THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Business Information Security

- Week 04: Risk Management - Part 1 (Ch. 5)
- Week 05: Risk Management - Part 2 (Ch. 5)

Dr Alex Pudmenzky

Semester 2, 2024

What is GRC?

In the realm of cybersecurity, **Governance, Risk Management, and Compliance (GRC)** serves as a fundamental framework. It guides organizations in implementing robust security measures by integrating critical elements:

Governance: This encompasses policies, rules, and frameworks that align with business goals. It defines responsibilities for key stakeholders, such as the board of directors and senior management. Good corporate governance includes ethics, accountability, transparent information sharing, conflict resolution policies, and resource management.

Risk Management: Businesses face various risks—financial, legal, strategic, and security-related. Proper risk management involves identifying these risks and finding ways to mitigate them. For instance, risk assessments help uncover security vulnerabilities in computer systems.

Compliance: Compliance involves adhering to rules, laws, and regulations. It applies to both external regulations set by industry bodies and internal corporate policies.

Why is GRC important? Implementing GRC programs allows businesses to make better decisions in a risk-aware environment. An effective GRC strategy helps stakeholders set policies, comply with regulations, and align the entire company around shared values and actions. Benefits include data-driven decision-making and responsible operations.

What is GRC?

In the realm of cybersecurity, **Governance, Risk Management, and Compliance (GRC)** serves as a fundamental framework. It guides organizations in implementing robust security measures by integrating critical elements:

Governance: This encompasses policies, rules, and frameworks that align with business goals. It defines responsibilities for key stakeholders, such as the board of directors and senior management. Good corporate governance includes ethics, accountability, transparent information sharing, conflict resolution policies, and resource management.

You are here!

Risk Management: Businesses face various risks—financial, legal, strategic, and security-related. Proper risk management involves identifying these risks and finding ways to mitigate them. For instance, risk assessments help uncover security vulnerabilities in computer systems.

Compliance: Compliance involves adhering to rules, laws, and regulations. It applies to both external regulations set by industry bodies and internal corporate policies.

Why is GRC important? Implementing GRC programs allows businesses to make better decisions in a risk-aware environment. An effective GRC strategy helps stakeholders set policies, comply with regulations, and align the entire company around shared values and actions. Benefits include data-driven decision-making and responsible operations.

Imagine your next professional interview, you have a business degree and the committee asks you:

“How would you approach risk management?”

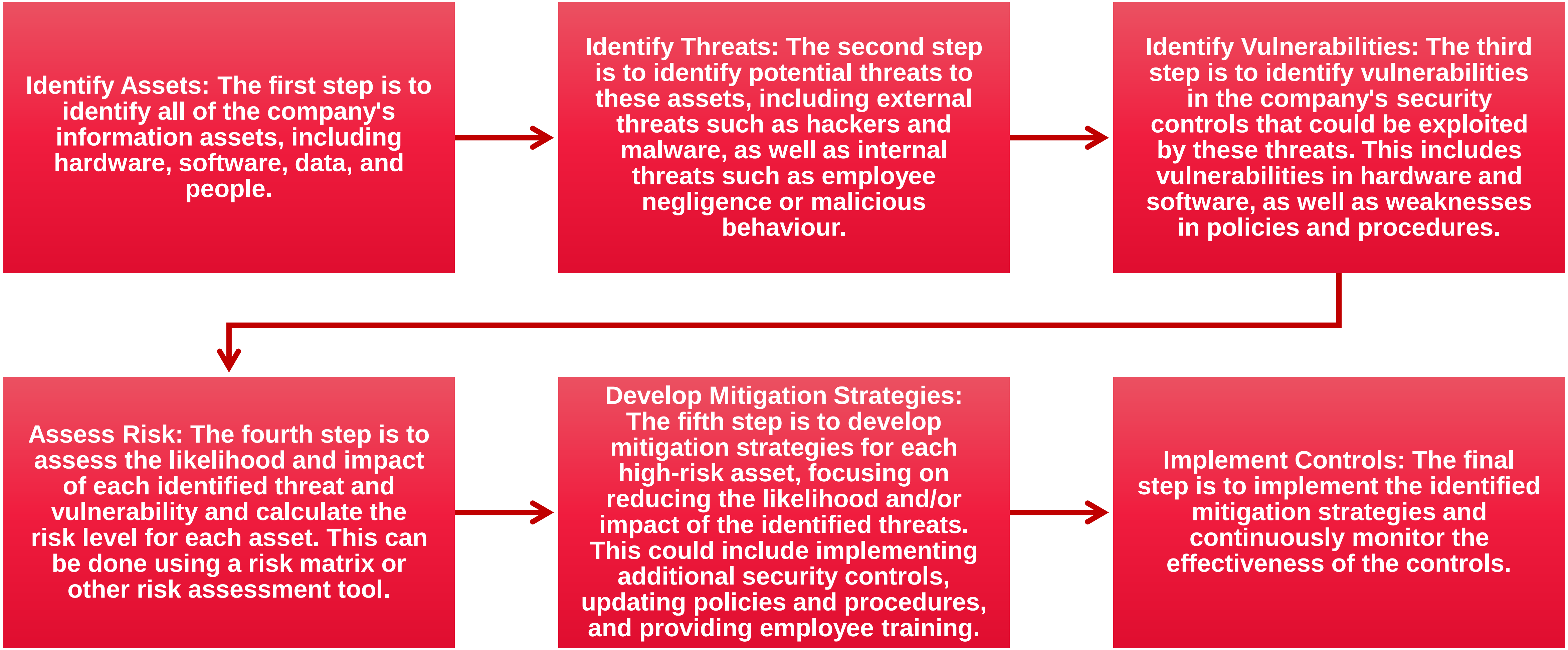
Introduction – Overview (1)

Organisations must design and create safe environments in which business processes and procedures can function.

Risk management: process of identifying and controlling risks facing an organisation – comprises three major undertakings:

1. **Risk identification**: process of examining an organisation's current IT security situation
2. **Risk assessment**: determining the extent to which the assets are exposed or at risk
3. **Risk control**: applying controls to reduce risks to an organisation's data and information systems

Cybersecurity risk assessment: Standard methodology



Identify Assets: The first step is to identify all of the company's information assets, including hardware, software, data, and people.

Identify Threats: The second step is to identify potential threats to these assets, including external threats such as hackers and malware, as well as internal threats such as employee negligence or malicious behaviour.

Identify Vulnerabilities: The third step is to identify vulnerabilities in the company's security controls that could be exploited by these threats. This includes vulnerabilities in hardware and software, as well as weaknesses in policies and procedures.

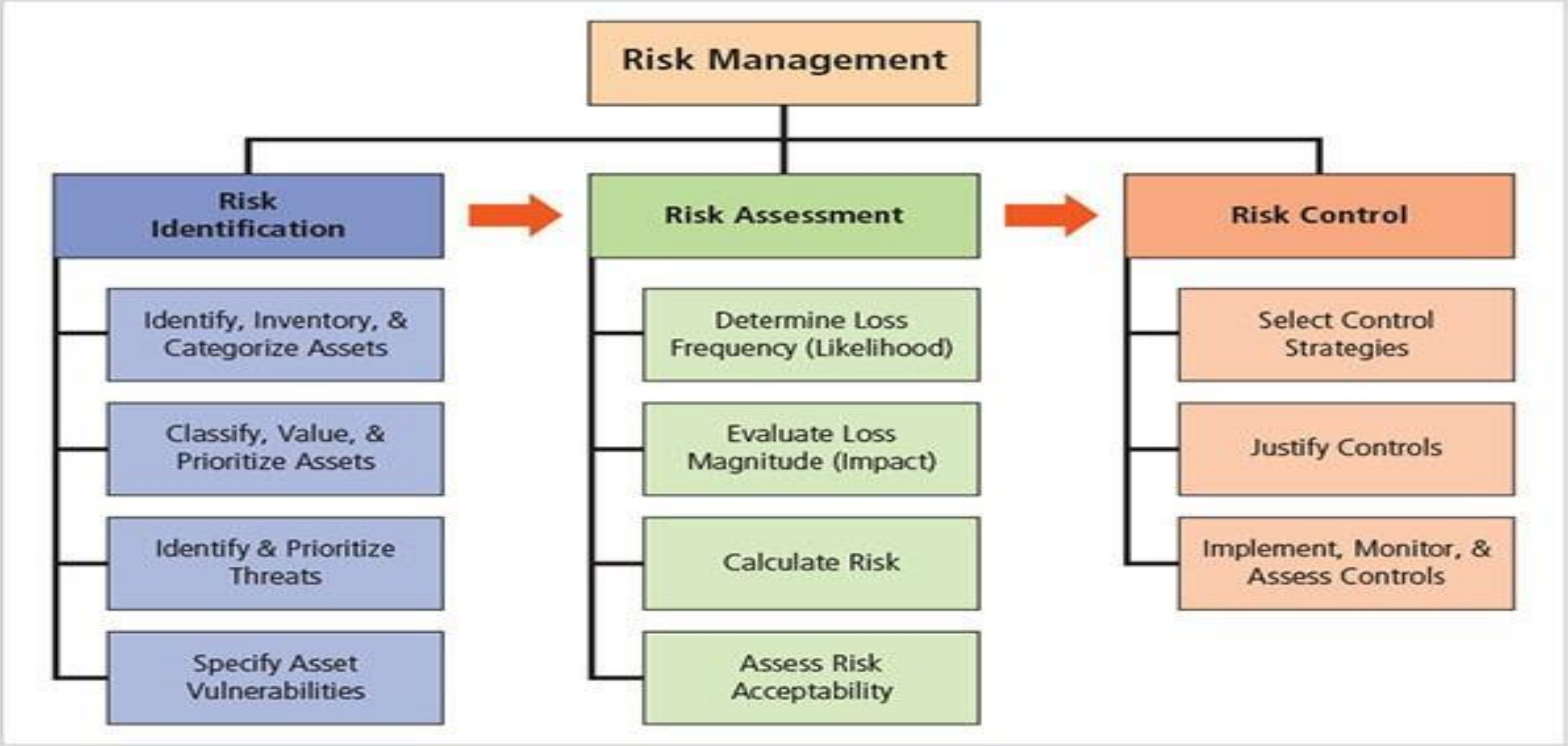
Assess Risk: The fourth step is to assess the likelihood and impact of each identified threat and vulnerability and calculate the risk level for each asset. This can be done using a risk matrix or other risk assessment tool.

Develop Mitigation Strategies: The fifth step is to develop mitigation strategies for each high-risk asset, focusing on reducing the likelihood and/or impact of the identified threats. This could include implementing additional security controls, updating policies and procedures, and providing employee training.

Implement Controls: The final step is to implement the identified mitigation strategies and continuously monitor the effectiveness of the controls.

