Management, Incident, Ethics

ICT 3156

IPSITA UPASANA

Security Planning

- Electronic form of data gives a false sense of requiring no security.
- Example.
- Every organization using computers to create and store valuable assets should perform thorough and effective security planning. Why?
  - Every application has confidentiality, integrity, and availability requirements that relate to the data, programs, and computing machinery.
  - Users often do not appreciate the security risks associated with using computers.
- **Security plan:** A document that describes how an organization will address its security needs and priorities.
- The plan is subject to periodic review and revision as the organization's security needs change.

Organizations and Security Plans

- Good security plan:
    - An official record of **current security practices.**
    - A **blueprint for orderly change** to improve those practices.
- A carefully written plan, supported by management, notifies employees that security is important to management (and therefore to everyone).
- Thus, the security plan has to have appropriate content and has to produce desired effects.
- 3 aspects of writing a security plan:
    - What it should contain.
    - Who writes it.
    - How to obtain support for it.

Contents of a Security Plan

Policy	The goals of a computer security effort and the willingness of the people involved to work to achieve those goals.
Current State	The status of security at the time of the plan.
Requirements	Recommending ways to meet the security goals.
Recommended Controls	Mapping controls to the vulnerabilities identified.
Accountability	Documenting who is responsible for each security activity.
Timetable	Identifying when different security functions are to be done.
Maintenance	Specifying a structure for periodically updating the security plan.

Policy

- A **security policy** is a high-level statement of purpose and intent.
- The policy statement must answer three essential questions:
  - Who should be allowed access?
  - To what system and organizational resources should access be allowed?
  - What types of access should each user be allowed for each resource?
- The policy statement should specify the following:
  - The organization’s goals on security.
  - Where the responsibility for security lies.
  - The organization’s commitment to security.

Current Status Assessment

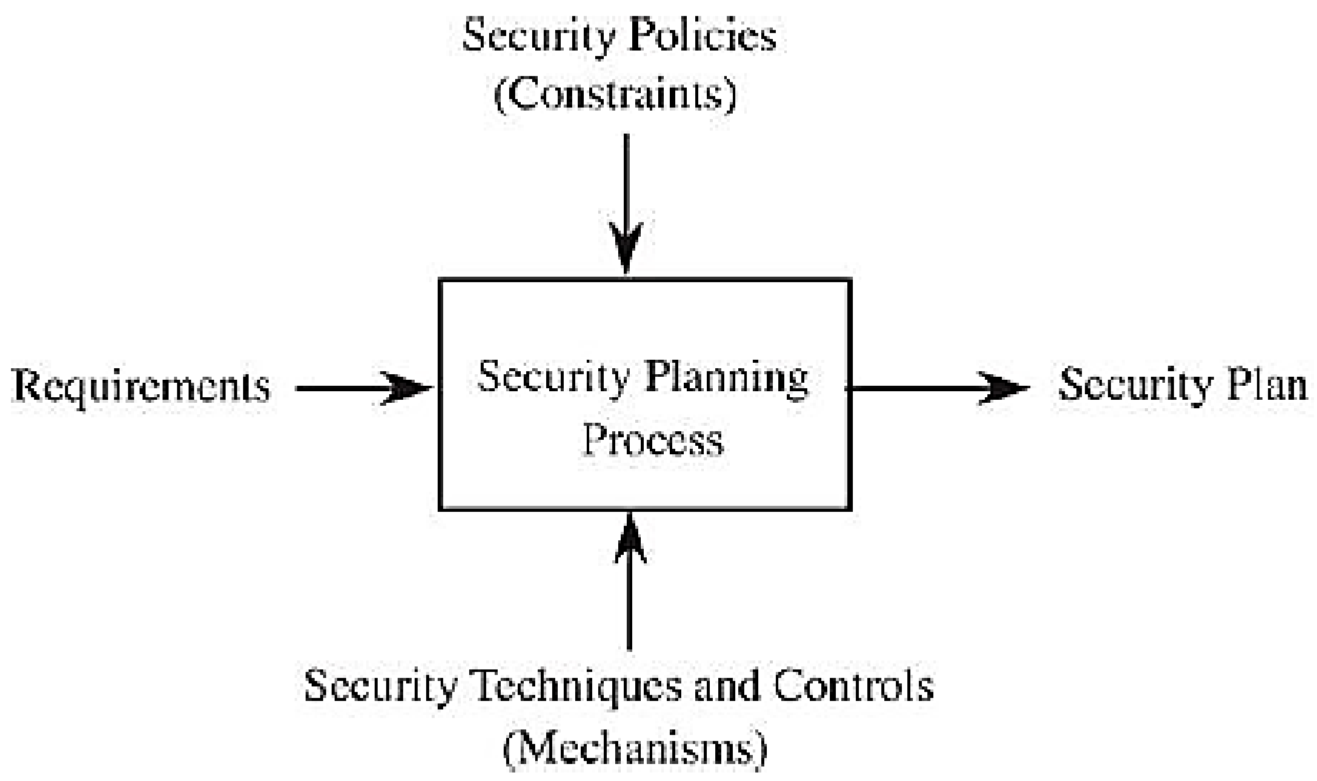
- To be able to plan for security, an organization must understand the vulnerabilities to which it may be exposed: perform a **risk analysis**.
- The risk analysis forms the basis for describing the current status of security.
- Status portion of the plan also defines the limits of responsibility for security.
- It describes not only **which assets** are to be protected but also **who** is responsible for protecting them.
- Vulnerabilities can also result from new situations. The security plan should detail the process to be followed when someone identifies a new vulnerability.

Security Requirements

- Requirements: functional or performance **demands** (organizational and external) placed on a system to ensure a desired level of security.
- The requirements are usually derived from organizational needs.
- Requirements v/s **constraints** and controls.
- A constraint is an aspect of the security policy that constrains, circumscribes, or directs the implementation of the requirements.
- Requirements explain **what** should be accomplished, not how. Always leave the implementation details to the designers, whenever possible.

Security Requirements

- Different aspects of system analysis support the security planning process.
- Inputs to the Security Plan
- The requirements should address all aspects of security: CIA.



Security Requirements

- Requirements must have these characteristics:
  - Correctness
  - Consistency
  - Completeness
  - Realism
  - Need
  - Verifiability
  - Traceability

- The requirements may then be constrained by budget, schedule, performance, policies, governmental regulations, and more.
- Given the requirements and constraints, developers then choose appropriate controls.

Recommended Controls

- The security plan must also recommend what controls should be incorporated into the system to meet those requirements.
- The recommended controls address implementation issues: how the system will be designed and developed to meet stated security requirements.

Accountability: Responsibility for Implementation

- A security plan documents who is responsible for implementing security. No one responsible implies no action.
- The plan makes explicit who is accountable should some requirement not be met or some vulnerability not be addressed.
- Some examples could be:
    - Users
    - Project leaders Managers
    - Database administrators
    - Information officers
    - Personnel staff members

Timetable

- Security plan includes timetables. Purpose:
    - Shows how and when the elements of the plan will be performed.
    - Management can track the progress of implementation.
- Specify the order in which the controls are to be implemented so that the most serious exposures are covered as soon as possible.
- The plan must be extensible. Why?
    - Conditions will change: New **equipment** will be acquired, new degrees and **modes** of connectivity will be requested, and new **threats** will be identified.
- Security aspects of changes should be considered **as a part of** preparing for the change, not for adding security **after the change** has been made.
- The plan should also contain a schedule for **periodic** review.

Maintenance

- Why maintenance?
  - As users, data, and equipment change, new exposures may develop.
  - The current means of control may become obsolete or ineffective.
- We must also find ways for evaluating a system’s security to be sure that the system is as secure as we intend it to be.
- Thus, the security plan must call for reviewing the security situation periodically.

Handling Incidents

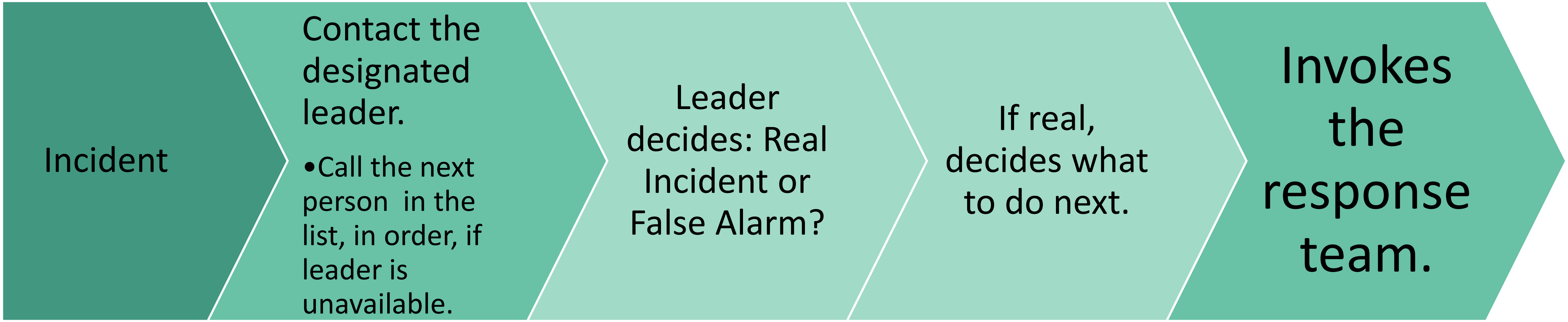
- What would you do when a file suddenly disappears? Or an unusual name appears on the list of active processes?
- Individuals must take responsibility for their own environments. What about bigger organizations?
- Organizations develop a **capability** to handle incidents from receiving the first report and investigating it.

Incident Response Plans

- An incident response plan details how to address security incidents of all types.
- An incident could be a single event, a series of events, or an ongoing problem.
- An incident response plan should
  - define what constitutes an incident.
  - identify who is responsible for taking charge of the situation.
  - describe the plan of action.
- The plan usually has **three phases**: advance planning, triage, and running the incident.
- Fourth phase: review. Useful after the situation abates so that this incident can lead to improvement for future incidents.

Advance Planning

- What to do when an incident happens? Example: Fire in a building.
- An **incident response plan** tells whom to contact in the event of an incident, which may be just an unconfirmed, unusual situation.
- With an incident response plan in place, everybody is trained in **advance**.



Incident

Contact the designated leader.

- Call the next person in the list, in order, if leader is unavailable.

Leader decides: Real Incident or False Alarm?

If real, decides what to do next.

Invokes the response team.

Responding

- The response team is the set of people charged with responding to the incident.
- The response team may include:
    - Director: person in charge of the incident.
    - Technician(s): people who perform the technical part of the response. Role of lead technician?
    - Advisor(s): legal, human resources, or public relations staff members as appropriate.
- Incident responders first perform **triage**: They investigate what has happened.
- Incident responders follow the case until they have identified the cause and **done as much as possible to return the system to normal.**
- Then the team finishes documenting its work and declares the incident over.

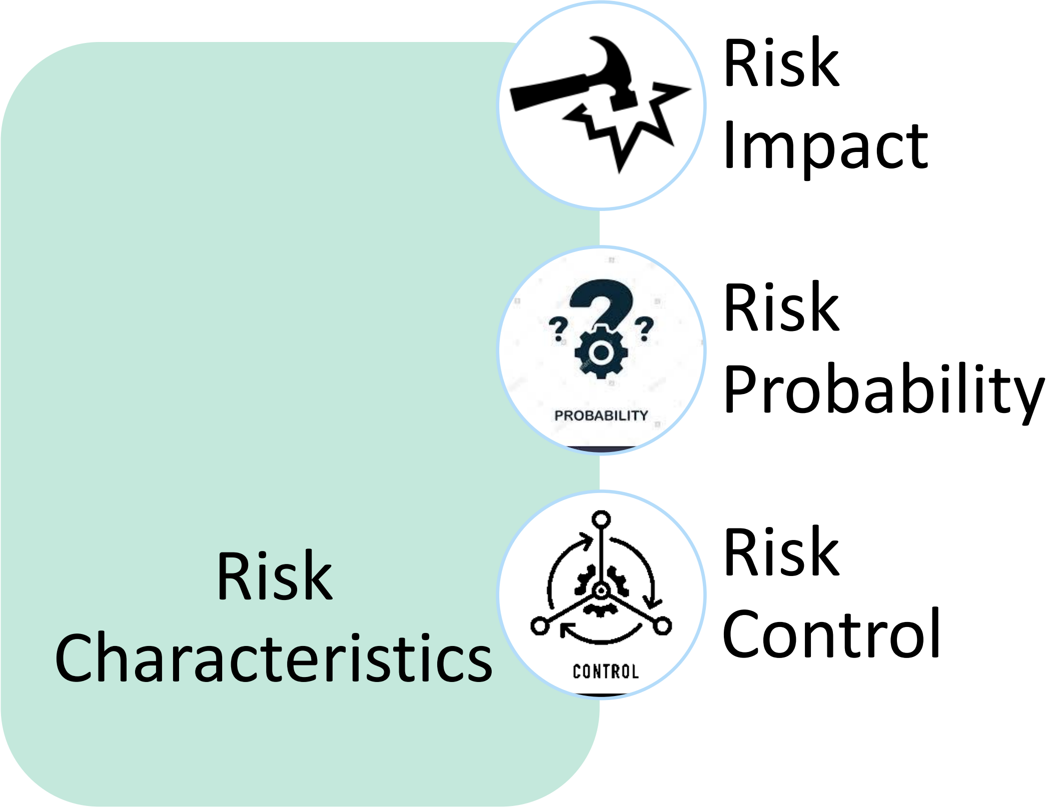
After the Incident Is Resolved

- The team will hold a **review** after the incident to consider two things:
- Is any security control action to be taken?
- Did the incident response plan work?
- The incident response plan ensures that incidents are handled promptly, efficiently, and with minimal harm.

Risk Analysis

- A **risk** is a potential problem that the system or its users may experience.
- **Risk analysis** is an organized process for **identifying** the most significant **risks** in a computing environment, **determining** the **impact** of those risks, and **weighing** the **desirability** of applying various controls against those risks.
- It is a management activity which is at **the heart of security planning**.

Risk Exposure: Quantifies the effects of a risk.
Risk Exposure = Risk Impact* Risk Probability.



