

Lab 4 Risk management methodology

1. Identifying assets
2. Calculation of attack likelihood
3. Risk assessment: risk identification, risk analysis, risk evaluation (**Lab 4_a**)
4. Quantitative and qualitative methods
5. Risk treatment options

1. Identifying assets

Assets include servers, client contact information, sensitive partner documents, trade secrets and so on. Remember, what you as a technician think is valuable might not be what is actually most valuable for the business. Therefore, you need to work with business users and management to create a list of all valuable assets. For each asset, gather the following information, as applicable:

- Software
- Hardware
- Data
- Interfaces
- Users
- Support personnel
- Mission or purpose
- Criticality
- Functional requirements
- IT security policies
- IT security architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security environment
- Environmental security

2. Calculation of attack likelihood

Annual loss expectancy is a calculation that helps you to determine the expected monetary loss for an asset due to a particule risk over a single year. You can calculate ALE as a part of your business's quantitative cost-benefit analysis for any given investment or project idea.

ALE is a calculation to estimate for the decrease in value or capability of an asset after an adverse event

Calculated for each critical asset or by category

The result is used as budget amount for a control or countermeasure to mitigate the loss.

Calculation of **Annualized Loss Expectancy** is one that is very famous, within the Certified Information Systems Security Professional (CISSP) practice and it's borrowed from insurance companies.

It's a calculation to estimate a rough order of magnitude for the decrease in value or capability of an asset after an adverse event occurs. It is performed for each critical asset or for each category of assets. The result of this is a budget amount that will be used for controls or countermeasures that will be employed to mitigate the loss in some effective way.

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

$$\text{SLE} = \text{AV} \times \text{EF}$$

AV is the **Asset Value**. This needs to reflect the **total cost of operation** or **ownership** of the given asset. So, it reflects everything material about that asset. We multiply that by the **Exposure Factor**. This represents the amount of capacity or capability or value that will be lost through the adverse event occurring. Taking the product of these two, we produce the **Single Loss Expectancy**, shown there as a the **SLE**.

Then the particular event characteristics that produce an **Annual Rate of Occurrence** of whatever the effective element is that causes this loss, we calculate how often that will happen, causing the **Single Loss Expectancy** over a period of time.

The **ARO** is normally represented as a decimal:

If it's greater than 1 that means it happens more frequent than one time per year

If it is equal 1, then obviously that means one time per year

If it's a decimal less than 1 then that means it doesn't happen every year but some periodic interval over a period of years.

So, we multiply those together and we come up with the **Annualized Loss Expectancy**. Now this number, the **ALE** is what is the budget amount that will be used for decision making process about what controls or countermeasures that will be put in place to mitigate the **Single Loss Expectancy**, for each event occurrence.

For example, let's say that you calculate an **ALE** of \$10,000 and figure it would cost \$15,000 a year to eliminate the risk; based on these numbers, you might decide that the cost isn't worth the risk.

Of course, not all situations are that simple. For instance, suppose you understand that a HIPAA (Health Insurance Portability and Accountability Act) violation might cost you \$100 per violation up to a maximum fine of \$250,000. That might seem manageable, but digging deeper into information that you may not have considered could reveal that if the violation is due to willful negligence, the impact could be as high as \$1.5 million.

This example illustrates that while quantitative risk analysis provides a reliable and objective way to potential risks, the results are only as good as the data you put into the process.

Moreover, remember that ALE determines the cost of the risk. Do not confuse ALE with the total cost of ownership (TCO), which assesses the cost of a particular solution.

Here is an overview of how to calculate ALE. Each term is explained in further detail below.

Inventory your information assets and determine the asset value (AV) of each. Identify the potential threats to each asset.

For each threat, do the following:

1. Determine the exposure factor (EF) to that threat for each information asset.
2. Calculated the single loss expectancy (SLE) using this formula: $\text{AV} \times \text{EF} = \text{SLE}$
3. Calculate the annual rate of occurrence (ARO).

4. Calculate the annualized loss expectancy (ALE) using this formula: $SLE \times ARO = ALE$

Asset value — Many of your assets are tangible items, such as computers, servers and software. Other assets are intangible, like expertise, databases, plans and sensitive information.

Because most organizations have a limited budget for risk assessment, you will likely have to limit the scope of the remaining steps to mission-critical assets. Accordingly, you need to define a standard for determining the importance of each asset. Common criteria include the asset's monetary value, legal standing and importance to the organization. Once the standard has been approved by management and formally incorporated into the risk assessment security policy, use it to classify each asset as critical, major or minor

The asset value is the total value of the specific asset; if your server is worth \$6,000, your AV is \$6,000.

Here are some questions to consider to find your AV:

- What did you pay to acquire or build the asset in question?
- What is your liability if the asset becomes compromised?
- What is the production cost if the asset is made unavailable?
- What is the asset's value to outside users?
- In what other ways would loss of the asset affect your business?

Exposure factor — This is the percentage of the value of a given asset that gets lost as a result of a specific incident. If you expect to lose a quarter of the value of an asset in an incident, then your EF for that asset is 0.25 (25%). Remember that you can only calculate the EF in relation to a specific risk, such as a security breach or natural disaster. Also keep in mind that a loss can exceed the value of a given asset; in such cases, the EF would be greater than 1.0 (more than 100%).

Single loss expectancy — This is the amount of money you expect to lose each time a specific asset is lost or compromised. For instance, you may expect to lose \$300 each time your business server breaks down, or you might lose \$1,500 every time a laptop is lost or stolen. To calculate single loss expectancy, multiply the AV and EF.

