ITI8610 Software Assurance

Risk. Definitions. Taxonomy

Aleksandr Lenin

Risk

ISO Guide 73:2009:

A **risk** is an **effect of uncertainty on objectives**

Effect is the expectancy of the random outcome (either positive or negative)

Consider, for instance,
Financial risk (gambling, giving loans)
Security risk
Safety risk

What is a security risk?

- What is security?
- What is a security risk?

Security Considerations

- What are we afraid of?
- What to protect?
- Against what to protect?
- What are the potential consequences?
- What are the possibilities to protect?
- Are we protected reasonably enough?
- What would be the best coarse of action for the time being?

Assets

If an organization places any value on an item under its control and deems that item important enough to protect, it is labeled an asset for the purposes of risk management and analysis.

An asset is *anything* in the environment that has value to the stakeholders.

Assets

Assets include, but are not limited to:

Information : a file, a database, records on tape or other type of storage, ...

IT infrastructure : HW, SW, middleware, servers, services, networks, ...

Physical infrastructure : facilities, premises, equipment, devices, ...

Competitive advantage : products, processes, technology, know-hows, business secrets, ...

Assets

Financial : stocks, debtors, investors, market share, ...

Intangibles : relationship with clients, allies, partners, contractors, competitors, ...

Personnel : top-level management, top-quality specialists, other irreplaceable key personnel, ...

...

Asset Value

- What are the value of an asset to the company?
- How big are the maintenance expenses?
- How much profit does it bring to the company?
- How much would it be worth to the competition?
- How much would it cost to recreate or recover?
- How much does it cost to acquire or develop?
- How much liability are you under pertaining to protection of this asset?

Asset Value

Issues that contribute to the value of an asset

Purchase cost	Development cost	Administrative / management cost
Maintenance cost	Cost to acquiring	Cost to protect and sustain
Value to owners and users	Value to competitors	Intellectual Property (IP) value
Market value (sustainable price)	Replacement Cost	Productivity enhancement or degradation
Operational costs	Liability of asset loss	Usefulness

Threats

Any *potential occurrence of an event* that may *cause undesirable outcome* for an organization as a whole or for a specific asset is a *threat*.

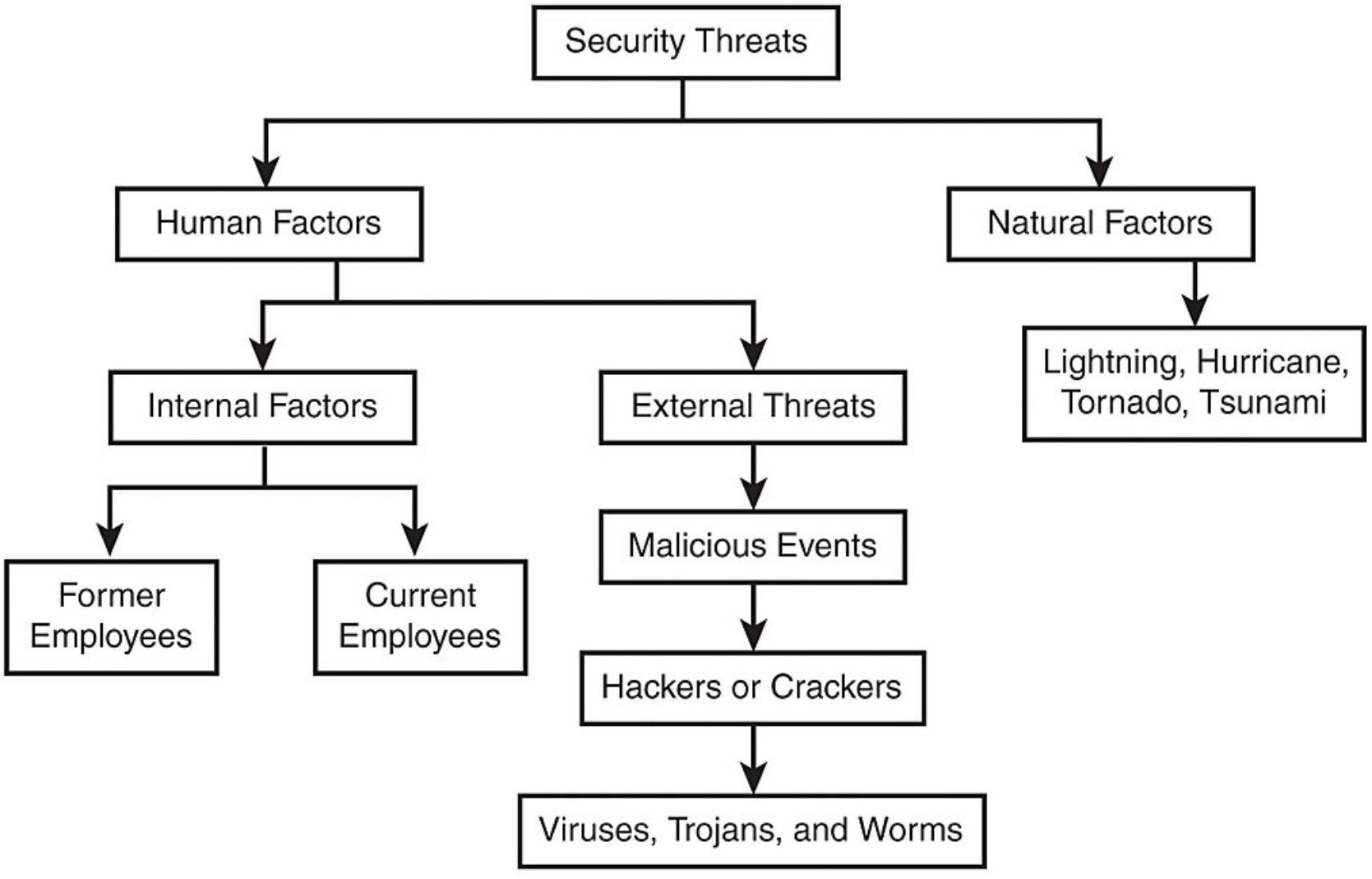
Threats are targeted against and *affect* one or more *assets*.

