IS4231
Information Security Management

Lecture 8

Risk Management – Assessing Risk

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 6

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

risk management can be very general - just discussing enterprise risk

Topics

- Risk management role and process
- Risk identification
- Risk assessment
- Risk evaluation

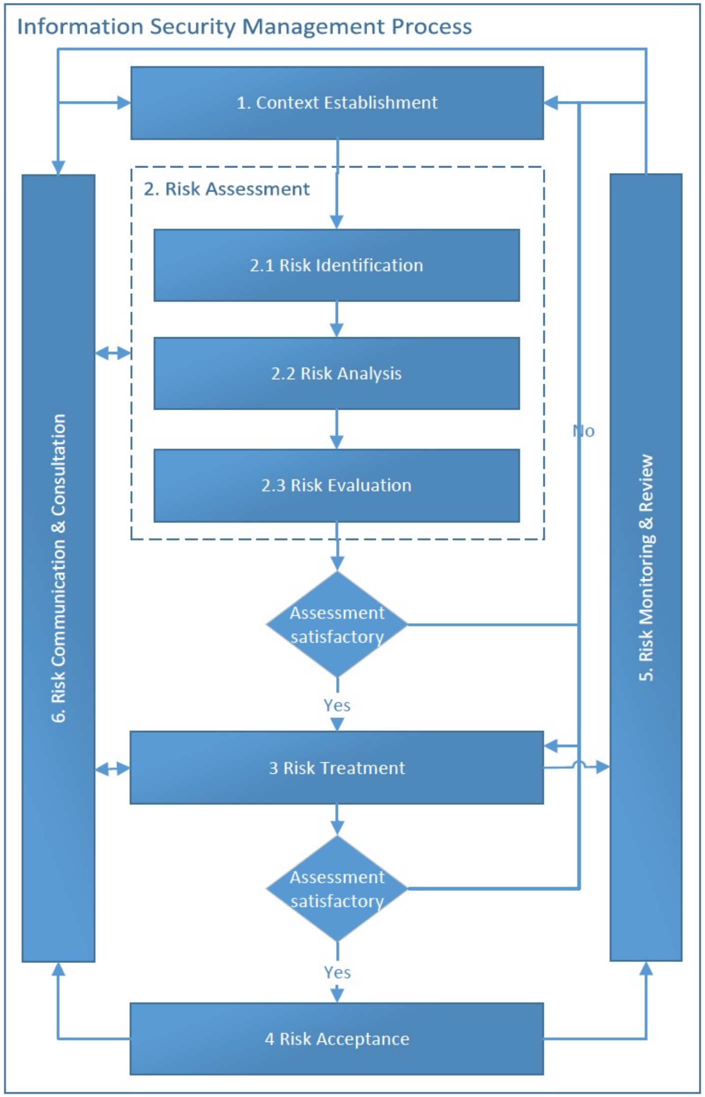
Introduction to Risk Management

Why Risk Management

- Risk Management
  - The process of discovering and assessing the risks to an organization’s operations and determining how those risks can be controlled and mitigated
  - The process involved discovering and understanding answers to some key questions regarding the risk associated with an organization’s information assets:
    - Where and what is the risk (risk identification)?
    - How severe is the current level of risk (risk analysis)?
    - Is the current level of risk acceptable (risk evaluation)?
    - What do I need to do to bring the risk to an acceptable level (risk treatment)?

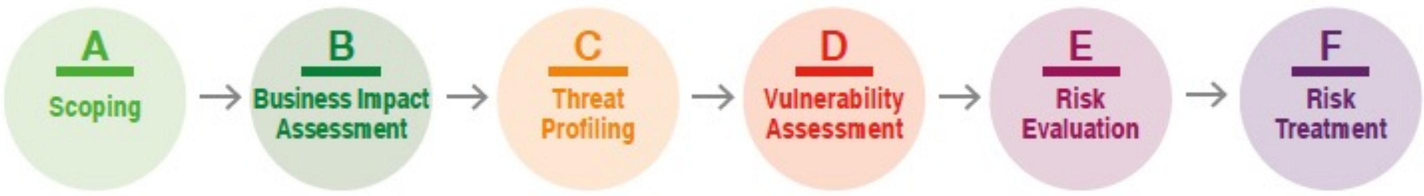
Introduction to Risk Management

- ISO27005: Risk Management
  - ISMS risk management process
    - 1. Context Establishment
    - 2. Risk Assessment
      - □ 2.1 risk identification
      - □ 2.2 risk analysis
      - □ 2.3 risk evaluation
    - 3. Risk Treatment
    - 4. Risk Acceptance
    - 5. Risk Monitoring & Review
    - 6. Risk Communication & Consultation



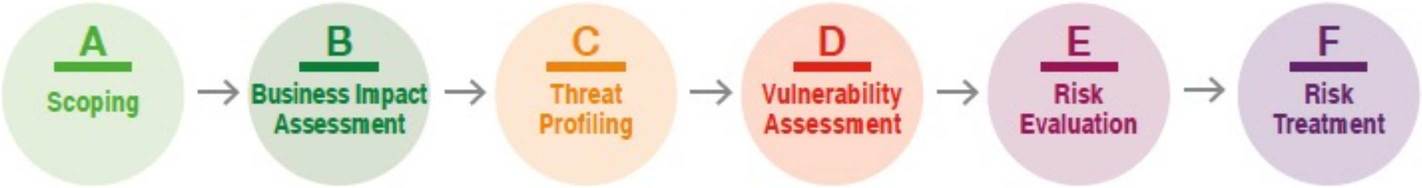
Introduction to Risk Management (cont.)

- IRAM$_2$
  - ISF Information Risk Assessment Methodology 2
    - Six-phase process for information risk management
      - 1. Scoping
      - 2. BIA
        - Assess worst-case scenarios-the potential business impact if information assets become compromised
      - 3. Threat profiling
        - Mapping different types of threats, both malicious and accidental, that could potentially affect the business



Introduction to Risk Management (cont.)

- $IRAM_2$
  - ISF Information Risk Assessment Methodology 2
    - Six-phase process for information risk management
      - □ 4.Vulnerability assessment:
        - □ Assess your vulnerabilities to different threat events and the strength of any controls already in place
      - □ 5. Risk evaluation
        - □ Evaluates the organization's risk appetite and likelihood of a successful threat in light of the previous findings.
      - □ 6. Risk treatment
        - □ Develop practical approaches to address the information risks which have been identified.



Risk Identification: Assets Analysis

Risk Assessment

- What information assets do I own?
  - Which ones are the most important ones?
- What are the threats against them?
  - Which threats pose the most danger?
- How vulnerable am I?
  - Which vulnerabilities should be addressed with high priority?

Thus, threat agents use vulnerabilities to attack information assets

Risk Identification

- Risk Identification
  - The recognition, enumeration,and documentation of risks to an organization's information assets
- It begins with the process of self-examination
- Managers:

1) Identify the organization's information assets

2) Classify and categorize them into useful groups

3) Prioritize them by overall importance

Identification of Information Assets

- Information Assets
  - Any asset that collects, stores, processes, or transmits information, or any collection, set, or databases of information that is of value to the organizations.

6 main categories

- People
- Procedure
- Data
- Software
- Hardware
- Networking

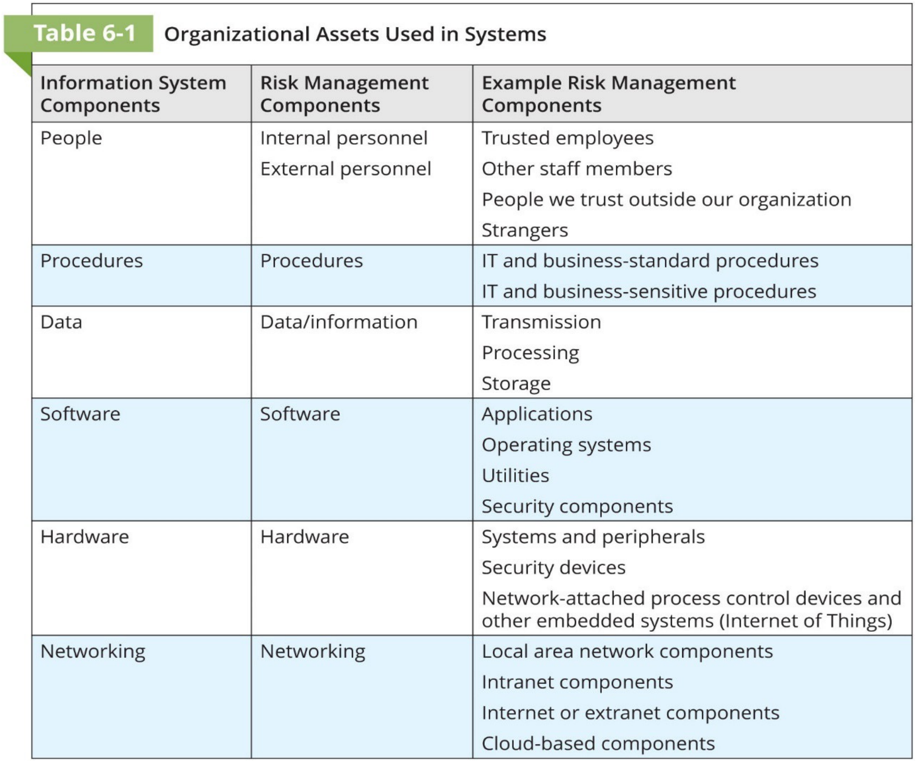


Table 6-1 Organizational Assets Used in Systems

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 their hardware, network, and software components

different organisations might have different ways to store and manage each asset

- When deciding which attributes to track for each information asset, consider the following list of potential attributes:
  - 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

Identifying 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

ISO27k: Asset Management

- Inventory of assets:
  - Digital data
  - Hardcopy information
  - Software
  - Infrastructure
  - Information services and service providers
  - Physical security and safety related
  - Business relationships
  - People

ISO27k: Asset Management (cont.)

