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*.

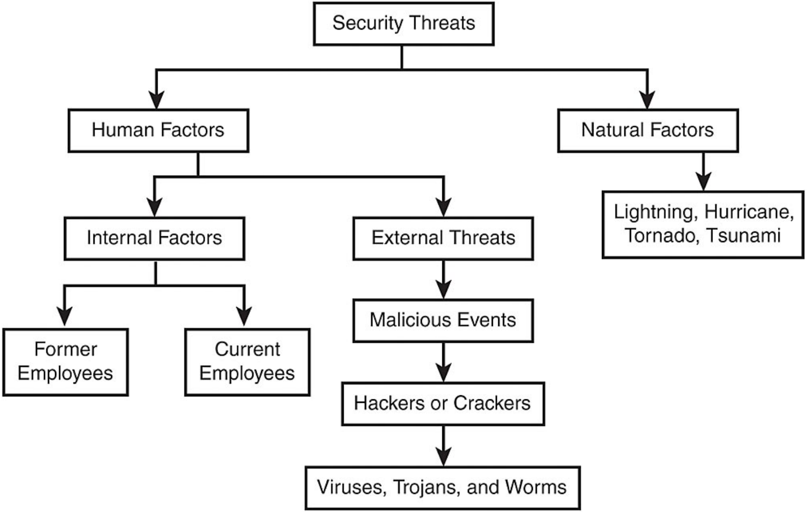
Threats are targeted against and *affect* one or more *assets*.

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

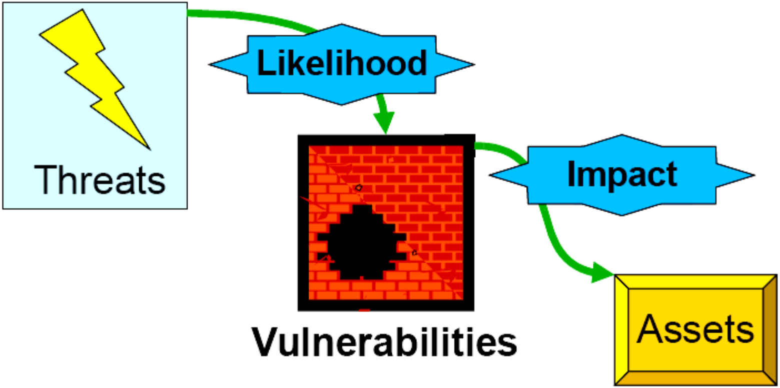
A *vulnerability* is a characteristic of any aspect of the infrastructure that renders it, or some portion of it, susceptible to damage and compromise.

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.

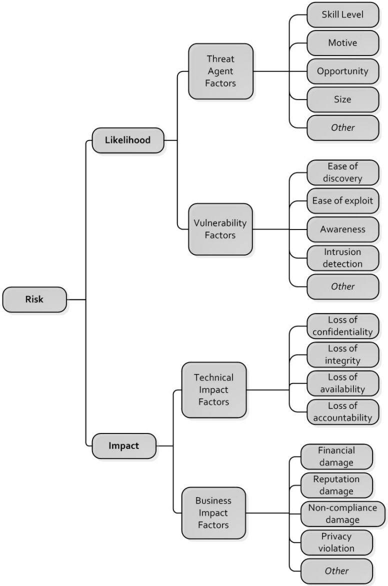
If a vulnerability is exploited, loss or damage to assets may occur.

Threat agents intentionally exploit vulnerabilities.