Threats may be *environmental* and *human-made* (intentional and unintentional/accidental).

Threats may originate from individuals, organizations, HW, SW, networks, structure, or nature.

Threat *consequences* have varying degree of severity.

Threats


Security Threats
Human Factors
Natural Factors
Internal Factors
External Threats
Lightning, Hurricane, Tornado, Tsunami
Former Employees
Current Employees
Malicious Events
Hackers or Crackers
Viruses, Trojans, and Worms

Threat Categories

Physical damage: fire, water, vandalism, power loss, natural disasters

Human interaction: accidental or intentional action or inaction that can disrupt productivity

Equipment malfunction: failure of systems and devices

Misuse of data: selling trade secrets, disclosure, fraud, espionage, theft

Loss of data: intentional or unintentional loss of information through destructive means

...

Vulnerability

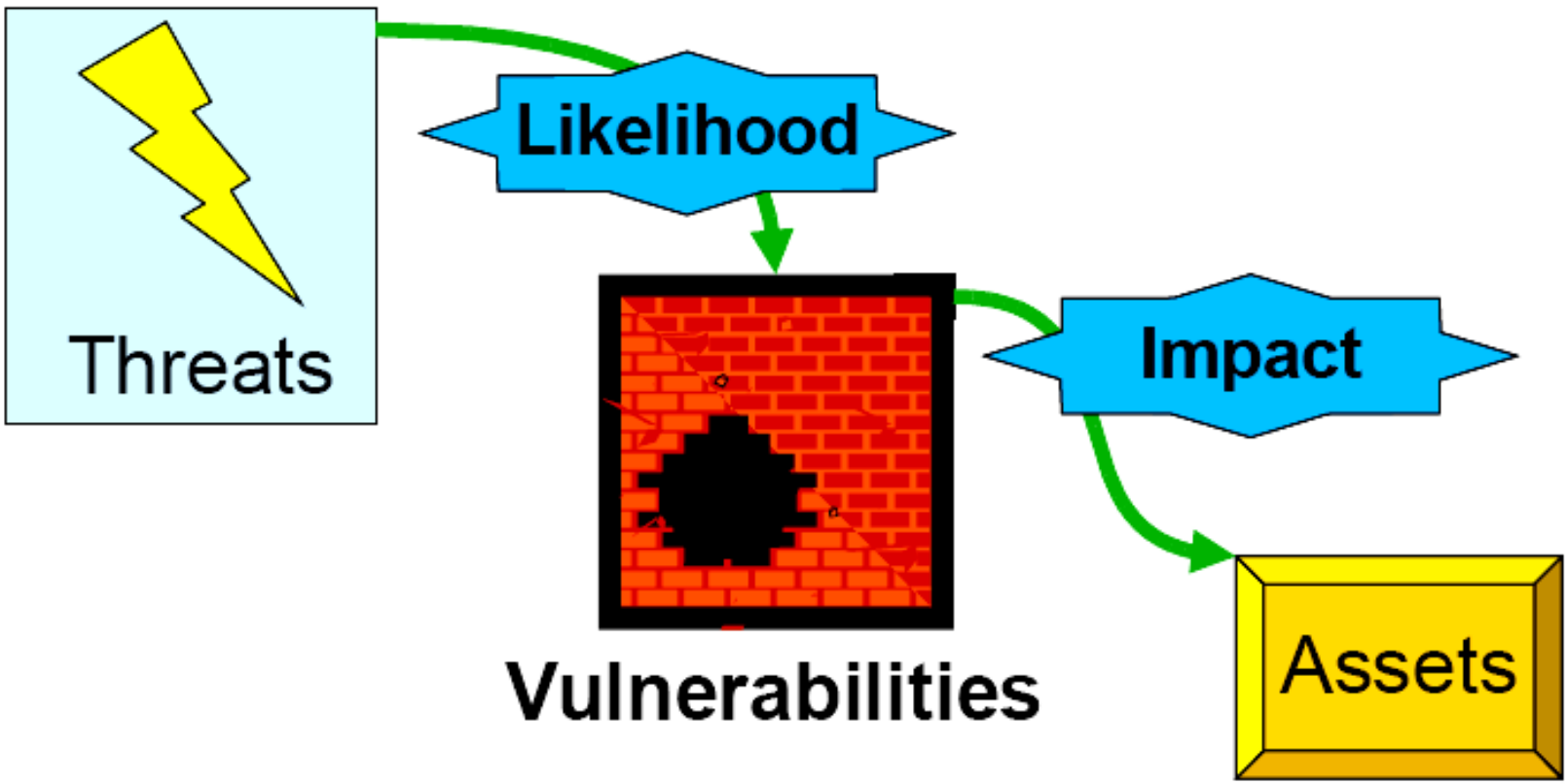
A *vulnerability* is a characteristic of any aspect of the infrastructure that renders it, or some portion of it, susceptible to damage and compromise.