- Inventory of assets:
  - Digital data
    - E.g., business data of all kinds and all locations; IT/support data; etc.,
  - Hardcopy information
    - E.g., system and process documentation (covering specifications, architecture and design, installation, operation, use , management…); licenses, agreements and contracts; disaster recovery plans; etc.,
  - Software
    - E.g., system software plus patches and vulnerability disclosures; applications, IT management utilities, databases and middleware; etc.;
  - Infrastructure
    - E.g., servers, network devices (e.g., routers, switches, load balancers, VPN devices, web proxy servers), security devices (e.g., gateways and firewalls, IDPS, SIEM), communications devices (e.g., modems, Internet connections), cables, end user devices, etc.;

ISO27k: Asset Management (cont.)

- Inventory of assets:
  - Information services and service providers
    - E.g., Internet and cloud services, Pentest services; etc.,;
  - Physical security and safety related
    - E.g., smoke detectors, alarms and fire suppression systems; power provision including UPS and generators; air conditioning plus temperature monitoring and alarms; server racks, card access controls, keys; etc.;
  - Business relationships

    ie: contracts are considered business secrets
    - With external parties e.g., suppliers, partners, etc,;
  - People
    - In particular, any critical or valuable individuals with unique knowledge, experience skills.

Classifying and Categorizing Information Assets

- Determine whether initial asset categories are meaningful to the organization
- Inventory should reflect each asset's sensitivity and security priority
  - A data classification scheme should be developed that categorize the assets based on their sensitivity and security needs
  - The category that an information asset is put into is indication of the level of protection needed
- Classification categories must be
  - *Comprehensive*
    - All inventories fit into a category
  - *Mutually exclusive*
    - Each asset is found in only one category

Question:

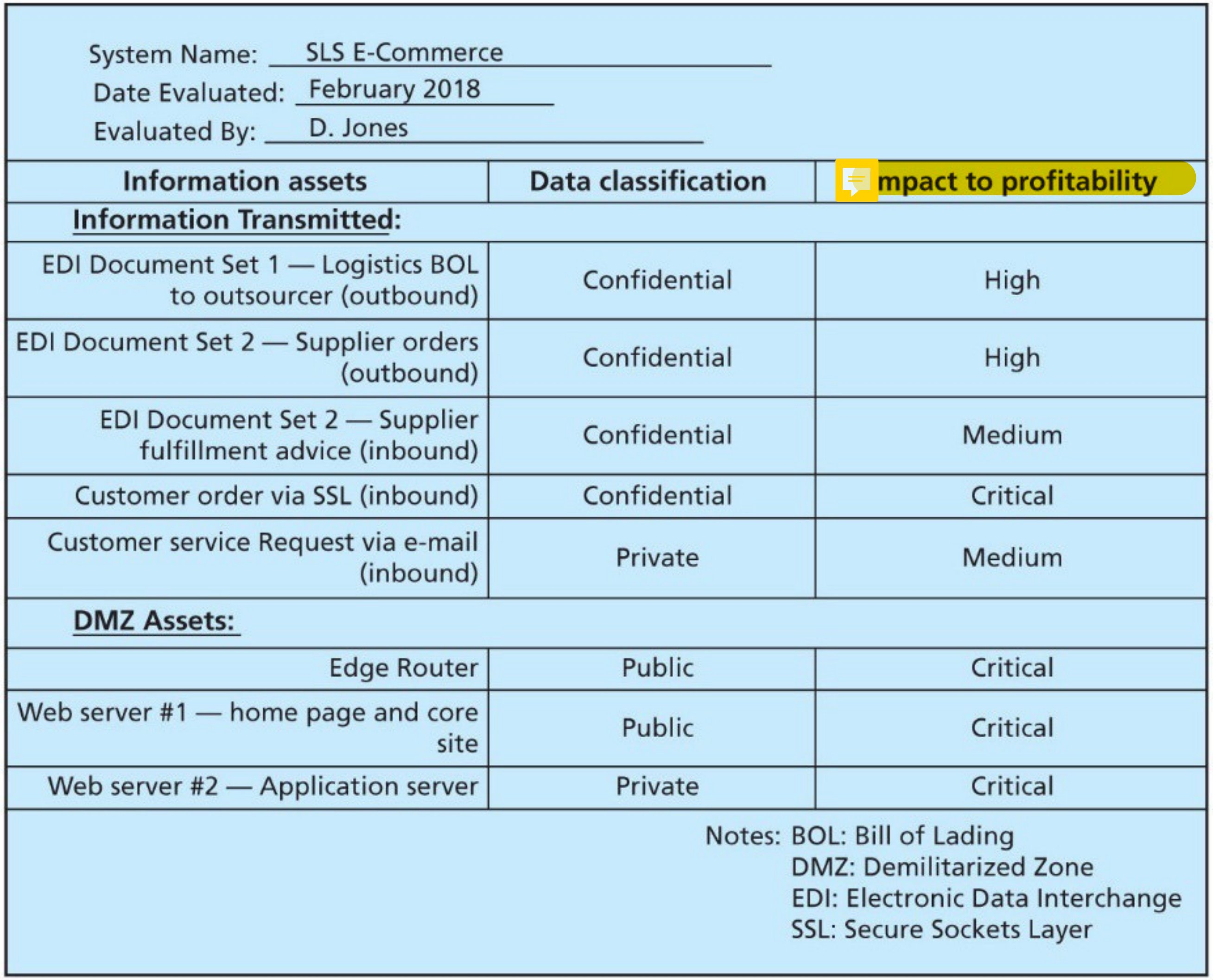
- Public Key Infrastructure Certificate Authority
  - Software/security component/cryptography
  - Software/security component/PKI

No this will not satisfy mutually exclusive criteria how to rank/prioritise in terms of criticality

Assessing Values for Information Assets

- Assign a relative value to each information asset
- Use comparative judgments to ensure the most valuable information assets are given the highest priority in the implementation of safeguards and controls:
  - Which information asset is *the most critical* to the success of the organization?
  - Which information asset generates *the most revenue*?
  - Which information asset generates *the highest profitability*?
  - Which information asset is *the most expensive to replace*?
  - Which information asset is *the most expensive to protect*?
  - Which information 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

Figure 6-3 Sample asset classification scheme

Prioritizing (Rank Ordering) Information Assets

- The final step in the risk identification process is to prioritize, or rank order the assets
- This goal can be achieved by using a weighted table analysis