Risk Characteristics

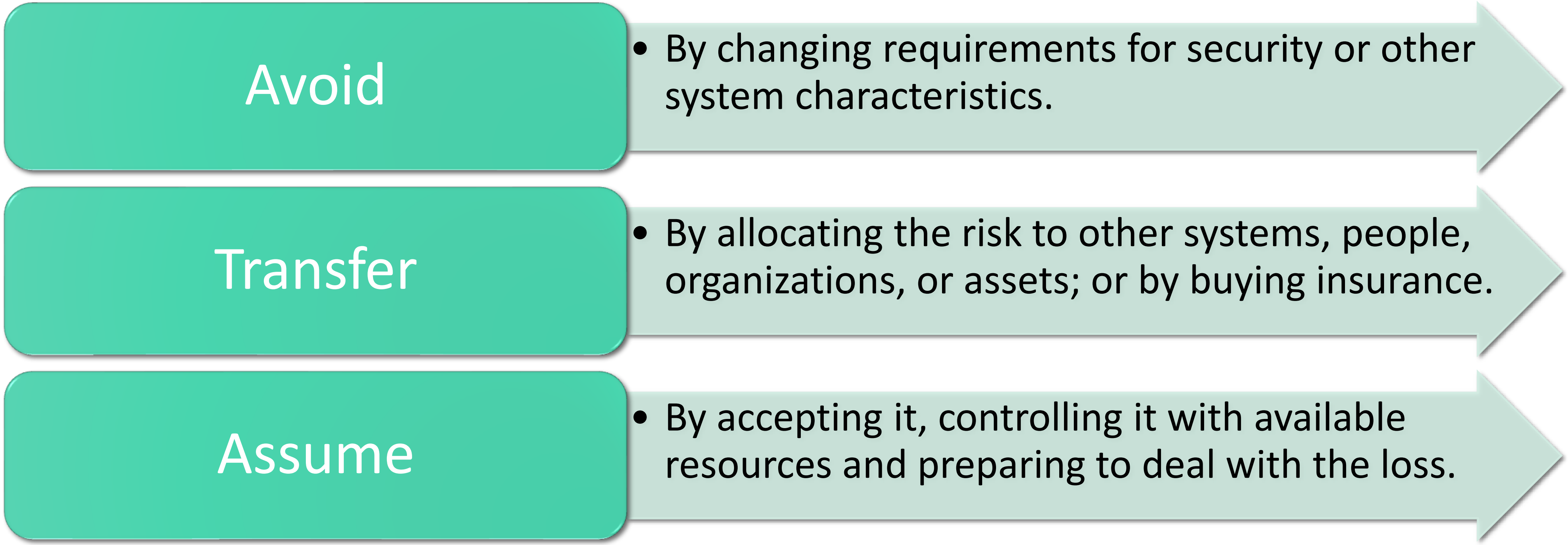
Risk Impact

Risk Probability

Risk Control

Risk Analysis

- Three strategies for dealing with risk:



Avoid

- By changing requirements for security or other system characteristics.

Transfer

- By allocating the risk to other systems, people, organizations, or assets; or by buying insurance.

Assume

- By accepting it, controlling it with available resources and preparing to deal with the loss.

Risk Analysis

- Costs are associated not only with the risk’s potential impact but also with reducing it.
- **Risk leverage** is the amount of benefit per unit spent.
- It is the difference in risk exposure divided by the cost of reducing the risk.

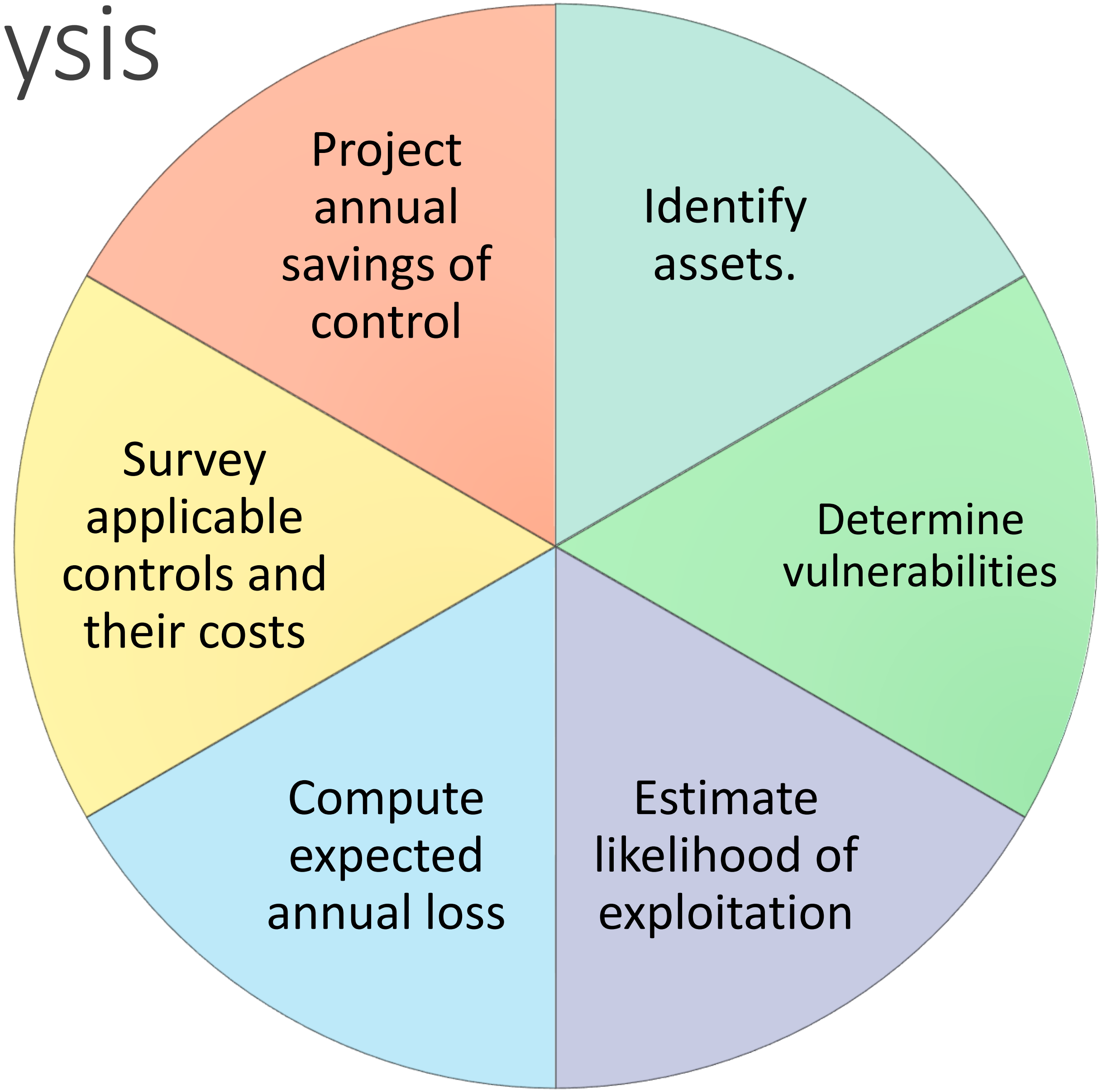
$$\frac{(Risk\ Exposure\ before\ reduction) - (Risk\ Exposure\ after\ reduction)}{(Cost\ of\ risk\ reduction)}$$

- The leverage measures value for money spent: A risk reduction of $100 for a cost of $10, a 10:1 reduction, is quite a favorable result.

Risk Analysis

- Risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause.
- Summary:
  - Identify and list all exposures in the computing system of interest.
  - For each exposure, identify possible controls and their costs.
  - Cost–benefit analysis: Does it cost less to implement a control or to accept the expected cost of the loss?

Steps of a Risk Analysis



Identify assets.

Determine vulnerabilities

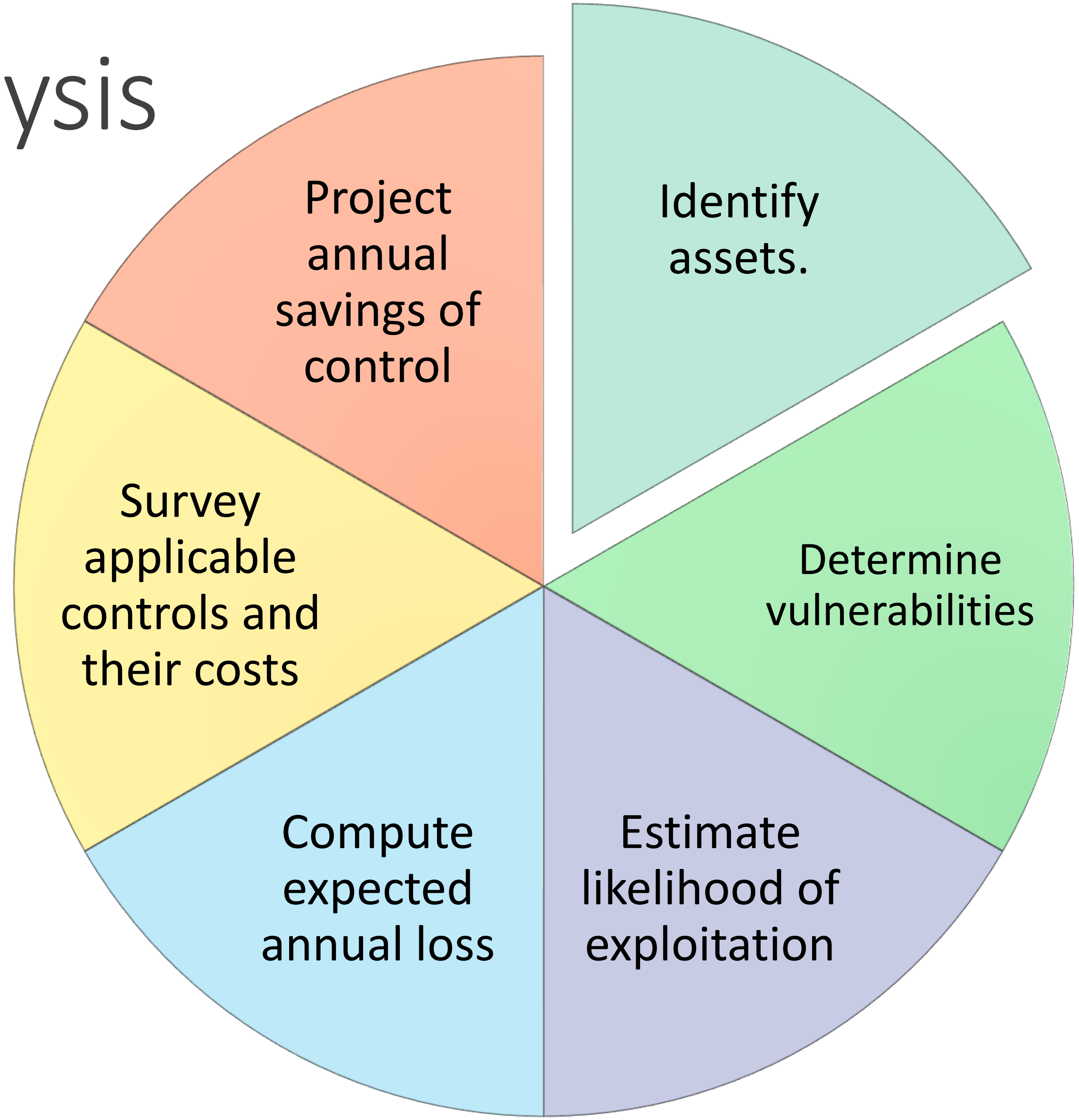
Estimate likelihood of exploitation

Compute expected annual loss

Survey applicable controls and their costs

Project annual savings of control

Steps of a Risk Analysis



Identify assets.

Determine vulnerabilities

Estimate likelihood of exploitation

Compute expected annual loss

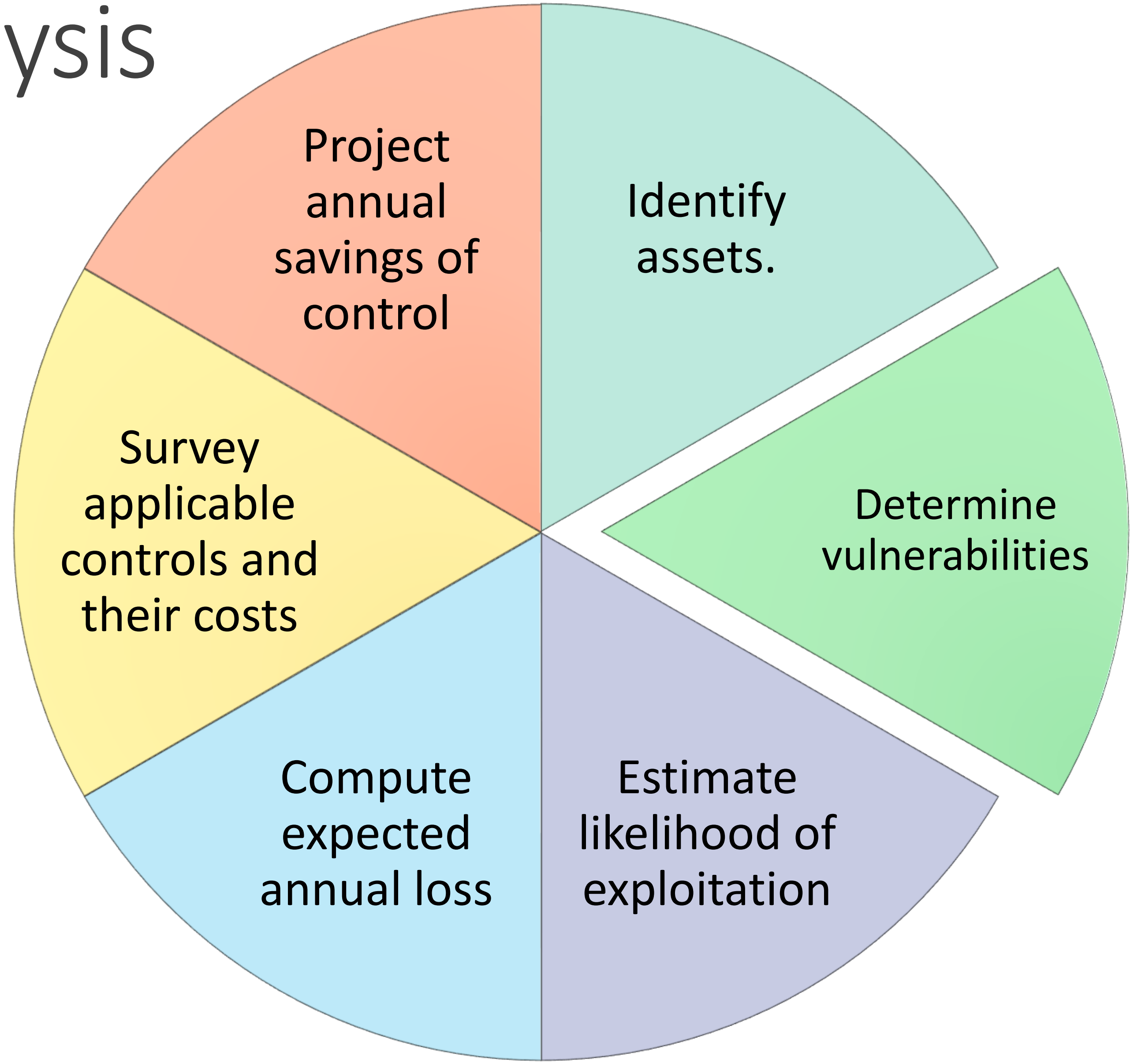
Survey applicable controls and their costs

Project annual savings of control

Identify assets

- Before we can identify vulnerabilities, we must first decide what we need to protect.
  - Hardware
  - Software
  - Data
  - People
  - Documentation
  - Supplies
  - Reputation
  - Availability
- No two organizations will have the same assets to protect. Something that is valuable in one organization may not be as valuable to another.
- Not all business assets are tangible, and not all are easy to value.

Steps of a Risk Analysis



Identify assets.

