**Quantitative Risk Analysis**

The quantitative method results in concrete probability percentages.

That means the end result is a report that has dollar figures for levels

of risk, potential loss, cost of countermeasures, and value of

safeguards. This report is usually fairly easy to understand, especially

for anyone with knowledge of spreadsheets and budget reports. Think

of quantitative analysis as the act of assigning a quantity to risk—in

other words, placing a dollar figure on each asset and threat. However,

a purely quantitative analysis is not sufficient; not all elements and

aspects of the analysis can be quantified because some are qualitative,

subjective, or intangible.

The process of quantitative risk analysis starts with asset valuation and

threat identification. Next, you estimate the potential and frequency of

each risk. This information is then used to calculate various cost

functions that are used to evaluate safeguards.

The six major steps or phases in quantitative risk analysis are as

follows (Figure 2.5):

1. Inventory assets, and assign a value (asset value, or AV). (Asset

value is detailed further in a later section of this chapter named

“Asset Valuation.”)

2. Research each asset, and produce a list of all possible threats of

each individual asset. For each listed threat, calculate the exposure

factor (EF) and single loss expectancy (SLE).

3. Perform a threat analysis to calculate the likelihood of each threat

being realized within a single year—that is, the annualized rate of

occurrence (ARO).

4. Derive the overall loss potential per threat by calculating the

annualized loss expectancy (ALE).

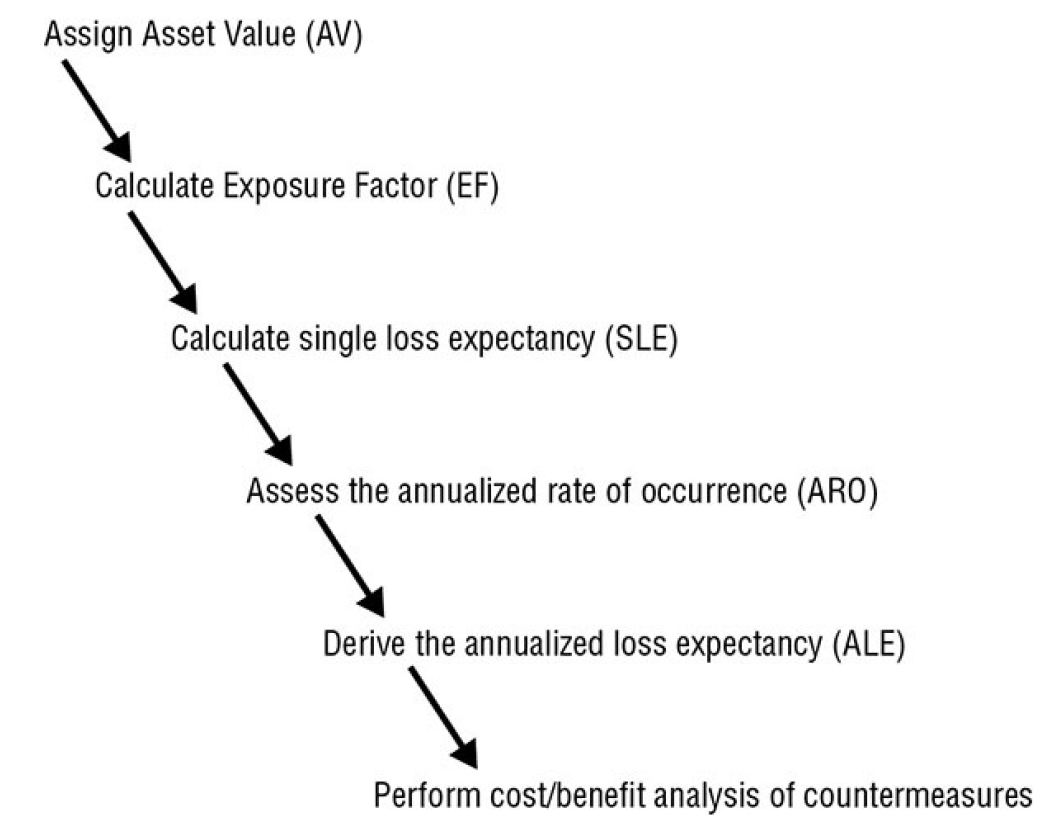
5. Research countermeasures for each threat, and then calculate the

changes to ARO and ALE based on an applied countermeasure.

6. Perform a cost/benefit analysis of each countermeasure for each

threat for each asset. Select the most appropriate response to each

threat.



The cost functions associated with quantitative risk analysis include

the exposure factor, single loss expectancy, annualized rate of

occurrence, and annualized loss expectancy:

**Exposure Factor** The *exposure factor (EF)* represents the

percentage of loss that an organization would experience if a specific

asset were violated by a realized risk. The EF can also be called the loss

potential. In most cases, a realized risk does not result in the total loss

of an asset. The EF simply indicates the expected overall asset value

loss because of a single realized risk. The EF is usually small for assets

that are easily replaceable, such as hardware. It can be very large for

assets that are irreplaceable or proprietary, such as product designs or

a database of customers. The EF is expressed as a percentage.