A flaw, loophole, oversight, error, limitation, susceptibility in the infrastructure or any other aspect of an organization, the absence of or the weakness of a security measure. is called a vulnerability.

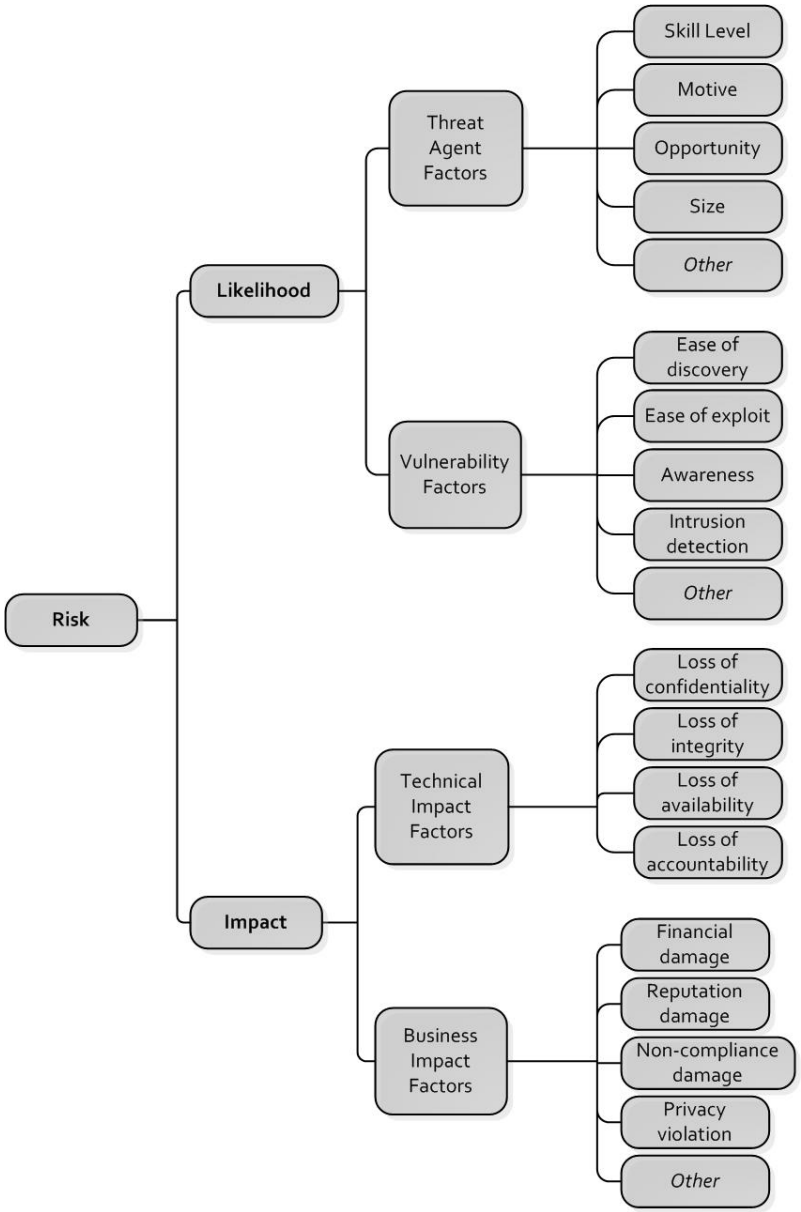
If a vulnerability is exploited, loss or damage to assets may occur.

Threat agents intentionally exploit vulnerabilities.