Determine vulnerabilities

Estimate likelihood of exploitation

Compute expected annual loss

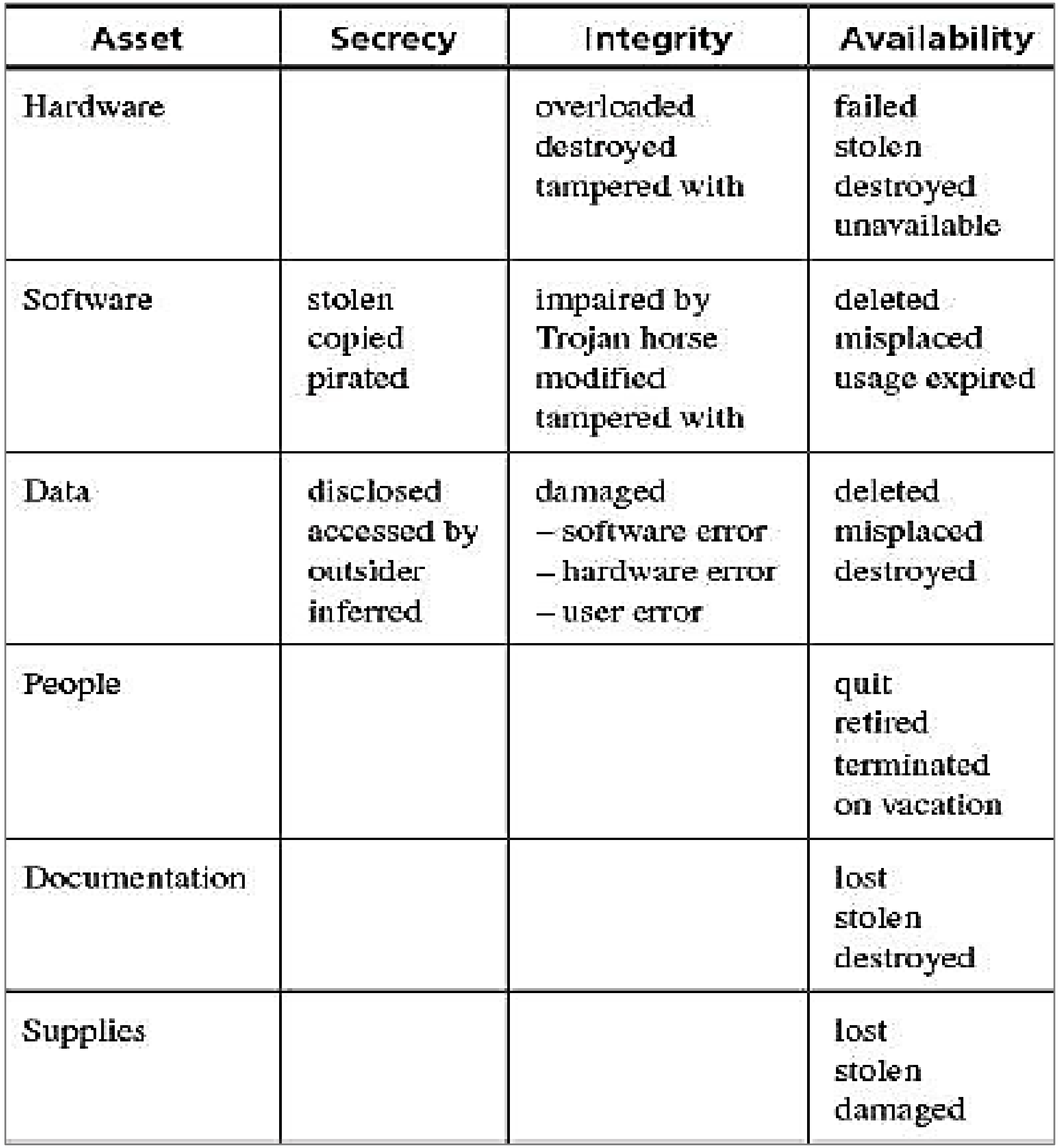
Survey applicable controls and their costs

Project annual savings of control

Determine vulnerabilities

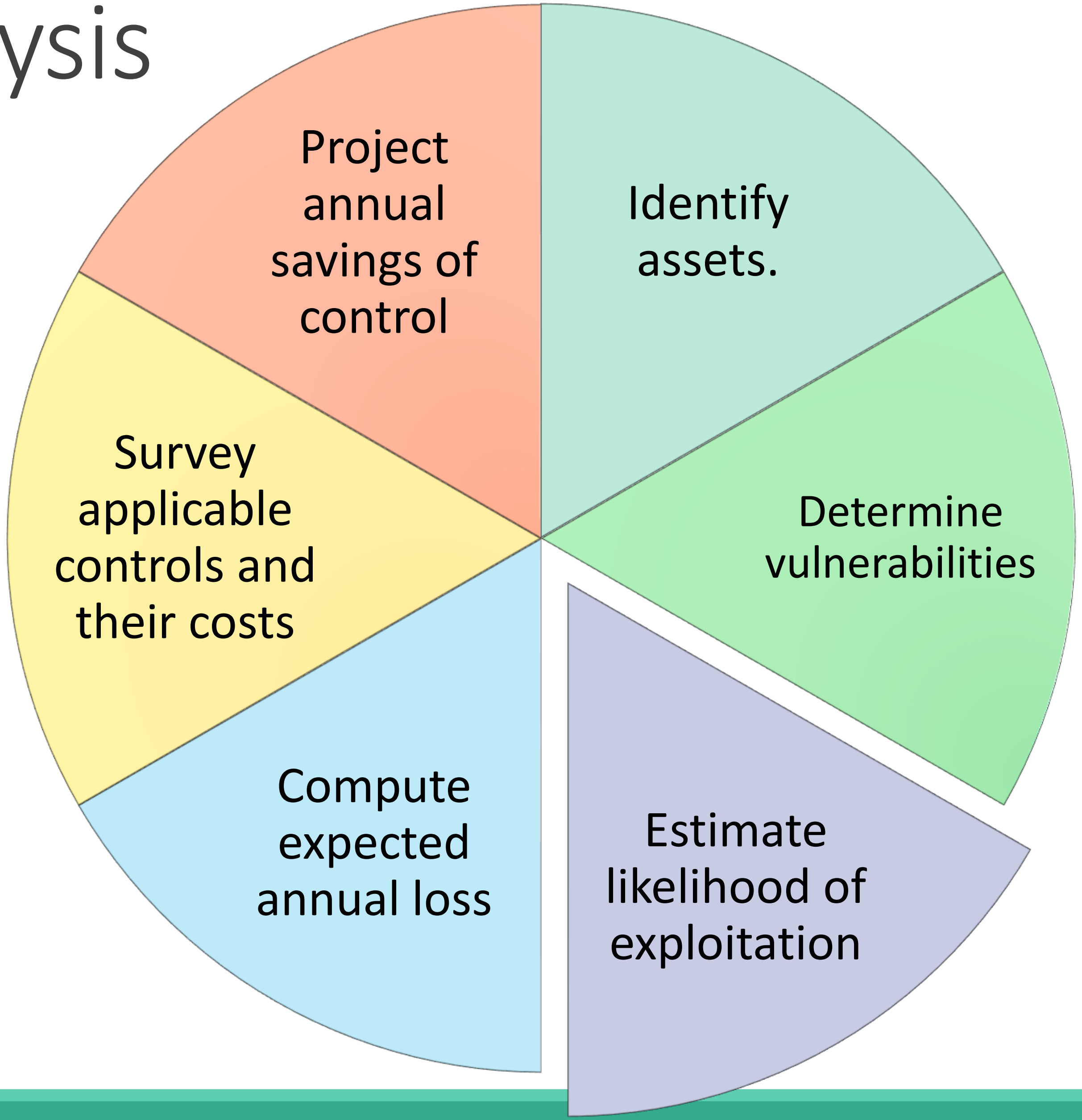
- This step requires imagination; we want to predict what damage might occur to the assets and from what sources.
- Develop a clear idea of the nature of vulnerabilities. This nature derives from the need to ensure the three basic goals of computer security: CIA.
- One vulnerability can affect more than one asset or cause more than one type of loss.
- There is no simple checklist or easy procedure to list all vulnerabilities.
- To organize the way we consider threats and assets, we can use a matrix.

Assets and Attacks



Asset	Secrecy	Integrity	Availability
Hardware		overloaded destroyed tampered with	failed stolen destroyed unavailable
Software	stolen copied pirated	impaired by Trojan horse modified tampered with	deleted misplaced usage expired
Data	disclosed accessed by outsider inferred	damaged – software error – hardware error – user error	deleted misplaced destroyed
People			quit retired terminated on vacation
Documentation			lost stolen destroyed
Supplies			lost stolen damaged

Steps of a Risk Analysis

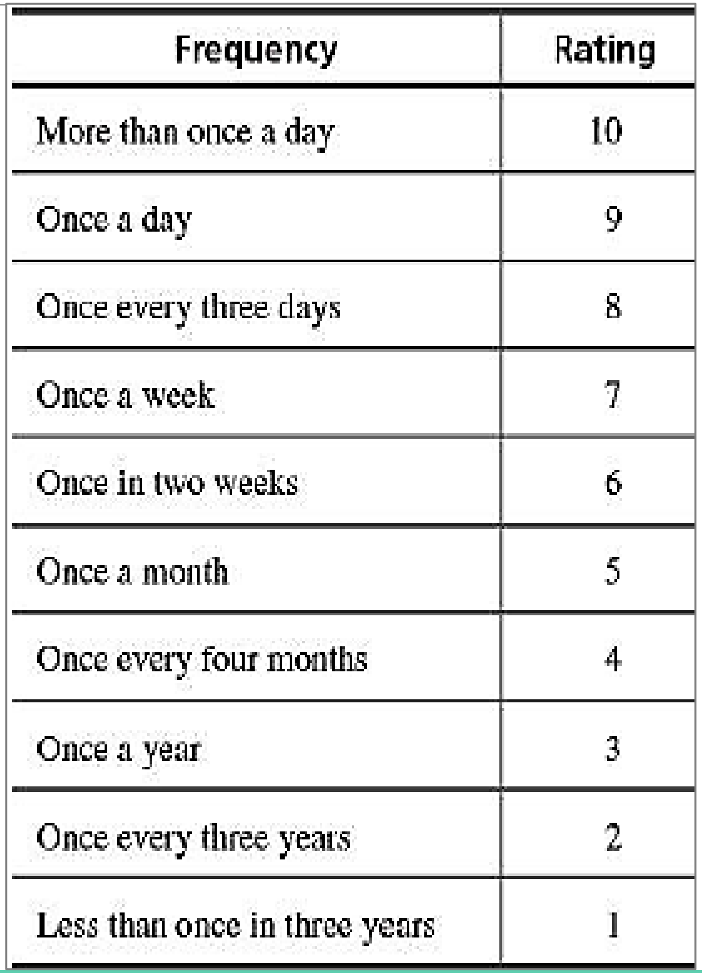

Identify assets.
Determine vulnerabilities
Estimate likelihood of exploitation
Compute expected annual loss
Survey applicable controls and their costs
Project annual savings of control

Estimate likelihood of exploitation

- Determine how often each exposure is likely to be exploited.
- **Likelihood** of occurrence relates to the **stringency** of the existing controls and the likelihood that someone or **something will evade** the existing controls.
- In some cases, the number of occurrences of events can be estimated in a given time period. Depends on the fact that a system is already built and has been in use for some period of time.
- In many cases usage data are not available. In this case, we may ask an analyst to estimate likelihood by reviewing a table based on a similar system.

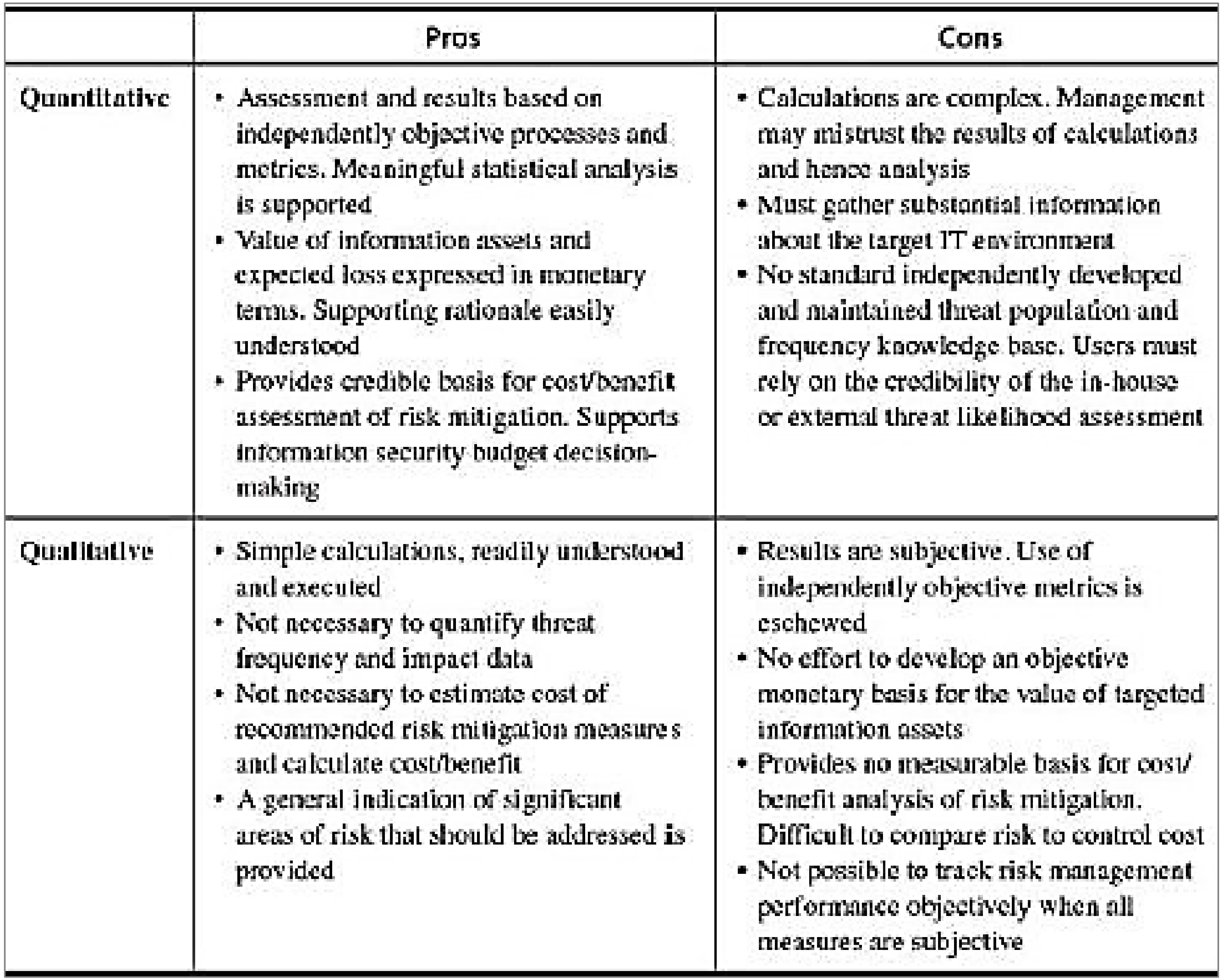
Estimate likelihood of exploitation

- **Quantitative risk analysis**: numbers can be assigned to various risks.
- **Qualitative risk analysis**: descriptive adjectives are used to rate risks (“highly likely”, “improbable”, and so on)
- Qualitative assessment is more appropriate in situations where it is difficult to quantify risk.
- Often, qualitative risks are then assigned a numeric value.
- Estimates of value and event likelihood are just estimates; their purpose is to locate points of most serious vulnerability.



