk

Documenting the Results of Risk Assessment

- The final summarized document is the ranked vulnerability risk worksheet
  - Asset – a list of vulnerable assets
  - Asset impact – results from the weighted factor analysis worksheet
  - Vulnerability – list uncontrolled vulnerabilities
  - Vulnerability likelihood – the likelihood of the realization of the vulnerability by a threat agent
  - Risk-rating factor – the figure calculated by multiplying the asset impact and its likelihood

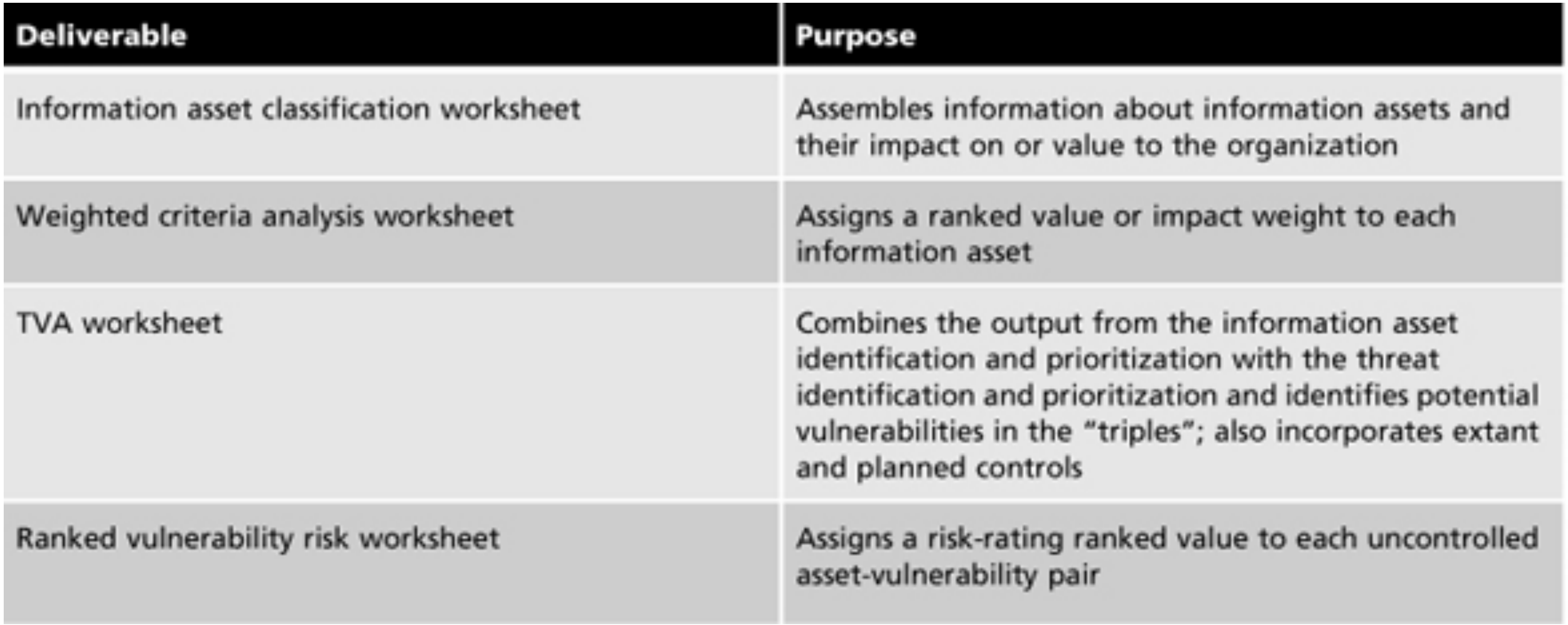
Ranked Vulnerability Risk Worksheet



Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Webserver denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.1	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.1	1

Documenting the Results of Risk Assessment

- **Deliverables**



Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
TVA worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization and identifies potential vulnerabilities in the “triples”; also incorporates extant and planned controls
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset-vulnerability pair