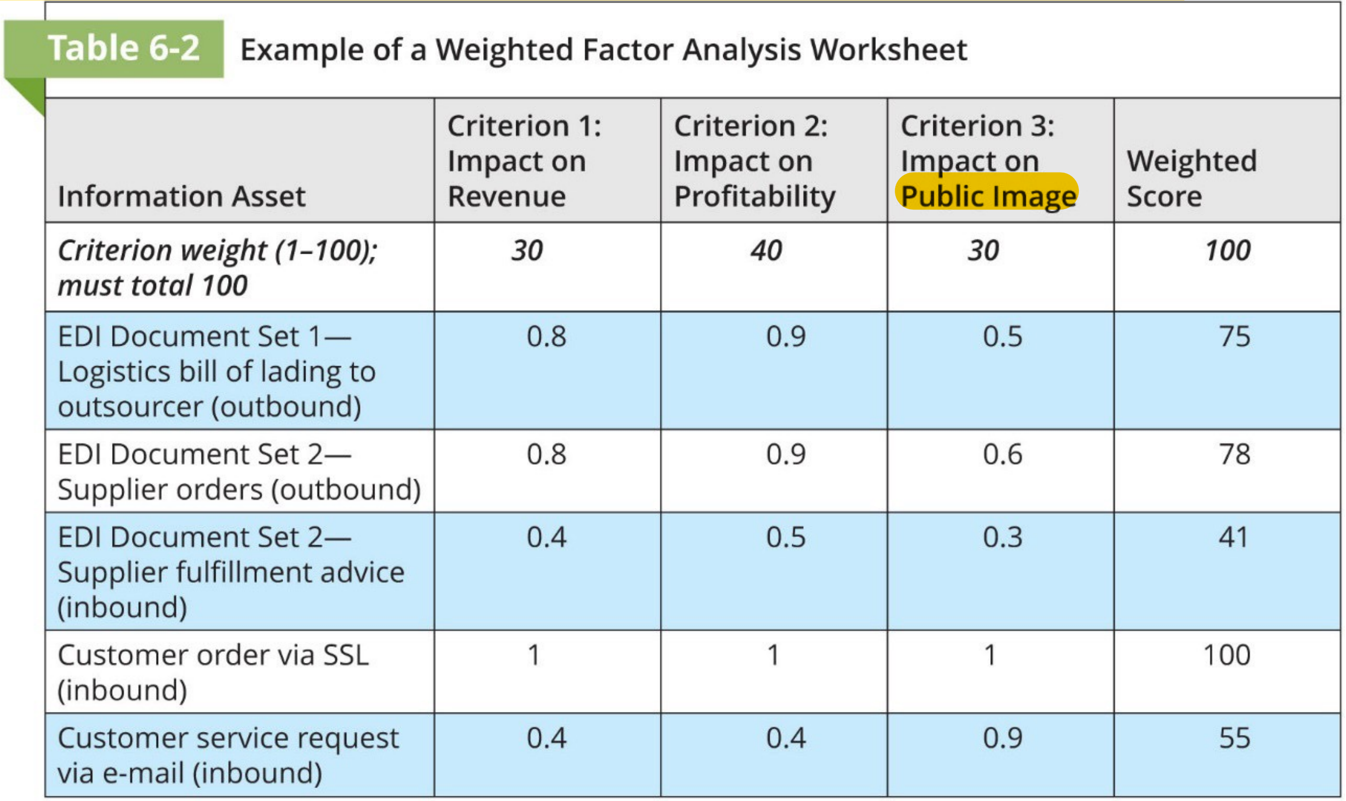
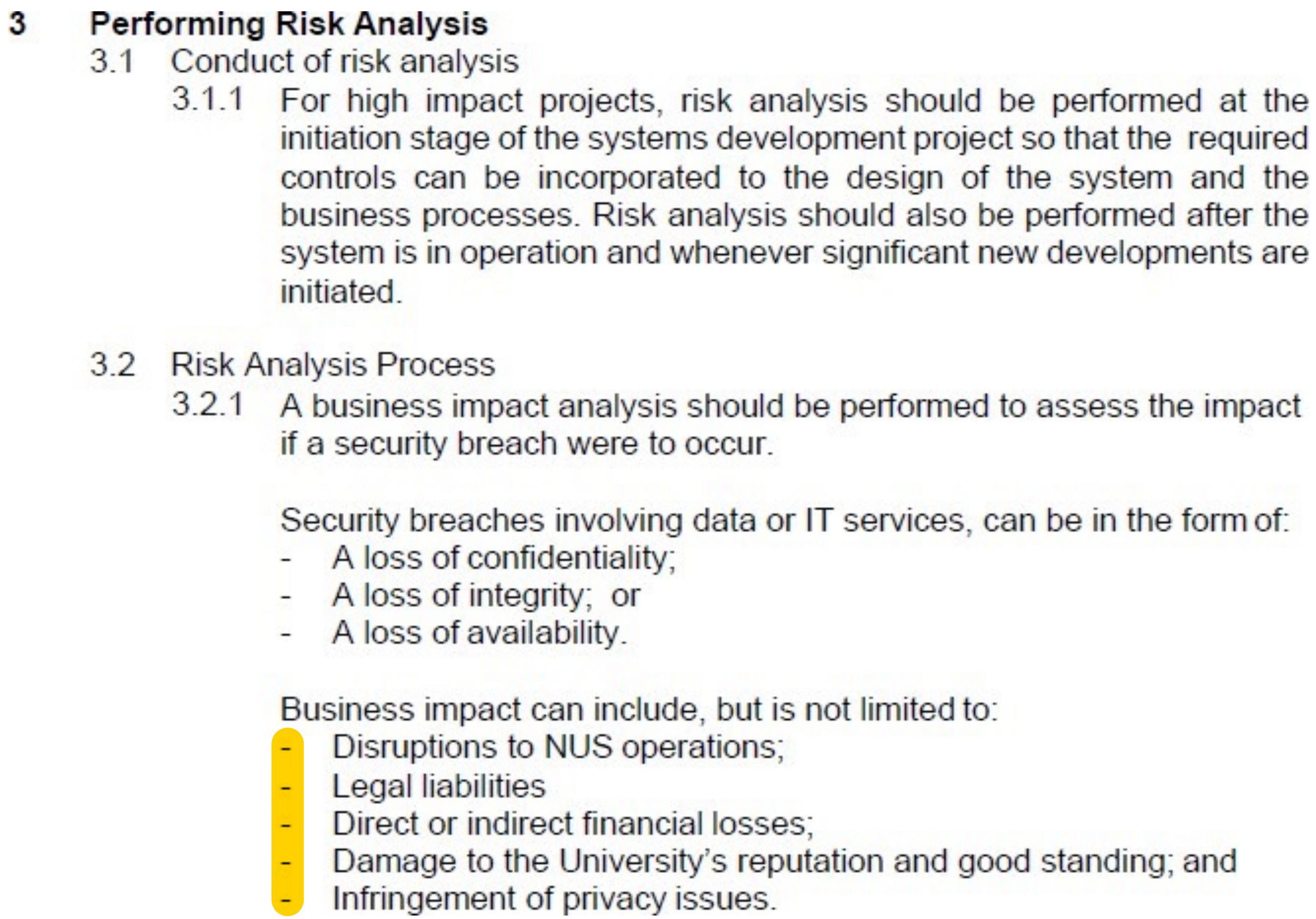


Table 6-2 Example of a Weighted Factor Analysis Worksheet

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*	*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

Note: In the table, EDI = Electronic Data Interchange and SSL = Secure Sockets Layer.

Example: NUS Risk Analysis



3 Performing Risk Analysis

3.1 Conduct of risk analysis

3.1.1 For high impact projects, risk analysis should be performed at the initiation stage of the systems development project so that the required controls can be incorporated to the design of the system and the business processes. Risk analysis should also be performed after the system is in operation and whenever significant new developments are initiated.

3.2 Risk Analysis Process

3.2.1 A business impact analysis should be performed to assess the impact if a security breach were to occur.

Security breaches involving data or IT services, can be in the form of:

- A loss of confidentiality;
- A loss of integrity; or
- A loss of availability.

Business impact can include, but is not limited to:

- Disruptions to NUS operations;
- Legal liabilities
- Direct or indirect financial losses;
- Damage to the University's reputation and good standing; and
- Infringement of privacy issues.

Risk Identification:Threats Analysis

What is Threat Assessment?

- Armed with a properly classified inventory, you can assess potential weakness in each information asset - a process known as threat assessment.
- Three aspects
  - Threat identification
  - Threat assessment
  - Vulnerability assessment

the goal at the end of the day is to find internal weaknesses
- but now it would be to analyse external threats (environment)
to better understand internal vulnerabilities

- Threats
  - Circumstance or event that can adversely impact operations, assets, individuals through an information system.
  - To keep risk management 'manageable'…
    - Identify realistic threats and investigate those further