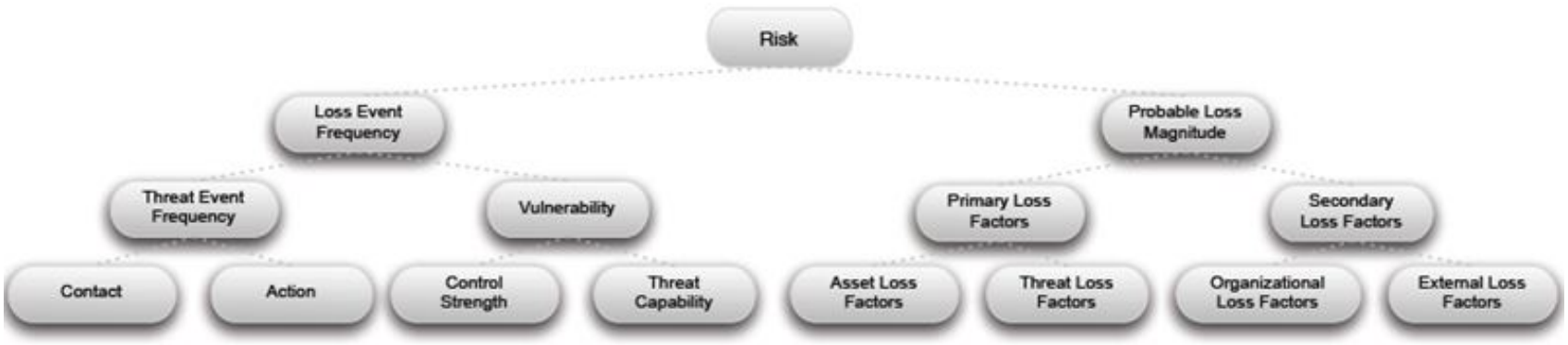
Terminology Recap



OWASP Decomposition of Risk Factors



The Open Group Risk Taxonomy



The Open Group Risk Taxonomy

Impact

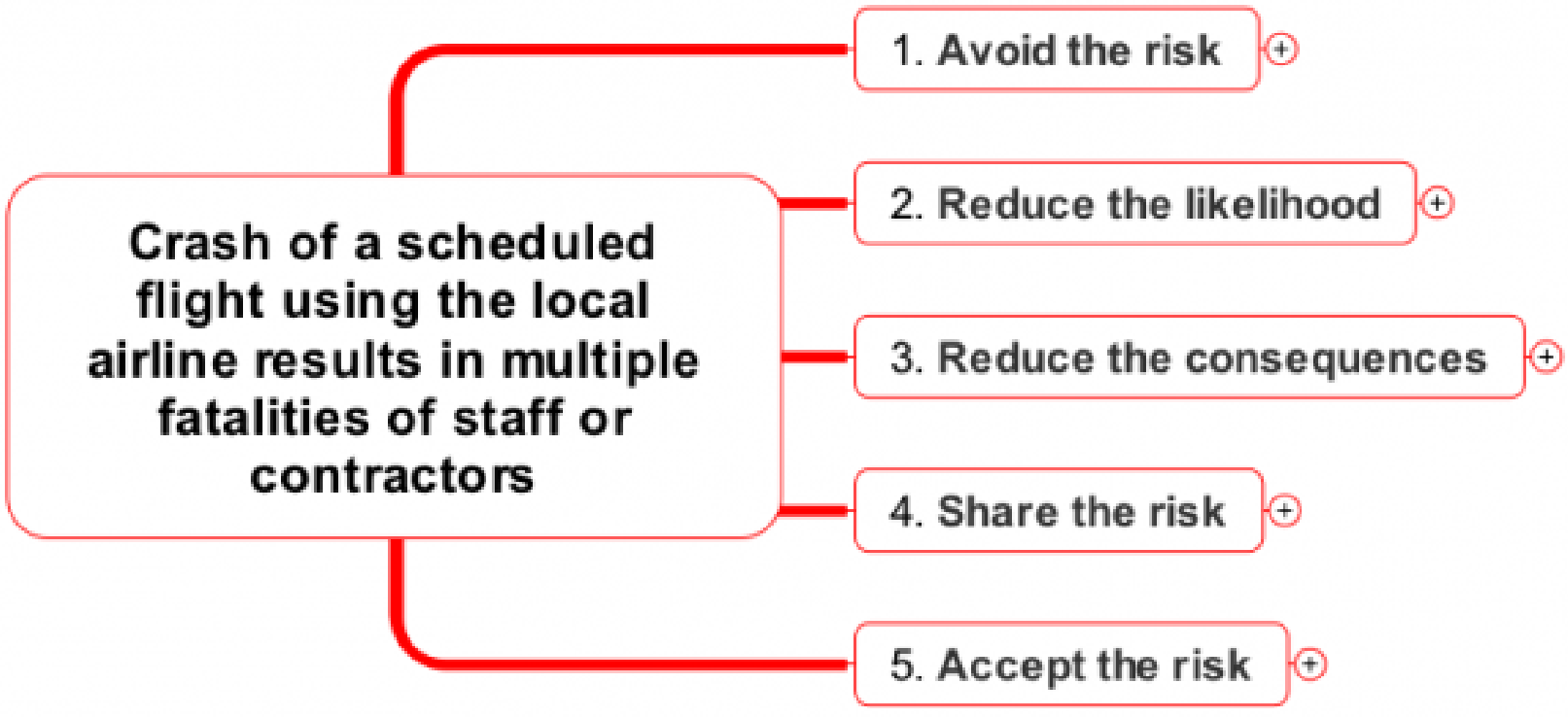
Impact is an estimation for loss in the case of threat materialization

