جامعة الامير سلطان
PRINCE SULTAN
UNIVERSITY
1998

Risk Management Lifecycle

CYS403

جامعة الأمير سلطان
Prince Sultan University

- CLO 2: Synthesize the principles of cyber security risk management and a framework of components: identification, protection, detection, response and recovery.
- CLO 3: Develop a working knowledge of types of policy, how policy is created, how to implement and manage policy, measurement practices, and audit of policy

- Overview on the Risk management lifecycle
- Asset Valuation

Risk Management

- Risk management: identification, assessment, and prioritization of risks.
- Managing risk is one of the key responsibilities of every manager within the organization
- In any well-developed risk management program, two formal processes are at work
  - Risk identification and assessment
  - Risk control

Accountability for Risk Management

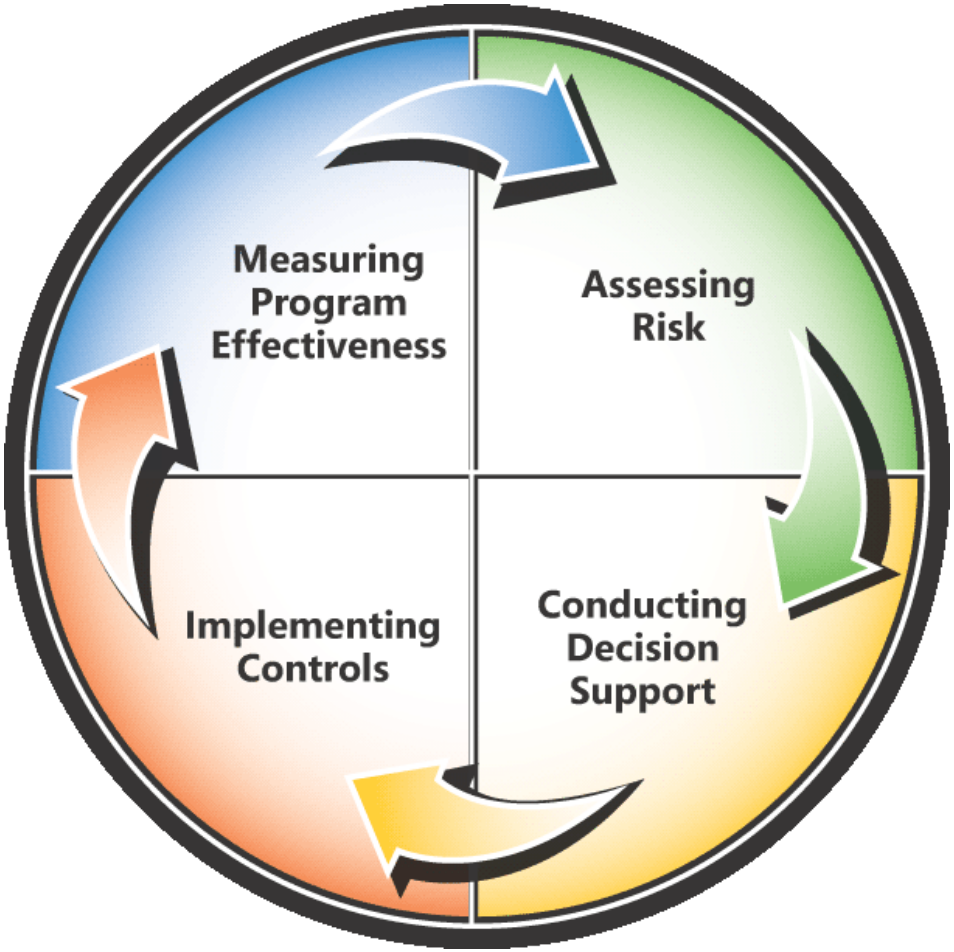
Communities of interest must work together

- **Cyber Security** – leadership role in addressing risk
- **Information Technology** – role involves building and maintaining secure systems
- **Management** – role involves resource allocation and prioritization of security concerns
- **Users** – crucial role in (early) detection, and proper response to threats

