CSIT988

Security, Ethics and Professionalism

Week 9: Risk Management: Identifying and Assessing Risk

Subject Coordinator: *Khoa Nguyen*

School of Computing and Information Technology

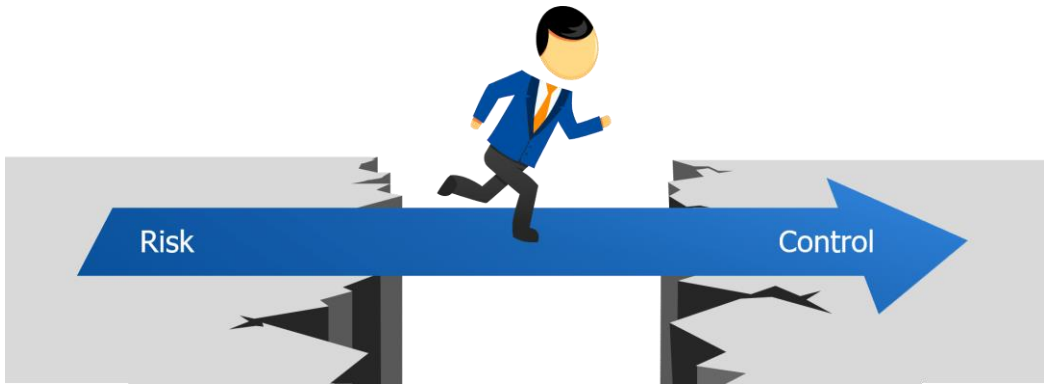
Autumn 2025

Learning 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

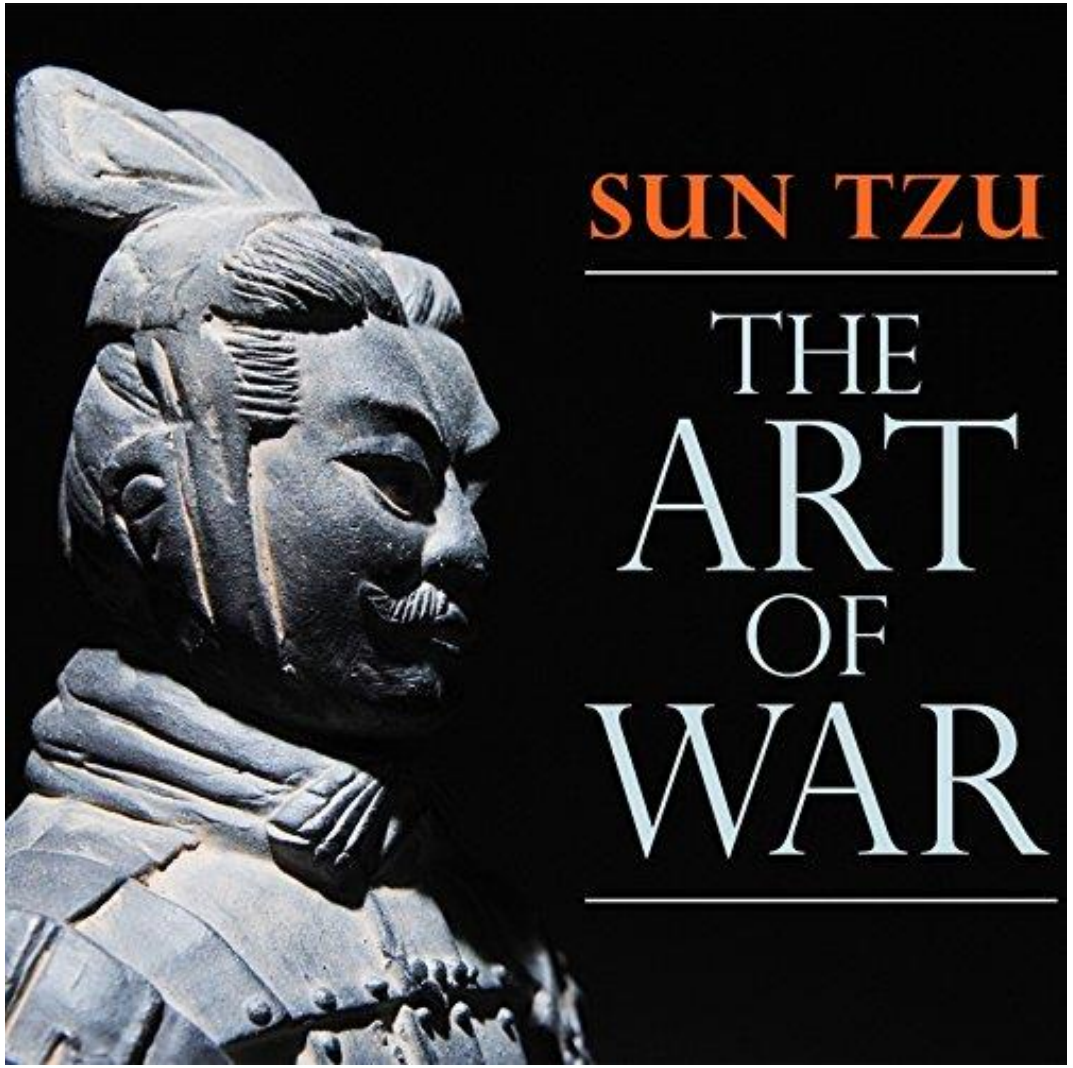
Reference: Chapter 8 of the textbook

- InfoSec departments are created primarily to manage IT risk
- 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 (this lecture)
  - Risk control (next lecture)



Each manager in the organization should focus on reducing risk. This is often done within the context of communities of interest:

- **General management**: structure the IT and InfoSec functions to ensure the successful defense of the organization's information assets
- **IT management**: serve the IT needs of the broader organization, exploit the special skills and insights of the InfoSec community
- **InfoSec management**: lead the way with skill, professionalism, and flexibility as it works with the other communities of interest to balance the constant trade-offs between InfoSec utility and security.



- “If you know the enemy and know yourself, you need not fear the result of a hundred battles

- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat

- If you know neither the enemy nor yourself, you will succumb in every battle”

-- Sun Tzu

Knowing Yourself

- When operating any kind of organization, a certain amount of risk is always involved.
- For an organization to manage risk properly, managers should understand how information is processed, stored, and transmitted.
- **Knowing yourself** in this context requires knowing which information assets are valuable to the organization, identifying, categorizing, and classifying those assets, and understanding how they are currently being protected. Armed with this knowledge, the organization can then initiate an in-depth risk management program.