Is usually measured in monetary units

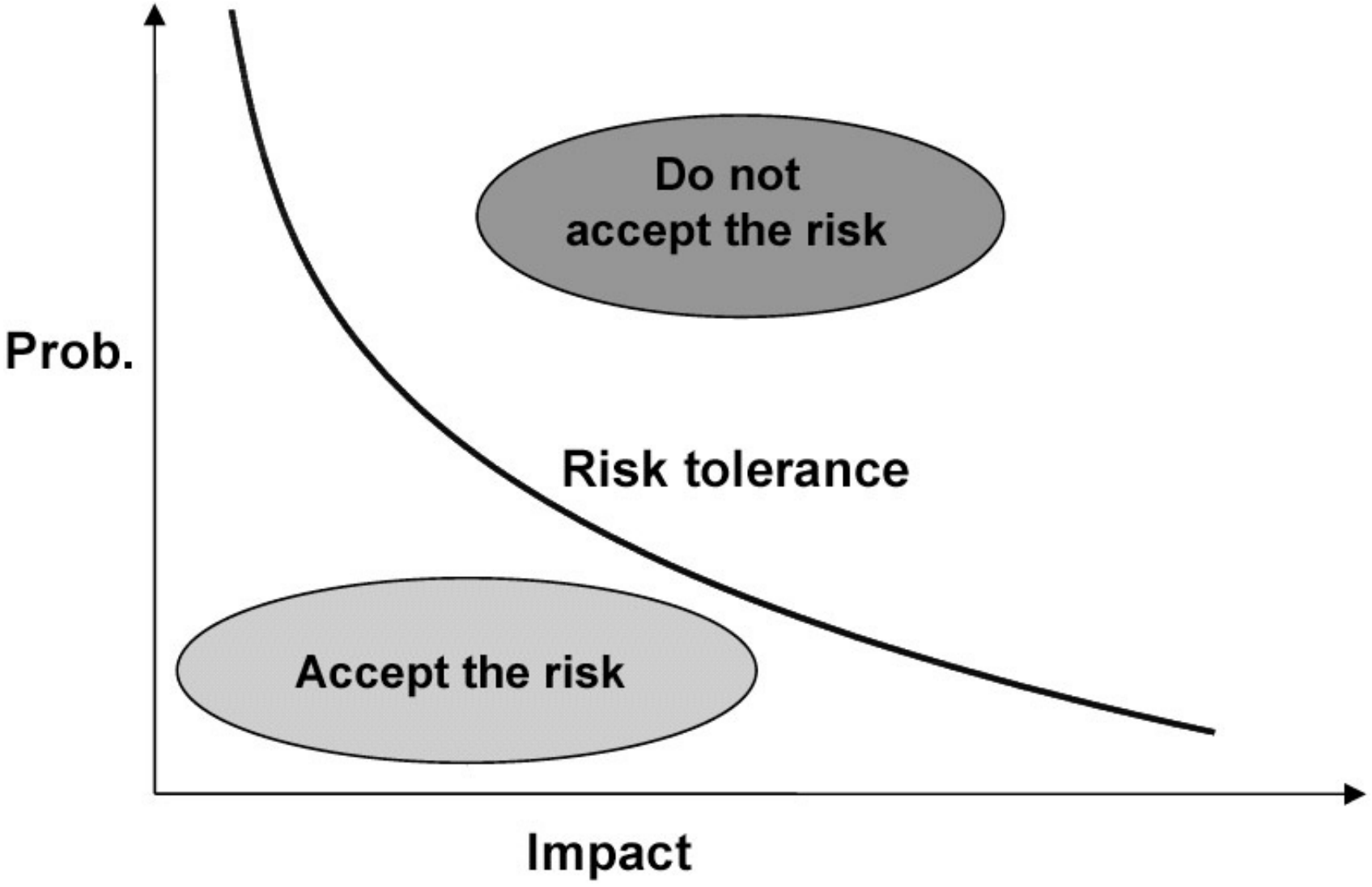
Impact does not mean that an event resulting in loss is actually occurring or will occur in foreseeable future