Risk management cycle

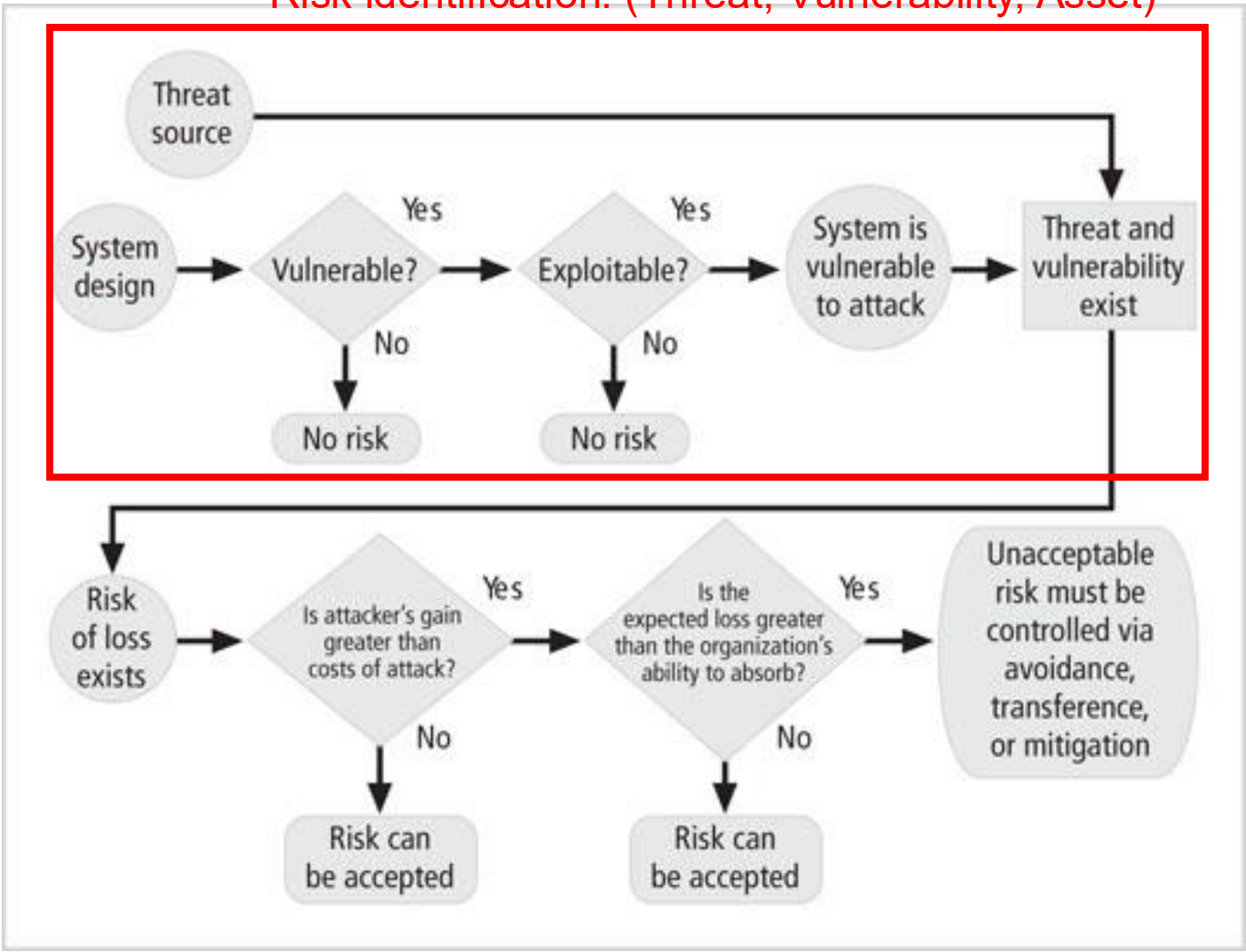
From http://technet.microsoft.com/en-us/library/cc750827.aspx

- Risk identification
  - Identify
  - Measure
  - Prioritize
- Control measures
  - Cost benefit analysis



Risk management action points

Risk identification: (Threat, Vulnerability, Asset)



Steps in Risk Management

- Identifying risks: (Threat vulnerability matrix, Asset impact)
- Assessing risks: quantitative vs. qualitative
- Evaluating the risk controls (CBA model)
  - Determining which control options are cost-effective
- Acquiring or installing the appropriate controls
- Overseeing processes to ensure that the controls remain effective
- Summarizing the findings

Risk Identification

Asset Identification, valuation, ranking

- Asset Identification : Asset inventory
  - Identify information assets
    - Includes people, procedures, data and information, software, hardware, and networking elements
    - This step should be done without pre-judging the value of each asset
      - Values will be assigned later in the process
  - Determine which attributes of each information asset should be tracked

Information Asset Inventory creation (contd.)