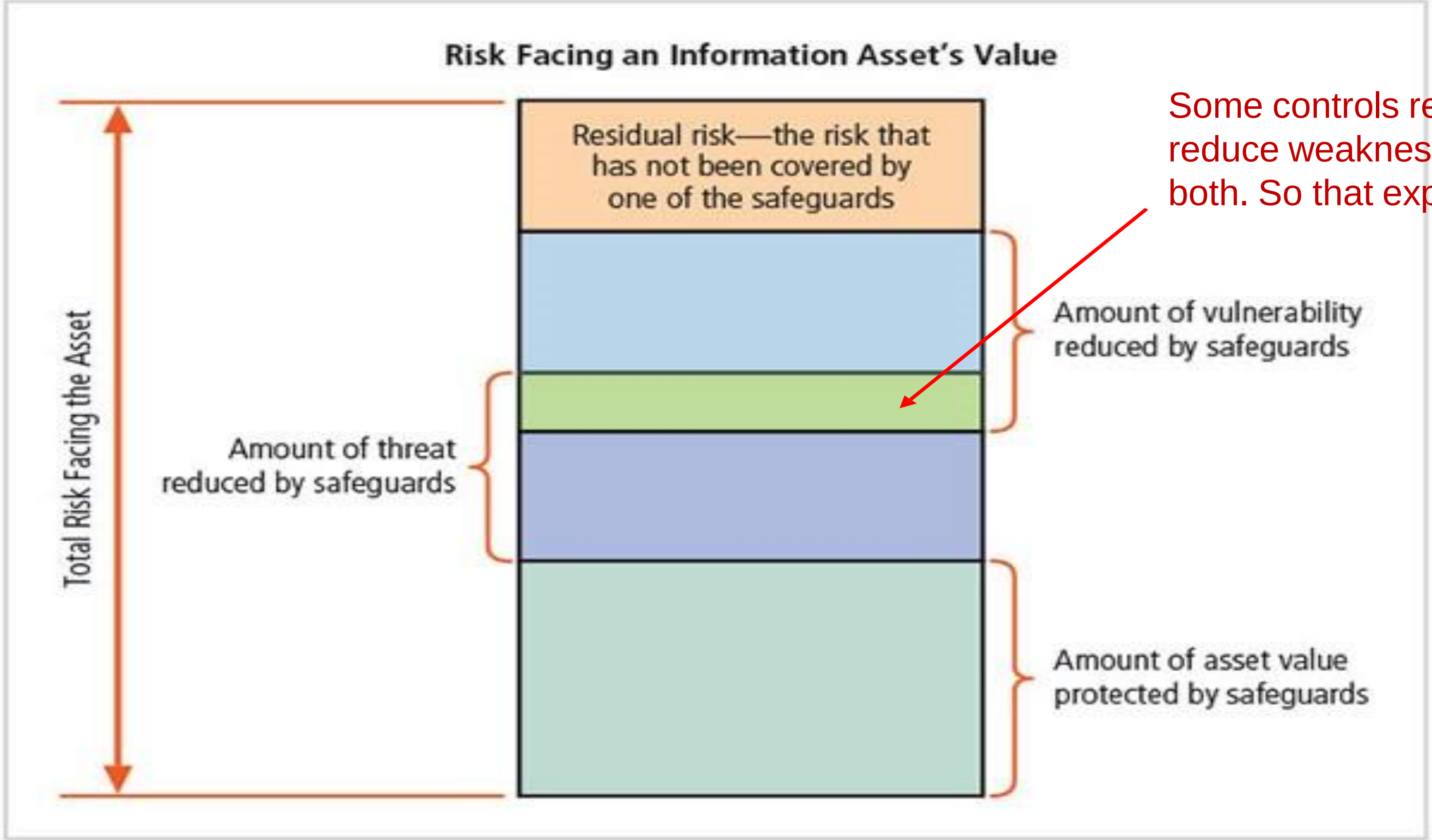
Introduction – Overview (2)

- **Know yourself**: identify, examine, and understand the information and systems currently in place
- **Know the ‘threats’**: identify, examine, and understand the threats facing the organisation
- Responsibility of each *community of interest* within an organisation to manage the risks that are encountered


Risk Management
Risk Identification
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Risk Assessment
Determine Loss Frequency (Likelihood)
Evaluate Loss Magnitude (Impact)
Calculate Risk
Assess Risk Acceptability
Risk Control
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

Risk management discussion point!

- Organisation **must define level of risk it can live with (most probably it will never be zero) – Why?**
- **Risk appetite** (aka *risk tolerance*): Defines quantity and nature of risk that organisations are willing to accept as trade-offs between perfect security and unlimited accessibility
- **Residual risk**: Risk that has not been completely removed, shifted, or planned for

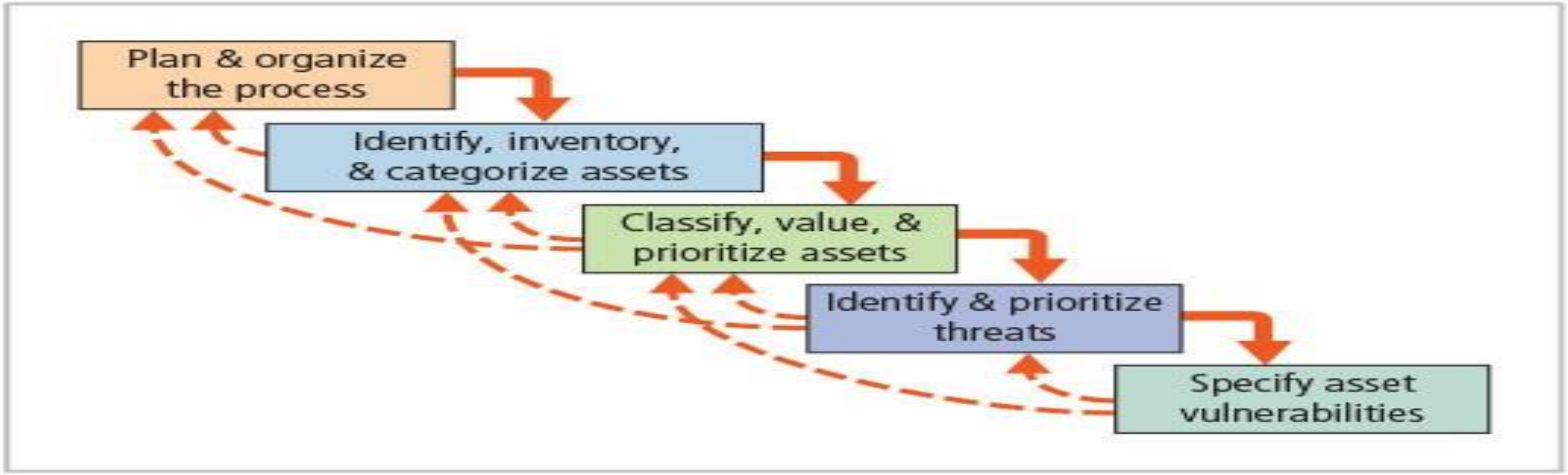

Risk Facing an Information Asset's Value
Total Risk Facing the Asset
Residual risk—the risk that has not been covered by one of the safeguards
Amount of vulnerability reduced by safeguards
Amount of threat reduced by safeguards
Amount of asset value protected by safeguards

Some controls reduce threats, some controls reduce weakness, and some controls do both. So that explains the overlap.

Risk identification (we now discuss the overall process)

- Risk management involves **identifying**, **classifying**, and **prioritising** an organisation's assets
- In risk management, the principle of **mutually exclusive** and **collectively exhaustive** (MECE) is often applied. This principle ensures that all possible risks are identified (collectively exhaustive) and that there is no overlap between the risks (mutually exclusive)
- A threat assessment process identifies and quantifies the risks facing each asset
- Components of risk identification
  - People
  - Procedures
  - Data
  - Software
  - Hardware

Risk identification – a "*project management*" approach


Plan & organize the process
Identify, inventory, & categorize assets
Classify, value, & prioritize assets
Identify & prioritize threats
Specify asset vulnerabilities

- First step in the Risk Identification process is to follow your project management principles
- Begin by **organising a team** with representation across all affected groups
- The process must then be **planned** out
  - Periodic deliverables
  - Reviews
  - Presentations to management

  } Project controls
- Tasks laid out, assignments made and timetables discussed
- Iterative process!

Asset identification and inventory

- Iterative process; begins with identification of assets, including all elements of an organisation's system
- Assets are then classified and categorized

	Traditional system components	Information asset components	Risk management system components
1	**People**	Internal personal	Trusted employees and other staff
		External personnel	People at trusted organisations strangers and visitors
	Procedures	Procedures	IT and business standard IT and business-sensitive procedures
	Data	Data/information	Transmission Processing Storage
2	**Software**	Software	Applications Operating system Security components
	Hardware	Hardware	Systems and peripherals Security devices
	Network	Networking components	Intranet components Internet or DMZ* components

*DMZ = Demilitarised zone

1. People, procedures, and data asset identification

- Human resources, documentation, and data information assets are more difficult to identify
- Important asset attributes:
  - People: position name/number/ID; supervisor; security clearance level; special skills
  - Procedures: description; intended purpose; what elements it is tied to; storage location for reference; storage location for update
  - Data: classification; owner/creator/ manager; data structure size; data structure used; online/offline; location; backup procedures employed

2. Hardware, software, and network asset identification

- What information attributes to track depends on:
  - Needs of organisation/risk management efforts
  - Preferences/needs of the security and information technology communities
- Asset attributes to be considered are: name; IP address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity
- Automated tools can identify system elements for hardware, software, and network components

Best Network Inventory Tools - Updated 2024 (Paid & Free) (comparitech.com)

SolarWinds Network Configuration Manager This tool automatically discovers every device on your network and creates an asset list that is constantly updated.

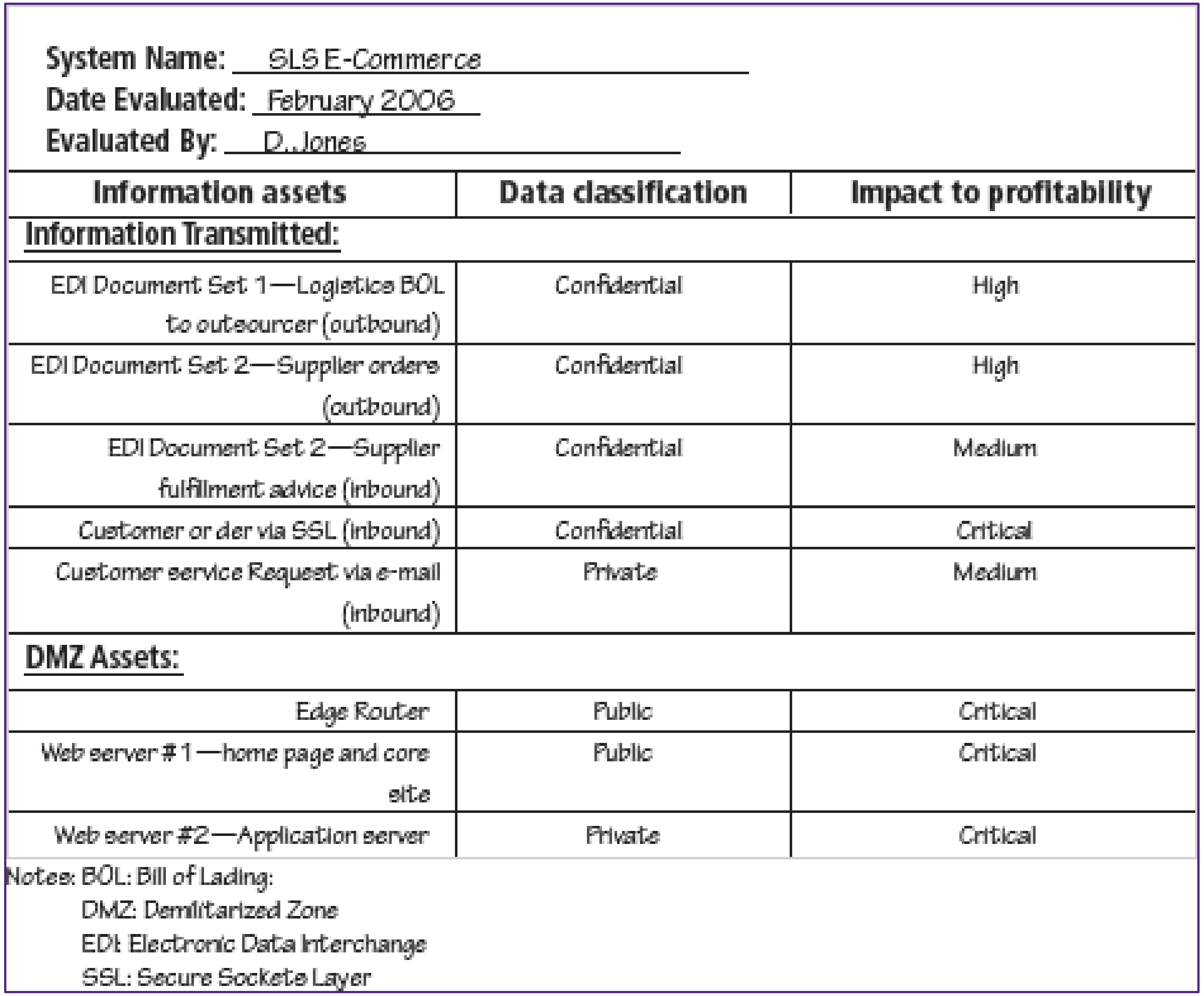
Information asset valuation

So we‘ve succeeded in identifying and we‘re confident we‘ve identified a comprehensive, mutually exlusive list of assets across the various functional areas. Now we have to **value** each of those assets.