Threat categories

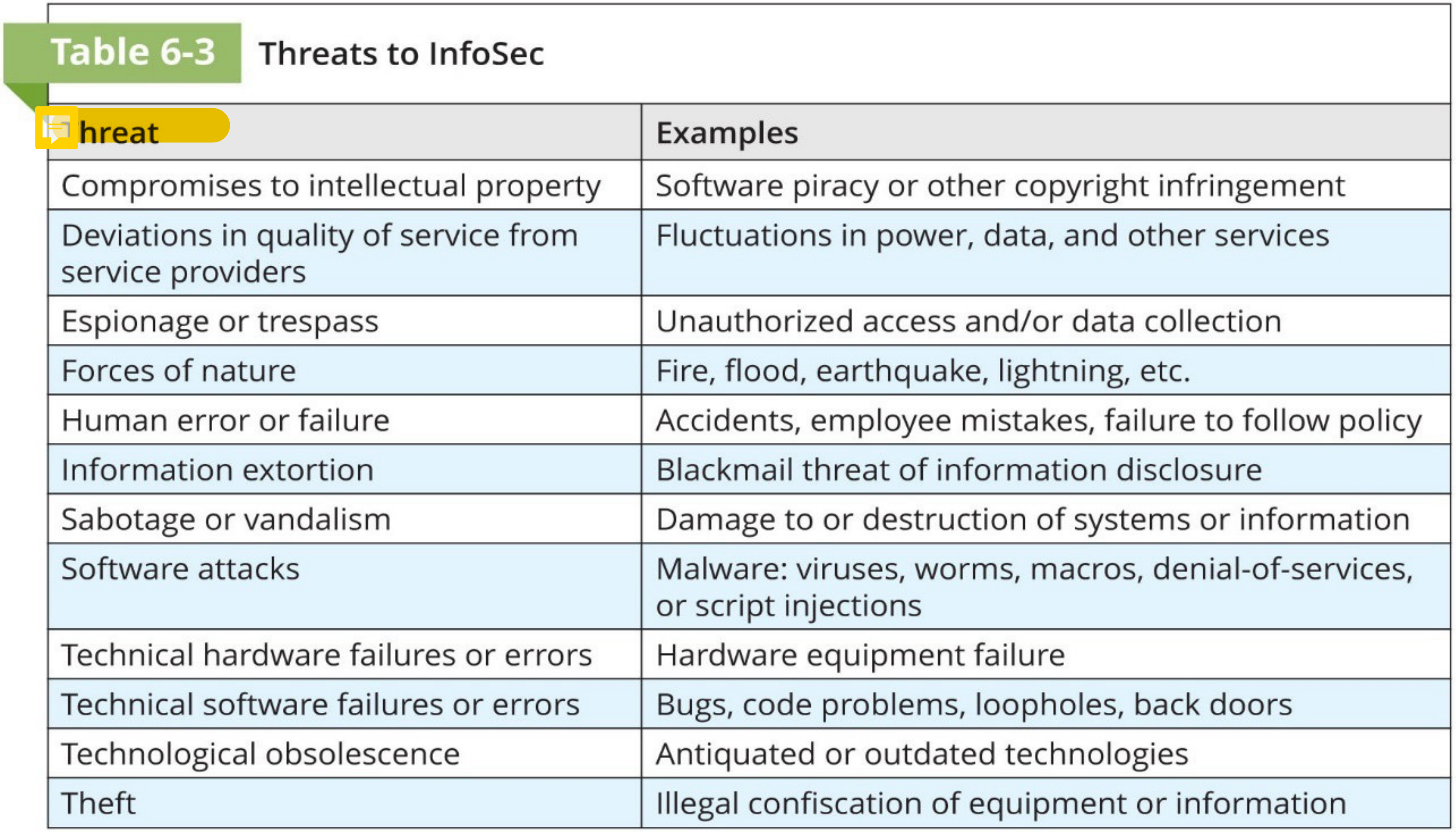


Table 6-3 **Threats to InfoSec**

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.

Threat Assessment

- The following questions can help in understanding the various threats and their potential effects on an information asset
- Which threats
  - represent *an actual danger* to our organization's information?
  - are *internal* and which are *external*?
  - have the *highest probability of occurrence*?
  - have the *highest probability of success*?
  - could result in the *greatest loss* if successful?
  - are the organization *least prepared to handle*?
  - *cost the most* to *protect against*?
  - *cost the most* to *recover from*?

Prioritizing Threats

- Just as it did with 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
- In extreme cases, the organization may want to perform such an assessment of each threat *by asset*, if the severity of each threat is different depending on the nature of the information asset under evaluation

Vulnerability Assessment

- Once the organization has identified and prioritized both its information assets and the threats facing those assets it can begin to compare information asset to threats
- Review every information asset for <u>all vulnerabilities to every identified threat</u>
  - Vulnerability =
    - Specific avenue that threat agents can exploit to attack the information asset
    - Flaw or weakness in an information asset, security procedure, design or control that can be exploited accidentally or on purpose to breach security of the asset
- A list should be created for each information asset to document its vulnerability to each possible or likely attack

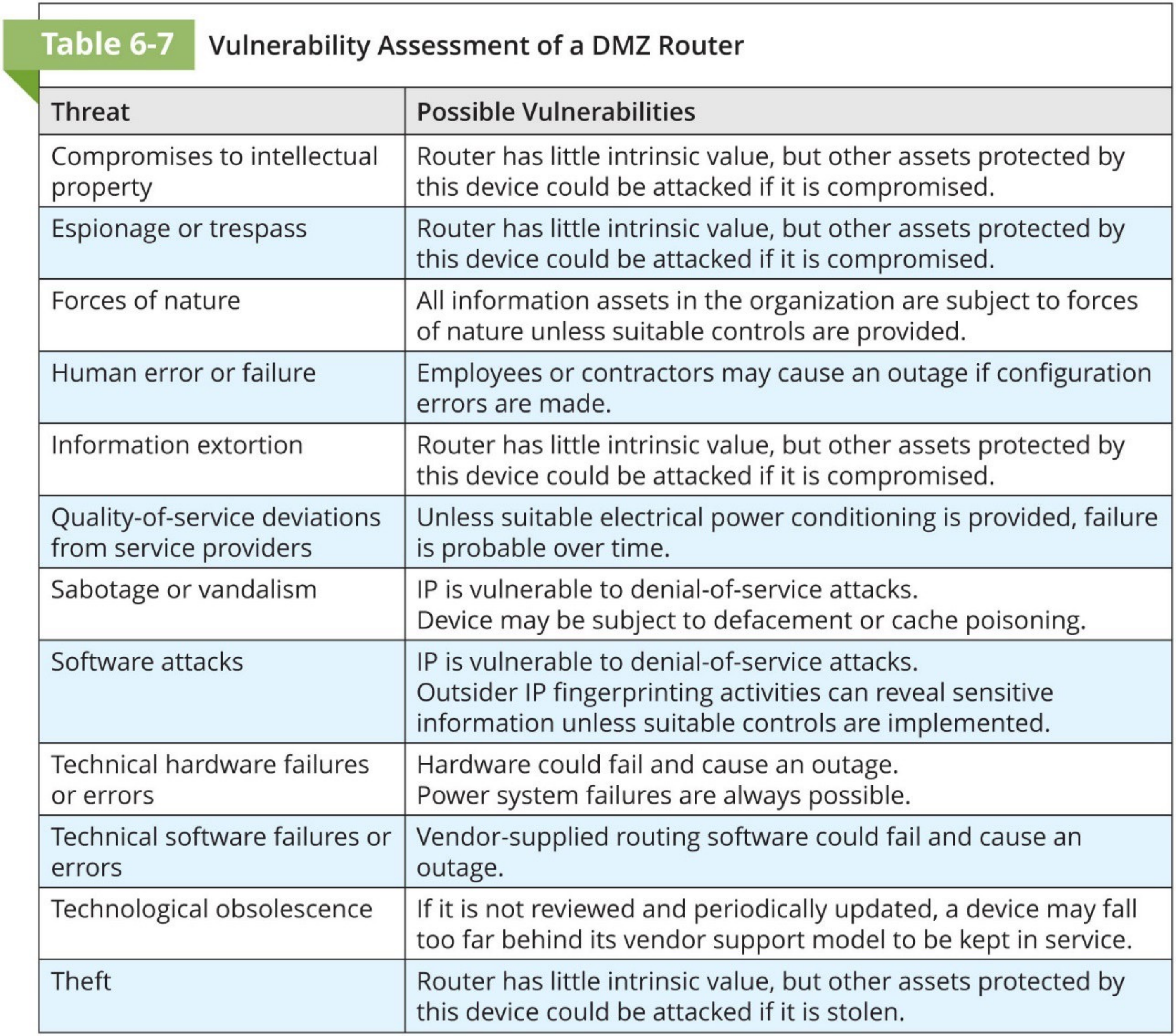
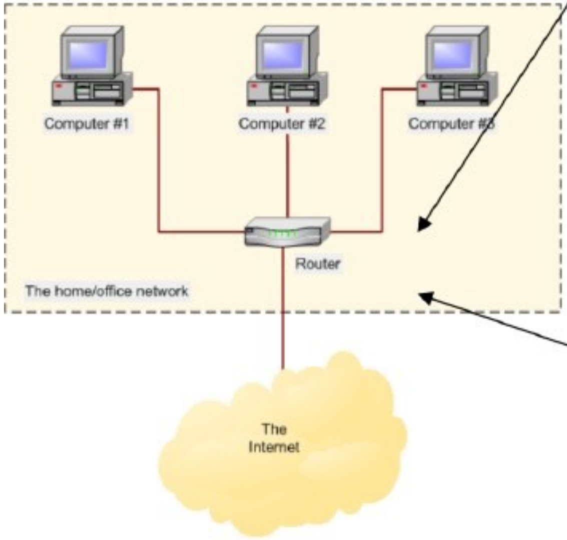


Table 6-7 Vulnerability Assessment of a DMZ Router

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.



router

Asset

temperature control in router/server room is not adequate ⇒ router overheats and shuts downs

[control weakness, design flaw]

net. administrator allows access to unauthor. user ⇒ unauthor. user uploads a virus, router crashes

[control / procedural weakness]