**Single Loss Expectancy** The EF is needed to calculate the SLE. The

*single loss expectancy (SLE)* is the cost associated with a single

realized risk against a specific asset. It indicates the exact amount of

loss an organization would experience if an asset were harmed by a

specific threat occurring.

The SLE is calculated using the following formula:

SLE = asset value (AV) \* exposure factor (EF)

or more simply:

SLE = AV \* EF

The SLE is expressed in a dollar value. For example, if an asset is

valued at $200,000 and it has an EF of 45 percent for a specific threat,

then the SLE of the threat for that asset is $90,000.

**Annualized Rate of Occurrence** The *annualized rate of*

*occurrence (ARO)* is the expected frequency with which a specific

threat or risk will occur (that is, become realized) within a single year.

The ARO can range from a value of 0.0 (zero), indicating that the

threat or risk will never be realized, to a very large number, indicating

that the threat or risk occurs often. Calculating the ARO can be

complicated. It can be derived from historical records, statistical

analysis, or guesswork. ARO calculation is also known as probability

determination. The ARO for some threats or risks is calculated by

multiplying the likelihood of a single occurrence by the number of

users who could initiate the threat. For example, the ARO of an

earthquake in Tulsa may be .00001, whereas the ARO of an

earthquake in San Francisco may be .03 (for a 6.7+ magnitude), or you

can compare the ARO of an earthquake in Tulsa of .00001 to the ARO

of an email virus in an office in Tulsa of 10,000,000.

**Annualized Loss Expectancy** The *annualized loss expectancy*

*(ALE)* is the possible yearly cost of all instances of a specific realized

threat against a specific asset.

The ALE is calculated using the following formula:

ALE = single loss expectancy (SLE) \* annualized rate of occurrence

(ARO)

Or more simply:

ALE = SLE \* ARO

For example, if the SLE of an asset is $90,000 and the ARO for a

specific threat (such as total power loss) is .5, then the ALE is $45,000.

On the other hand, if the ARO for a specific threat (such as

compromised user account) is 15, then the ALE would be $1,350,000.

The task of calculating EF, SLE, ARO, and ALE for every asset and

every threat/risk is a daunting one. Fortunately, quantitative risk

assessment software tools can simplify and automate much of this

process. These tools produce an asset inventory with valuations and

then, using predefined AROs along with some customizing options

(that is, industry, geography, IT components, and so on), produce risk

analysis reports. The following calculations are often involved:

**Calculating Annualized Loss Expectancy with a Safeguard** In

addition to determining the annual cost of the safeguard, you must

calculate the ALE for the asset if the safeguard is implemented. This

requires a new EF and ARO specific to the safeguard. In most cases,

the EF to an asset remains the same even with an applied safeguard.

(Recall that the EF is the amount of loss incurred if the risk becomes

realized.) In other words, if the safeguard fails, how much damage does

the asset receive? Think about it this way: If you have on body armor

but the body armor fails to prevent a bullet from piercing your heart,

you are still experiencing the same damage that would have occurred

without the body armor. Thus, if the safeguard fails, the loss on the

asset is usually the same as when there is no safeguard. However, some

safeguards *do* reduce the resultant damage even when they fail to fully

stop an attack. For example, though a fire might still occur and the

facility may be damaged by the fire and the water from the sprinklers,

the total damage is likely to be less than having the entire building

burn down.

Even if the EF remains the same, a safeguard changes the ARO. In fact,

the whole point of a safeguard is to reduce the ARO. In other words, a

safeguard should reduce the number of times an attack is successful in

causing damage to an asset. The best of all possible safeguards would

reduce the ARO to zero. Although there are some perfect safeguards,

most are not. Thus, many safeguards have an applied ARO that is

smaller (you hope much smaller) than the non-safeguarded ARO, but

it is not often zero. With the new ARO (and possible new EF), a new

ALE with the application of a safeguard is computed.

With the pre-safeguard ALE and the post-safeguard ALE calculated,

there is yet one more value needed to perform a cost/benefit analysis.

This additional value is the annual cost of the safeguard.

**Calculating Safeguard Costs** For each specific risk, you must

evaluate one or more safeguards, or countermeasures, on a

cost/benefit basis. To perform this evaluation, you must first compile a

list of safeguards for each threat. Then you assign each safeguard a

deployment value. In fact, you must measure the deployment value or

the cost of the safeguard against the value of the protected asset. The

value of the protected asset therefore determines the maximum

expenditures for protection mechanisms. Security should be cost

effective, and thus it is not prudent to spend more (in terms of cash or

resources) protecting an asset than its value to the organization. If the

cost of the countermeasure is greater than the value of the asset (that

is, the cost of the risk), then you should accept the risk.