Questions below (and others) help develop *criteria* for asset valuation

Which information asset:

- Is most *critical* to organisation’s success?
- Generates the most *revenue/profitability*?
- Would be most *expensive* to replace or protect?
- Would be the *most embarrassing* or cause greatest liability if revealed?



System Name: SLS E-Commerce
Date Evaluated: February 2006
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

Information asset valuation (cont'd)

Information asset **prioritisation** (most likely to have **multiple valuation criteria** – **why**? **Who makes these criteria?**)

- Create weighting for each category based on the answers to questions
- Calculate relative importance of each asset using weighted factor analysis
- List the assets in order of importance using a weighted factor analysis worksheet

The values that the project team, using senior management policy, have allocated to the asset.

Information Asset	Criterion 1: Impact to Revenue	Criterion 2: Impact to Profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100	***30***	***40***	***30***	***100***
EDI document set 1-logistics BOL 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 is: Identifying and prioritising threats

- Realistic threats need investigation; unimportant threats are set aside
- Threat assessment:
  - Which threats **present danger to assets**?
  - Which threats **represent the most danger to information**?
  - **How much would it cost to recover from attack**?
  - **Which threat requires greatest expenditure to prevent**?

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviation in quality of service from service provides	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 of failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of system or information
Software attacks	Malware: viruses, worms, macros, denial of services, or script injections

Then we need to analyse our vulnerabilities and prioritise them: **Vulnerability analysis**

- **Vulnerabilities**: specific avenues threat agents can exploit to attack an information asset.
- Examine how each threat could be perpetrated and list organisation’s assets and vulnerabilities.
- Process works best when people with diverse backgrounds within organisation work iteratively in a series of brainstorming sessions.
- How can we prioritise vulnerabilites?

Prioritising vulnerabilities (#1)

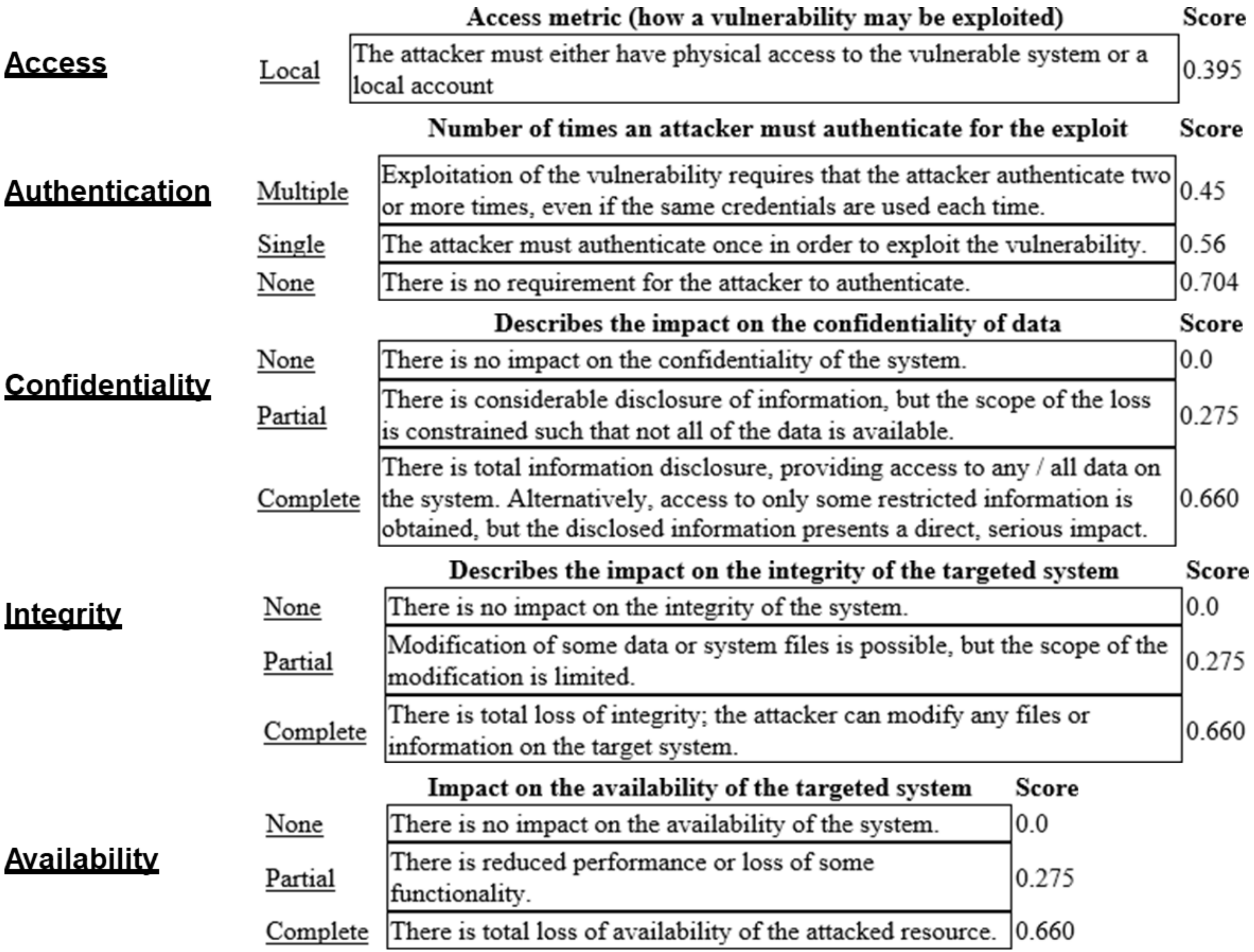
- The **Common Vulnerability Scoring System** (**CVSS**) is a free, open industry standard for assessing the severity of computer system security vulnerabilities.
- CVSS aims to assign severity scores to vulnerabilities, allowing flexibility for responders to prioritize responses and resources according to threat.
- Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit.
- Scores range from 0 to 10, with 10 being the most severe.
- Some of the metrics are described in overview below:

- The CVSS describes 6 base metrics: attack vector (how exploited), attack complexity (easy or difficult), authentication (the levels of authentication for the exploit), confidentiality (impact on confidentiality of data), integrity (of system), availability (of system).

- These six metrics are then used to produce a CVSS vector for the vulnerability.

CVSS v4.0: https://www.first.org/cvss/v4.0/specification-document

Identifying and prioritising threats (#2)



		Access metric (how a vulnerability may be exploited)	Score
Access	Local	The attacker must either have physical access to the vulnerable system or a local account	0.395

		Number of times an attacker must authenticate for the exploit	Score
Authentication	Multiple	Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.	0.45
	Single	The attacker must authenticate once in order to exploit the vulnerability.	0.56
	None	There is no requirement for the attacker to authenticate.	0.704

		Describes the impact on the confidentiality of data	Score
Confidentiality	None	There is no impact on the confidentiality of the system.	0.0
	Partial	There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.	0.275
	Complete	There is total information disclosure, providing access to any / all data on the system. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.	0.660

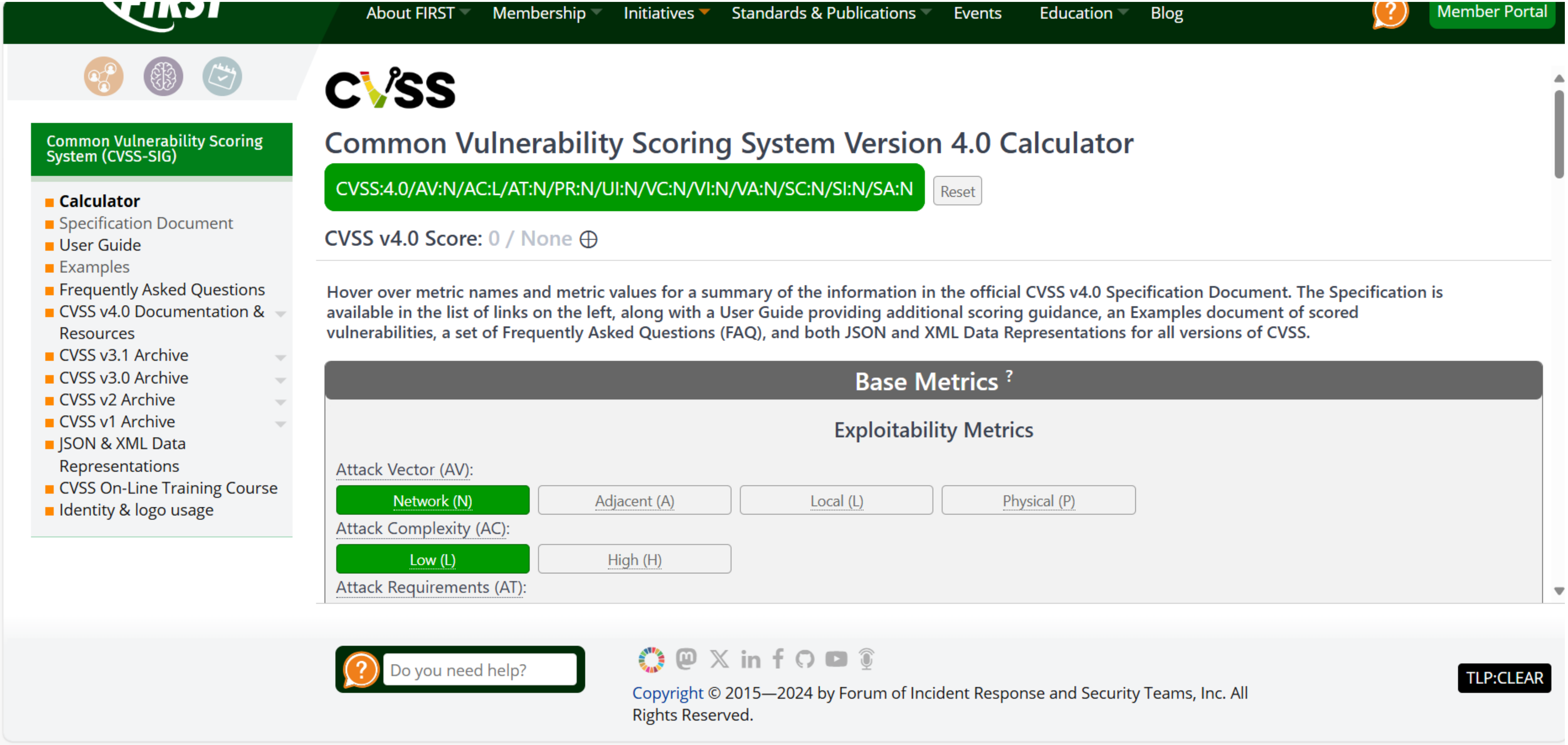
		Describes the impact on the integrity of the targeted system	Score
Integrity	None	There is no impact on the integrity of the system.	0.0
	Partial	Modification of some data or system files is possible, but the scope of the modification is limited.	0.275
	Complete	There is total loss of integrity; the attacker can modify any files or information on the target system.	0.660

		Impact on the availability of the targeted system	Score
Availability	None	There is no impact on the availability of the system.	0.0
	Partial	There is reduced performance or loss of some functionality.	0.275
	Complete	There is total loss of availability of the attacked resource.	0.660

Common Vulnerability Scoring System (CVSS) Website

https://www.first.org/cvss/

Common Vulnerability Scoring System Version 4.0 Calculator (first.org)



Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Score: 0 / None

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics ?