Vulnerability

Act of Human Error or Failure

Threat

The TVA Worksheet

- Two lists produced at the end of risk identification process
  - Prioritized list of assets and their vulnerabilities
  - Prioritized list of threats facing the organization based on a weighted table
- Combine these two lists into a **Threats-Vulnerabilities-Assets** (TVA) worksheet
  - T1V1A1-Vulnerability 1 that exists between Threat 1 and Asset 1

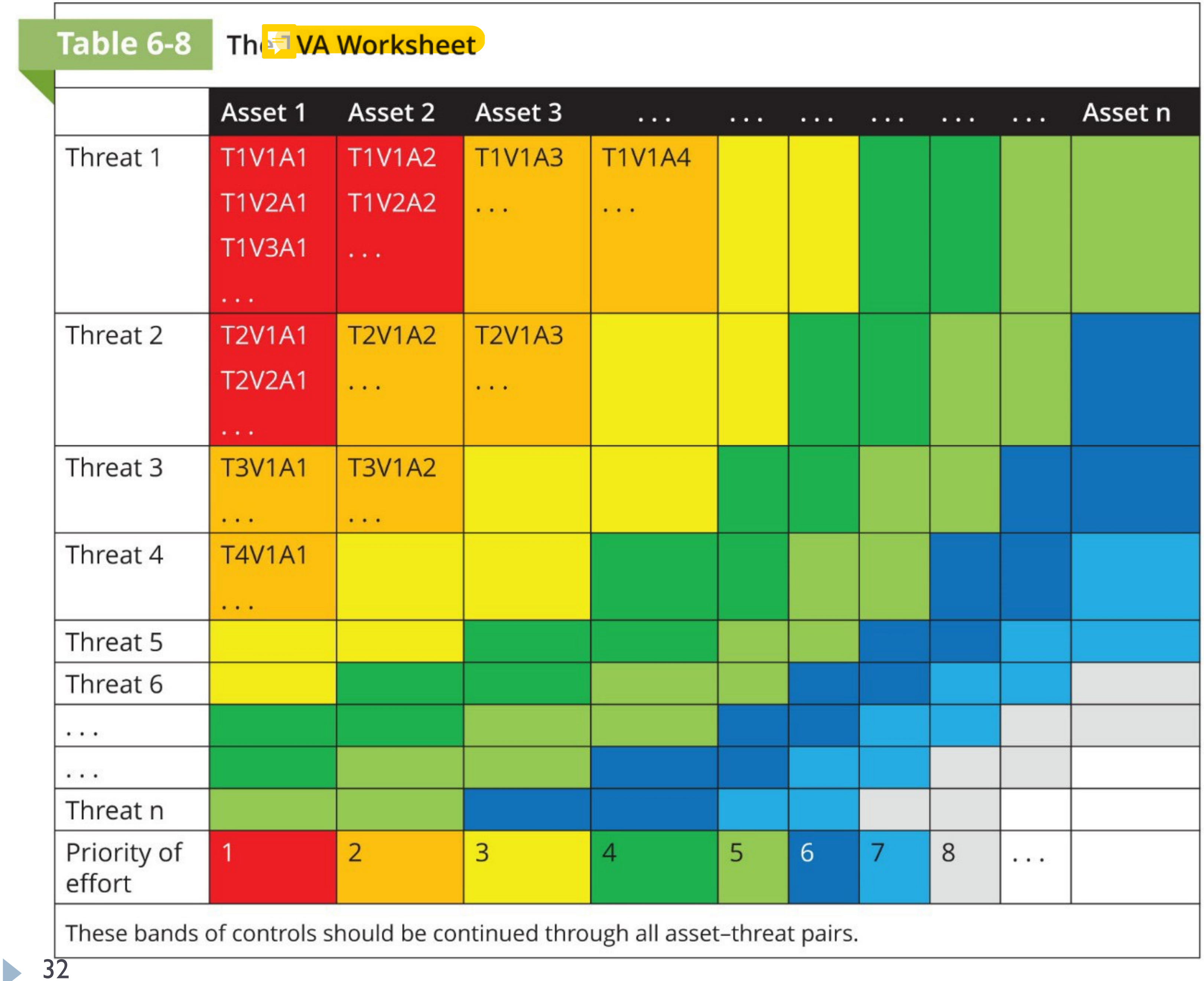


Table 6-8 The TVA Worksheet

	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.

Risk Assessment: Risk Analysis

Risk Estimate Factors

- Risk assessment
  - Assessing the *relative risk of each vulnerability*
  - While this number does not mean anything in absolute terms, it enables you to gauge the relative risk associated with each vulnerable information asset, and it facilitates the creation of comparative ratings later in the risk treatment process
  - Estimating risk is not an exact science; thus some practitioners use calculated values for risk estimation, whereas others rely on broader methods of estimation.
  - 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.

Determining the Likelihood of a Threat Event

- Likelihood is the overall rating - a numerical value on a defined scale - of the probability that a specific vulnerability will be exploited
- A simple method of assessing risk likelihood is to score the event on a rating scale:

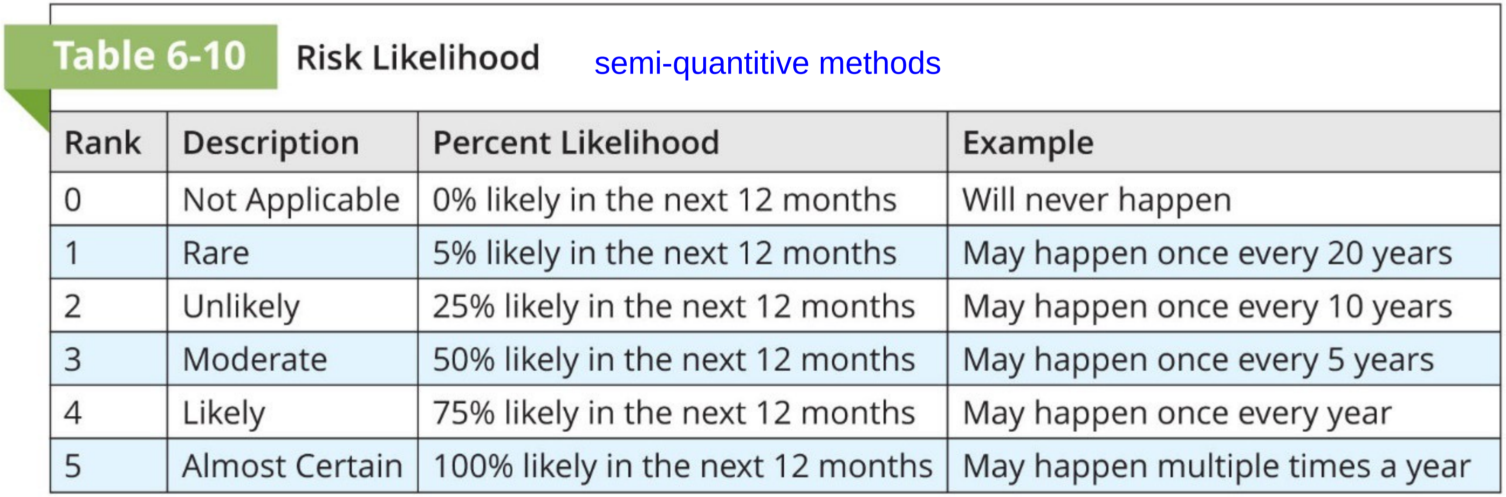


Table 6-10 Risk Likelihood

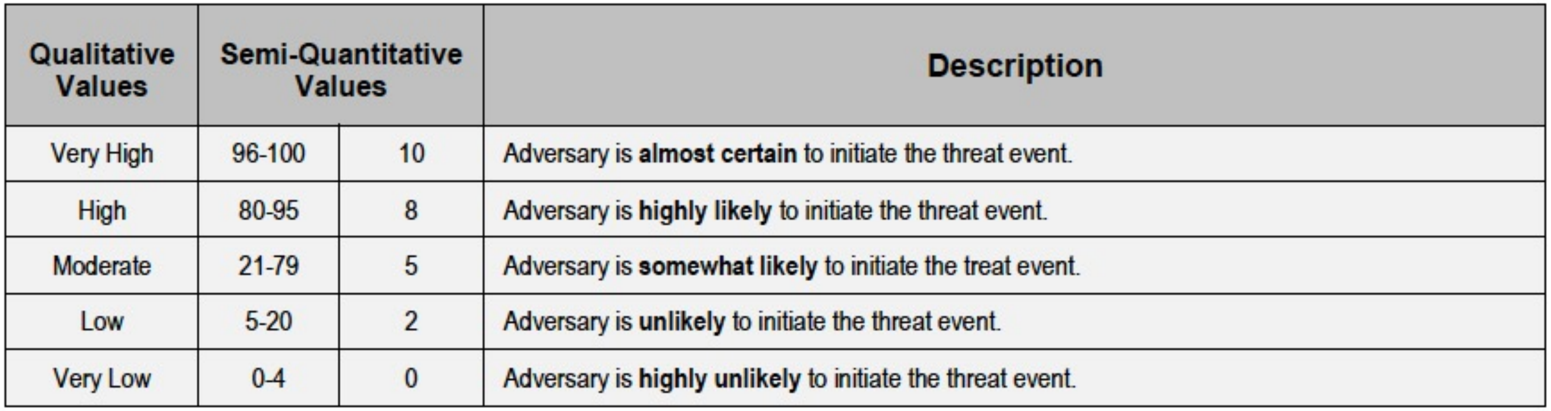
semi-quantitive methods

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months	Will never happen
1	Rare	5% likely in the next 12 months	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months	May happen once every 10 years
3	Moderate	50% likely in the next 12 months	May happen once every 5 years
4	Likely	75% likely in the next 12 months	May happen once every year
5	Almost Certain	100% likely in the next 12 months	May happen multiple times a year

Source: Clearwater Compliance IRM.