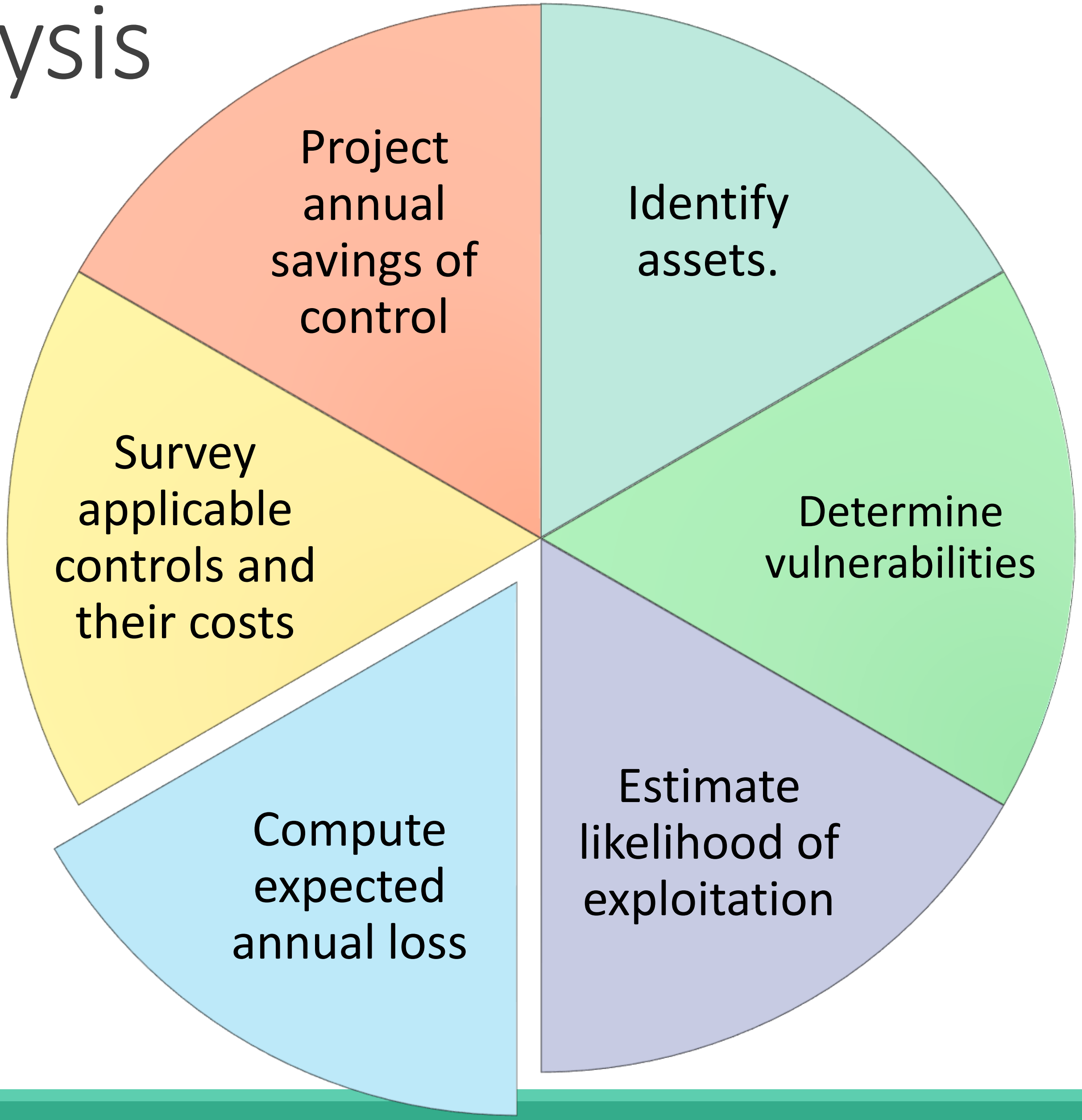
Frequency	Rating
More than once a day	10
Once a day	9
Once every three days	8
Once a week	7
Once in two weeks	6
Once a month	5
Once every four months	4
Once a year	3
Once every three years	2
Less than once in three years	1

Comparing Quantitative to Qualitative Risk Assessment



	Pros	Cons
Quantitative	• Assessment and results based on independently objective processes and metrics. Meaningful statistical analysis is supported • Value of information assets and expected loss expressed in monetary terms. Supporting rationale easily understood • Provides credible basis for cost/benefit assessment of risk mitigation. Supports information security budget decision-making	• Calculations are complex. Management may mistrust the results of calculations and hence analysis • Must gather substantial information about the target IT environment • No standard independently developed and maintained threat population and frequency knowledge base. Users must rely on the credibility of the in-house or external threat likelihood assessment
Qualitative	• Simple calculations, readily understood and executed • Not necessary to quantify threat frequency and impact data • Not necessary to estimate cost of recommended risk mitigation measures and calculate cost/benefit • A general indication of significant areas of risk that should be addressed is provided	• Results are subjective. Use of independently objective metrics is eschewed • No effort to develop an objective monetary basis for the value of targeted information assets • Provides no measurable basis for cost/benefit analysis of risk mitigation. Difficult to compare risk to control cost • Not possible to track risk management performance objectively when all measures are subjective

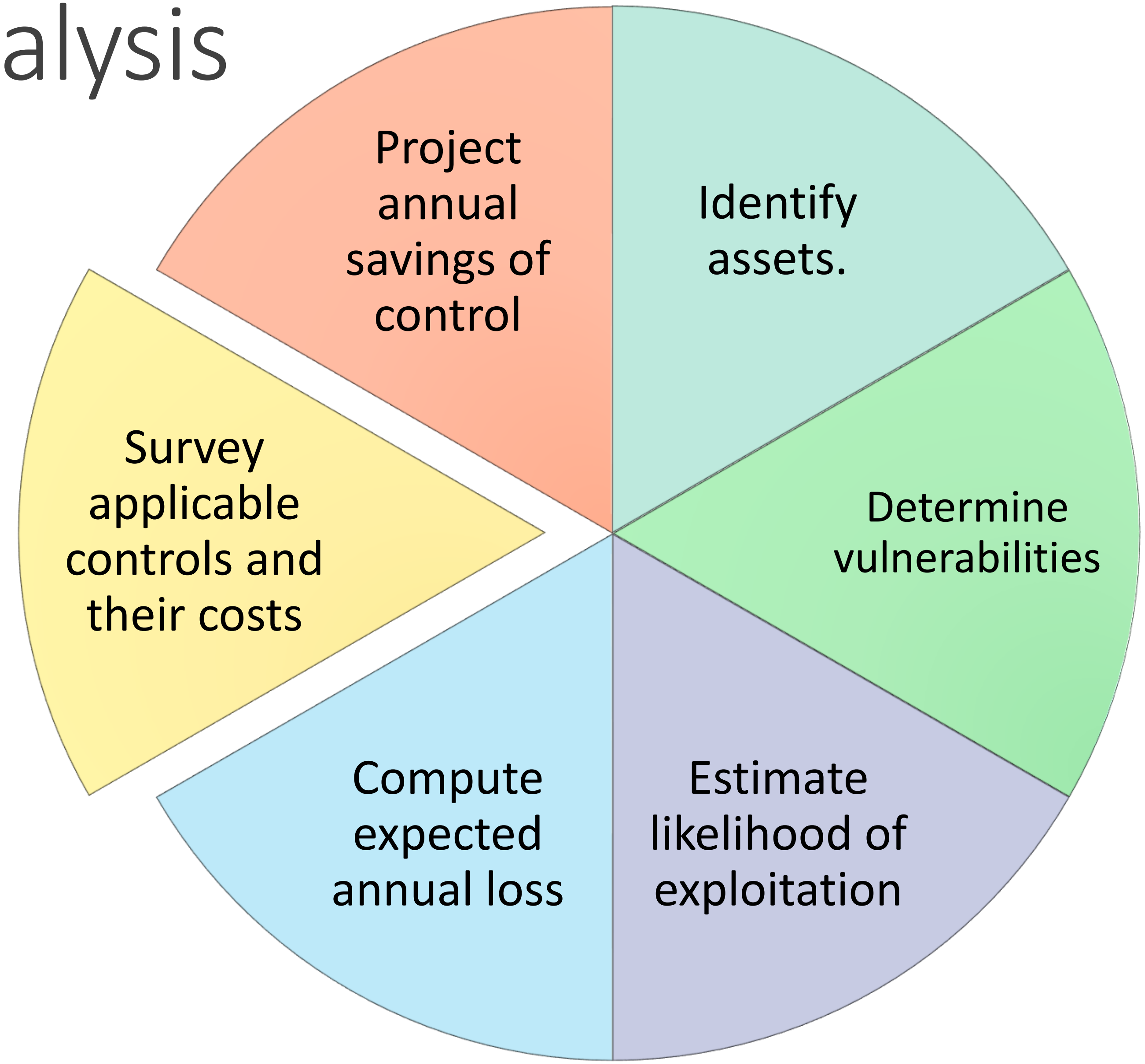
Steps of a Risk Analysis


Identify assets.
Determine vulnerabilities
Estimate likelihood of exploitation
Compute expected annual loss
Survey applicable controls and their costs
Project annual savings of control

Compute expected annual loss

- This value is difficult to determine .
- Some costs are easy to obtain. Some costs are substantially harder to measure: costs in restoring a system to its previous state, reinstalling software, or deriving a piece of information.
- Hidden costs must also be accounted.
- Estimates of expected loss are necessarily imprecise; relative sizes are more important than absolute values.
- The vulnerabilities in computer security are often considerably higher than managers expect.
- Realistic estimates of potential harm can raise concern and suggest places in which attention to security is especially needed.

Steps of a Risk Analysis



Identify assets.

Determine vulnerabilities

Estimate likelihood of exploitation

Compute expected annual loss

Survey applicable controls and their costs

Project annual savings of control

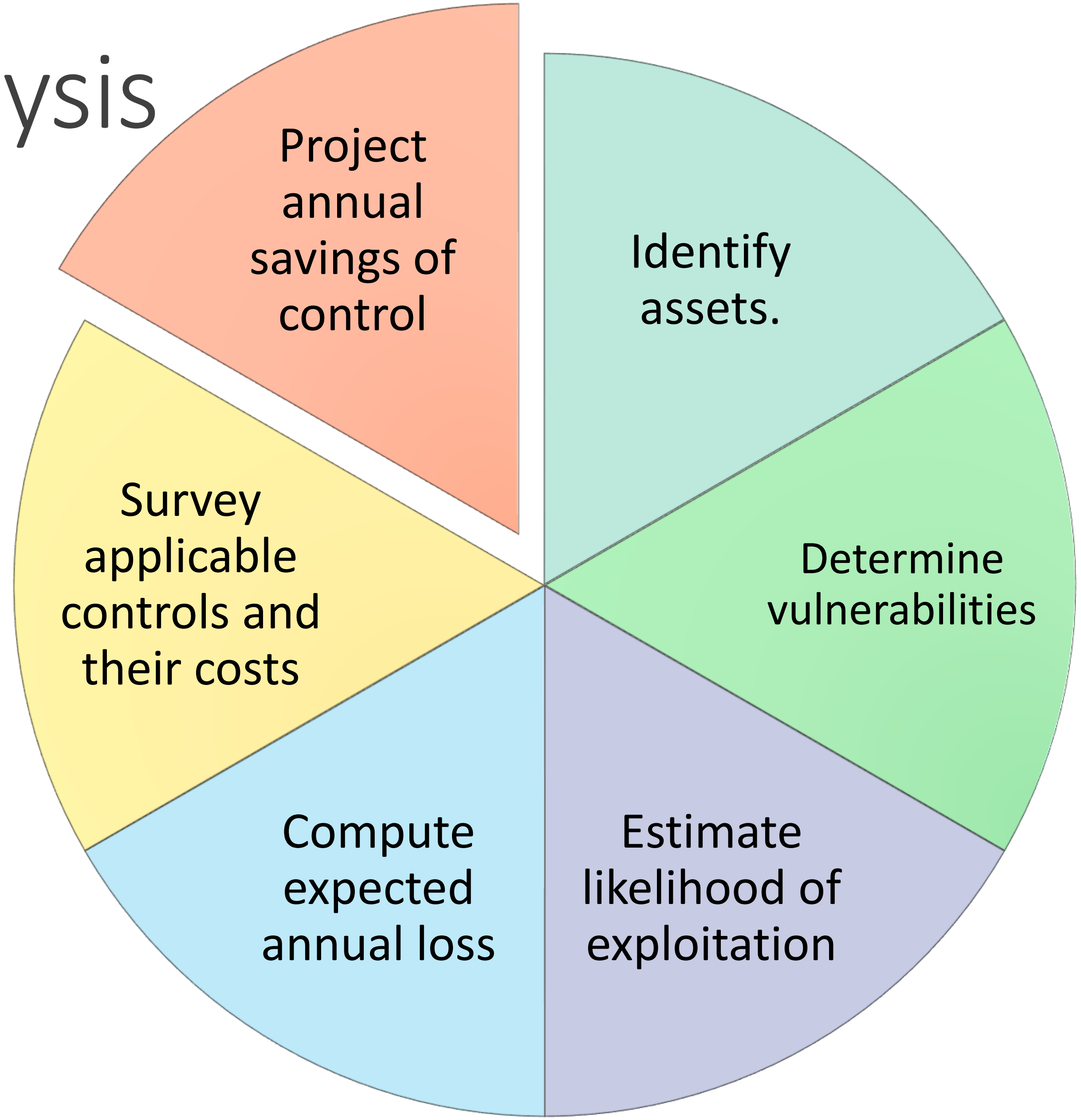
Survey applicable controls and their costs

- Each vulnerability must be matched with at least one appropriate security technique.
- Expected loss estimates can be used to help decide which controls, alone or in concert, are the most cost effective for a given situation.
- Things to consider while choosing controls:
    - Controls can overlap. Example.
    - One control may cover multiple vulnerabilities.
    - Controls have positive and negative effects.
    - Controls are not perfect. They can fail.
    - Some controls are stronger than others. Some are more usable.

Survey applicable controls and their costs

- We know: Risk analysis involves building a multidimensional array: assets, vulnerabilities, likelihoods, controls.
- Mapping controls to vulnerabilities may involve using graph theory to select a minimal set of controls that address all vulnerabilities.
- What is the advantage of careful, systematic documentation of all these data?
- Each choice can be analyzed, and the side effects of changes are apparent.
- With a manageable number of assets and vulnerabilities, determining controls (some of which may already be in place) need not be extensive, as long as some control covers each major vulnerability.