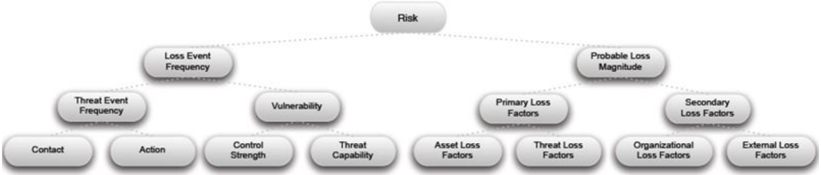
Terminology Recap



OWASP Decomposition of Risk Factors



The Open Group Risk Taxonomy



The Open Group Risk Taxonomy

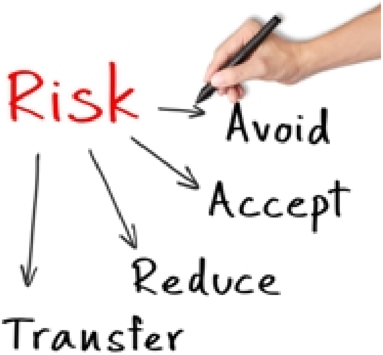
Impact

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

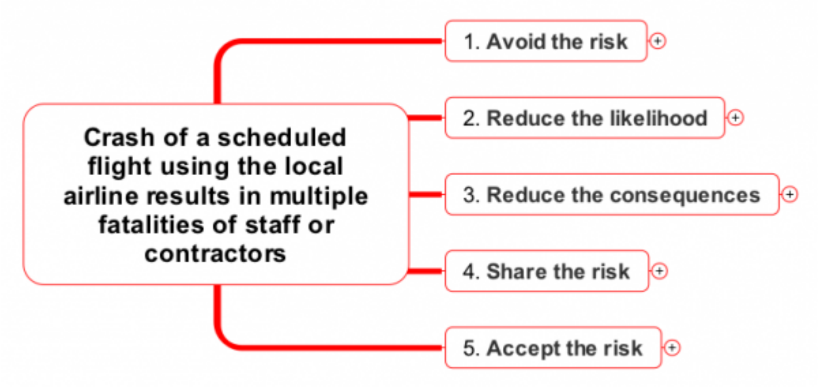
Is usually measured in monetary units

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

Risk Treatment



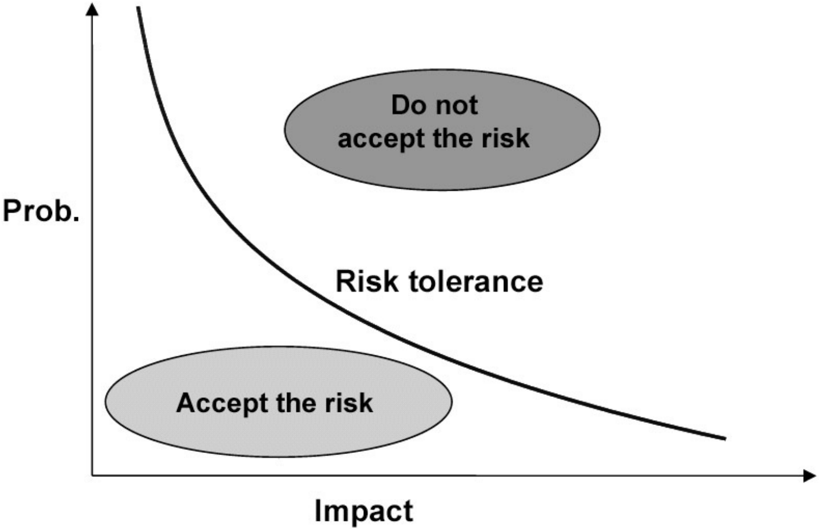
Risk Treatment



Crash of a scheduled flight using the local airline results in multiple fatalities of staff or contractors

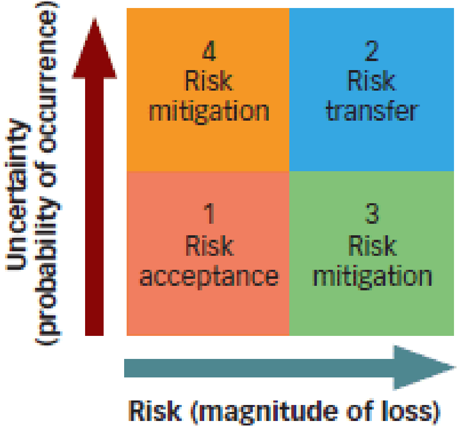
1. Avoid the risk
2. Reduce the likelihood
3. Reduce the consequences
4. Share the risk
5. Accept the risk