Exploitability Metrics

Attack Vector (AV): [✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Attack Requirements (AT):

Copyright © 2015—2024 by Forum of Incident Response and Security Teams, Inc. All Rights Reserved.

TVA worksheet (a simple summary)

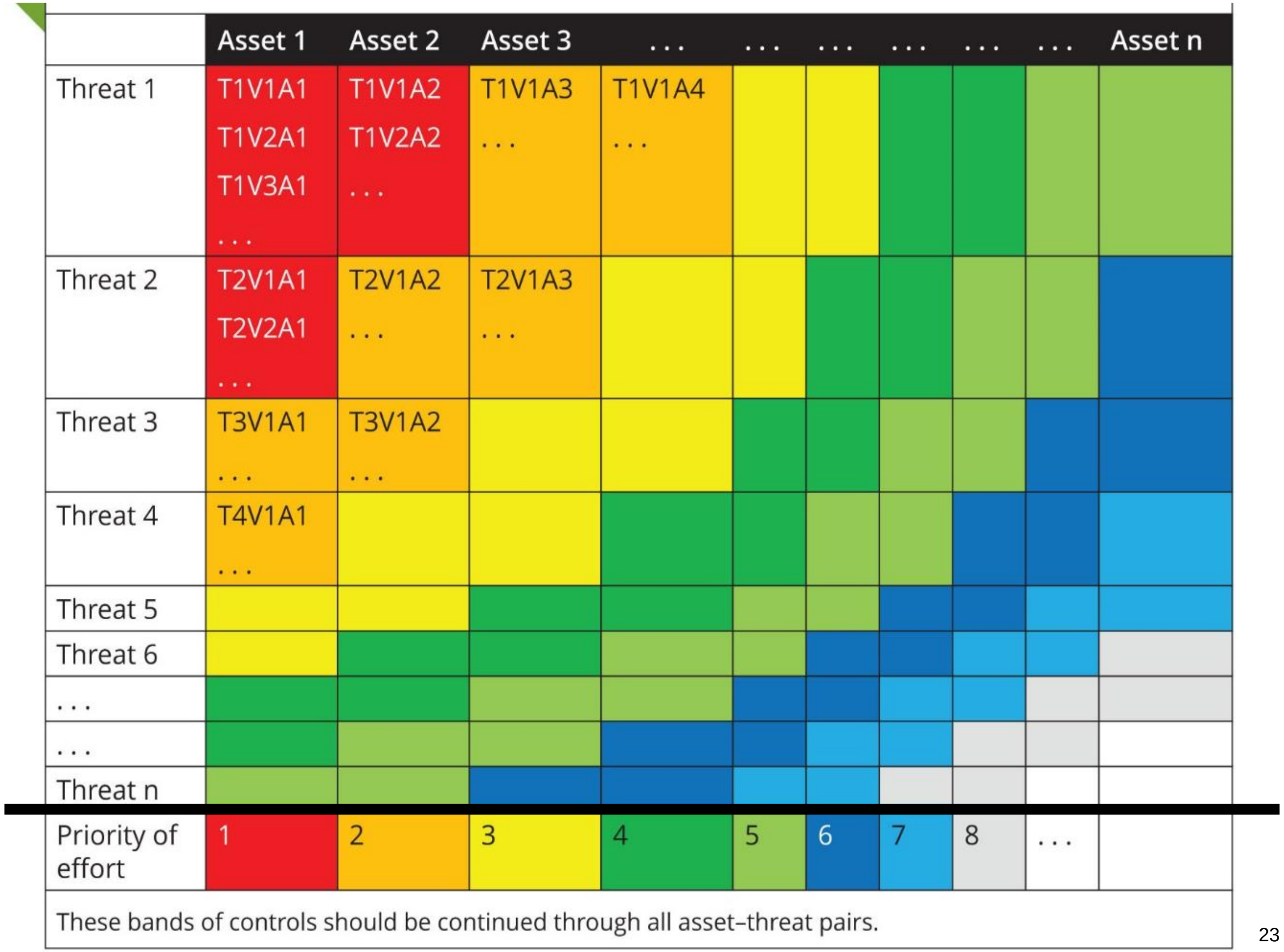
At end of risk identification process, there should be two lists:

- **list of assets** and **their vulnerabilities**.
- **List of threats** facing the organisation

Combination of these two lists into a Threats-Vulnerabilities-Assets (TVA) worksheet

Most important assets towards the left

Most important threats towards the top

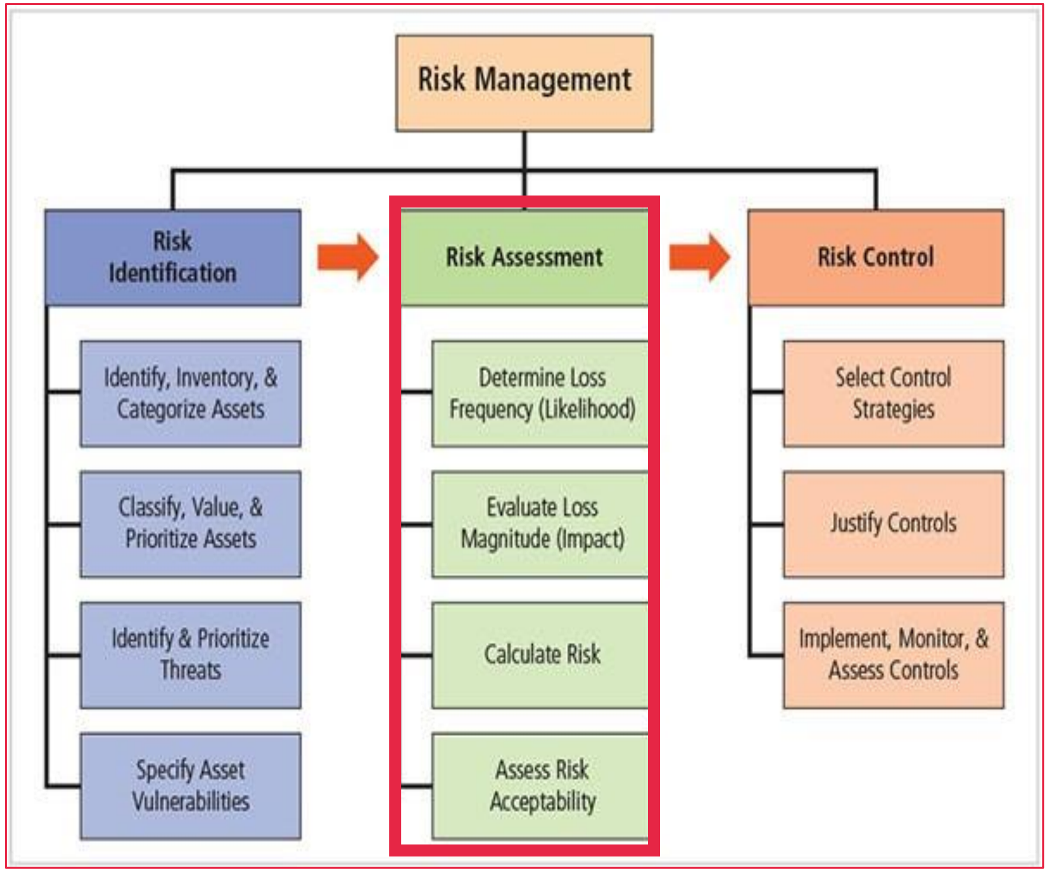


	Asset 1	Asset 2	Asset 3	. . .	. . .	. . .	. . .	. . .	. . .	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 . . .	T1V1A2 T1V2A2 . . .	T1V1A3 . . .	T1V1A4 . . .						
Threat 2	T2V1A1 T2V2A1 . . .	T2V1A2 . . .	T2V1A3 . . .							
Threat 3	T3V1A1 . . .	T3V1A2 . . .								
Threat 4	T4V1A1 . . .									
Threat 5										
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 assessment *evaluates the relative risk for each vulnerability*
- Assigns *a risk rating or score to each information asset*

  (a 'relative' meaning – not absolute)
- We must be CONSISTENT whichever approach we use!
- The goal at this point: create a method for evaluating the ***relative*** risk of each listed vulnerability
- We shall consider several approaches: (text book, NIST, one selected from industry)

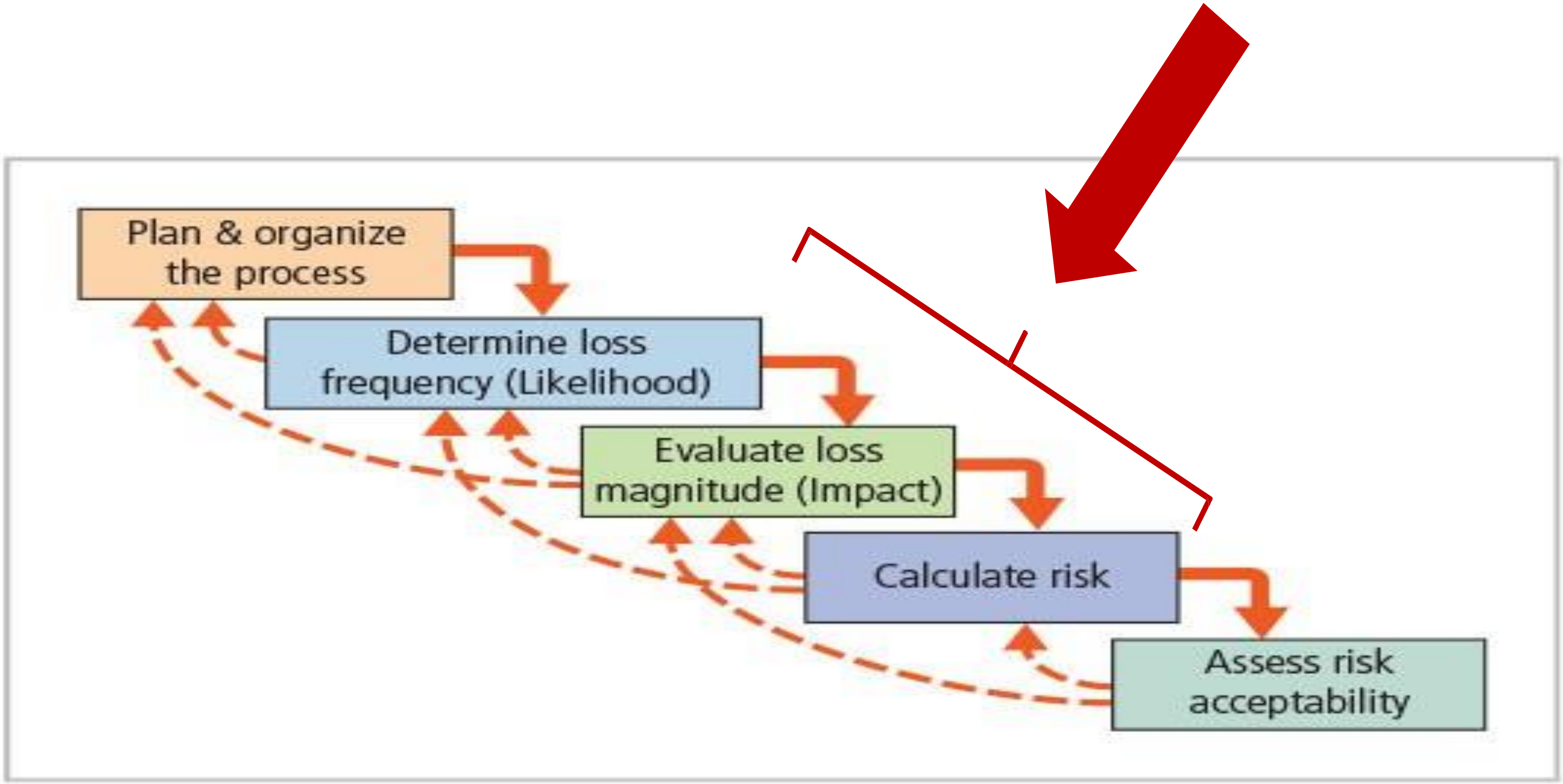

Risk Management
Risk Identification
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Risk Assessment
Determine Loss Frequency (Likelihood)
Evaluate Loss Magnitude (Impact)
Calculate Risk
Assess Risk Acceptability
Risk Control
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