Steps of a Risk Analysis

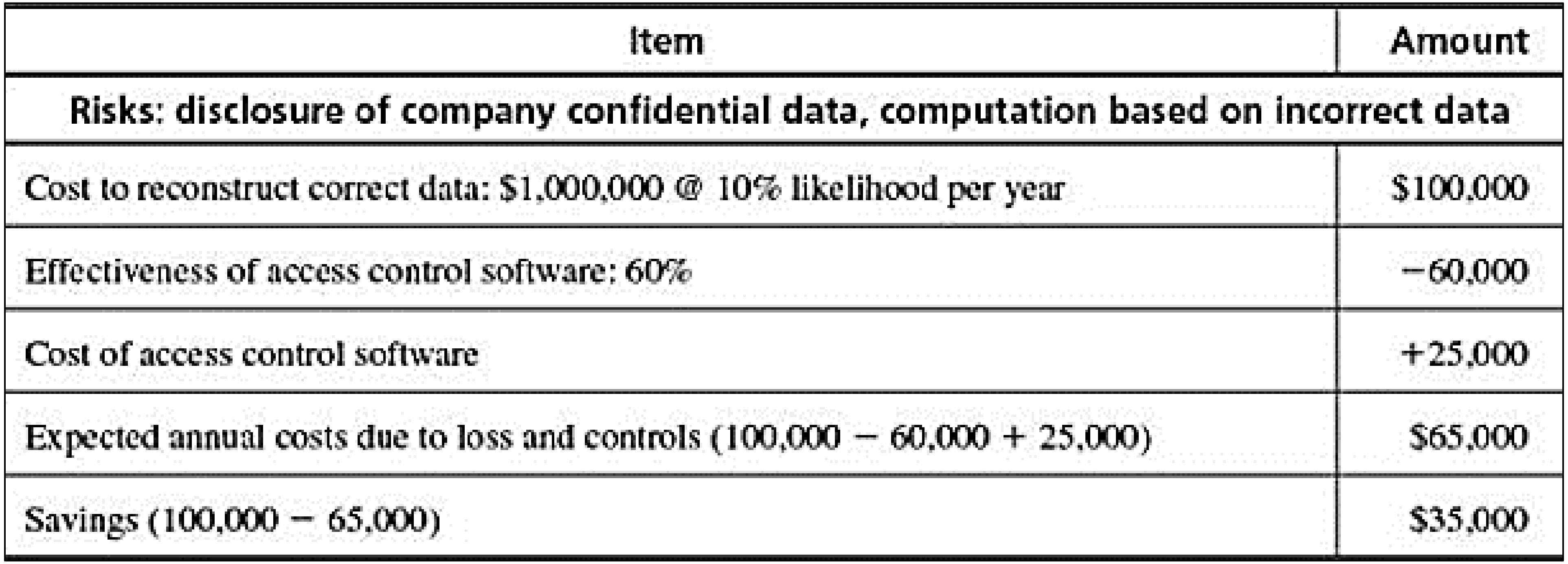


Identify assets.
Determine vulnerabilities
Estimate likelihood of exploitation
Compute expected annual loss
Survey applicable controls and their costs
Project annual savings of control

Project annual savings of control

- Determine whether the costs outweigh the benefits of preventing or mitigating the risks.
- Effective cost of a given control = Actual cost of the control - Any expected loss from using the control.
- True cost of a control may be:
    - positive if the control is expensive to administer or introduces new risk in another area of the system.
    - negative if the reduction in risk is greater than the cost of the control.

Project Costs and Savings

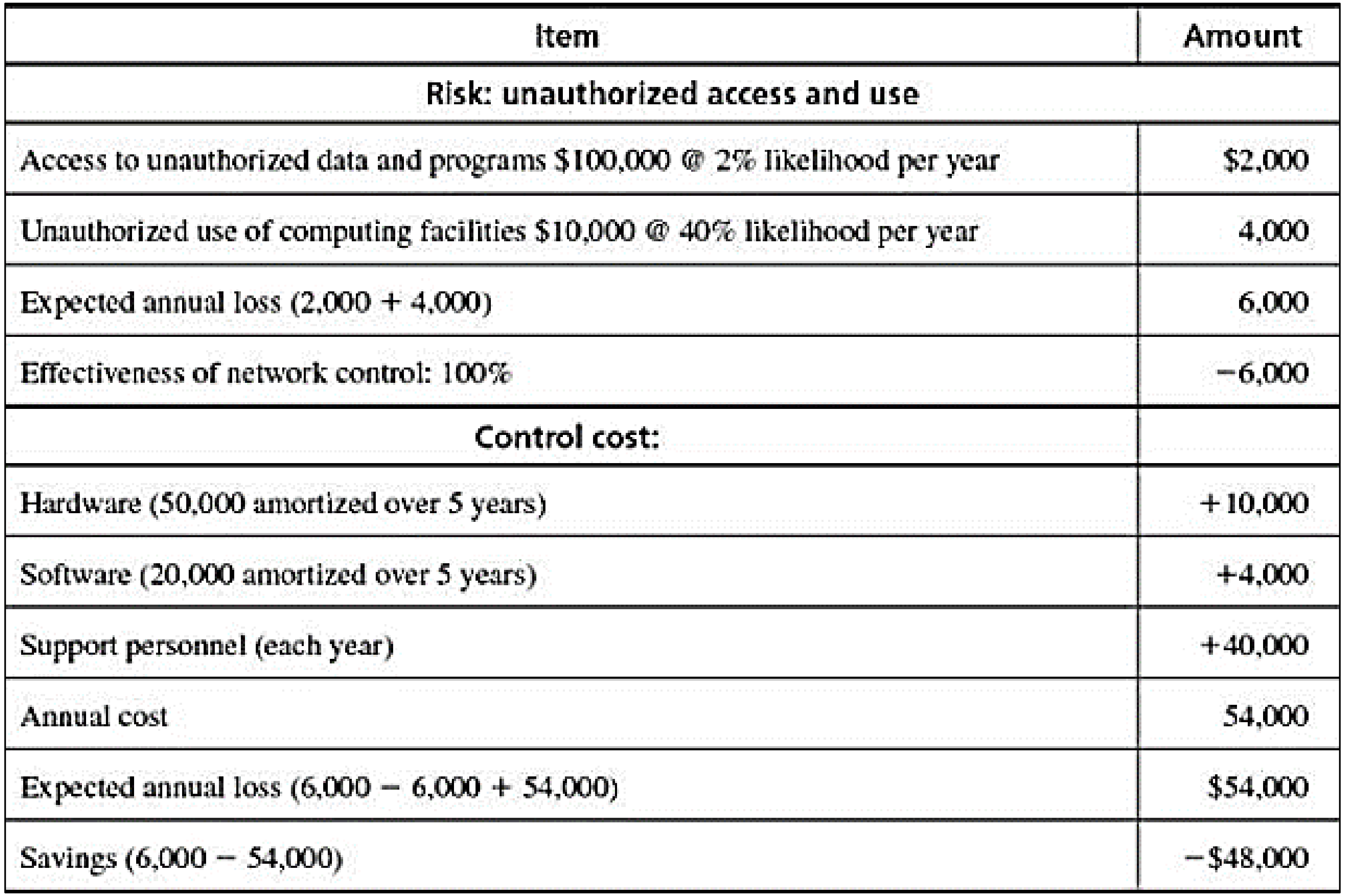


Item	Amount
Risks: disclosure of company confidential data, computation based on incorrect data	
Cost to reconstruct correct data: $1,000,000 @ 10% likelihood per year	$100,000
Effectiveness of access control software: 60%	−60,000
Cost of access control software	+25,000
Expected annual costs due to loss and controls (100,000 − 60,000 + 25,000)	$65,000
Savings (100,000 − 65,000)	$35,000

Justification of Access Control Software

Project Costs and Savings

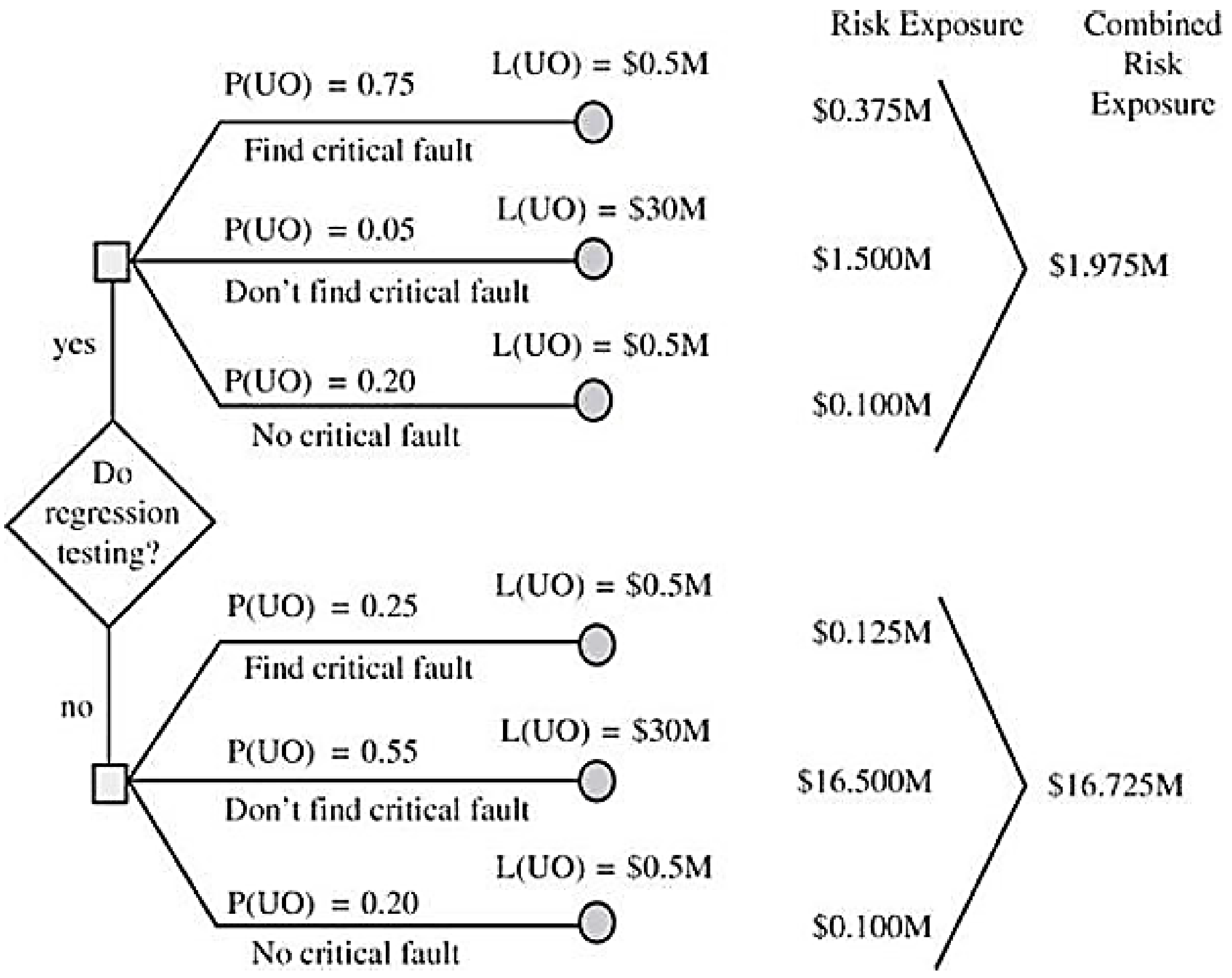
Cost/Benefit Analysis for Replacing Network Access



Item	Amount
Risk: unauthorized access and use	
Access to unauthorized data and programs $100,000 @ 2% likelihood per year	$2,000
Unauthorized use of computing facilities $10,000 @ 40% likelihood per year	4,000
Expected annual loss (2,000 + 4,000)	6,000
Effectiveness of network control: 100%	−6,000
Control cost:	
Hardware (50,000 amortized over 5 years)	+10,000
Software (20,000 amortized over 5 years)	+4,000
Support personnel (each year)	+40,000
Annual cost	54,000
Expected annual loss (6,000 − 6,000 + 54,000)	$54,000
Savings (6,000 − 54,000)	−$48,000

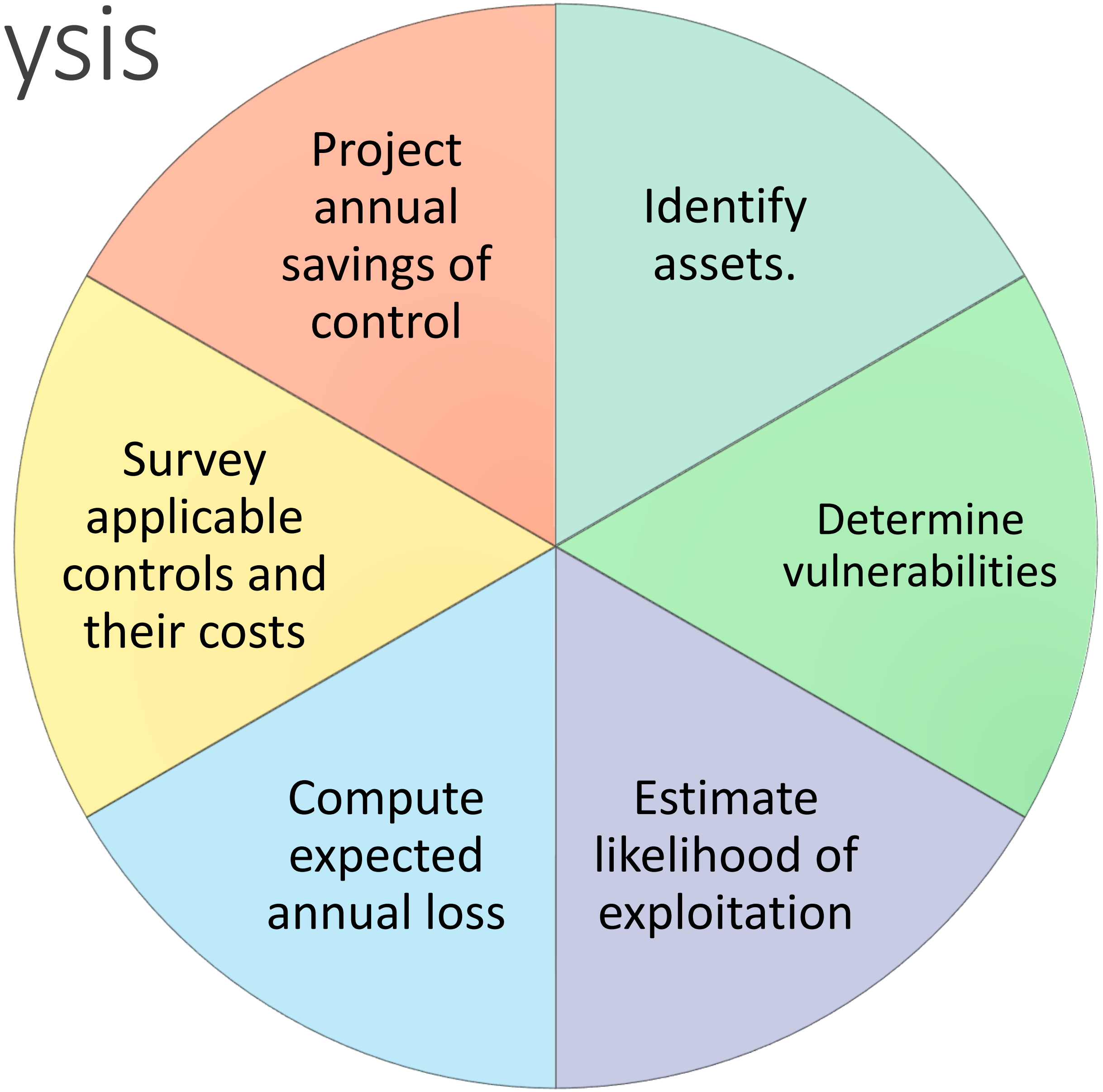
Project Costs and Savings

We can use a graphical depiction to contrast the economics involved in choosing among several strategies.



Risk Calculation for Regression Testing

Steps of a Risk Analysis



Identify assets.

Determine vulnerabilities

Estimate likelihood of exploitation

Compute expected annual loss

Survey applicable controls and their costs

Project annual savings of control

Reasons to Perform a Risk Analysis

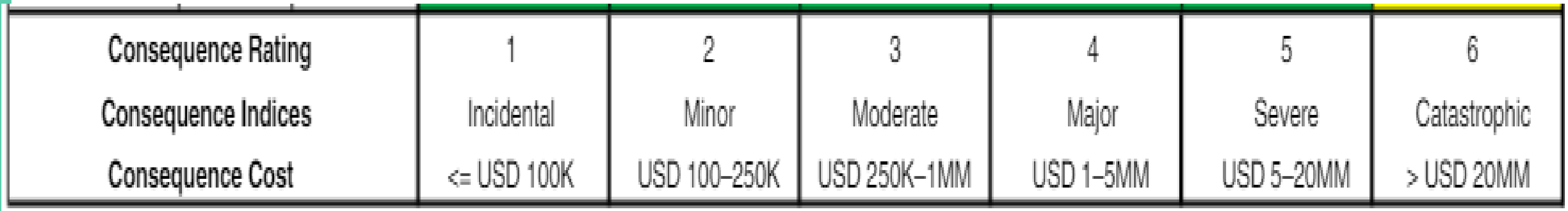
- Improve awareness.
- Relate security mission to management objectives.
- Identify assets, vulnerabilities, and controls.
- Improve basis for decisions.
- Justify expenditures for security.
- Risk analysis provides a rational basis for spending for security, justifying both the things to spend on and the amounts to spend.