Determining the Likelihood of a Threat Event

- NIST SP 800-30 r1. Managing Information Security risk Organizations
  - Suggested kelihood scale



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

numeric numbers makes ranking easier

Assessing Potential Impact on Asset Value

- Impact – The magnitude of harm resulting from a threat event exploiting a vulnerability (or set of vulnerabilities).

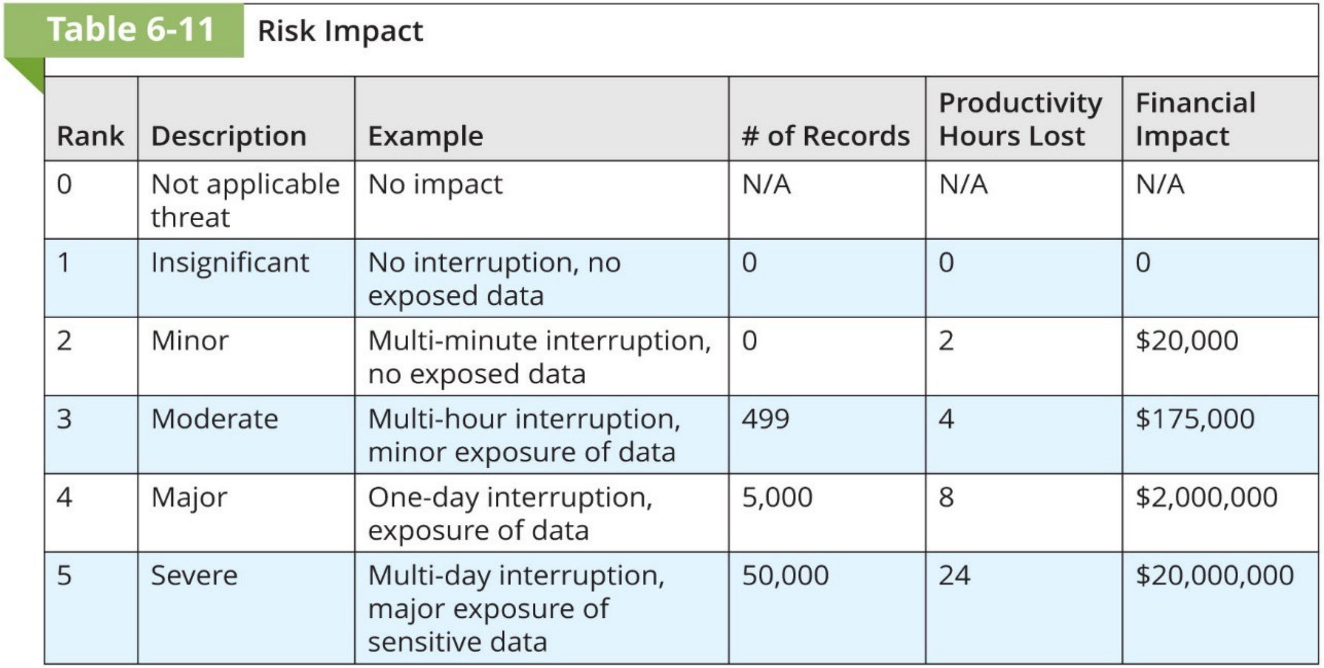


Table 6-11 Risk Impact

Rank	Description	Example	# of Records	Productivity Hours Lost	Financial Impact
0	Not applicable threat	No impact	N/A	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2	$20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4	$175,000
4	Major	One-day interruption, exposure of data	5,000	8	$2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24	$20,000,000

Source: Clearwater Compliance IRM.

Risk Determination

- Most organizations go with a simple formular:
  - Risk = Likelihood × Impact

- Practice:
  - Information asset 2 faced with threat 2 is at risk with general vulnerabilities 2 and 3. The risk rating for A2V2T2 has a Likelihood rating of 4 and an Impact rating of 4. The risk rating for A2V3T2 has a Likelihood rating of 3 and an Impact rating of 2. The resulting risk rating for A2V2T2 / A2V3T2 is ?
    - A2V2T2 : ? 16
    - A2V3T2 : ? 6

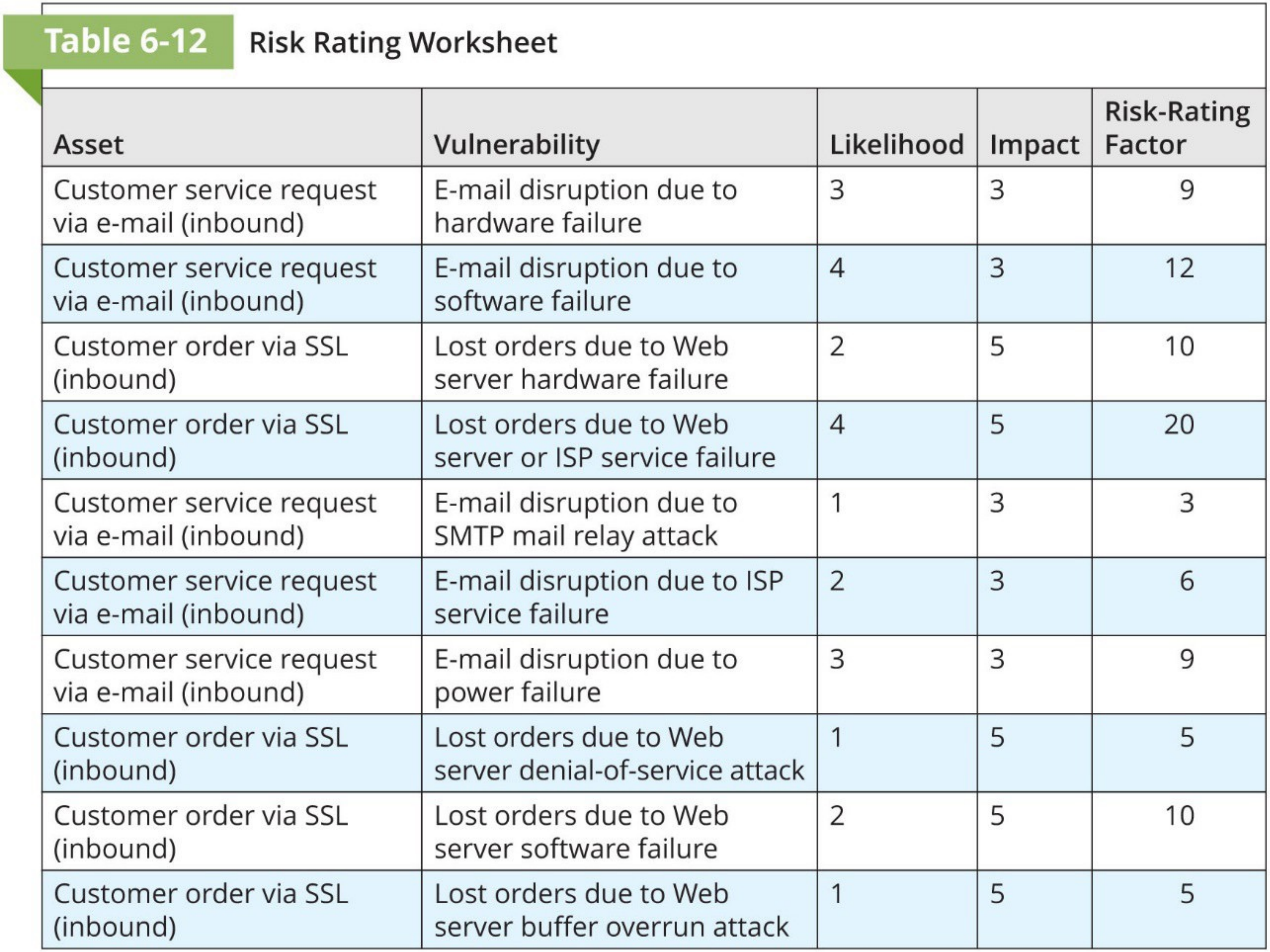
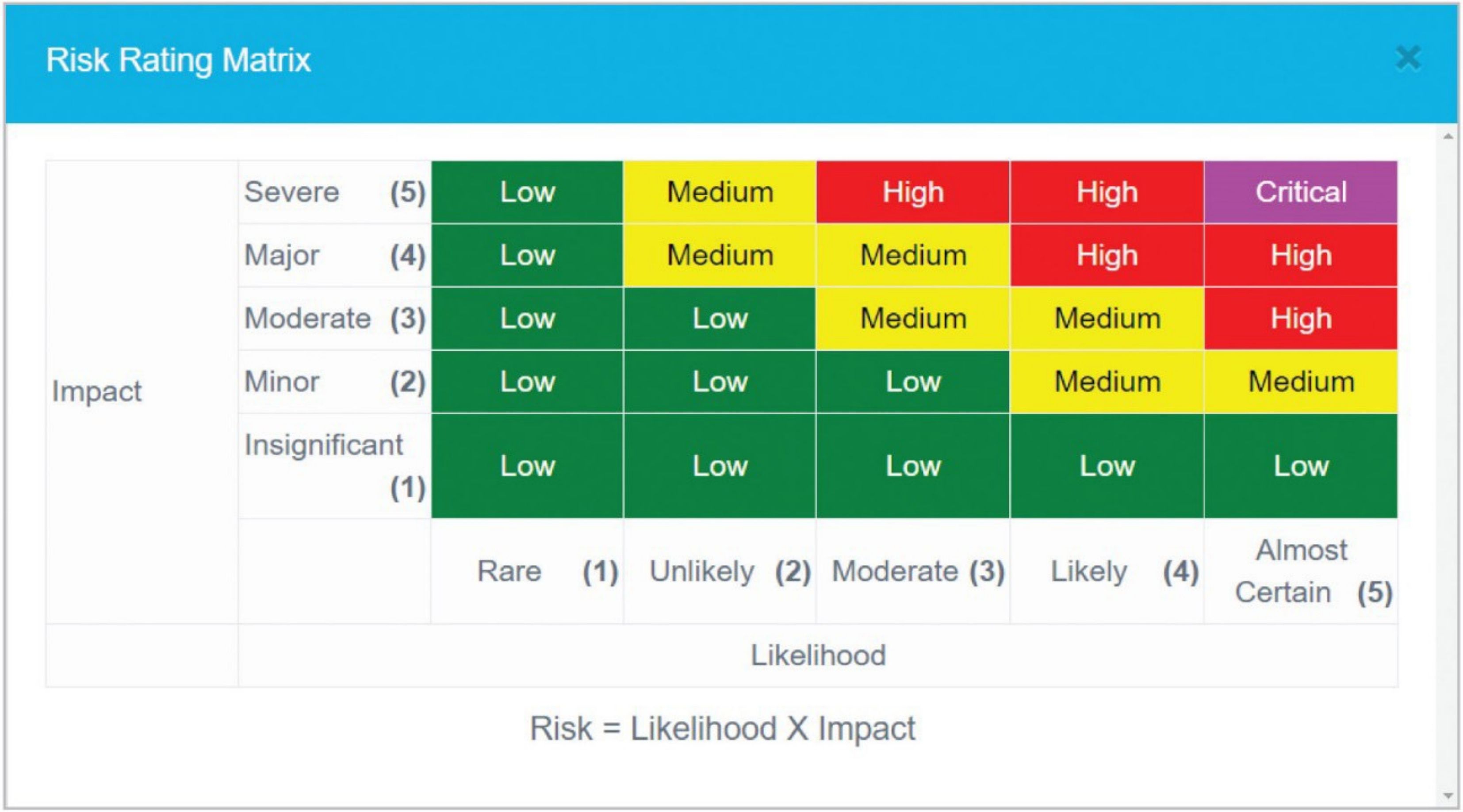