- Risk management is a process, which means the safeguards and controls that are devised and implemented are not “install-and-forget” devices (discussed in the next lecture).

Knowing the Enemy

- **Knowing the enemy:** Identifying, examining, and understanding the threats facing the organization's information assets
  - Managers must fully identify those threats that pose risks to the organization and the security of its information assets

- Risk management is the process of discovering and assessing the risks to an organization's operations and determining how those risks can be controlled or mitigated

- Risk analysis is the identification and assessment of levels of risk in the organization; it is a major component of risk management.

Accountability for Risk Management

- All communities of interest bear responsibility for risk management. Each has a particular strategic role:
  - **InfoSec:** Because members of the InfoSec community best understand the threats and attacks that introduce risk, they often take a leadership role in addressing risk.
  - **IT:** This group must help to build secure systems and ensure their safe operation.
  - **Management and users:** This group plays a part in the early detection and response process. They also ensure that sufficient resources (money and personnel) are allocated to the InfoSec and IT groups to meet the security needs.

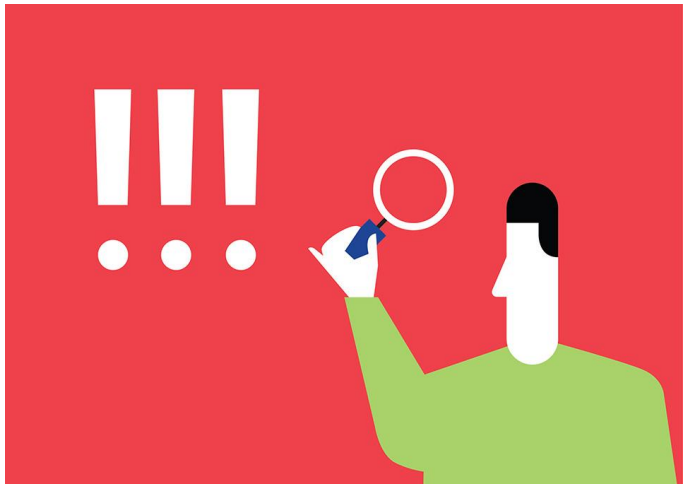
Accountability for Risk Management

- The three communities of interest must work together to address every level of risk, ranging from full-scale disasters to the smallest mistake made by an employee. To do so, they must be actively involved in the following activities:
  - Evaluating the 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 findings