Constraints

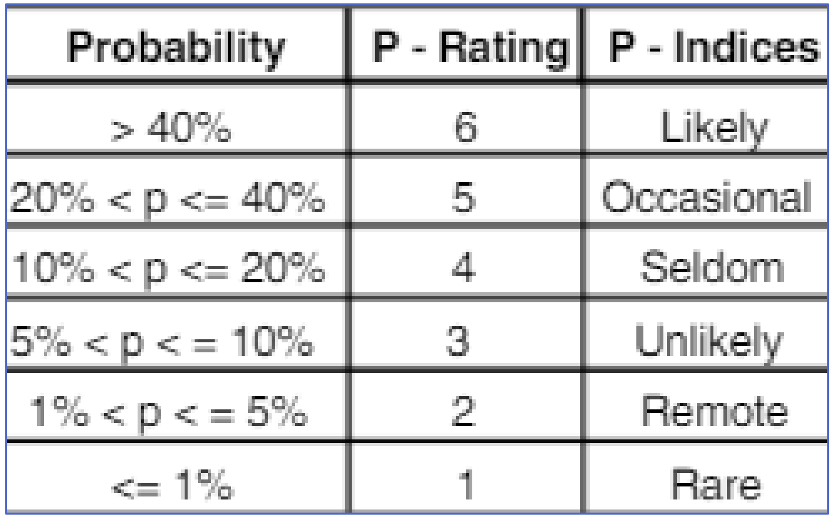
- False sense of precision and confidence.
- Hard to perform.
- Immutability.
- Lack of accuracy.

Risk Matrix (RM)

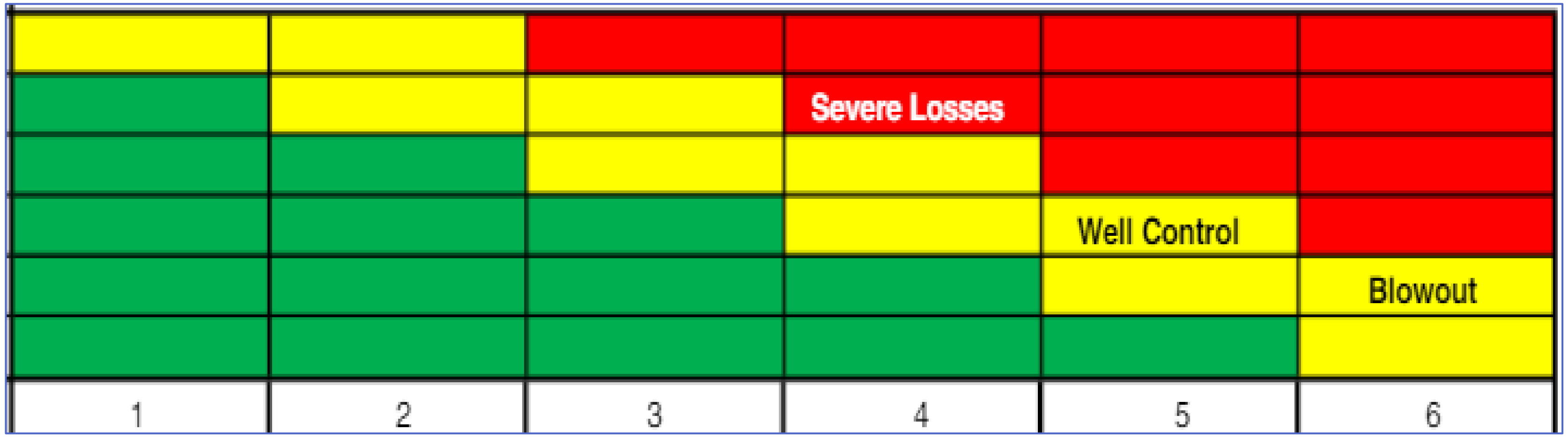
- A graphical presentation of the likelihood, or probability, of an outcome and the consequence should that outcome occur.
- Consequences are often defined in monetary terms.
- RMs tend to be focused on outcomes that could result in loss, rather than gain.
- Objective of the RM : to prioritize risks and risk-mitigation actions.



Consequence Rating	1	2	3	4	5	6
Consequence Indices	Incidental	Minor	Moderate	Major	Severe	Catastrophic
Consequence Cost	<= USD 100K	USD 100–250K	USD 250K–1MM	USD 1–5MM	USD 5–20MM	> USD 20MM

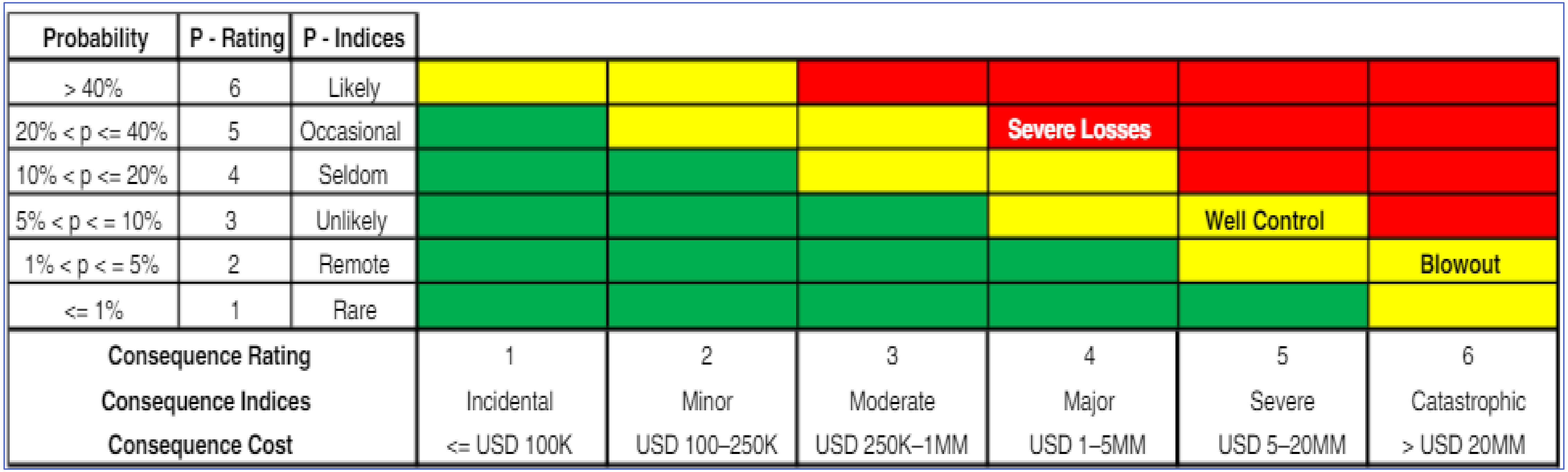


Probability	P - Rating	P - Indices
> 40%	6	Likely
20% < p <= 40%	5	Occasional
10% < p <= 20%	4	Seldom
5% < p < = 10%	3	Unlikely
1% < p < = 5%	2	Remote
<= 1%	1	Rare



🟨	🟨	🟥	🟥	🟥	🟥
🟩	🟨	🟨	🟥 Severe Losses	🟥	🟥
🟩	🟩	🟨	🟨	🟥	🟥
🟩	🟩	🟩	🟨	🟨 Well Control	🟥
🟩	🟩	🟩	🟩	🟨	🟨 Blowout
🟩	🟩	🟩	🟩	🟩	🟨
1	2	3	4	5	6

Risk Matrix (RM)



Probability	P - Rating	P - Indices						
> 40%	6	Likely	🟨	🟨	🟥	🟥	🟥	🟥
20% < p <= 40%	5	Occasional	🟩	🟨	🟨	🟥 Severe Losses	🟥	🟥
10% < p <= 20%	4	Seldom	🟩	🟩	🟨	🟨	🟥	🟥
5% < p < = 10%	3	Unlikely	🟩	🟩	🟩	🟨	🟨 Well Control	🟥
1% < p < = 5%	2	Remote	🟩	🟩	🟩	🟩	🟨	🟨 Blowout
<= 1%	1	Rare	🟩	🟩	🟩	🟩	🟩	🟨
Consequence Rating			1	2	3	4	5	6
Consequence Indices			Incidental	Minor	Moderate	Major	Severe	Catastrophic
Consequence Cost			<= USD 100K	USD 100–250K	USD 250K–1MM	USD 1–5MM	USD 5–20MM	> USD 20MM

Advantages of RM

- Identifies the gravest project risks.
- Creates and presents the risk situation with minimal effort (e.g. as an Excel diagram).
- Presents the risk situation visually and comprehensively.
- Presents the risk situation simply for everyone because no prior knowledge is required to understand it.
- Assesses the efficiency of your risk measures.

A risk matrix visualizes risks together with the possible extent of damage and their likelihood of occurring.

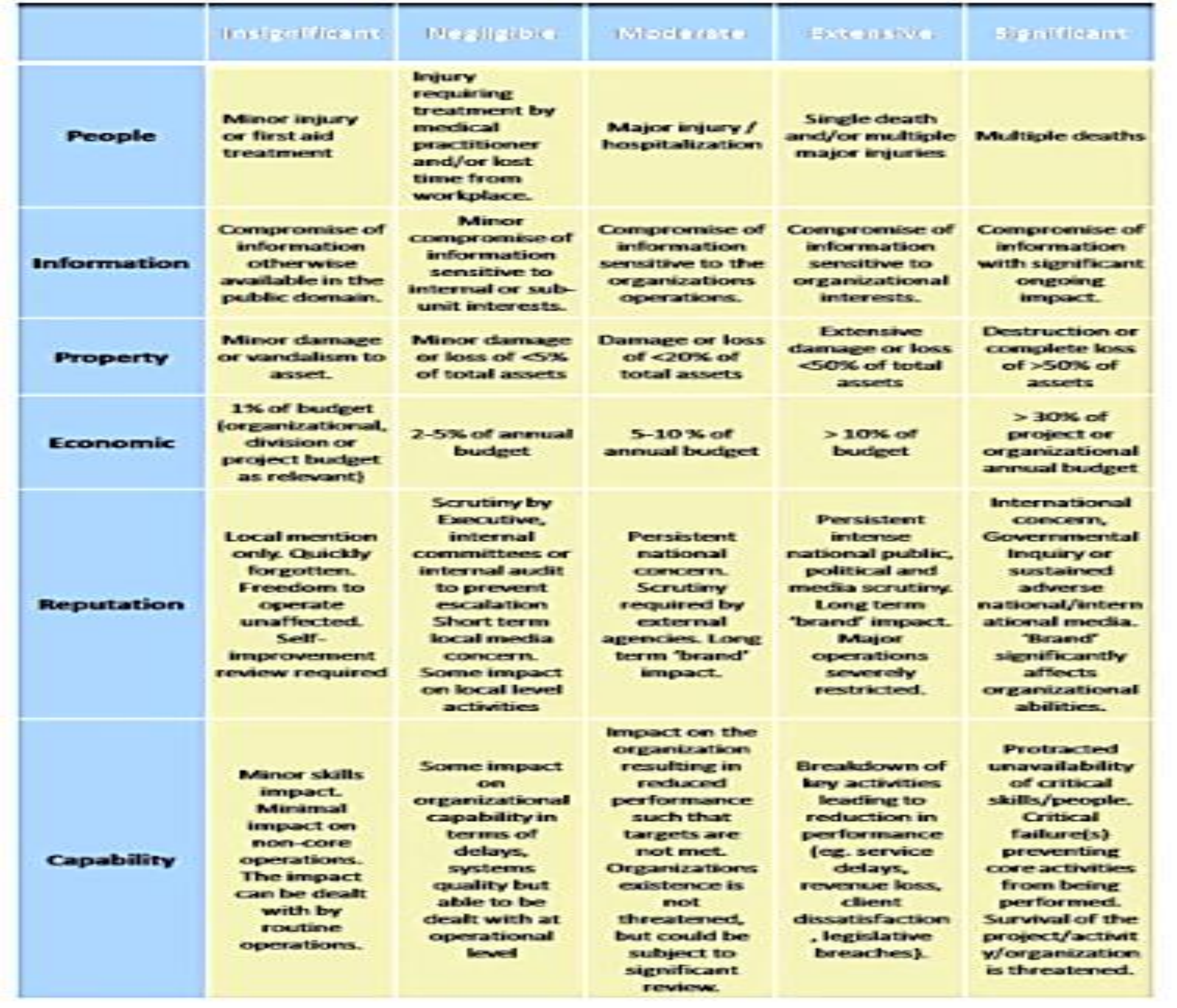
“What’s Wrong with Risk Matrices?” by Tony Cox

- They can correctly and unambiguously compare only a small fraction of randomly selected pairs of hazards and can assign identical ratings to quantitatively different risks.
- They can mistakenly assign higher qualitative ratings to quantitatively smaller risks to the point where with risks that have negatively correlated frequencies and severities, they can lead to worse-than-random decisions.
- They can result in suboptimal resource allocation as effective allocation of resources to risk treatments cannot be based on the categories provided by risk matrices
- Categorizations of severity cannot be made objectively for uncertain consequences. Assessment of likelihood and consequence and resulting risk ratings require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks.