Numerous factors are involved in calculating the value of a

countermeasure:

Cost of purchase, development, and licensing

Cost of implementation and customization

Cost of annual operation, maintenance, administration, and so on

Cost of annual repairs and upgrades

Productivity improvement or loss

Changes to environment

Cost of testing and evaluation

Once you know the potential cost of a safeguard, it is then possible to

evaluate the benefit of that safeguard if applied to an infrastructure. As

mentioned earlier, the annual costs of safeguards should not exceed

the expected annual cost of asset loss.

**Calculating Safeguard Cost/Benefit** One of the final

computations in this process is the *cost/benefit calculation* or

*cost/benefit analysis* to determine whether a safeguard actually

improves security without costing too much. To make the

determination of whether the safeguard is financially equitable, use the

following formula:

ALE before safeguard – ALE after implementing the safeguard –

annual cost of safeguard (ACS) = value of the safeguard to the

company

If the result is negative, the safeguard is not a financially responsible

choice. If the result is positive, then that value is the annual savings

your organization may reap by deploying the safeguard because the

rate of occurrence is not a guarantee of occurrence.

The annual savings or loss from a safeguard should not be the only

consideration when evaluating safeguards. You should also consider

the issues of legal responsibility and prudent due care. In some cases,

it makes more sense to lose money in the deployment of a safeguard

than to risk legal liability in the event of an asset disclosure or loss.

In review, to perform the cost/benefit analysis of a safeguard, you must

calculate the following three elements:

The pre-countermeasure ALE for an asset-and-threat pairing

The post-countermeasure ALE for an asset-and-threat pairing

The ACS (annual cost of the safeguard)

With those elements, you can finally obtain a value for the cost/benefit

formula for this specific safeguard against a specific risk against a

specific asset:

(pre-countermeasure ALE – post-countermeasure ALE) – ACS

Or, even more simply:

(ALE1 – ALE2) – ACS

The countermeasure with the greatest resulting value from this

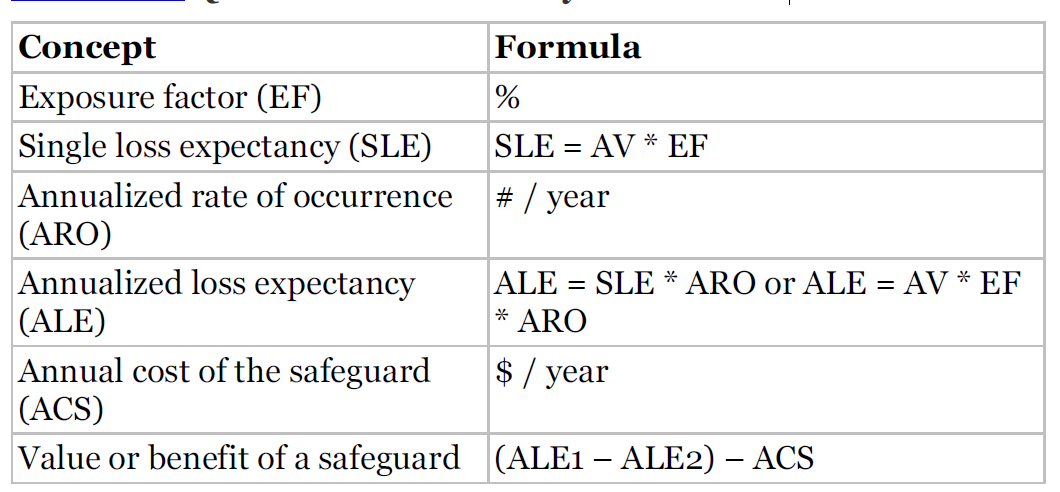
cost/benefit formula makes the most economic sense to deploy against

the specific asset-and-threat pairing.

Table 2.1 illustrates the various formulas associated with quantitative

risk analysis.

**TABLE 2.1 Quantitative risk analysis formulas**



It is important to realize that with all the calculations used in the

quantitative risk assessment process, the end values are used for

prioritization and selection. The values themselves do not truly reflect

real-world loss or costs due to security breaches. This should be

obvious because of the level of guesswork, statistical analysis, and

probability predictions required in the process.

Once you have calculated a cost/benefit for each safeguard for each

risk that affects each asset, you must then sort these values. In most

cases, the cost/benefit with the highest value is the best safeguard to

implement for that specific risk against a specific asset. But as with all

things in the real world, this is only one part of the decision-making

process. Although very important and often the primary guiding factor,

it is not the sole element of data. Other items include actual cost,

security budget, compatibility with existing systems, skill/knowledge

base of IT staff, and availability of product as well as political issues,

partnerships, market trends, fads, marketing, contracts, and

favoritism. As part of senior management or even the IT staff, it is your

responsibility to either obtain or use all available data and information

to make the best security decision for your organization.

Most organizations have a limited and all-too-finite budget to work

with. Thus, obtaining the best security for the cost is an essential part

of security management. To effectively manage the security function,

you must assess the budget, the benefit and performance metrics, and

the necessary resources of each security control. Only after a thorough

evaluation can you determine which controls are essential and

beneficial not only to security, but also to your bottom line.