NIST = National Institute of Science and Technology from the US

Risk calculation – a ‘project’ approach (flow, feedback, control)

For the purpose of a simplistic relative risk assessment:

Risk = *Loss frequency* * *loss magnitude* + an element of uncertainty (5-10%)


Plan & organize the process
Determine loss frequency (Likelihood)
Evaluate loss magnitude (Impact)
Calculate risk
Assess risk acceptability

Calculating risk (text book approach – page 283)

For the purpose of **relative risk assessment**: **Risk** is calculated as follows:

Step 1

The Probability of a Successful Attack on the Organisation

(Loss Frequency = ***Likelihood*** * ***Attack Success Probability***)

*** (MULTIPLIED BY)**

Step 2

The Expected Loss from a Successful Attack

(Loss Magnitude = ***Asset Value*** * ***Probable Loss)***

+ (PLUS)

Step 3

The **Uncertainty of estimates** of all stated values

Information asset valuation (cont'd)

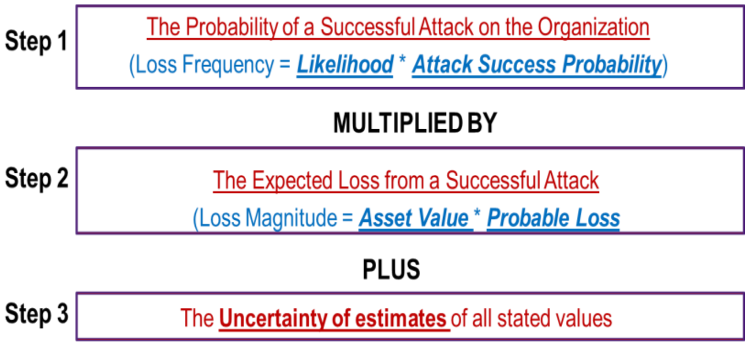
Information asset **prioritisation** (most likely to have **multiple valuation criteria – why**? **Who makes these criteria?**)

- Create weighting for each category based on the answers to questions
- Calculate relative importance of each asset using weighted factor analysis
- List the assets in order of importance using a weighted factor analysis worksheet

The values that the project team, using senior management policy, have allocated to the asset.

Information Asset	Criterion 1: Impact to Revenue	Criterion 2: Impact to Profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100	***30***	***40***	***30***	***100***
EDI document set 1-logistics BOL 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

Step 1: Loss frequency



Step 1 The Probability of a Successful Attack on the Organization
(Loss Frequency = Likelihood * Attack Success Probability)

MULTIPLIED BY

Step 2 The Expected Loss from a Successful Attack
(Loss Magnitude = Asset Value * Probable Loss

PLUS

Step 3 The Uncertainty of estimates of all stated values

First, we need to determine how probable it is that an attack is successful.

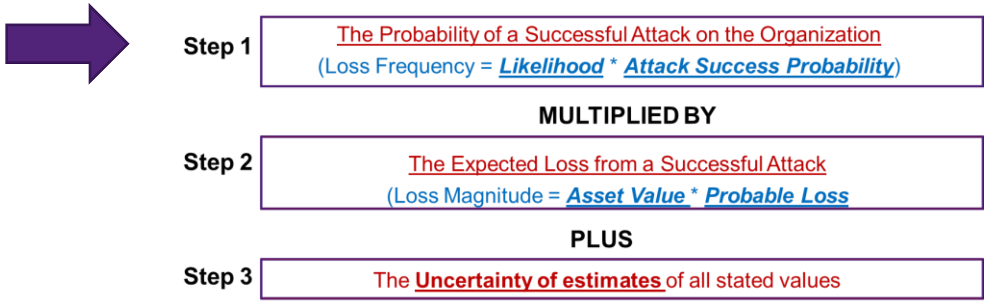
Loss frequency describes an assessment of the likelihood of an attack combined with expected probability of success given the current level of controls in place

- Likelihood: Use *external references* for values that have been reviewed/adjusted for your circumstances AND '*risk actuals*' of your organisation; value subject to uncertainty
  - Assign numeric **value to likelihood, typically annual value**
  - Targeted by hackers once every five years – annualized likelihood of attack: 1/5, 20 percent
  - Web defacement two times each year – annualized likelihood of attack 200 percent

  - ***See next slide also***

- **Success probability:** Estimate a quantitative value (e.g., 10 percent) for the likelihood of a successful attack; value subject to uncertainty. This also involves consideration of the current level of protection – this further complicates the calculation.

Likelihood (part of step 1)



Step 1 The Probability of a Successful Attack on the Organization
(Loss Frequency = ***Likelihood*** * ***Attack Success Probability***)

MULTIPLIED BY

Step 2 The Expected Loss from a Successful Attack
(Loss Magnitude = ***Asset Value*** * ***Probable Loss***

PLUS

Step 3 The **Uncertainty of estimates** of all stated values

- The probability that a specific vulnerability will be the object of a successful attack

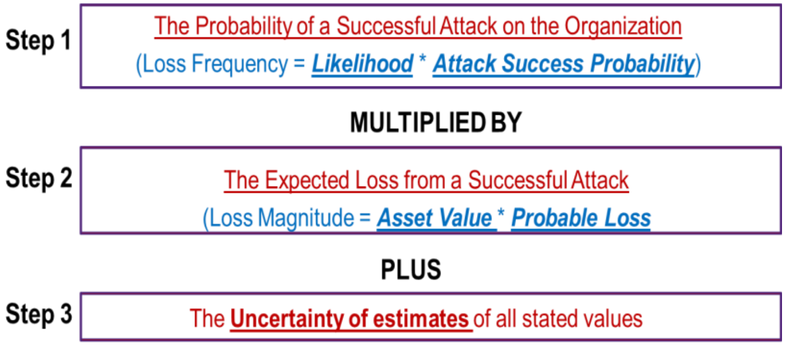
- *NIST SP 800-30*: Assign numeric value: number between 0.1 (low) and 1.0 (high), or a number between 1 and 100
  - *Zero not used since vulnerabilities with zero likelihood are removed from asset/vulnerability list*

- Use selected rating model (whichever is selected) **consistently**

- Use external references for values that have been reviewed/adjusted for your circumstances – remember our reference to ‘risk actuals’

NIST SP = National Institute of Standards and Technology , SP = Special Publications (on Blackboard)

Step 2: Loss magnitude



Step 1: The Probability of a Successful Attack on the Organization
(Loss Frequency = ***Likelihood*** * ***Attack Success Probability***)

MULTIPLIED BY

Step 2: The Expected Loss from a Successful Attack
(Loss Magnitude = ***Asset Value*** * ***Probable Loss***)

PLUS

Step 3: The **Uncertainty of estimates** of all stated values

We need to determine how much of an information asset could be lost in a successful attack

Loss magnitude (sometimes asset exposure)

Combines two components: (1) the value of information asset with (2) the percentage of asset lost in the event of a successful attack

Difficulties involve:

- *Valuing* an information asset (e.g. a database server for sales transactions from customers and one for employee salary)
- *Estimating* the percentage of information asset lost during best-case, worst-case, and most likely scenarios

Clearly this step is also subject to possible error/uncertainty

Set text: page 286

Example (1) – text book (page 287)

Information asset A is on online e-commerce database. 10% chance of attack this year (1 attack every 10 years). 50% chance of success based on current asset vulnerabilities and protection mechanisms. Asset value is 50 (*how is this derived*) and 100% of the asset would be compromised by a successful attack. Assumption: data 90% accurate.

$$\text{Total Risk is: } \overbrace{(10\% * 50\%) * (\ \underline{50} * 100\%)}^{\text{risk calculation}} + \overbrace{10\% \text{ of risk calculation}}$$

Asset A Total Risk is: 2.5 + 0.25 = **2.75**

RISK is

The Probability of a Successful Attack on the organisation

(Loss [event] Frequency = *Likelihood * Attack Success Probability*)

Multiplied by

The Expected Loss from a Successful Attack

([Event] Loss Magnitude = *Asset Value * Probable Loss)*

Plus

The Uncertainty of estimates of all stated values

Example (2) – text book (page 287)

Information asset B is an internal personnel database behind a firewall. 1% chance of attack this year. 10% chance of success based on current asset vulnerabilities and protection mechanisms. Asset value is 25 on a scale of 1 to 100 and 50% of the asset would be compromised by a successful attack. Assumption: data 90% accurate.

Risk is: (1% * 10%) * (25 * 50%) + 10% of risk calculation

Asset B risk is: 0.01375

Which has the higher level of risk – what would you do?

RISK is
The Probability of a Successful Attack on the Organisation
(Loss [event] Frequency = *Likelihood * Attack Success Probability*)
Multiplied by
The Expected Loss from a Successful Attack
([Event] Loss Magnitude = *Asset Value * Probable Loss=*
Plus
The Uncertainty of estimates of all stated values

Risk assessment (2) - NIST

- NIST SP (Special Publication) 800-30 r1 (on Blackboard)
- Definitive document for RISK ASSESSMENT
- **RISK = LIKELIHOOD * LEVEL OF IMPACT** (appendix I)

- SP800-30 contains qualitative and quantitative strategies
- SP800-30 is on Blackboard (week 4 material)

- **How can risk be ‘so simply’ described** (in contrast with the text book)?