Some other Problems

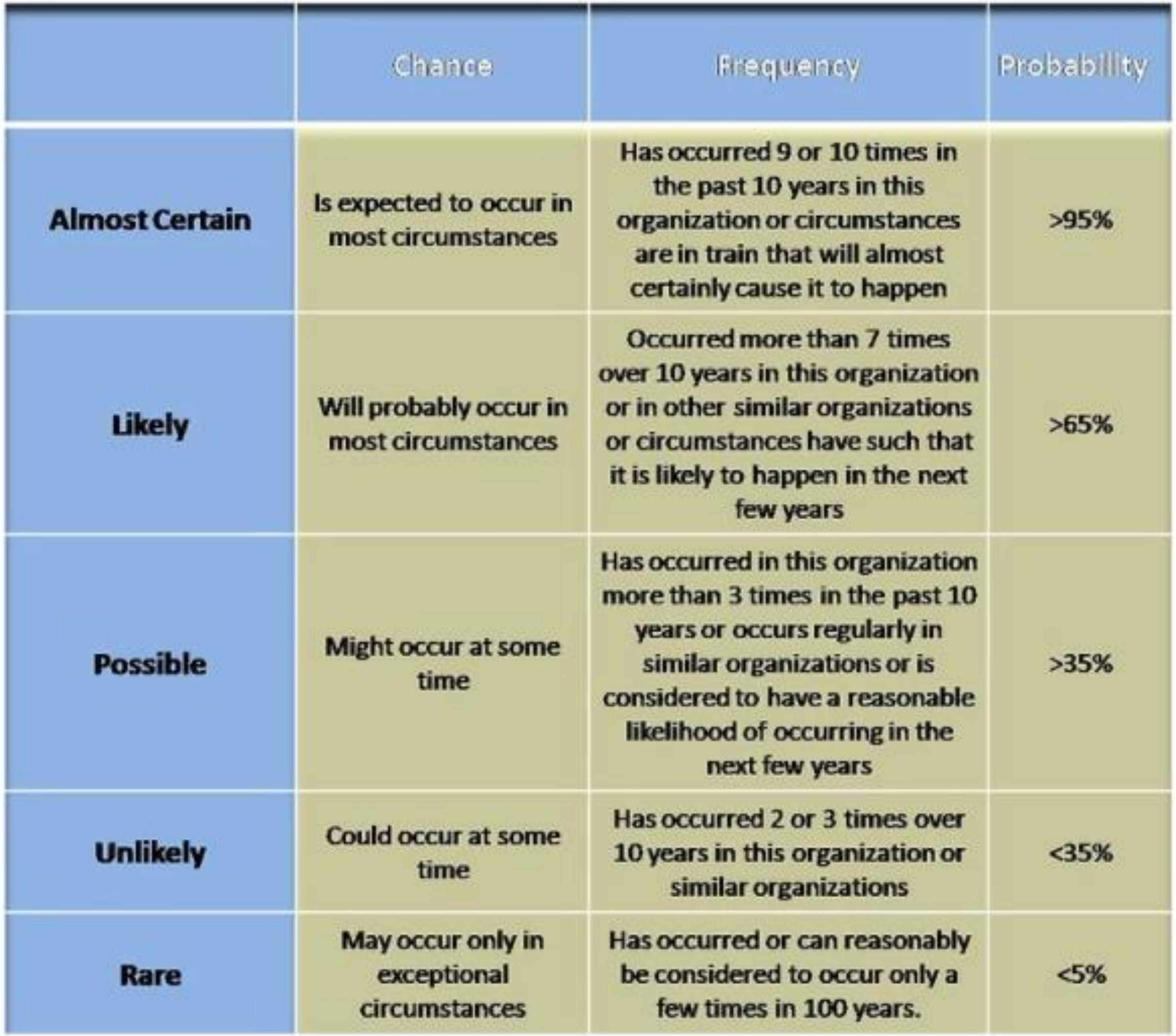
- Don’t include any assessment of timeframes.
- Ambiguous inputs and outputs.
- Can oversimplify the complexity or volatility of a risk.
- And many more.

Consequences



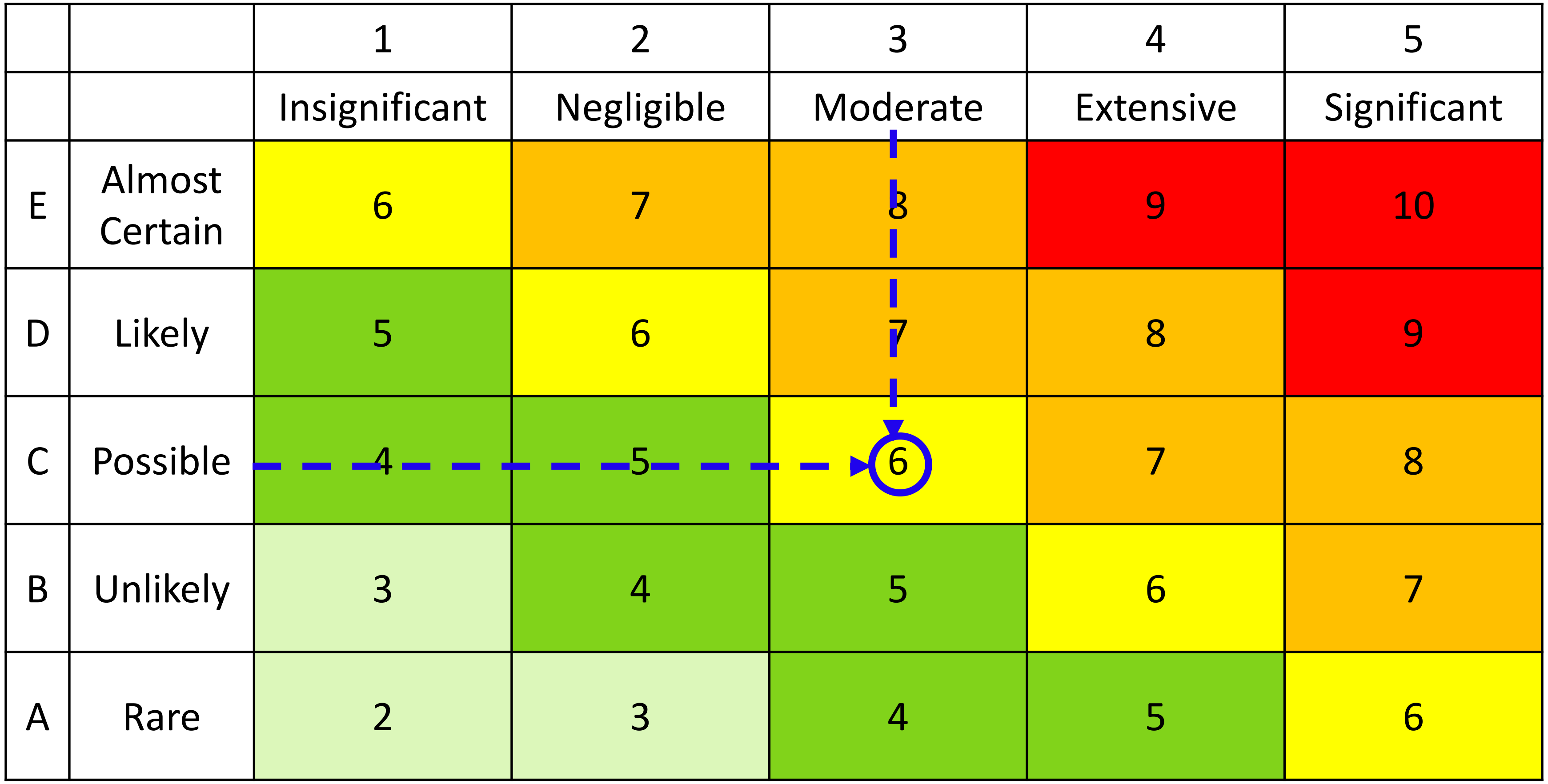
	Insignificant	Negligible	Moderate	Extensive	Significant
People	Minor injury or first aid treatment	Injury requiring treatment by medical practitioner and/or lost time from workplace.	Major injury / hospitalization	Single death and/or multiple major injuries	Multiple deaths
Information	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to the organizations operations.	Compromise of information sensitive to organizational interests.	Compromise of information with significant ongoing impact.
Property	Minor damage or vandalism to asset.	Minor damage or loss of <5% of total assets	Damage or loss of <20% of total assets	Extensive damage or loss <50% of total assets	Destruction or complete loss of >50% of assets
Economic	1% of budget (organizational, division or project budget as relevant)	2-5% of annual budget	5-10 % of annual budget	> 10% of budget	> 30% of project or organizational annual budget
Reputation	Local mention only. Quickly forgotten. Freedom to operate unaffected. Self-improvement review required	Scrutiny by Executive, internal committees or internal audit to prevent escalation. Short term local media concern. Some impact on local level activities	Persistent national concern. Scrutiny required by external agencies. Long term "brand" impact.	Persistent intense national public, political and media scrutiny. Long term "brand" impact. Major operations severely restricted.	International concern, Governmental Inquiry or sustained adverse national/international media. "Brand" significantly affects organizational abilities.
Capability	Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations.	Some impact on organizational capability in terms of delays, systems quality but able to be dealt with at operational level	Impact on the organization resulting in reduced performance such that targets are not met. Organizations existence is not threatened, but could be subject to significant review.	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches).	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organization is threatened.

Likelihood



	Chance	Frequency	Probability
Almost Certain	Is expected to occur in most circumstances	Has occurred 9 or 10 times in the past 10 years in this organization or circumstances are in train that will almost certainly cause it to happen	>95%
Likely	Will probably occur in most circumstances	Occurred more than 7 times over 10 years in this organization or in other similar organizations or circumstances have such that it is likely to happen in the next few years	>65%
Possible	Might occur at some time	Has occurred in this organization more than 3 times in the past 10 years or occurs regularly in similar organizations or is considered to have a reasonable likelihood of occurring in the next few years	>35%
Unlikely	Could occur at some time	Has occurred 2 or 3 times over 10 years in this organization or similar organizations	<35%
Rare	May occur only in exceptional circumstances	Has occurred or can reasonably be considered to occur only a few times in 100 years.	<5%

Damage or Loss of <20% of total assets: Moderate



		1	2	3	4	5
		Insignificant	Negligible	Moderate	Extensive	Significant
E	Almost Certain	6	7	8	9	10
D	Likely	5	6	7	8	9
C	Possible	4	5	[✓ 6]	7	8
B	Unlikely	3	4	5	6	7
A	Rare	2	3	4	5	6

Very Low	Managed by routine procedures
Low	Monitor and manage by routine procedures
Medium	Management responsibility must be specified
High	Senior management attention needed
Very High	Immediate action required by the executive with detailed planning, resource allocation, and regular monitoring

Lie Factor

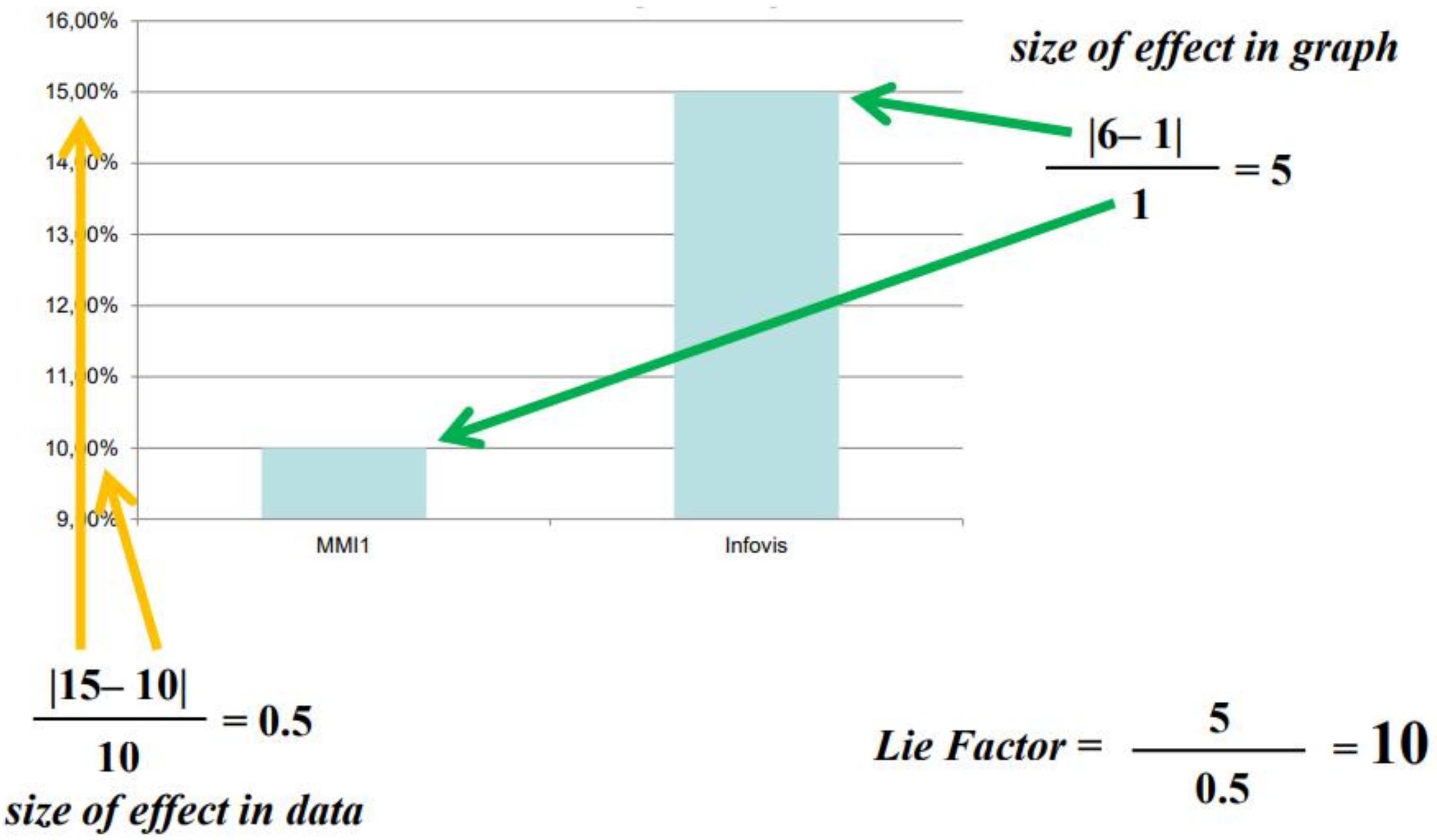
- A value to describe the relation between the **size of effect shown in a graphic** and the **size of effect shown in the data**.
- “The representation of numbers, as physically measured on the surface of the graphic itself, should be directly proportional to the quantities represented.” (Edward Tufte, “The Visual Display of Quantitative Information”, 1983.)

$$\text{Lie Factor} = \frac{\text{size of effect shown in graphic}}{\text{size of effect in data}}$$

$$\text{Size of effect} = \frac{|\text{second value} - \text{first value}|}{\text{first value}}$$

- **Lie Factor should be close to 1.**

Lie Factor



size of effect in graph

$$\frac{|6-1|}{1} = 5$$

$$\frac{|15-10|}{10} = 0.5$$

size of effect in data

$$\textit{Lie Factor} = \frac{5}{0.5} = 10$$

Calculate the Lie Factor

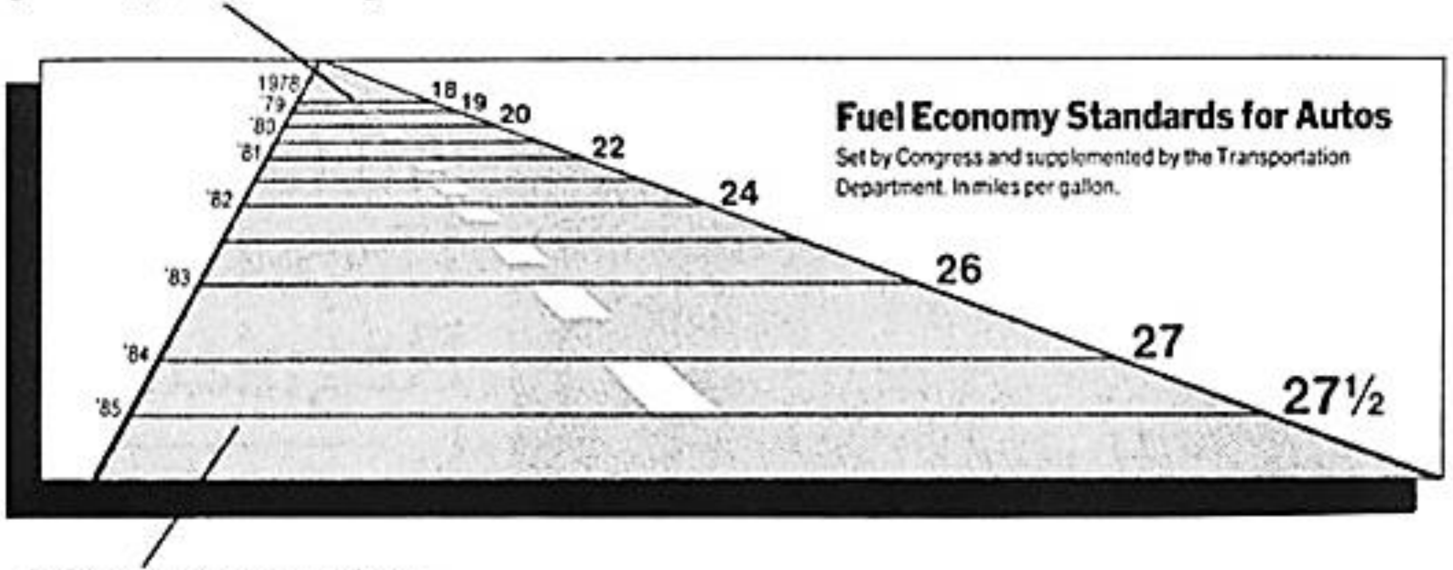
Size of Effect in Graph =$\frac{|5.3-0.6|}{0.6} = 7.83$

Size of Effect in Data =$\frac{|27.5-18|}{18} = 0.53$

Lie Factor=$\frac{7.83}{0.53} = 14.8$

The standard required an increase in mileage from 18 to 27.5, an increase of 53%. The magnitude of increase shown in the graph is 783%, which results in a lie factor of 14.8! [Friendly, 2005]

This line, representing 18 miles per gallon in 1978, is 0.6 inches long.