Table 6-12 Risk Rating Worksheet

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5



Risk Rating Matrix

Impact	Severe (5)	Low	Medium	High	High	Critical
	Major (4)	Low	Medium	Medium	High	High
	Moderate (3)	Low	Low	Medium	Medium	High
	Minor (2)	Low	Low	Low	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
	Likelihood					

Risk = Likelihood X Impact

Figure 6-10 Clearwater Compliance IRM risk rating matrix

Source: Clearwater Compliance IRM.

uncertainty in estimation can come from
- over estimation
- under estimation

Uncertainty

- It is not possible to know everything about every vulnerability, such as the likelihood of an attack against an asset or how great an impact a successful attack would have on the organization
- 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
- One formula of estimating risk uses the following:
  - Risk = Likelihood of the exploitation of a vulnerability x Impact of the information asset ± uncertainty

Uncertainty

- Practice:
  - Information asset 2 faced with threat 2 is at risk with general vulnerabilities 2 and 3.The risk rating for A2V2T2 has a Likelihood rating of 4 and an Impact rating of 4.The risk rating for A2V3T2 has a Likelihood rating of 3 and an Impact rating of 2.You estimate that assumptions and data are 80 percent accurate.The resulting risk rating for A2V2T2 / A2V3T2 is ?
    - A2V2T2 : ?
    - A2V3T2 : ? 6 ± 1.2

Documenting the Results of Risk Assessment

- The efforts to compile risks into a comprehensive list allow the organization to make informed choices from the best available information
- It is also of value for future iterations of the process to document the results in a reusable form

Documenting the Results of Risk Assessment

- What to document
  - Risk Scenario
    - Threat event, vulnerability, asset, consequence
      - □ E.g., Malware installed on POS terminals with no white-list application installation rule applied, makes credit card data stolen.
  - Identification date
  - Existing measures
  - Current risk
  - Treatment plan
  - Progress status
  - Residual risk
  - Risk Owner

CSA recommendation - also benchmarked with US standard

Risk Evaluation

- Once the risk ratings are calculated for all TVA triples, the organization needs to decide whether it can live with the analyzed level of risk—in other words, the organization must determine its *risk appetite*
  - Risk Appetite:
    - The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility

NHS and bank will not have the same risk appetite

- This is the **risk evaluation** stage
- The organization must translate its risk appetite from the general statement developed by the RM framework team (and based on guidance from the governance group) to a numerical value it can compare to each analyzed risk

Risk Evaluation

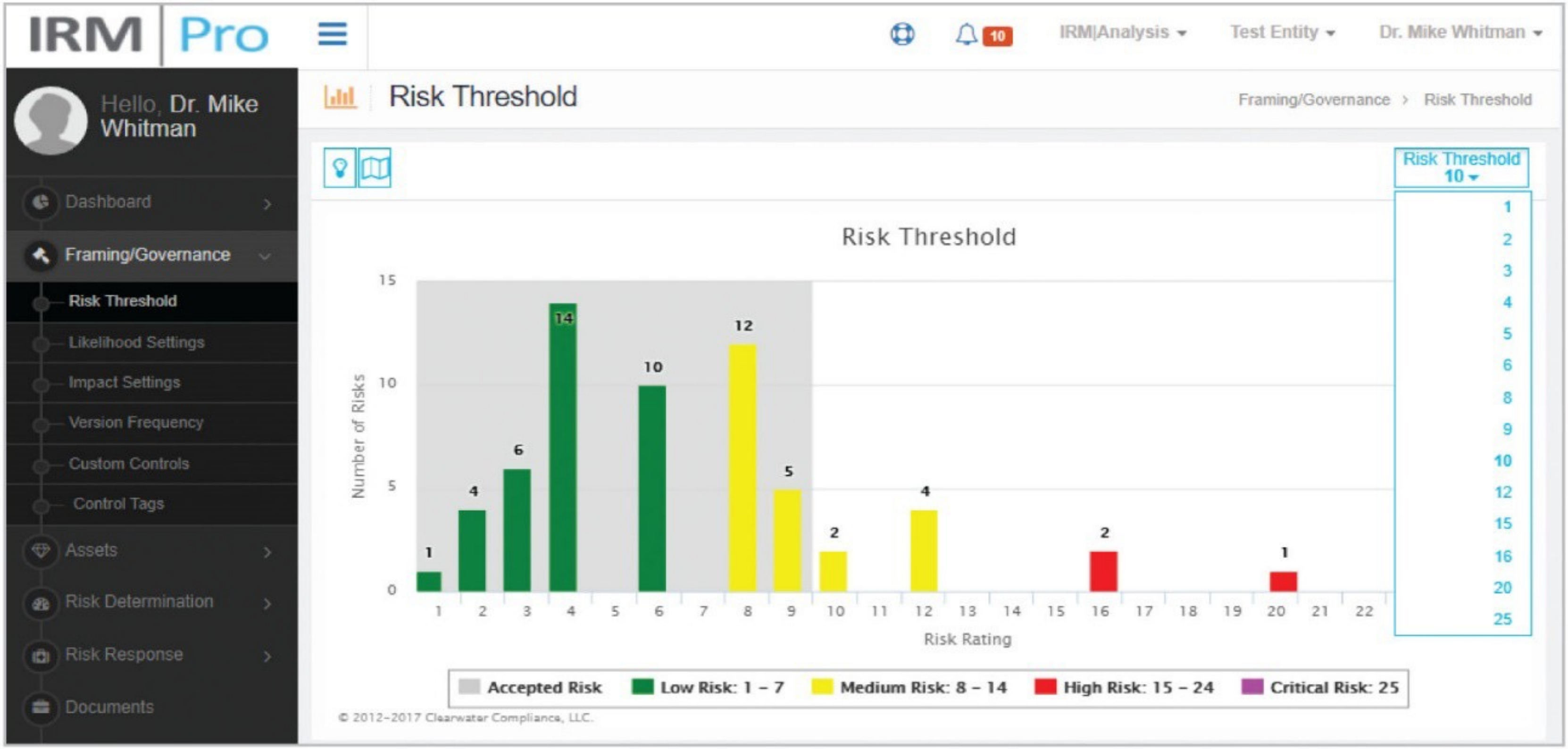


Figure 6-12 Clearwater Compliance IRM risk threshold

Source: Clearwater Compliance IRM.