Risk Treatment



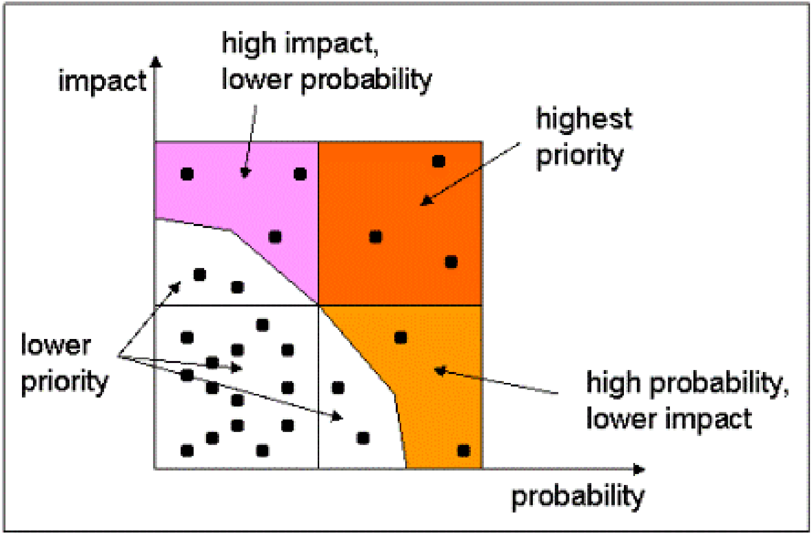
Risk Treatment

Risk levels / FIGURE 1



4 Risk mitigation	2 Risk transfer
1 Risk acceptance	3 Risk mitigation

Risk Treatment



Security Controls

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

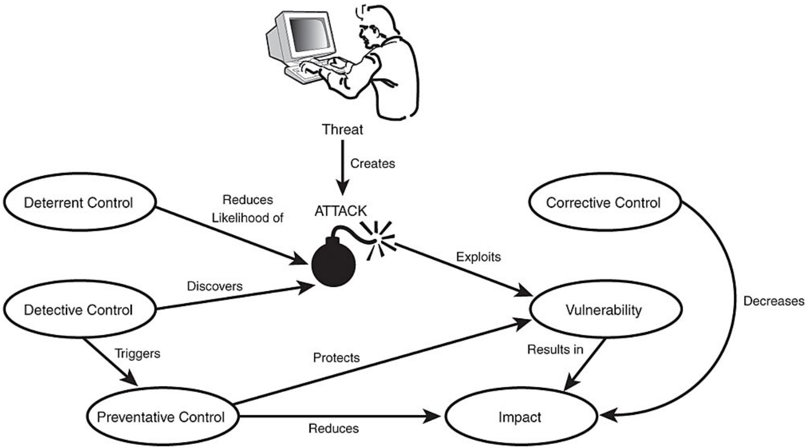
- Installing a SW patch
- Making a configuration change
- Hiring physical security guards
- Installing security surveillance cameras
- Electrifying a fense
- Hardening security policies and operational procedures
- ...

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.

Financial Risk

- Types of risk related to financing, including financial transactions, loans, etc.
- Often is understood to include only the potential or financial loss and uncertainty about its extent
- Portfolio Theory by Harry Markowitz (1952) – the science of managing market and financial risks
- Modern portfolio theory uses slightly different definitions of risk

Financial Risk

Main categories of financial risk are:

- Asset-backed risk – risks related to interest rate, term modification, prepayment
- Credit risk
- Foreign investment risk
- Liquidity risk – liquidity of assets and funding
- Market risk – equity risk, interest rate risk, currency risk, commodity risk
- Model risk
- Operational risk (including legal risk)

Financial Risk

Typically, financial risk is measured in terms of Annual Loss Expectancy (ALE)

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

Annual Loss Expectancy (ALE) – expected total yearly loss of all instances of a specific threat against a specific asset

Single Loss Expectancy (SLE) – impact associated with a single materialized risk against a specific asset.