Risk Treatment

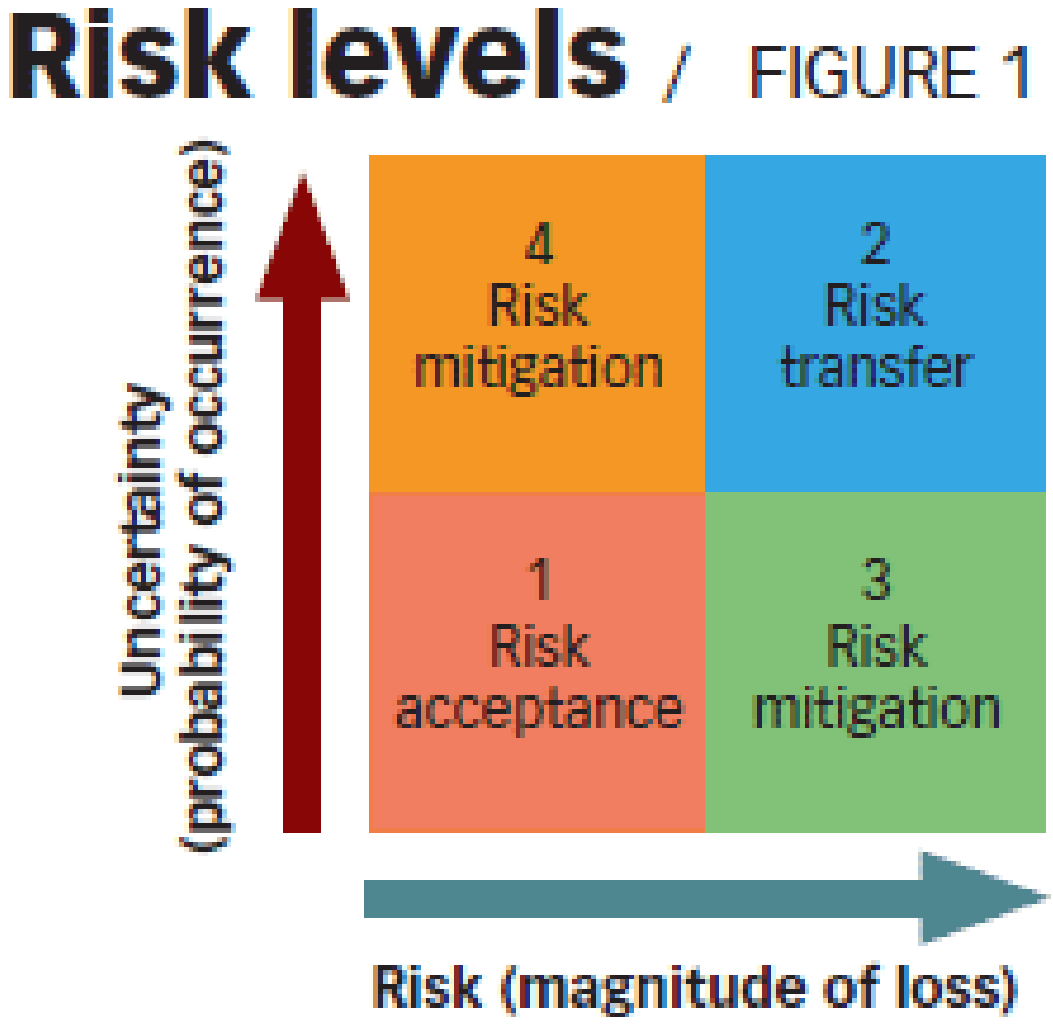
Risk Treatment



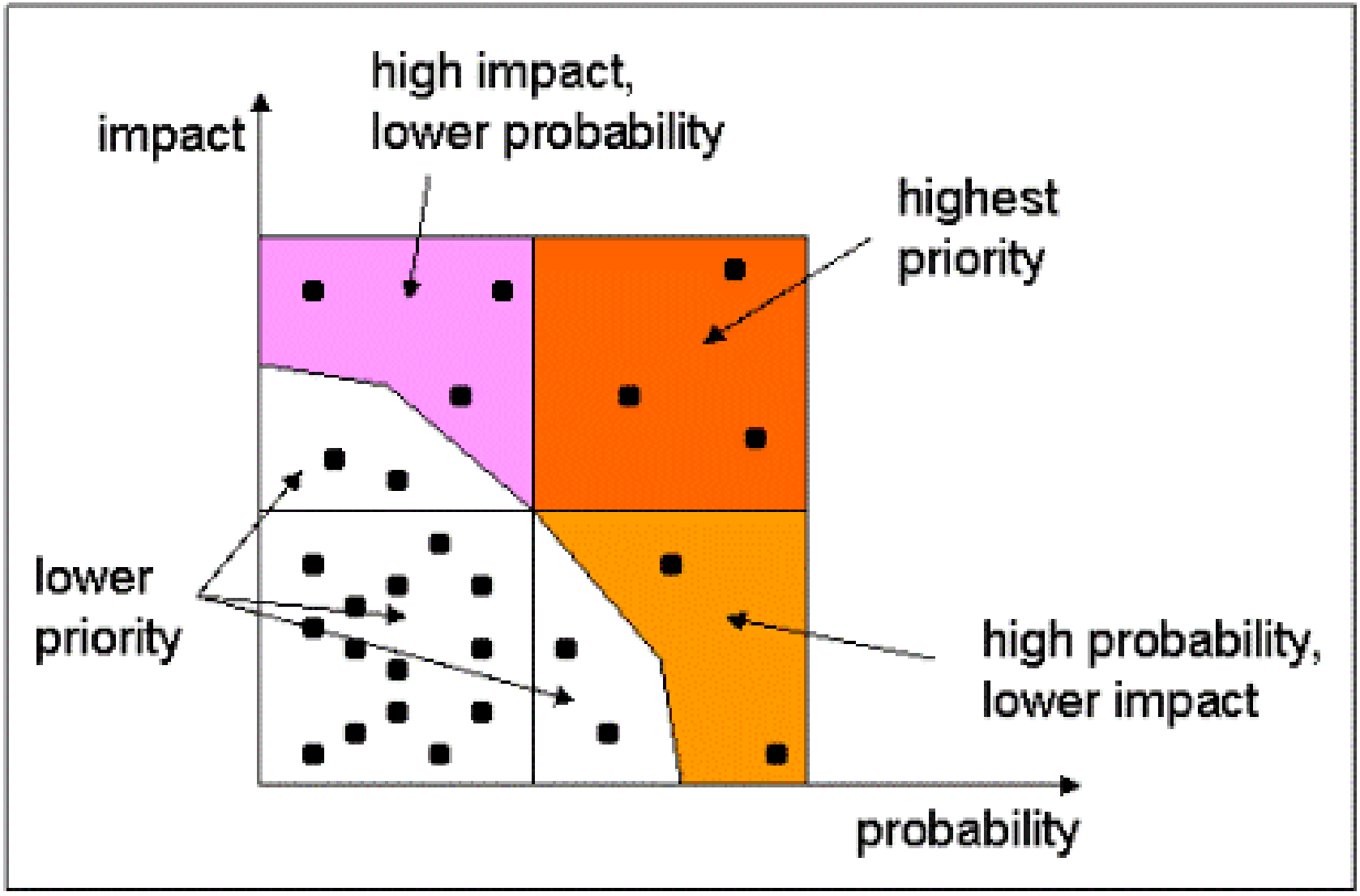
Risk Treatment



Risk Treatment



Risk Treatment



Security Controls

Security controls are the only means by which risks are mitigated.