Risk assessment (3) – another approach

- For the purpose of **relative risk assessment**:
  - Risk EQUALS
  - Likelihood of vulnerability occurrence
  - TIMES value (or impact)
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Formula (3):
(*Risk = likelihood * asset_value - % controlled + % uncertain*)

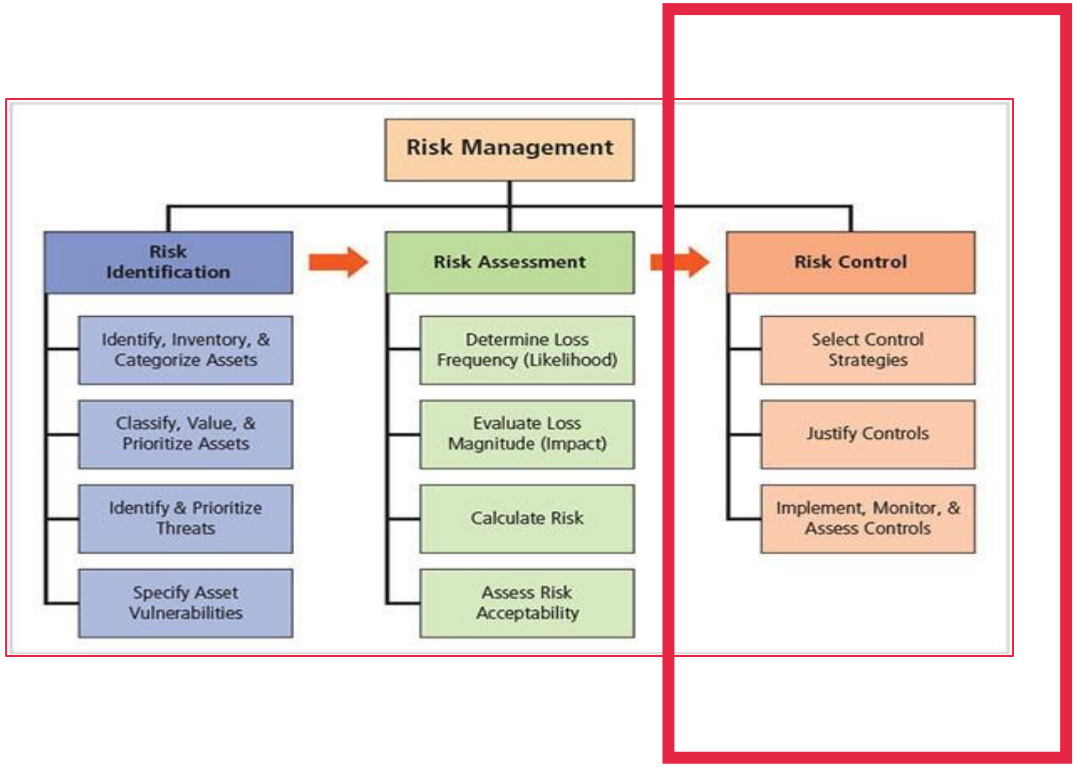
Other approaches are described in the text book (p. 290+). We shall not consider them (or examine them) – but be aware that variations exist.

Vulnerability Discovery and Recording (separate doc)…

More on risk assessment documentation next week…

Identify possible controls

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas
- Residual risk is risk that remains to information asset even after existing control has been applied
- There are three general categories of controls:
  - Policies
  - Programs (training, education, security awareness)
  - Technologies (authentication, PW, 2FA)


Risk Management
Risk Identification
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Risk Assessment
Determine Loss Frequency (Likelihood)
Evaluate Loss Magnitude (Impact)
Calculate Risk
Assess Risk Acceptability
Risk Control
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

Documenting the results of the risk assessment

- Final summary comprised in **ranked vulnerability risk worksheet**
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor.

Asset	Asset relative value	Vulnerability	Loss frequency	Loss magnitude
Customer service request via email (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order secured (inbound)	100	Lost orders due to web server hardware failure	0.1	10
Customer order via secured (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 order via secured (inbound)	100	Lost orders due to web server denial-of-service attack	0.025	2.5
Customer order via secured (inbound)	100	Lost orders due to web server software failure	0.01	1

- What is the relative risk of an E-Mail disruption due to hardware failure of a ‘Customer service request (email)’?
- Explain the asset values.

Risk control strategies (5 of these)

Once ranked vulnerability risk worksheet complete, must choose one of five strategies to control each risk:

1. Defend

- Attempts to prevent exploitation of the vulnerability
- Preferred approach
- Accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods:
  - **Application of policy**
  - **Training and education**
  - **Applying technology**

Risk control strategies (cont’d)

2. Transfer

- Control approach that attempts to shift risk to other assets, processes, or organisations
- If lacking, organisation should hire individuals/firms that provide security management and administration expertise
- Organisation may then transfer risk associated with management of complex systems to another organisation experienced in dealing with those risks

3. Mitigate

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans
  - Incident response plan (IRP): define the actions to take while incident is in progress
  - Disaster recovery plan (DRP): most common mitigation procedure
  - Business continuity plan (BCP): encompasses continuation of business activities if catastrophic event occurs

Risk control strategies (cont'd)

4. Accept

- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection

5. Terminate

- Directs the organisation to avoid those business activities that introduce uncontrollable risks
- May seek an alternate mechanism to meet customer needs

Summary of risk control strategies (cont’d)

Risk control strategy	Categories used by NIST SP 800-30, Rev. 1	Categories used by ISACA and ISO/IEC 27001	Others
Defense	Research and acknowledgement	Treat	Self-protection
Transference	Risk transference	Transfer	Risk transfer
Mitigation	Risk limitation and risk planning	Tolerate (partial)	Self-insurance (partial)
Acceptance	Risk assumption	Tolerate (partial)	Self-insurance (partial)
Termination	Risk avoidance	Terminate	Avoidance

Selecting a risk control strategy

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb on strategy selection can be applied:
  - When a vulnerability exists
  - When a vulnerability can be exploited
  - *When attacker’s cost is less than potential gain*
  - When potential loss is substantial

Justifying controls

- Before implementing one of the control strategies for a specific vulnerability, the organisation must explore all consequences of vulnerability to information asset.
- There are several ways to determine the advantages/disadvantages of a specific control:

Cost Benefit Analysis (1 of 3)

- **Sums the benefits of an action THEN subtracts the costs of that action**
- Formal process to document this is called cost benefit analysis or economic feasibility study
- Items that affect cost of a control or safeguard include: cost of development or acquisition; training fees; implementation cost; service costs; cost of maintenance
- Benefit: value an organisation realises using controls to prevent losses from a vulnerability
- Asset valuation: process of assigning financial value or worth to each information asset

- Once asset valuation is performed, an organisation can begin to estimate the potential loss that could occur from an exploited vulnerability or threat occurrence.

Cost Benefit Analysis (2 of 3)

Several questions must be asked:

- What damage would occur from an exploited vulnerability or threat occurrence
- What would it cost to recover from the attack – as well as the financial damage
- What is the **single loss expectancy (SLE)** for each risk?
  - **SLE = asset value × exposure factor (EF)**
  - Example: if a Web site has an estimated value of $1 million, and a hacker defacement could damage 10% of the Web site, the SLE is $1 million * 0.10.

Once asset valuation is completed, we can calculate how much loss is expected from a single attack and how often these attacks occur. We can use the annualized loss expectancy (ALE) for this:

ALE = single loss expectancy (SLE) × annualized rate of occurrence (ARO)

In our previous Web site example, the ARO could be **0.50** (how often is this?). This gives us ALE = $100,000 * 0.50 = $50,000

Consequently, this business can expect to lose $50,000 every year – this gives us a basis for expenditure

Cost Benefit Analysis (3 of 3)

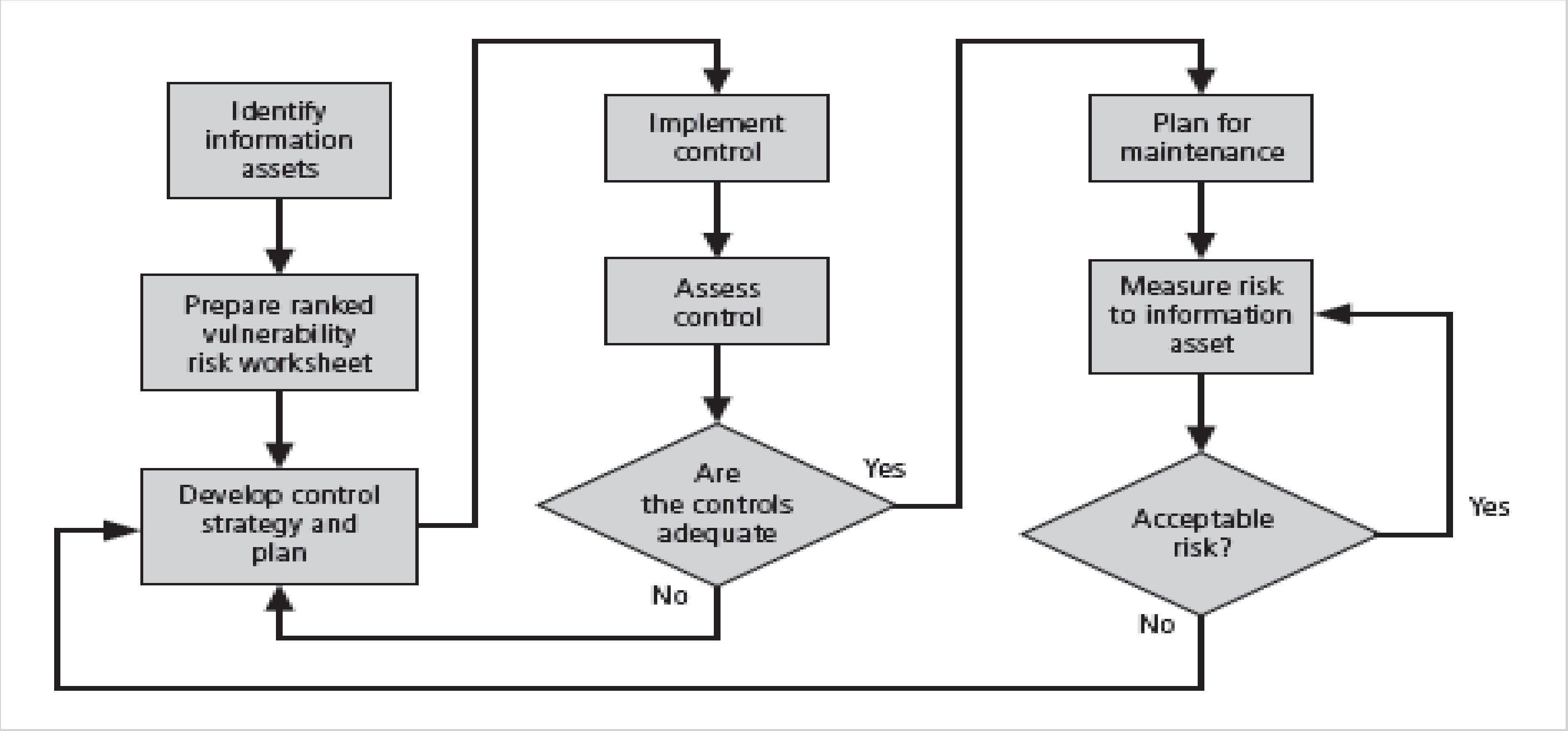
- CBA determines if alternative being evaluated is worth cost incurred to control vulnerability
  - CBA most easily calculated using Annualized Loss Expectancy (ALE) from earlier assessments, before implementation of proposed control:

CBA = ALE(prior) – ALE(post) – ACS

- ALE(prior) is annualized loss expectancy of risk before implementation of control
- ALE(post) is estimated ALE based on control being in place for a period of time
- ACS is the annualized cost of the safeguard

Evaluation, assessment, and maintenance of risk controls

- Selection and implementation of control strategy is not end of process
- Strategy and accompanying controls must be monitored/reevaluated on ongoing basis to determine effectiveness and to calculate more accurately the estimated residual risk
- **Process continues as long as organisation continues to function**


Identify information assets
Prepare ranked vulnerability risk worksheet
Develop control strategy and plan
Implement control
Assess control
Are the controls adequate
Yes
No
Plan for maintenance
Measure risk to information asset
Acceptable risk?
Yes
No

Qualitative versus quantitative risk control practices

- Performing the previous steps using actual values or estimates is known as quantitative assessment

- Possible to complete steps using evaluation process based on characteristics using non-numerical measures; called qualitative assessment (low, medium, high, very high)

- Utilizing scales rather than specific estimates relieves organisation from difficulty of determining exact values