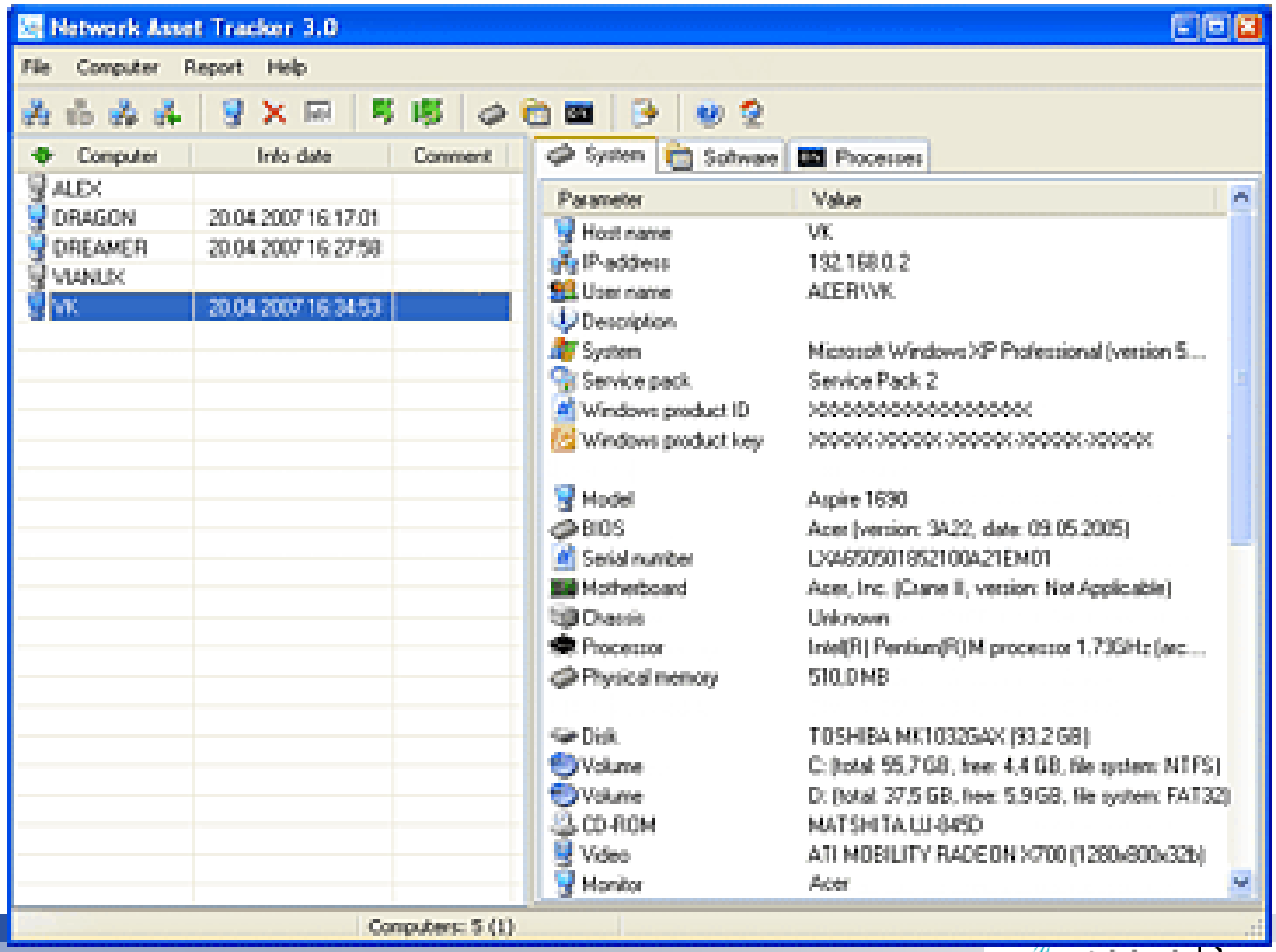
IT system components	Risk management components	
People	People inside an organization People outside an organization	Trusted employees Other staff People at organizations we trust Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking component	Intranet components Internet or extranet components

Information Asset Inventory creation (contd.)

- Potential asset attributes (for physical Devices)
  - Name
  - Asset tag
  - IP address
  - MAC address
  - asset type
  - Serial number
  - manufacturer name
  - Manufacturer's model or part number
  - Software version, update revision, or FCO number
  - Physical location/ logical location
  - Controlling entity

Example: Network Asset tracker

- http://www.misutilities.com/network-asset-tracker/howtouse.html



Information Asset Inventory creation (contd.)

- Sample attributes for people
  - Position name/number/ID
  - Supervisor name/number/ID
  - Security clearance level
  - Special skills

Information Asset Inventory creation (contd.)

