1.
competitive advantage

2.
avoidance of competitive disadvantage

3.
risk management

4.
risk assessment

5.
risk identification

6.
risk control

7.
risk tolerance

8.
Risk appetite

9.
residual risk

10.
dumpster diving

2.
The adoption and implementation of a business model, method, technique, resource, or technology to prevent being outperformed by a competing organization; working to keep pace with the competition through innovation, rather than falling behind.

1.
The adoption and implementation of an innovative business model, method, technique, resource, or technology in order to outperform the competition.

4.
A determination of the extent to which an organization's information assets are exposed to risk.

3.
The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.

6.
The application of controls that reduce the risks to an organization's information assets to an acceptable level.

5.
The recognition, enumeration, and documentation of risks to an organization's information assets.

8.
The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

7.
See *risk appetite*.

10.
An information attack that involves searching through a target organization's trash and recycling bins for sensitive information.

9.
The risk to information assets that remains even after current controls have been applied.

11.
security clearance

12.
data classification scheme

13.
clean desk policy

14.
threat assessment

15.
asset valuation

16.
threats-vulnerabilities-assets (TVA) worksheet

17.
attack success probability

18.
threats-vulnerabilities-assets (TVA) triples

19.
Loss frequency

20.
likelihood

12.

A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it.

11.

A personnel security structure in which each user of an information asset is assigned an authorization level that identifies the level of classified information he or she is “cleared” to access.

14.

An evaluation of the threats to information assets, including a determination of their potential to endanger the organization.

13.

An organizational policy that specifies employees must inspect their work areas and ensure that all classified information, documents, and materials are secured at the end of every work day.

16.

A document that shows a comparative ranking of prioritized assets against prioritized threats, with an indication of any vulnerabilities in the asset/threat pairings.

15.

The process of assigning financial value or worth to each information asset.

18.

A pairing of an asset with a threat and an identification of vulnerabilities that exist between the two. This pairing is often expressed in the format $T_xV_yA_z$, where there may be one or more vulnerabilities between Threat X and Asset Z. For example, T1V1A2 would represent Threat 1 to Vulnerability 1 on Asset 2.

17.

The number of successful attacks that are expected to occur within a specified time period.

20.

The probability that a specific vulnerability within an organization will be the target of an attack.

19.

The calculation of the likelihood of an attack coupled with the attack frequency to determine the expected number of losses within a specified time range.

21.
defense risk control strategy

22.
loss magnitude

23.
asset exposure

24.
termination risk control strategy

25.
acceptance risk control strategy

26.
transference risk control strategy

27.
mitigation risk control strategy

28.
cost avoidance

29.
exposure factor (EF)

30.
single loss expectancy (SLE)

22.
Also known as event loss magnitude, the combination of an asset’s value and the percentage of it that might be lost in an attack.

21.
The risk control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards. Also known as the avoidance strategy.

24.
The risk control strategy that eliminates all risk associated with an information asset by removing it from service.

23.
See *loss magnitude*.

26.
The risk control strategy that attempts to shift risk to other assets, other processes, or other organizations.

25.
The risk control strategy that indicates the organization is willing to accept the current level of risk. As a result, the organization makes a conscious decision to do nothing to protect an information asset from risk and to accept the outcome from any resulting exploitation.

28.
The financial savings from using the defense risk control strategy to implement a control and eliminate the financial ramifications of an incident.

27.
The risk control strategy that attempts to reduce the impact of the loss caused by a realized incident, disaster, or attack through effective contingency planning and preparation.

30.
In a cost-benefit analysis, the calculated value associated with the most likely loss from an attack. The SLE is the product of the asset’s value and the exposure factor.

29.
In a cost-benefit analysis, the expected percentage of loss that would occur from a particular attack.

31.
cost-benefit analysis (CBA)

32.
annualized rate of occurrence (ARO)

33.
annualized loss expectancy (ALE)

34.
annualized cost of a safeguard (ACS)

35.
qualitative assessment

36.
Benchmarking

37.
quantitative assessment

38.
metrics-based measures

39.
process-based measures

40.
best business practices

32.
In a cost-benefit analysis, the expected frequency of an attack, expressed on a per-year basis.

31.
Also known as an economic feasibility study, the formal assessment and presentation of the economic expenditures needed for a particular security control, contrasted with its projected value to the organization.

34.
In a cost-benefit analysis, the total cost of a control or safeguard, including all purchase, maintenance, subscription, personnel, and support fees, divided by the total number of expected years of use.

33.
In a cost-benefit analysis, the product of the annualized rate of occurrence and single loss expectancy.

36.
An attempt to improve information security practices by comparing an organization’s efforts against practices of a similar organization or an industry-developed standard to produce results it would like to duplicate. Sometimes referred to as external benchmarking.

35.
An asset valuation approach that uses categorical or non-numeric values rather than absolute numerical measures.

38.
Performance measures or metrics based on observed numerical data.

37.
An asset valuation approach that attempts to assign absolute numerical measures.

40.
Security efforts that are considered among the best in the industry.

39.
Performance measures or metrics based on intangible activities.

41.
Performance gaps

42.
baselining

43.
Organizational feasibility

44.
baseline

45.
Operational feasibility

46.
political feasibility

47.
behavioral feasibility

48.
technical feasibility

42.

The process of conducting a baseline. See also *baseline*.

41.

The difference between an organization’s observed and desired performance.

44.

An assessment of the performance of some action or process against which future performance is assessed; the first measurement (benchmark) in benchmarking.

43.

An examination of how well a particular solution fits within the organization’s strategic planning objectives and goals.

46.

An examination of how well a particular solution fits within the organization’s political environment—for example, the working relationship within the organization’s communities of interest or between the organization and its external environment.

45.

An examination of how well a particular solution fits within the organization’s culture and the extent to which users are expected to accept the solution. Also known as *behavioral feasibility*.

48.

An examination of how well a particular solution is supportable given the organization’s current technological infrastructure and resources, which include hardware, software, networking, and personnel.

47.

See *operational feasibility*.