This line, representing 27.5 miles per gallon in 1985, is 5.3 inches long.

[Tufte, 1991]

Cyber Terrorism

- A wide range of moderate definitions for cyber terrorism were proposed, especially in the period between 1997 and 2001.
- The reason for the incoherence of the definitions stems from the fact that their origin lay in quite different expert fields such as law enforcement, international studies, anti-terror, information security, and information operations.

Cyber Terrorism Definition

The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents (FBI, 1997).

The use or threat of action designed to influence the government or an international governmental organisation or to intimidate the public, or a section of the public; made for the purposes of advancing a political, religious, racial or ideological cause.
It involves or causes:

- *serious violence against a person;*
- *serious damage to a property;*
- *a threat to a person's life;*
- *a serious risk to the health and safety of the public; or*
- *serious interference with or disruption to an electronic system (UK Terrorism Act 2000).*

A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda (FBI, 2004).

Cyber Terrorism Definition

The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting information and communication technology-based control of real-world physical processes; and it involves or causes:

- *violence to, suffering of, serious injuries to, or the death of (a) persons(s),*
- *serious damage to a property,*
- *a serious risk to the health and safety of the public,*
- *a serious economic loss,*
- *a serious breach of ecological safety,*
- *a serious breach of the social and political stability and cohesion of a nation.*

Emerging Threats

- Modern Living: Smart TV, Domotics.
- Health Sector: Pacemaker, insulin pumps.
- Finance: NFC
- Transport: Smart Vehicles
- Smart Meters: for gas, water, and other utilities.
- Smart Living: Smart Equipment (fridge, washing machine, etc.): platform for DDoS
- IoT

Ethical Issues in Computer Security

Disclaimer

The content is purely academical.

All contents are from the prescribed textbook.

There are no personal opinions involved.

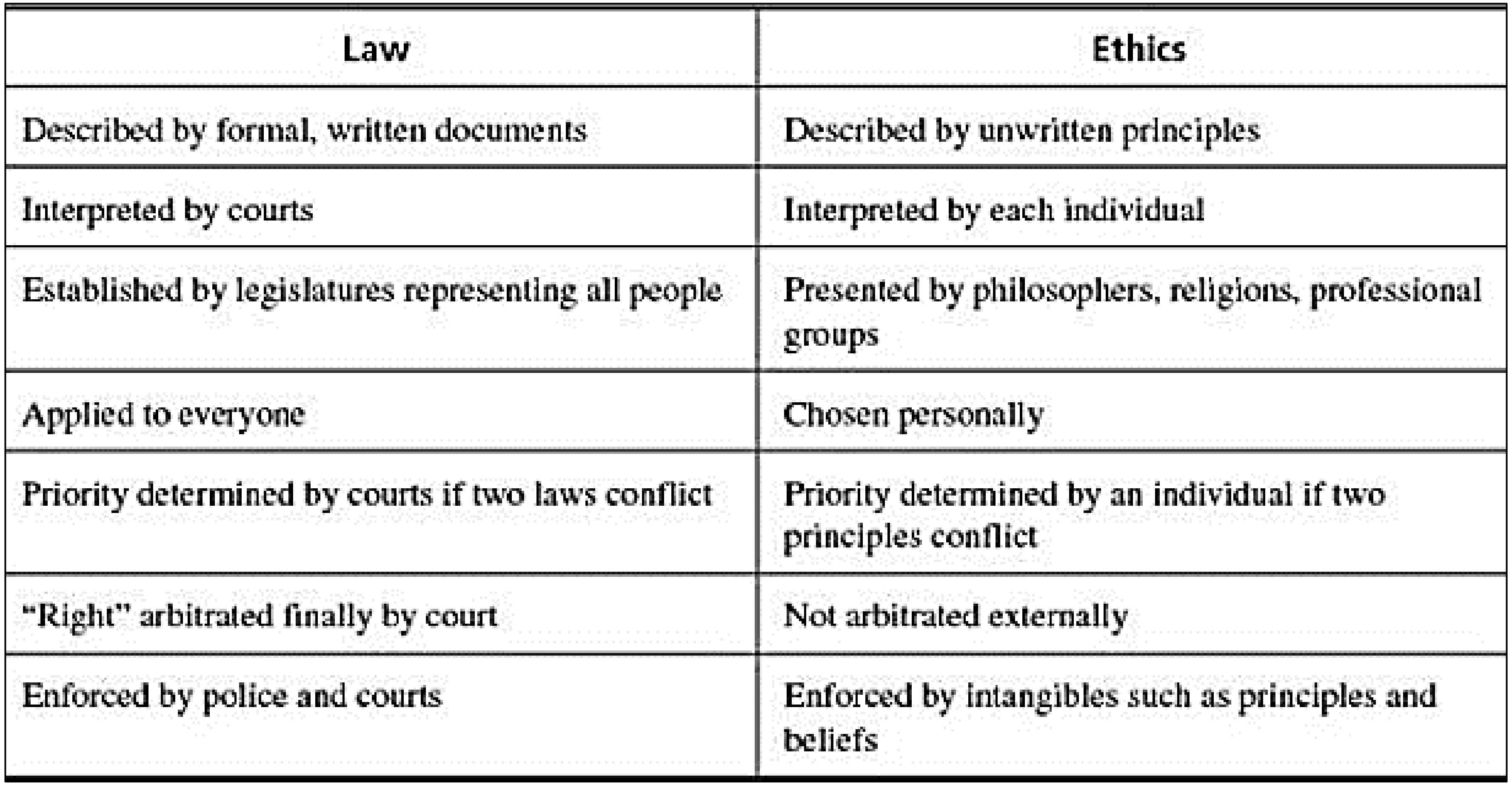
Ethical Issues in Computer Security

- Primary purpose: To explore some of the ethical issues associated with computer security and to show how ethics functions as a control.
- An **ethic** is an objectively defined standard of right and wrong.
- Ethical standards are often idealistic principles because they focus on one objective.
- In a given situation, however, several moral objectives may be involved, so people must determine **an action that is appropriate** considering **all the objectives.**
- A set of ethical principles is called an **ethical system**.

Law and Ethics

- Why ethics in Cyber Security?
- Difficult to think of all exceptions when drafting a law concerning computer affairs. Lawmakers may not be computer professionals.
- Even when a law is well conceived and well written, its enforcement may be difficult.
- Courts are overburdened.
- Impossible or impractical to develop laws to describe and enforce all forms of behavior acceptable to society.
- Society relies on ethics or morals to prescribe generally accepted standards of proper behavior.

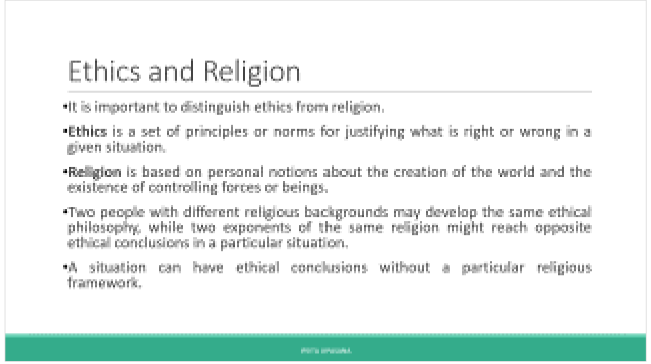
Differences Between the Law and Ethics



Law	Ethics
Described by formal, written documents	Described by unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures representing all people	Presented by philosophers, religions, professional groups
Applied to everyone	Chosen personally
Priority determined by courts if two laws conflict	Priority determined by an individual if two principles conflict
"Right" arbitrated finally by court	Not arbitrated externally
Enforced by police and courts	Enforced by intangibles such as principles and beliefs

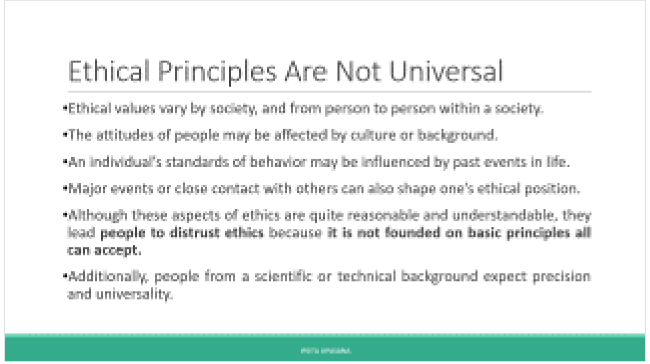
Studying Ethics

- Ethics are personal choices about right and wrong actions in a given situation.
- Difficult choices would be easier to make if there were a set of universal ethical principles to which everyone agreed.
- But the variety of social, cultural, and religious beliefs makes the identification of such a set of universal principles impossible.



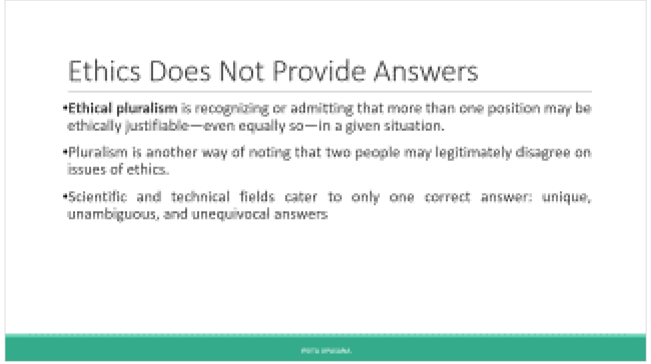
Ethics and Religion

- It is important to distinguish ethics from religion.
- **Ethics** is a set of principles or norms for justifying what is right or wrong in a given situation.
- **Religion** is based on personal notions about the creation of the world and the existence of controlling forces or beings.
- Two people with different religious backgrounds may develop the same ethical philosophy, while two exponents of the same religion might reach opposite ethical conclusions in a particular situation.
- A situation can have ethical conclusions without a particular religious framework.



Ethical Principles Are Not Universal

- Ethical values vary by society, and from person to person within a society.
- The attitudes of people may be affected by culture or background.
- An individual's standards of behavior may be influenced by past events in life.
- Major events or close contact with others can also shape one's ethical position.
- Although these aspects of ethics are quite reasonable and understandable, they lead **people to distrust ethics** because **it is not founded on basic principles all can accept.**
- Additionally, people from a scientific or technical background expect precision and universality.



Ethics Does Not Provide Answers

- **Ethical pluralism** is recognizing or admitting that more than one position may be ethically justifiable—even equally so—in a given situation.
- Pluralism is another way of noting that two people may legitimately disagree on issues of ethics.
- Scientific and technical fields cater to only one correct answer: unique, unambiguous, and unequivocal answers

Ethics and Religion

- It is important to distinguish ethics from religion.
- **Ethics** is a set of principles or norms for justifying what is right or wrong in a given situation.
- **Religion** is based on personal notions about the creation of the world and the existence of controlling forces or beings.
- Two people with different religious backgrounds may develop the same ethical philosophy, while two exponents of the same religion might reach opposite ethical conclusions in a particular situation.
- A situation can have ethical conclusions without a particular religious framework.

Ethical Principles Are Not Universal

- Ethical values vary by society, and from person to person within a society.
- The attitudes of people may be affected by culture or background.
- An individual’s standards of behavior may be influenced by past events in life.
- Major events or close contact with others can also shape one’s ethical position.
- Although these aspects of ethics are quite reasonable and understandable, they lead **people to distrust ethics** because **it is not founded on basic principles all can accept.**
- Additionally, people from a scientific or technical background expect precision and universality.

Ethics Does Not Provide Answers

- **Ethical pluralism** is recognizing or admitting that more than one position may be ethically justifiable—even equally so—in a given situation.
- Pluralism is another way of noting that two people may legitimately disagree on issues of ethics.
- Scientific and technical fields cater to only one correct answer: unique, unambiguous, and unequivocal answers

Ethics Does Not Provide Answers

Some scientists reject or misunderstand ethics. Why?

- Ethics has no underlying framework, or it does not depend on fundamental truths. But the basis of science is presumed to be "truth."
- A statement is expected to be provably true, provably false, or unproven, but a statement can never be both true and false. Ethics does not provide these clean distinctions.
- There is no higher authority of ethical truth.

Ethical Reasoning

- Study of ethics can yield two positive results.
- In situations in which we already know what is right and what is wrong, ethics should help us justify our choice.
- If we do not know the ethical action to take in a situation, ethics can help us identify the issues involved so that we can make reasoned judgments.
- There are two schools of ethical reasoning:
    - Consequence-Based Principles: based on the good that results from actions.
    - Rule-Based Principles: based on certain prima facie duties of people.

Examining a Situation for Ethical Issues

- Several steps to make and justify an ethical choice.
- Understand the situation. Learn the facts of the situation. Ask questions of interpretation or clarification. Attempt to find out whether any relevant forces have not been considered.
- Know several theories of ethical reasoning. To make an ethical choice, know how to justify it.
- List the ethical principles involved. What different philosophies could be applied in this case? Do any of these include others?
- Determine which principles outweigh others. This is a subjective evaluation. It often involves extending a principle to a logical conclusion or determining cases in which one principle clearly supersedes another.
- Make and defend an ethical choice.

Consequence-Based Principles

- **Teleology** is the general name applied to many theories of behavior which focus on the goal, outcome, or consequence of the action.
- The teleological theory of ethics focuses on the **consequences of an action**. The action to be chosen is the one that results in the greatest future good and the least harm.
- Two important forms of teleology: Egoism and Utilitarianism.
- **Egoism** is the form that says a moral judgment is based on the positive benefits to the person taking the action.
- For **utilitarianism**, the reference group is the entire universe. The utilitarian chooses that action that will bring the greatest collective good for all people with the least possible negative for all.

Rule-Based Principles

- **Deontology** states that certain things are good in and of themselves. These things that are **naturally good** are good rules or acts, which require no higher justification.
- Rule-deontology is the school of ethical reasoning that believes certain universal, self evident, natural rules specify our proper conduct.
- Certain basic moral principles are adhered to because of our responsibilities to one another; these principles are often stated as rights: the right to know, the right to privacy, the right to fair compensation for work.
- Sir David Ross lists various duties incumbent on all human beings:
    - Fidelity, Reparation, Gratitude, Justice, Beneficence, Nonmaleficence, Self-improvement.

Incident Analysis with Ethics

- How to react in incidents, keeping ethical standpoints.
- Examples.

Book

- Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015, Chapter 10, 11.
- Akhgar B., Staniforth A. and Bosco F., Cyber Crime and Cyber Terrorism Investigator's Handbook (1e), Syngress Publishing, 2014, Chapter 2, 3.