Annual Rate of Occurrence (ARO) – expected frequency with which a specific threat or risk will occur within a single year.

Single Loss Expectancy

$$\text{SLE} = \text{Asset value} \times EF$$

EF (Exposure Factor) is percentage of loss in asset value in the result of threat occurrence

SLE is expressed as a monetary value

Imagine that you've got a system worth $100'000$ EUR. In the event of a fire, the remains the system will be worth 8000 EUR. In the event of fire, the asset will lose 92% of its value – therefore EF is 0.92

$$\text{SLE} = 100'000 \times 0.92 = 92000 \text{ EUR}$$

Annualized Rate of Occurrence

ARO is the expected frequency with which a single risk will occur within a year.

ARO value 0.0 means that a risk will never occur within a single year.

ARO may range from 0.0 to very large numbers indicating frequent occurrence of risk

ARO calculation is known as frequency determination. It is calculated by multiplying the likelihood of a single occurrence by the number of threat agents who would initiate the treat

For example, ARO of an earthquake in a city may be 0.00001, however, an ARO of a workstation infection in an office may be $10'000'000$.

Annual Loss Expectancy

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

If SLE of an asset is $90'000$ EUR and the ARO of the considered threat (such as total power loss) is 0.5, then the ALE is $90'000 \times 0.5 = 45'000$ EUR.

If the ARO for a specific threat were 15 (e.g. a compromised user account), the ALE would be $1'350'000$ EUR.

ALE Revisited

- Calculate ALE for the asset in the case when the security measure is deployed
  - This requires calculation of EF and ARO specific to the considered security measure
- Rationale baseline:
  - *the annual cost of security measure should not exceed the annual loss for the asset being protected by the security measure*

ALE Revisited

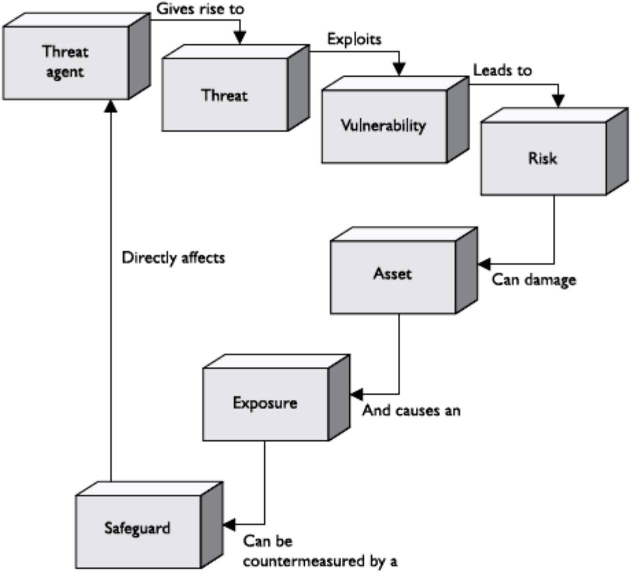
Value of the security measure to the company:

$$\begin{aligned}&\text{ALE before security measure deployment} -\\ &\text{ALE after security measure deployment} -\\ &\text{annual cost of the security measure}\end{aligned}$$

- If the result is negative, it is not rational to invest into the considered security measure
- If the result is positive, that value is the *annual savings* and the organization can benefit from investing into such a security measure and deploying it – it is worth its costs.

The annual savings or loss from a security measure should not be the only factor considered when evaluating available security measures

Risk Components



How do we measure risk?

- Use a structuted methodology
- Predefine general values to avoid confusion
- Identify risks
- Straightforward way:
  - Define the expected damage for each threat
  - Calculate Risk = Probability × Damage Potential
  - Try to estimate the values of risk components

Qualitative Approaches:

- The Delphi technique
- Scenarios
- FAIR (Factor Analysis of Information Risk)

Risk assessment matrices

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

thank you for your

attention