Qualitative versus *quantitative*: *NIST SP 800-30*

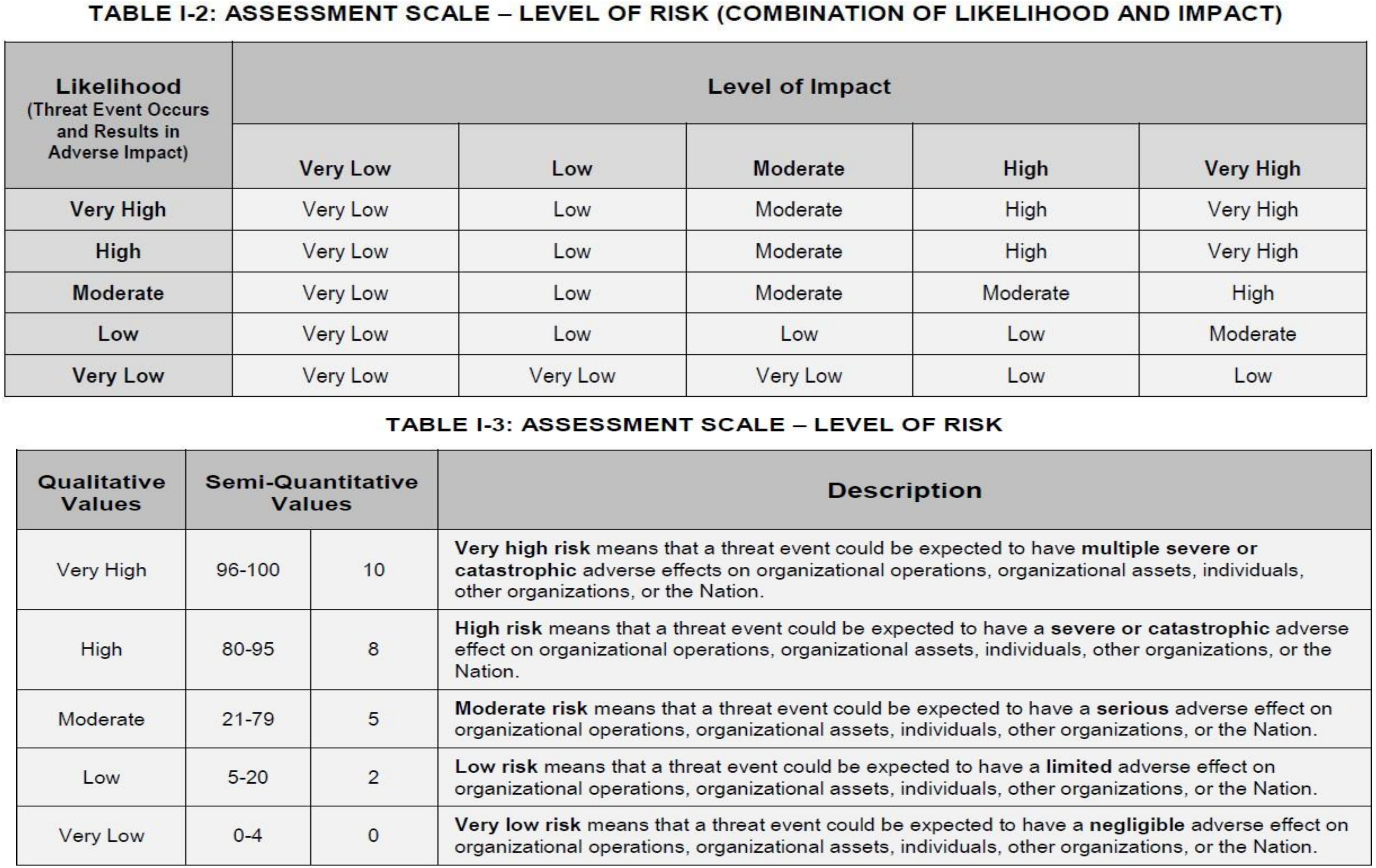


TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

PAGE I-1

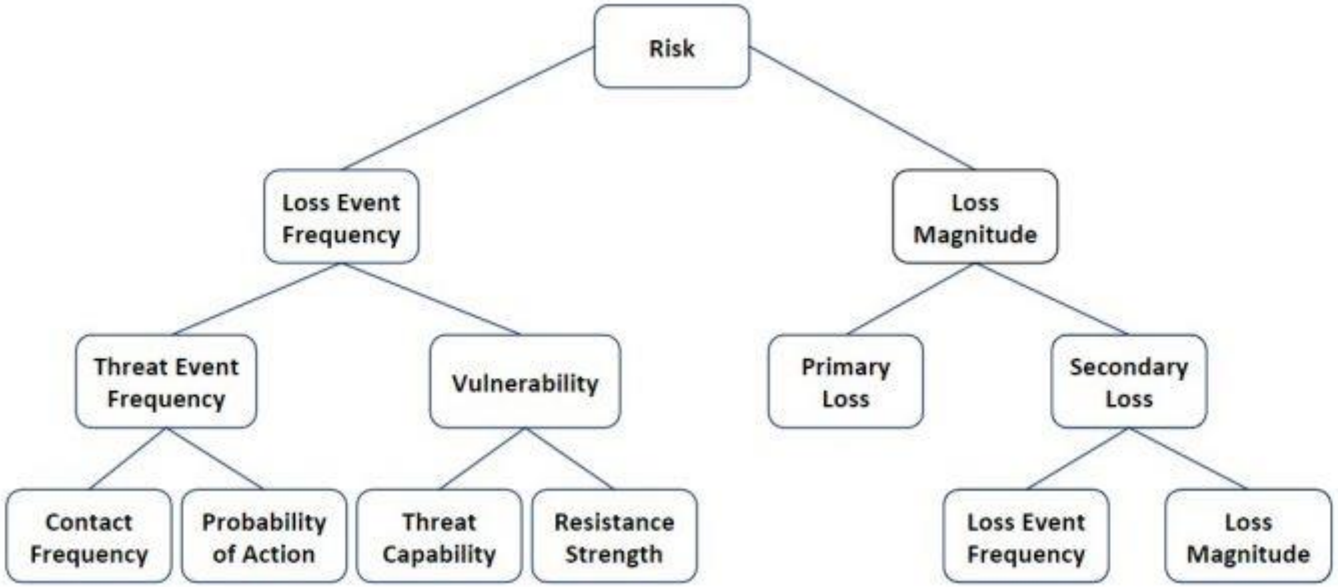
and

PAGE I-2

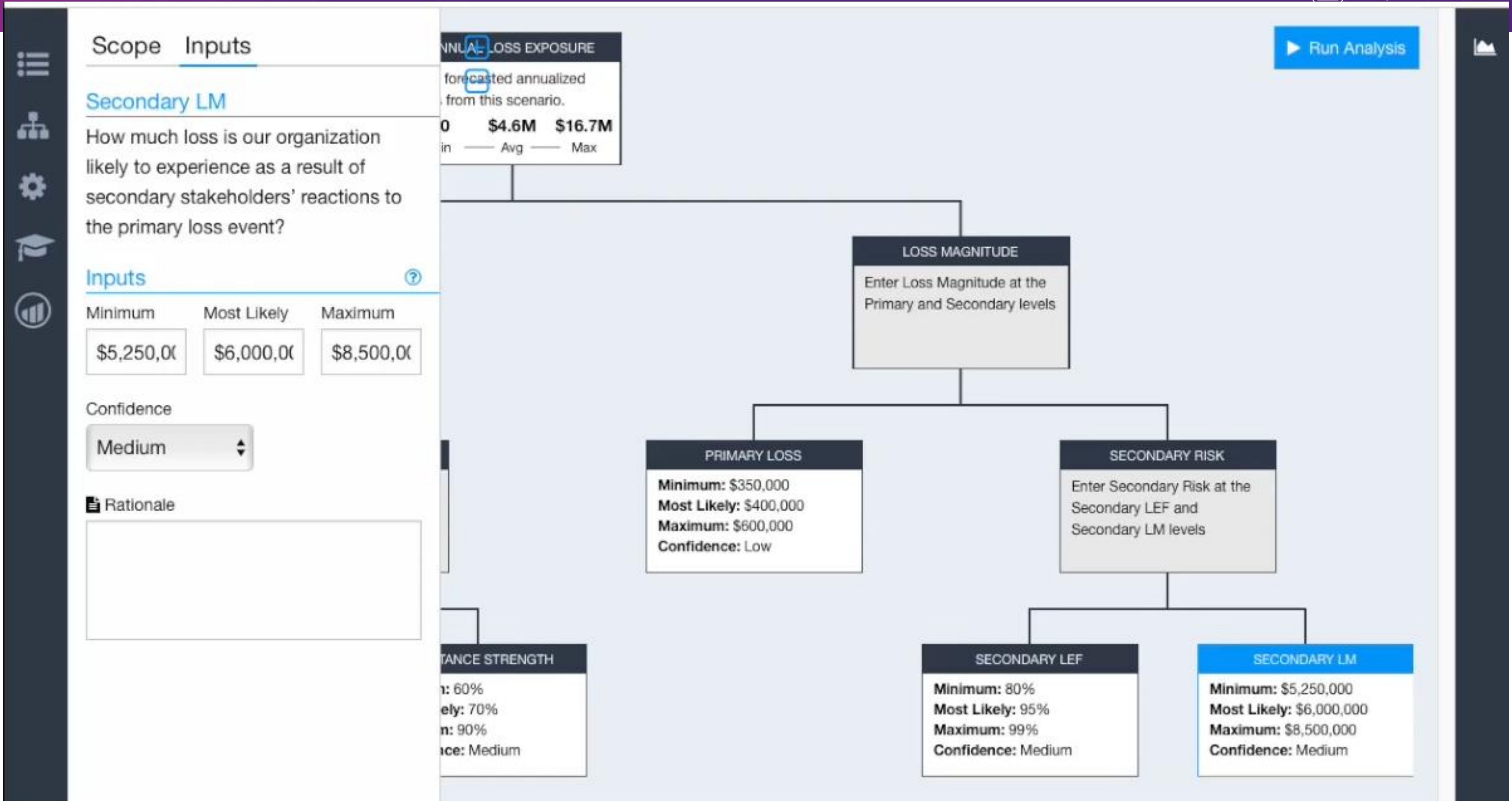
in Supplementary Material.

Quantitative methods: Example

FAIR (Factor Analysis of Information Risks) (www.fairinstitute.org)



It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of data loss events.



Secondary LM

How much loss is our organization likely to experience as a result of secondary stakeholders' reactions to the primary loss event?

Inputs

Minimum	Most Likely	Maximum
$5,250,0(	$6,000,0(	$8,500,0(

Confidence: Medium

Rationale

NNUAL LOSS EXPOSURE

forecasted annualized
from this scenario.