Risk Identification

- **Risk identification:** The recognition, enumeration, and documentation of risks to an organization's information assets. The first operational phase of risk management.
  - **Information asset:** any collection/set/database of info or any asset that collects/stores/ processes/transmits info of value to the organization.

- Risk identification begins with a self-examination process. At this stage, managers must
  1. Identify the organization's information assets
  2. Classify them
  3. Categorize them into useful groups
  4. Prioritize them by their overall importance



Identification of Information Assets

- Identifying information assets, including people, procedures, data, software, hardware, networking elements

- This step should be done without pre-judging the value of each asset
  - ➢ Values will be assigned later in the process

Information 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 Utilities Security components
Hardware	Hardware	Systems and peripherals Security devices Network-attached process control devices and other embedded systems (Internet of Things)
Networking	Networking	Local area network components Intranet components Internet or extranet components Cloud-based components

Identifying Hardware, Software and Network Assets

- Many organizations use asset inventory systems to keep track of hardware, network and software components. Otherwise, an equivalent manual process is necessary.
- Whether automated or manual, inventory process requires a certain amount of planning. One must determine which attributes of each information asset should be tracked (depending on the organization's needs and risk management efforts)
- Potential asset attributes
  - Name, IP address
  - MAC address, asset type
  - Serial number, manufacturer name
  - Manufacturer's model or part number
  - Software version, update revision or FCO (field change order) number
  - Physical location, logical location
  - Controlling entity

Identifying people, procedures and data assets

- Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the needed knowledge, experience, and judgment

- As these assets are identified, they should be recorded using a reliable data-handling process like the one used for hardware and software

- The record-keeping system should be flexible, allowing to link assets to attributes based on the nature of information asset being tracked.

Identifying people, procedures and data assets

- Basic attributes for people, procedures, and data assets

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

  - **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

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

Classifying and Categorizing Information Assets

- Determine whether the asset categories are meaningful
- Inventory should also reflect each asset's sensitivity and security priority
  - A classification scheme categorizes information assets based on their sensitivity and security needs
  - Each of these categories designates the level of protection needed for a particular information asset

- Some asset types, such as personnel, may require an alternative classification scheme that would identify the clearance needed to use the asset type
- Classification categories must be comprehensive and mutually exclusive

Assessing the Values of Information Assets

- As each information asset is identified, categorized, and classified, a relative value must be assigned to it. Relative values are comparative judgments intended to ensure that the most valuable information assets are given the highest priority when managing risk.
  - A relative assessment helps ensure that the higher value assets are protected first.

- **Relevant questions**
  - 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?

Sample asset classification worksheet

System Name: SLS E-Commerce
Date Evaluated: February 2018
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-mail (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

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***	***100***
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	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

- The final step in the risk identification process is to list the assets in order of importance
- This goal can be achieved by using a weighted factor analysis worksheet
- In this process, each information asset is assigned a score for each critical factor

Threat Assessment

- The ultimate goal of risk identification is to assess the circumstances and setting of each information asset to reveal any vulnerabilities. Armed with a properly classified inventory, you can assess potential weaknesses in each information asset—a process known as threat assessment.

- Any organization typically faces a wide variety of threats. If you assume that every threat can and will attack every information asset, then the project scope becomes too complex. To make the process less unwieldy, each step in the threat identification and vulnerability identification processes is managed separately and then coordinated at the end.

Identifying Threats

- 12 categories of threats to InfoSec
- Each threat presents a unique challenge to InfoSec and must be handled with specific controls that directly address the particular threat and the threat agent's attack strategy.

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Source: CACM.