Risk Assessment Deliverables

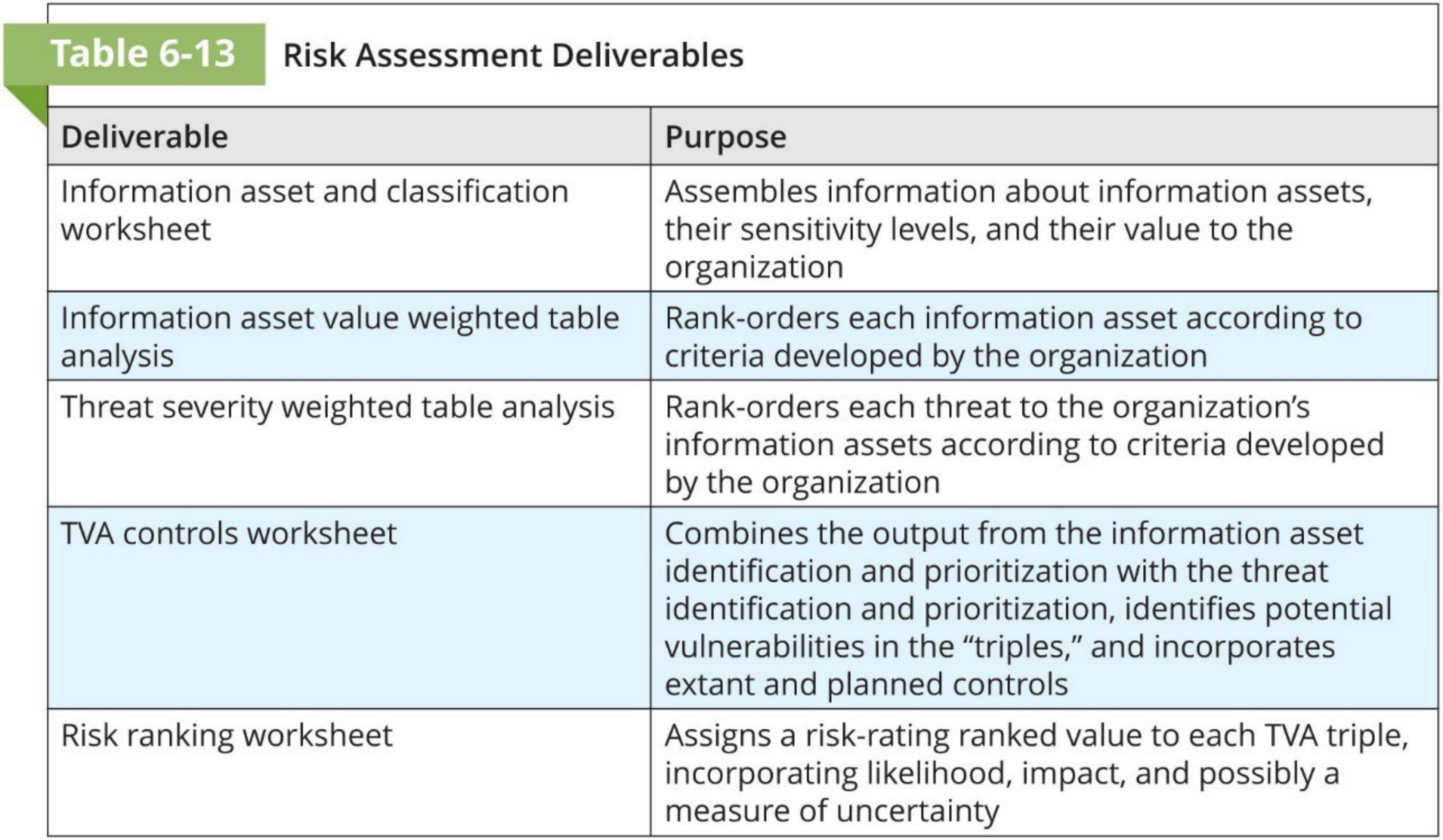
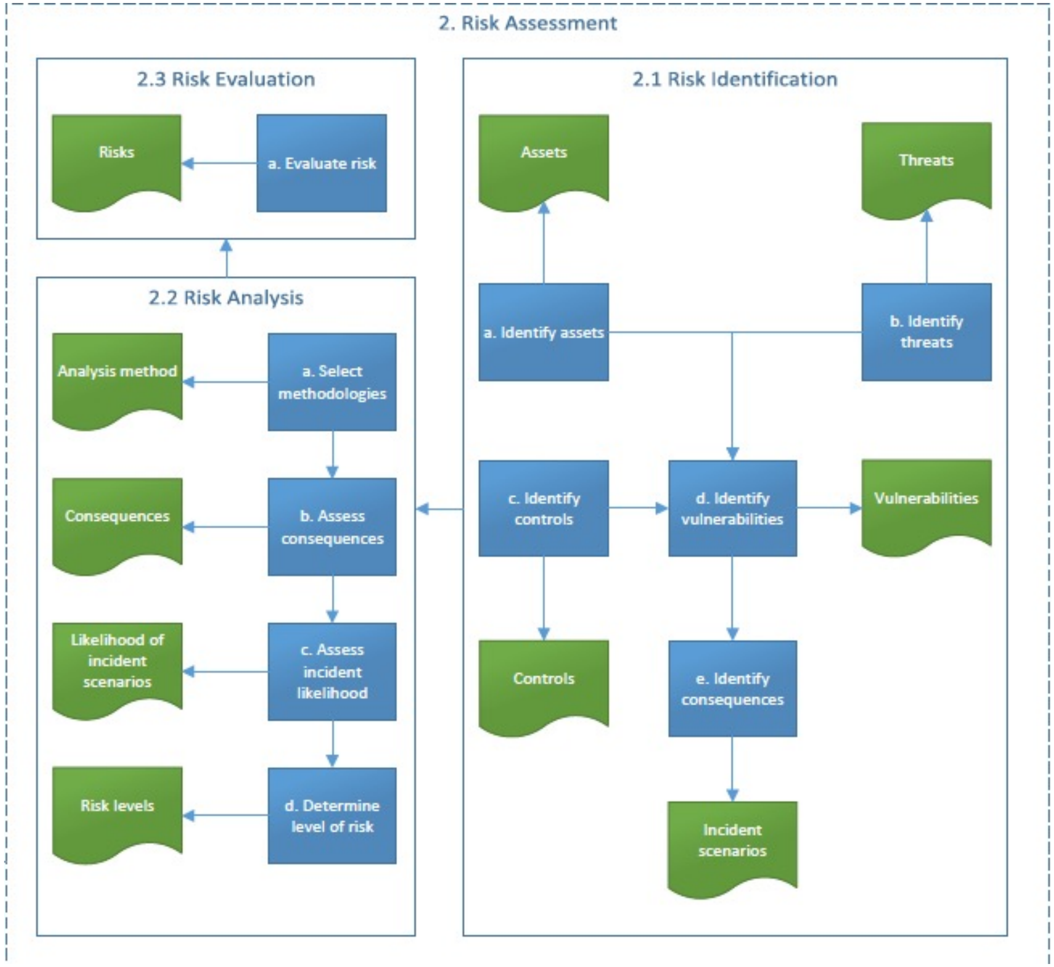


Table 6-13 Risk Assessment Deliverables

Deliverable	Purpose
Information asset and classification worksheet	Assembles information about information assets, their sensitivity levels, and their value to the organization
Information asset value weighted table analysis	Rank-orders each information asset according to criteria developed by the organization
Threat severity weighted table analysis	Rank-orders each threat to the organization's information assets according to criteria developed by the organization
TVA controls worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization, identifies potential vulnerabilities in the "triples," and incorporates extant and planned controls
Risk ranking worksheet	Assigns a risk-rating ranked value to each TVA triple, incorporating likelihood, impact, and possibly a measure of uncertainty

Risk Assessment

- ISO27005: Risk Management
  - 2. Risk Assessment



Next Week

- Lecture 9 – Risk Treatment
  - Chapter 7