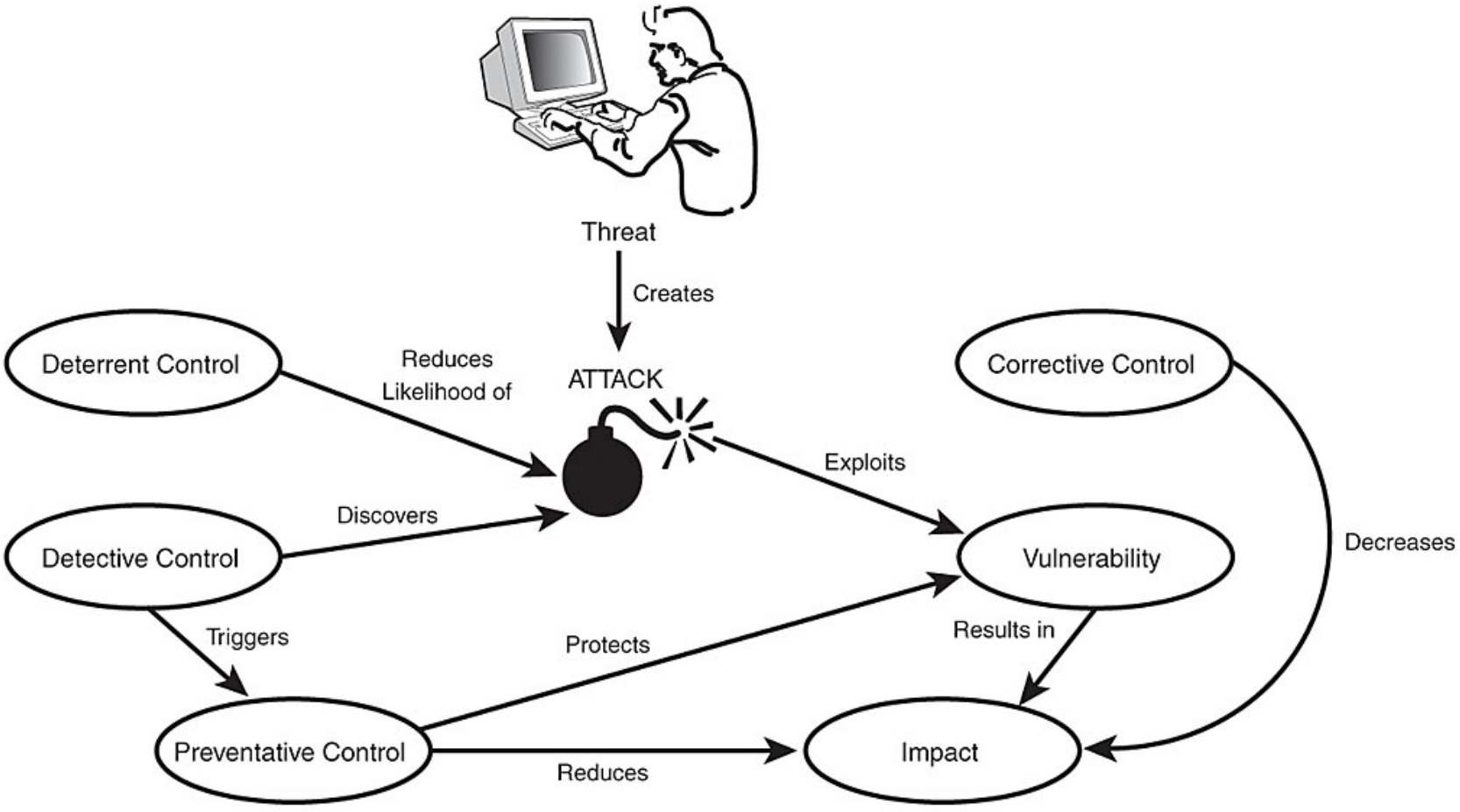
- Installing a SW patch
- Making a configuration change
- Hiring physical security guards
- Installing security surveillance cameras
- Electrifying a fense
- Hardening security policies and operational procedures
- ...

Security Controls

Cost of a security control includes, but is not limited to:

- Cost of purchase, development and licensing
- Cost of implementation, integration and customization
- Cost of deployment and annual operation
- Cost of maintenance and administration
- Cost of annual repairs and upgrades
- Productivity improvement or loss
- Changes to environment
- Cost of testing and evaluation

Security Controls



Residual Risk

The risk that remains after the security measures have been deployed.

Relates to any threats to the considered assets against which the higher-level management chooses not to deploy a corresponding security measure.

Risk that management has chosen to accept rather than mitigate.