- Before threats can be assessed in the risk identification process, each threat must be further examined to determine its potential to affect the targeted information asset. This process is a threat assessment

Assessing Threats

- Not all threats endanger every organization. Examine each of the categories of threats and eliminate any that do not apply to your organization.
- The amount of danger posed by a threat is sometimes difficult to assess.
- Questions helpful in understanding the various threats the organization faces and their potential effects on an information asset:
  - Which threats represent an actual danger to our information assets?
  - Which threats are internal and which are external?
  - Which threats have the highest probability of occurrence?
  - Which threats have the highest probability of success?
  - Which threats could result in the greatest loss if successful?
  - Which threats is the organization least prepared to handle?
  - Which threats cost the most to protect against?
  - Which threats cost the most to recover from?

Prioritizing Threats

- Similar to its treatment of information assets, the organization should conduct a weighted table analysis with threats.
  - The organization should list the categories of threats it faces, and then select categories that correspond to the questions of interest described earlier. Next, it assigns a weighted value to each question category, and finally it assigns a value to each threat with respect to each question category.

- The result is a prioritized list of threats the organization can use to determine the relative severity of each threat facing its assets

Vulnerability Assessment

- Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat. This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization.

- **Vulnerabilities** are specific avenues that threat agents can exploit to attack an information asset
  - A flaw or weakness in an information asset, security procedure, design, or control that can be exploited accidentally or on purpose to breach security.

Vulnerability assessment 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 stolen.