- Sample attributes for procedures,
  - Description
  - Intended purpose Software/hardware/networking elements to which it is tied
  - Location where it is stored for reference
  - Location where it is stored for update purposes

Information Asset Inventory creation (contd.)

- Sample attributes for data assets:
  - Classification (Sensitive, confidential, private, public)
  - Owner/creator/manager
  - Size of data structure
  - Data structure used
  - Online or offline
  - Location
  - Backup procedures

Information Asset Inventory creation (contd.)

- Some tools to be used in asset inventory
  - Network asset tracker
  - Asset management

Classifying and Categorizing Assets

- Determine/refine an asset classification scheme
- A classification scheme categorizes information assets based **on their sensitivity, security needs**
- Each category designates the level of protection needed for a particular information asset
- Some asset types, such as personnel, may require an alternative classification scheme
- Classification categories must be comprehensive and mutually exclusive

System Name: SLS E-Commerce
Date Evaluated: February 2008
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

Asset Valuation

- Determine the values of assets
- Assign a relative value.
  - Comparative judgments made to ensure that the most valuable information assets are given the highest priority.
  - Some factors should be considered in asset valuation
    - Asset cost
    - Asset impact on profitability
    - Asset impact on revenue
    - Asset impact on public image

Assessing Values for Information Assets - Questions

1. Which asset is the most critical to the success of the organization?
2. Which asset generates the most revenue?
3. Which asset generates the highest profitability?
4. Which asset is the most expensive to replace?
5. Which asset is the most expensive to protect?
6. Which asset's loss or compromise would be the most embarrassing or cause the greatest liability?

Example on asset valuation

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

Next: Asset ranking

- Prioritize according to value

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

Next step: Threat Identification

- After ranking the assets, the threads and volnurabulities should be assessed as in the last lecture.
  - The outcome is Threat vulnerability matrix
  - Prioritize the threats based on their score for each asset.

Threat		Mean	Standard Deviation	Weight	Weighted Rank
1.	Deliberate software attacks	3.99	1.03	546	**2178.3**
2.	Technical software failures or errors	3.16	1.13	358	**1129.9**
3.	Acts of human error or failure	3.15	1.11	350	**1101.0**
4.	Deliberate acts of espionage or trespass	3.22	1.37	324	**1043.6**
5.	Deliberate acts of sabotage or vandalism	3.15	1.37	306	**962.6**
6.	Technical hardware failures or errors	3.00	1.18	314	**942.0**
7.	Deliberate acts of theft	3.07	1.30	226	**694.5**
8.	Forces of nature	2.80	1.09	218	**610.9**
9.	Compromises to intellectual property	2.72	1.21	182	**494.8**
10.	Quality-of-service deviations from service providers	2.65	1.06	164	**433.9**
11.	Technological obsolescence	2.71	1.11	158	**427.9**
12.	Deliberate acts of information extortion	2.45	1.42	92	**225.2**

Vulnerability Assessment

Threat	Possible Vulnerabilities
Acts of human error or failure	Employees or contractors may cause an outage if configuration errors are made
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of sabotage or vandalism	IP is vulnerable to denial-of-service attacks Device may be subject to defacement or cache poisoning
Deliberate acts of theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate software attacks	Internet Protocol (IP) is vulnerable to denial-of-service attack; Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time
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

Examples

1. Asset: email servers,
   - vulnerability: antivirus software not updated,
   - threat: virus attack
2. Asset: router,
   - vulnerability: incorrect router configuration,
   - threat: network susceptible to reduction or loss of connectivity

Summary of Threat Vulnerability Analysis

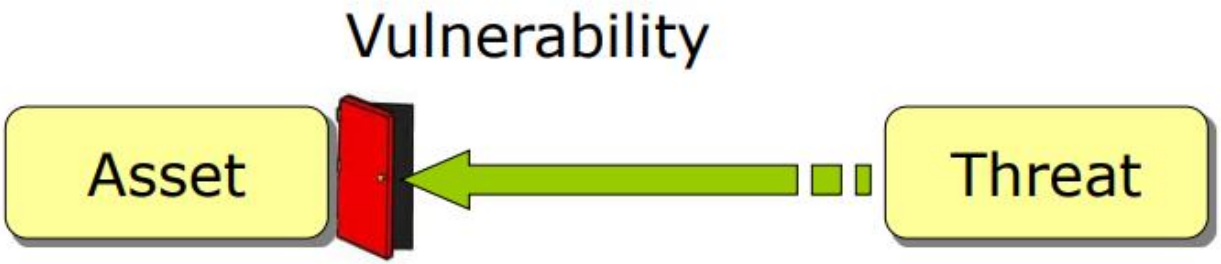
People
Procedure
Data
Software
Hardware
Networking

cause damage (loss)

flaw or weakness in asset's design, implementation, control or security procedure

exploit

Act of human error or failure
Deliberate act of trespass
Deliberate act of extortion
Deliberate act of sabotage
Deliberate software attacks
Technical software failures
Technical hardware failures
Forces of nature
Etc.