0	$4.6M	$16.7M
in	Avg	Max

LOSS MAGNITUDE

Enter Loss Magnitude at the Primary and Secondary levels

PRIMARY LOSS

Minimum: $350,000
Most Likely: $400,000
Maximum: $600,000
Confidence: Low

SECONDARY RISK

Enter Secondary Risk at the Secondary LEF and Secondary LM levels

TANCE STRENGTH

n: 60%
ely: 70%
n: 90%
nce: Medium

SECONDARY LEF

Minimum: 80%
Most Likely: 95%
Maximum: 99%
Confidence: Medium

SECONDARY LM

Minimum: $5,250,000
Most Likely: $6,000,000
Maximum: $8,500,000
Confidence: Medium

Product Demo Video: https://risklens.wistia.com/medias/ic0ph1zqdw

Summary (1)

- Risk identification: formal process of examining/documenting risk in information systems.
  - A risk management strategy enables identification, classification, and prioritisation of organisation's information assets
  - Residual risk: risk remaining to the information asset even after the existing control is applied

- Risk control: process of taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of components of an information system
- Five strategies are used to control risks that result from vulnerabilities:
  - Defend
  - Transfer
  - Mitigate
  - Accept
  - Terminate

Summary (2)

- Selecting a risk control strategy
  - Cost Benefit Analysis
  - Feasibility Study
- Qualitative versus Quantitative Risk Control
  - Best Practices and Benchmarks
- Risk Appetite: organisational risk tolerance
- Residual risk: risk remaining after application of risk controls
- Risk actuals: we can consider this the business memory of security process
- Convince budget authorities to spend up to value of asset to protect from identified threat
- Final control choice may be balance of controls providing greatest value to as many asset-threat pairs as possible

The University of Queensland Australia | CREATE CHANGE

Supplemental Material

An overview of threat and risk assessment – As per SANS Institute (www.sans.org)

An overview of threat and risk assessment (1) – As per SANS Institute (www.sans.org)

- Many different methodologies – all try to answer:
  a) What needs to be protected?
  b) Who/what are the threats and vulnerabilities?
  c) What are the implications if they were damaged or lost?
  d) What is the value to the organisation?
  e) What can be done to minimize exposure to the loss or damage

- Outcome: to provide recommendations that maximize the protection of (fundamentally) confidentiality, integrity and availability whilst still providing functionality and usability.

- By whom: internal or external resources (not having a vested interest in the organisation and be free from personal and external constraints which may impair independence.

An overview of threat and risk assessment (2) – As per SANS Institute (www.sans.org)

- **Core areas**:

  a) Scope

  b) Data collection

  c) Analysis of policies and procedures

  d) Threat analysis

  e) Vulnerability analysis

  f) Correlation and assessment of risk acceptability

An overview of threat and risk assessment (3) – As per SANS Institute (www.sans.org)

Scope

- Identifying the scope is one of the most important step in the process. The scope provides the analyst with what is covered and what is not covered in the assessment.
- Scope identifies what needs to be protected, the sensitivity of what is being protected and to what level and detail.
- The scope will also identify what systems and applications are included in the assessment.
- The analyst must keep in mind the intended audience of the final recommendations (i.e. senior management, IT department or certifying authority).
- Finally, the scope should indicate the perspective from which the analysis will take place, whether it is from an internal or external perspective or both. The level of detail is directly related to the intended recipient of the final analysis.

An overview of threat and risk assessment (4) – As per SANS Institute (www.sans.org)

Collecting data

- We must collect all policies and procedures currently in place and identifying those that are missing or undocumented.
- Interviews with key personnel can be conducted using questionnaires or surveys to assist in identifying assets and missing or out-of-date documentation.
- The systems or applications identified in the scope are enumerated and all relevant information gathered on the current state of those systems.

Service pack levels	Port scanning
Services running	Wireless leakage
Operating system type	Intrusion detection testing
Network applications running	Phone systems testing
Physical location of the systems	Firewall testing
Access control permissions	Network surveying

An overview of threat and risk assessment (4) – As per SANS Institute (www.sans.org)

Collecting data (cont'd)

Information on vulnerabilities and threats against the specific systems and services identified can be obtained from several resources:

a) Security Focus (www.securityfocus.com) – searchable databases of vulnerabilities and relevant news groups

b) Incidents.org (www.incidents.org) – information on current threats

c) Packet Storm (packetstromsecurity.org)

d) SANS (www.sans.org)

An overview of threat and risk assessment (5) – As per SANS Institute (www.sans.org)

Analyse the polices and procedures

- The review and analysis of the existing policies and procedures is done to gauge the compliance level within the organisation. An example of sources for policy compliance that can be used as a base line are:
  - ISO 27001/27002 (considered in some detail later in this course)
- It is important to identify the portions that are deemed not to be in compliance with respect to the specific industry and organisation. Care must be taken not to determine non-compliance when it is not necessary for the specific organisation/region or application.
- Because so many security standards exist, it is often difficult to determine which best applies to the organisation. Generic standards offer the most comprehensive view, but these often require security measures that are inappropriate in one or another industry. They fail to take into account the context.

An overview of threat and risk assessment (6) – As per SANS Institute (www.sans.org)

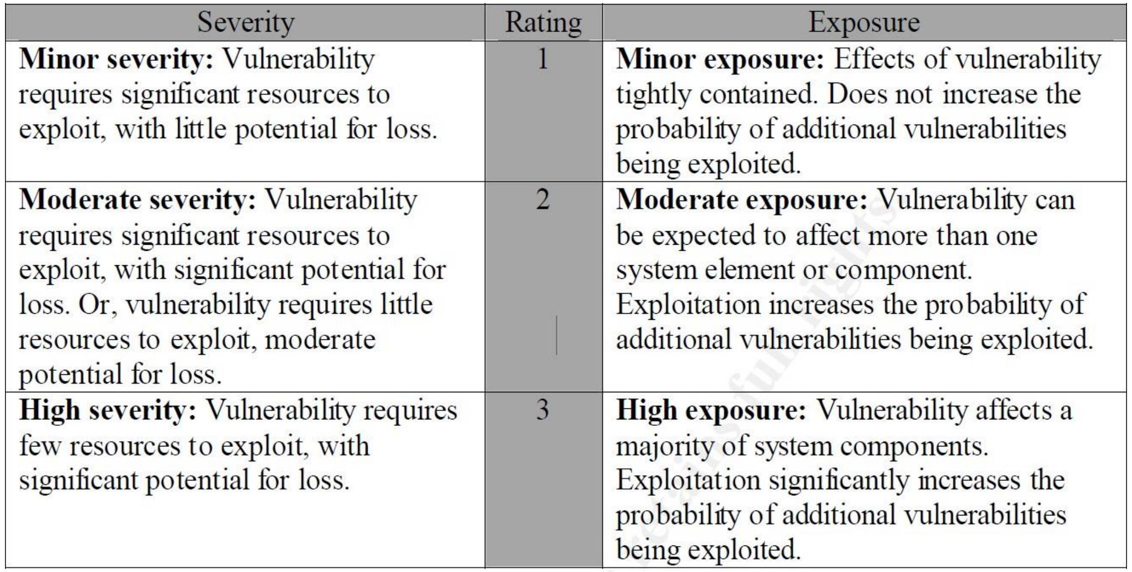
Vulnerability analysis (1)

- The purpose of vulnerability analysis is to take what was identified in the gathering of information and test to determine the current exposure, whether current safe guards are sufficient in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safe guards will be sufficient. Various tools can be used to identify specific vulnerabilities in systems: Nessus, SAINT, Whisker, Sara
- The problem faced within many organisations is the ability to effectively filter out the false positives inherent in assessment applications. The result of the various tools must be verified in order to accurately determine the reliability of the tools in use and to avoid protecting an area that in reality does not exist. False positive results can be mitigated by ensuring that the assessment applications are up to date with the latest stable signatures and patches

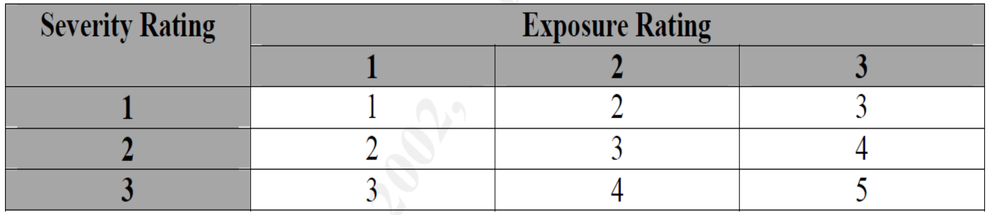
An overview of threat and risk assessment (6) – As per SANS Institute (www.sans.org)

Vulnerability analysis (2)

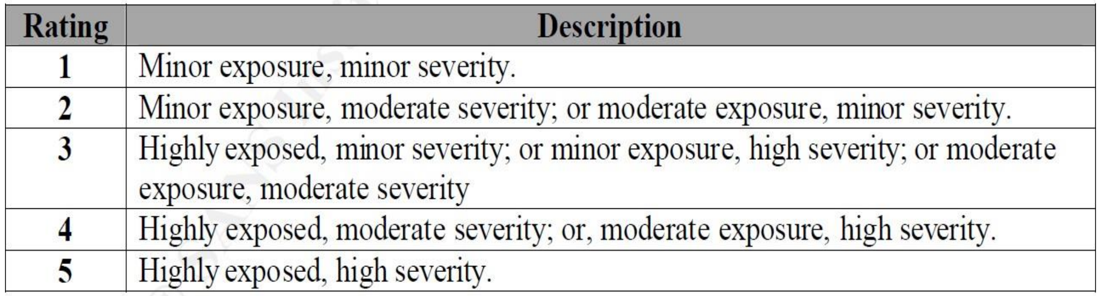
- The specific vulnerabilities can be graded according to the level of risk that they pose to the organisation, both internally and externally. A low rating can be applied to those vulnerabilities that are low in severity and low in exposure. Vulnerabilities would receive a high rating if the **severity** was high and the **exposure** was high.



Severity	Rating	Exposure
Minor severity: Vulnerability requires significant resources to exploit, with little potential for loss.	1	**Minor exposure:** Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited.
Moderate severity: Vulnerability requires significant resources to exploit, with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	2	**Moderate exposure:** Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High severity: Vulnerability requires few resources to exploit, with significant potential for loss.	3	**High exposure:** Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.



Severity Rating	Exposure Rating		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5



Rating	Description
1	Minor exposure, minor severity.
2	Minor exposure, moderate severity; or moderate exposure, minor severity.
3	Highly exposed, minor severity; or minor exposure, high severity; or moderate exposure, moderate severity
4	Highly exposed, moderate severity; or, moderate exposure, high severity.
5	Highly exposed, high severity.

An overview of threat and risk assessment (7) *– As per SANS Institute (www.sans.org)*

Threat analysis

- Threats are described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. The analysis will look at every element of risk that could conceivably happen. These threats can be split into Human and Nonhuman elements.

- Threats that are identified must be looked at in relation to the business environment and what affect they will have on the organisation. Threats go hand in hand with vulnerabilities and can be graded in a similar manner, measured in terms of **motivation** and **capability**. For example, the internal non-technical staff may have low motivation to do something malicious; however, they have a high level of capability due to their level of access on certain systems. A hacker, on the other hand, would have a high motivation for malicious intent and could have a high level of capability to damage or interrupt the business. Of course, motivation does not play a part in natural occurring phenomena. A low rating can be given where the threat has little or no capability or motivation. A high rating can be given for those threats that are highly capable and highly motivated.

An overview of threat and risk assessment (8) *– As per SANS Institute (www.sans.org)*

Conclusion

- In summary the threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organisation in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure.

- Organisations that do not perform a threat and risk analysis are leaving themselves open to situations that could disrupt, damage or destroy their ability to conduct business. Therefore the importance of performing a threat and risk analysis must be realized by management, by the staff supporting the infrastructure, and those that rely upon it for their business.

ESSENTIALS OF RISK MANAGEMENT:
1. DON'T DO ANYTHING WRONG TODAY.
2. DON'T DO ANYTHING WRONG TOMORROW.
3. REPEAT.
GLASBERGEN
© Randy Glasbergen / glasbergen.com

```
                  end
          end;                   func, std::vect
            write(Endtext);
      end.
      CREATE TABLE product(
            class MultinomialNB(object):
            def __init__(self):              std::co
      2})
                  self.X = None
                  self.y = None
            def __loading(self):
                  self.list_labels = cl.Counter(se
      int acc(std::function<int(int, int)> fun
            auto it = operands.begin();
            int result = func(*it, *(++it));
            if (operands.size() > 2) {
                  for (++it; it!=operands.end(); +
                        result = func(result, *(it);
                  }
            }
            return result;    CDog& operator=(c
```

Thank you