Risk Levels

Strategic	high-level goals, aligned with and supporting the mission
Tactical	tactical goals, programs, projects, resources
Operational	effective and efficient use of resources
Reporting	reliability of reporting
Compliance	compliance with applicable laws and regulations

Risk Levels

Risk Management (in general):

- Looks at various possibilities of loss
- Determines what could cause greatest loss
- Applies controls appropriately

Risk Levels

Strategic Planning:

- Produces fundamental long-term security decisions and actions
- Shapes and guides what is needed and how it can be achieved
- Includes
  - broad scale information gathering
  - exploration of alternatives
  - puts an emphasis on future applications

Risk Levels

Tactical Security Management:

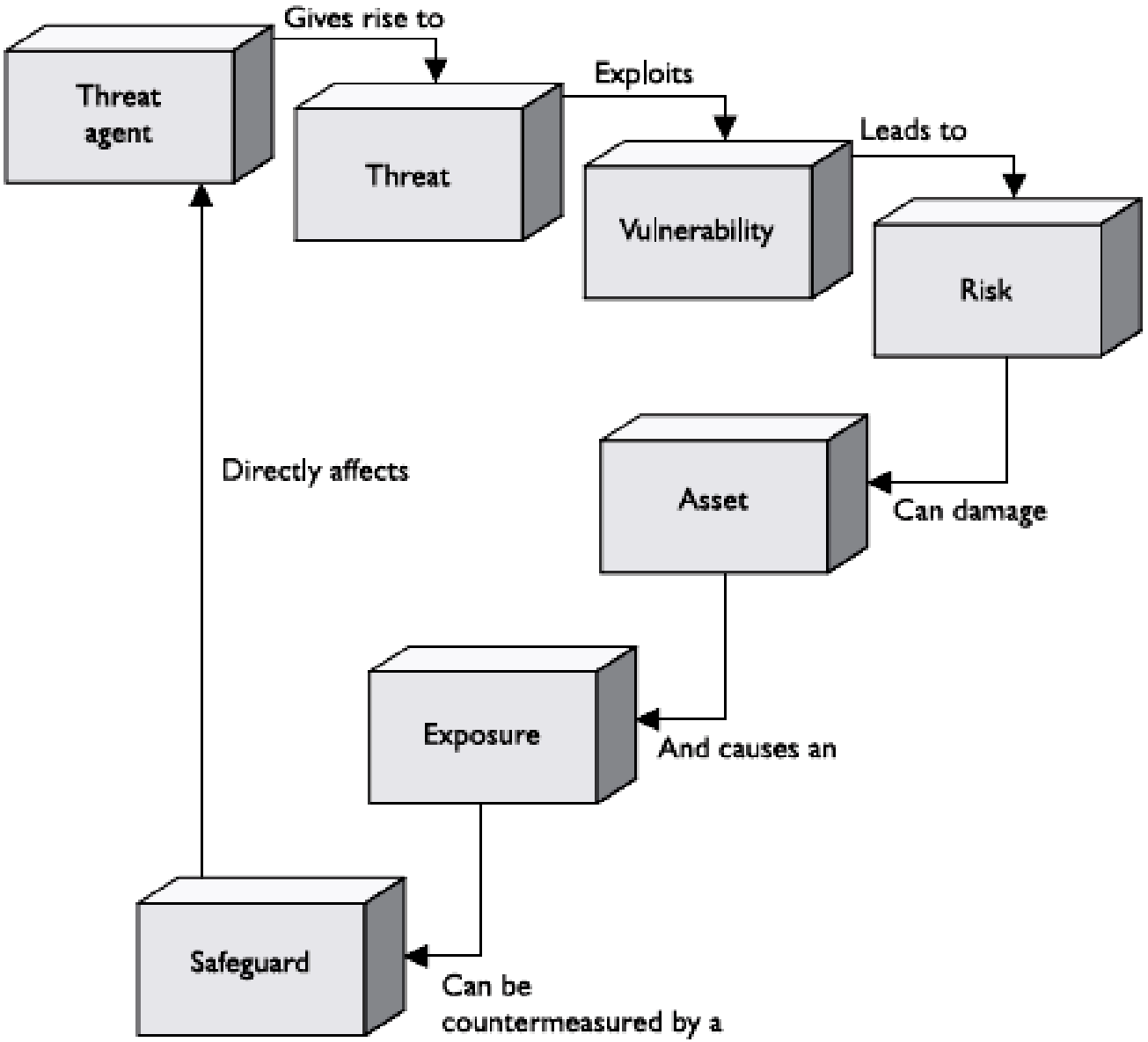
- Addresses daily operations that keep enterprise viable
- Managers set very general goals that require more than one year to achieve
- Tactical plans provide specifics for implementing the strategic plan

Risk Levels

Operational Security Management:

- Short-term plans concerning day-to-day work
- Aligned with long-term goals
- Supports tactical plans
- Examples:
  - Policies
  - Procedures
  - Methods
  - Rules
  - ...

Risk Components



How do we measure risk?

- Use a structured methodology
- Predefine general values to avoid confusion
- Identify risks
- Straightforward way:
  - Define the expected damage for each threat
  - Calculate Risk = Probability $\times$ Damage Potential
  - Use some risk assessment framework – estimate the values of risk components, i.a. with a defined risk taxonomy

Qualitative Approaches:

- The Delphi technique
- Scenarios
- Frameworks, i.e. FAIR (Factor Analysis of Information Risk)

Quantitative approaches

- availability of statistical data
- relying on expert estimations - unreliable
- different models requiring varying parameters