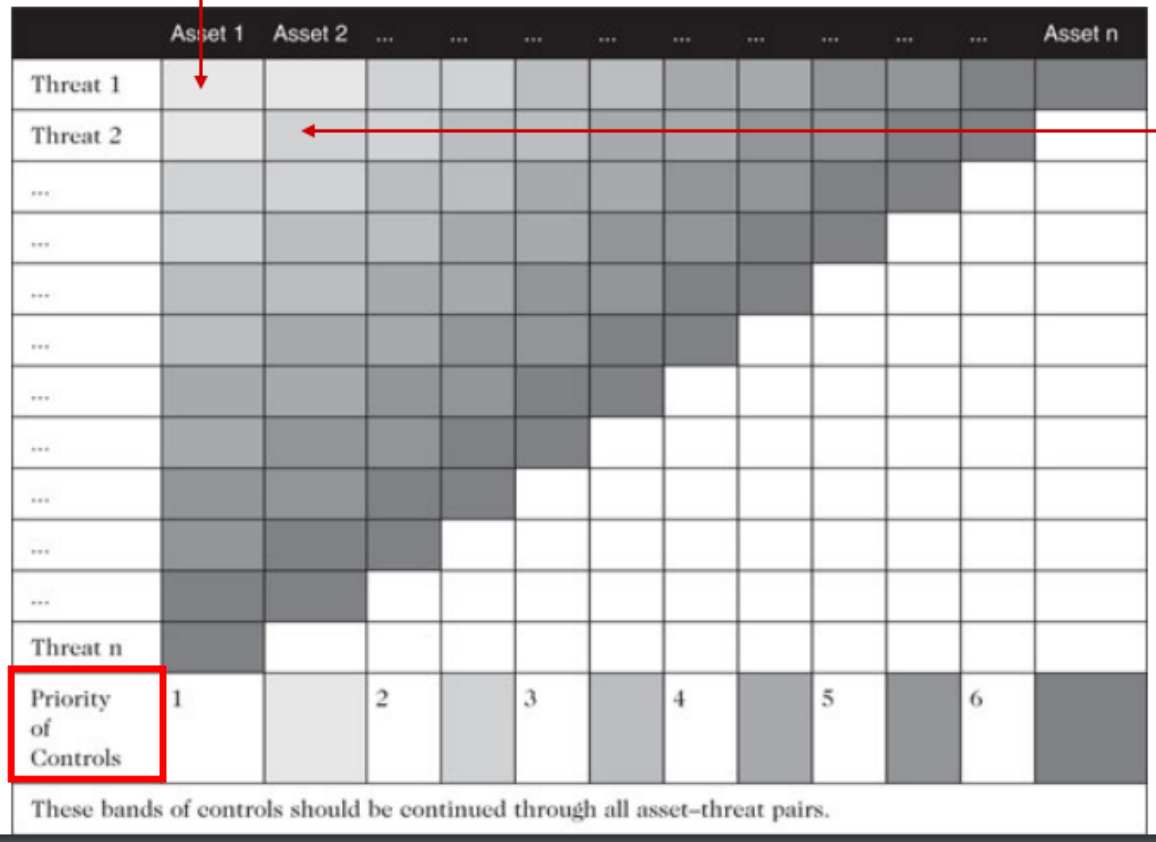


TVA Worksheet

- At the end of the risk identification process, a list of assets and their vulnerabilities has been developed
- Another list prioritizes threats facing the organization based on the weighted table discussed earlier
- These lists can be combined into a single worksheet called (Threat Vulnerability Asset (TVA worksheet)

TVA worksheet

If one or more vulnerabilities exist between T1 and A1, they can be categorized as:
T1V1A1 – Vulnerability 1 that exists between Threat 1 and Asset 1
T1V2A1 – Vulnerability 2 that exists between Threat 1 and Asset 1, …



If intersection between T2 and A2 has no vulnerability, the risk assessment team simply crosses out that box.

What is next?

- Risk assessment: Quantitative OR Qualitative