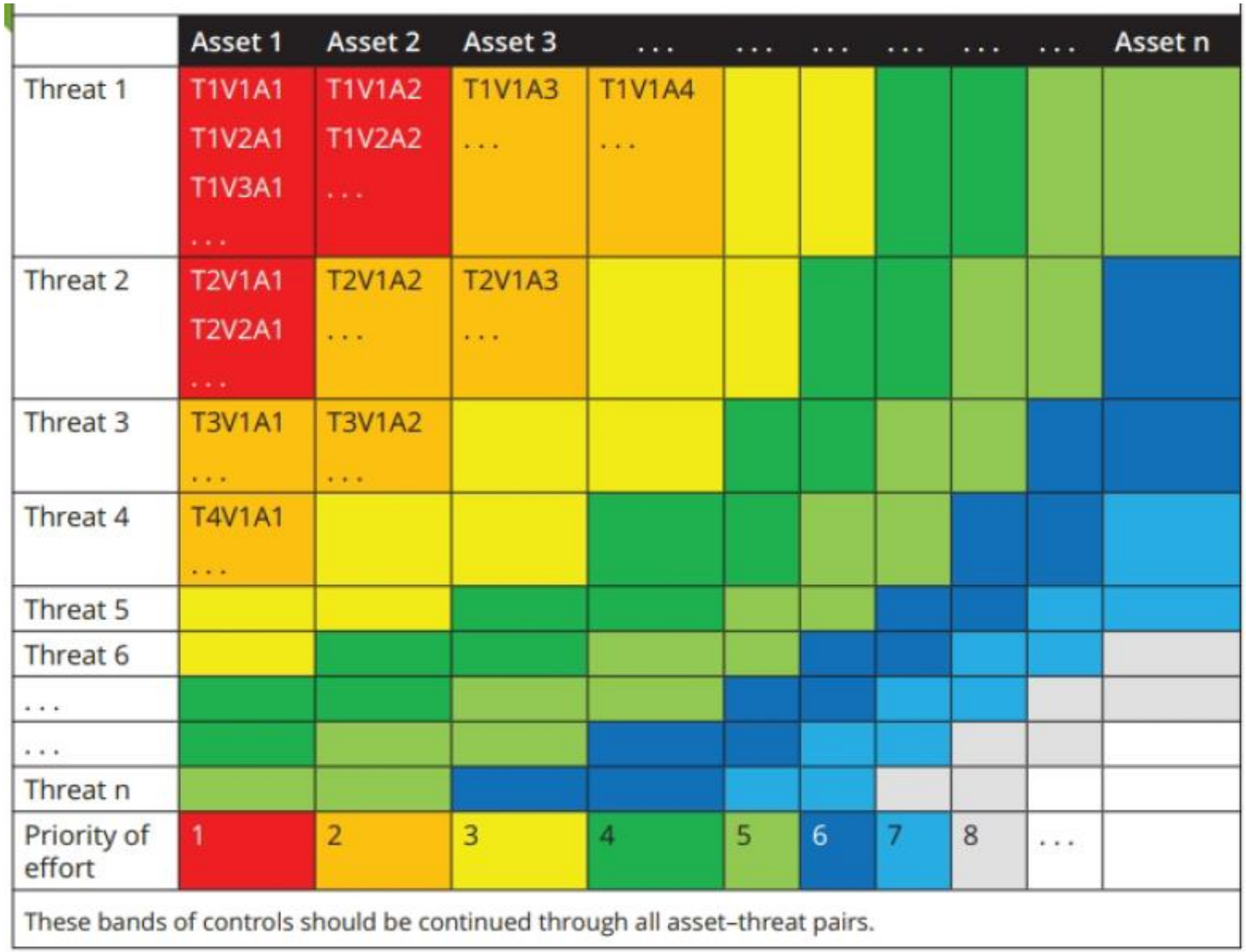
The TVA Worksheet

- At the end of the risk identification process, an organization should have
  - A prioritized list of assets
  - A prioritize list of threats facing those assets
  - A working knowledge of the vulnerabilities that exist between each threat and each asset
- These lists serve as the starting point for the next step in the risk management process: **risk assessment.**

- The prioritized lists of assets and threats can be combined into a single **Threats-Vulnerabilities-Assets (TVA)** worksheet
- A TVA worksheet lists the assets in priority order along one axis, and the threats in priority order along the other axis. The resulting grid provides a convenient method of examining the “exposure” of assets, allowing a simple vulnerability assessment.

Create a list of the TVA “triples” to facilitate your examination of the severity of the vulnerabilities.

- T1V1A1: Vulnerability 1 that exists between Threat 1 and Asset 1
- T1V2A1—Vulnerability 2 that exists between Threat 1 and Asset 1
- T2V1A1—Vulnerability 1 that exists between Threat 2 and Asset 1
- and so on



	Asset 1	Asset 2	Asset 3	. . .	. . .	. . .	. . .	. . .	. . .	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 . . .	T1V1A2 T1V2A2 . . .	T1V1A3 . . .	T1V1A4 . . .						
Threat 2	T2V1A1 T2V2A1 . . .	T2V1A2 . . .	T2V1A3 . . .							
Threat 3	T3V1A1 . . .	T3V1A2 . . .								
Threat 4	T4V1A1 . . .									
Threat 5										
Threat 6										
. . .										
. . .										
Threat n										
Priority of effort	1	2	3	4	5	6	7	8	. . .	
These bands of controls should be continued through all asset–threat pairs.										

Sample TVA spreadsheet

Risk Assessment

- Assessing the relative risk for each vulnerability is accomplished via a process called risk assessment.
- Risk assessment assigns a risk rating or score to each specific vulnerability.
  - This number gives an estimation of the relative risk associated with each vulnerable information asset

- Estimating risk is not an exact science. The formula in the next slide shows the factors used for calculating risks, some of which are estimates.
- The goal is to develop a repeatable method to evaluate the relative risk of each of the vulnerabilities that have been identified and added to the list.
  - Next lecture: How to determine more precise costs as well as projected expenses for the controls that reduce the risks.

A Formula for Relative Risk Assessment

$$R = (L_v \times I) \times (1 - R_c + U)$$

where

- R is the **risk** rating factor;
- L_v is the **likelihood** of vulnerability occurrence;
- I is the **impact value** of the information asset;
- R_c is the percentage of risk mitigated by **current controls**;
- U is the **uncertainty** of current knowledge of the vulnerability.

Likelihood

- Likelihood is the overall rating—a numerical value on a defined scale—of the probability that a specific vulnerability will be exploited.
- A commonly used scale rates likelihoods between 0.1 (low) and 1.0 (high)
  - Example: the likelihood of a system being damaged by a water leak could be rated as 0.1, while the likelihood of receiving at least one e-mail that contains a virus or worm in the next year would be rated as 0.5
- One can choose to use a different number scale, such as 1 to 10 or 1 to 100, depending on the granularity needed by the organization's process.
- Whatever rating system you employ for assigning likelihood, consistently use professionalism, experience, and judgment to determine the rating
  - For many asset/vulnerability combinations, existing sources have already determined their likelihood.

Assessing Potential Impact on Asset Value

- Once the probability of an attack by a threat has been evaluated, the organization typically looks at the possible **impact** or consequences of a successful attack. A feared consequence is the loss of asset value.

- The impact of an attack (most often as a loss in asset value) is of great concern to the organization in determining where to focus its protection efforts.

- The weighted tables used in risk identification can help organizations better understand the magnitude of a successful breach.

- Another good source of information is popular media venues that report on successful attacks in other organizations.

Percentage of Risk Mitigated by Current Controls and Uncertainty

- **Percentage of Risk Mitigated by Current Controls**
  - If a vulnerability is fully managed by an existing control, it can be set aside
  - If it is partially controlled, estimate what percentage of the vulnerability has been controlled

- **Uncertainty**
  - It is not possible to know everything about every vulnerability
  - The degree to which a current control can reduce risk is also subject to estimation error
  - Uncertainty is an estimate made by the manager using judgment and experience

Risk Determination

$$R = (L_v \times I) \times (1 - R_c + U)$$

- Asset A has impact value of 50. It has one vulnerability with a likelihood of 1.0 and with no current controls. Assumptions and data are 90% accurate.
  - L_v = 1.0
  - I = 50
  - R_c = 0
  - U = 100% - 90% = 10% = 0.1

- The vulnerability is hence rated by risk factor:

R = (1.0 x 50) x (1 – 0 + 0.1) = 55

Risk Determination

$$R = (L_v \times I) \times (1 - R_c + U)$$

- Asset B has impact value of 100 and has two vulnerabilities:
  - V2 has a likelihood 0.5, with a current control that addresses 50% of its risk;
  - V3 has a likelihood of 0.1 with no current controls.
  - Your assumptions and data are 80% accurate

- **V2:** L_v = 0.5, I = 100, R_c = 50% = 0.5, U = 100% - 80% = 20% = 0.2.
  Therefore, **R_2 = (0.5 × 100) x (1 – 0.5 + 0.2) = 35**
- **V3:** L_v = 0.1, I = 100, R_c = 0, U = 100% - 80% = 20% = 0.2.
  Therefore, **R_3 = (0.1 × 100) x (1 – 0 + 0.2) = 12**

Likelihood and Consequences

- Another approach to calculating risk based on likelihood is the likelihood and consequences rating from the Australian and New Zealand Risk Management Standard 4360 which uses qualitative methods to determine risk based on a threat's probability of occurrence and expected results of a successful attack.
- Consequences (i.e., impact assessment) are evaluated on 5 levels ranging from insignificant (level 1) to catastrophic (level 5), as assessed by the organization

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 and Consequences (cont'd)

- Qualitative likelihood assessments levels are represented by values ranging from A (almost certain) to E (rare), as determined by the organization

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

Likelihood and Consequences (cont'd.)

- When consequences and likelihoods are combined, the organization can determine which threats represent the greatest danger to the its information assets
- The resulting rankings can be inserted into TVA tables for use in risk assessment

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

Table 8-12 Qualitative risk assessment matrix

Note: E = Extreme risk: Immediate action required

H = High risk: Senior management attention required

M = Moderate risk: Management responsibility must be specified

L = Low risk: Management by routine procedures required

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas

- Purpose of this list: to identify areas of residual risk that may nor may not need to be reduced
  - ➢ residual risk is the risk that remains even after the existing control has been applied

- Three general categories of controls exist:
  - ➢ Policies
  - ➢ Programs
  - ➢ Technical controls

Documenting the Results of Risk Assessment

- Goals of the risk management process so far:
  - To identify information assets and their vulnerabilities
  - To rank them according to the need for protection

- In preparing this list, a wealth of factual information about the assets and the threats they face is collected.

- Information about the controls that are already in place is also collected

- The final summarized document is the **ranked vulnerability risk worksheet**

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 (cont'd.)

- What should the documentation package look like?
- What are the deliverables from this stage of the risk management project?
- The risk identification process should designate what function the reports serve, who is responsible for preparing them, and who reviews them

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

Risk identification and assessment deliverables