Annual rate of occurrence — This is the number of times you expect a specific incident to occur in one year. If you expect your server to crash five times per year, your ARO would be 5. If the ARO is less than 1, you express it as a percentage — for instance, if the likelihood of an incident is once every four years, the ARO for that incident would be 0.25 (25%).

Calculating ALE as part of a quantitative risk assessment is essential for making informed business decisions. While the process can be confusing and arduous at times, reliably determining risks and accurately calculating potential losses will provide valuable information to help you make smart business decisions. With ALE as a risk assessment tool, you can more effectively perform cost-benefit analysis and determine if employing specific countermeasures are worth the investment.

4. Quantitative and qualitative methods

Risk assessment is an essential component of risk management. It enables you to determine potential hazards that may negatively affect specific projects or result from certain decisions.

There are two types of risk analysis — quantitative and qualitative:

Quantitative risk analysis is an objective approach that uses hard numbers to assess the likelihood and impact of risks. The process involves calculating metrics, such as **annual loss expectancy**, to help you determine whether a given risk mitigation effort is worth the investment. The assessment requires well-developed project models and high-quality data.

Qualitative risk analysis is a quicker way to gauge the likelihood of potential risks and their impact so you can prioritize them for further assessment.

While quantitative risk analysis is objective, qualitative risk analysis is a subjective approach that ranks risks in broader terms, such as a scale of 1–5 or simply low, medium and high.

Both forms of risk analysis are valuable tools in risk management.

Quantitative risk analysis uses relevant, verifiable data to predict the probability of certain risk outcomes and their estimated monetary cost.

There are many different types of risks that IT pros need to consider, including the following:

- Human errors
- Hostile action, such as cyberattacks, unauthorized disclosure or misuse of data
- Application errors
- System or network malfunctions
- Physical damage from causes such as fire, natural disasters or vandalism
- What results do you get out of quantitative risk analysis?

Quantitative risk analysis helps you estimate:

- Possible outcomes of a given risk
- The probability of achieving specific objectives
- Realistic costs
- Project completion timelines
- When is quantitative risk analysis most useful?

Quantitative risk assessment helps you make smart, data-informed decisions for your business. You should perform a quantitative risk analysis when you need to:

- Decide whether to invest in specific projects or tools
- Choose countermeasures to mitigate potential sources of loss
- Provide detailed data about the chances of completing a project within budget and on schedule
- Create a contingency reserve for your project
- What is annual loss expectancy?

5. Risk treatment options: Acceptable Risk vs. Residual Risk

Total Risk: all risks and possible losses found or inherent in the context before any remediation is planned or performed.

From these we have to first assess what the **Acceptable Risk** would be that we have to meet and we have to compare that to the **Residual Risk**. In other words, we compare our target, the **Acceptable Risk** to what we actually achieve in the form of **Residual Risk**.

$$R_t > R_a \geq R_r$$

So, there you see the calculation, the ideal relationship between **Total Risk**, **Acceptable Risk** and **Residual Risk**. Total Risk will have the greatest value. Less than that will be the **Acceptable Risk**. **Acceptable Risk** and **Residual Risk** could be equal but **Acceptable Risk** should be greater than **residual**.

Now, where the **Residual Risk** is less than or equal to at its greatest to the **Acceptable Risk** limit by management, this has to be regarded as encompassing compliance items as part of the attainment of the **Acceptable Risk**.

And all of these should be based on total cost of ownership or operation of the asset in order to come up with an appropriate valuation method.

Acceptable Risk which represents a level of allowable exposure or loss or outage as defined by management. That an enterprise can absorb and continue operating without any sort of crippling effects. Now, **Acceptable Risk** does contain any sort of compliance requirement that has to be met and it can be something that might even be arbitrary but it's decided upon by management and it becomes the target that we have to achieve as a minimum for our risk assessments to be successful.

Acceptable Risk is defined as an **SLE** or **ALE** at or below defined threshold. Examples could be:

- a variance of up to 10% in operating expenses,
- a variance in uptime as measured against the Service Level Agreement commitment by a service provider of some kind
- a delay of five days in project completion which could represent five days of float or slack that might be in a project plan. That will make no difference and if it's achieved, in the delivery considered to be on-time of whatever the product is of a given project.

Residual Risk is the level of remaining exposure loss or potential outage that remains following risk reduction and mitigation efforts. This is what we actually achieve as compared to the Acceptable Risk which serves of our target

So the examples of this could be:

achieving an **ALE**, reduced by 40%. That is by modifying the asset to reduce its exposure to power fluctuations

decreasing data entry errors by 80% through operator training and better supervisory work quality checking.

adding hot-failover to a critical application system to eliminate lost service due to system failures

a process change where design review QA processes are done to improve time-to-market by 30 days per year by reducing in-stream-design re-work and break-fix activities.

Again, these are simply examples of what might highlight the **Residual Risk**, what we've actually achieved through our mitigation efforts.

Examples:

In this table, there are other examples of ALE and SLE values.

Threat	Asset	Value	Exposure Factor	SLE	Frequency of Occurrence	ALE
Fire	Facility	\$560,000	40.00%	\$224,000	0,25	\$56,000
Theft	Trade secret	\$43,500	92.00%	\$40,020	0,75	\$30,015
Tech Failure	File server	\$11,500	100.00%	\$11,500	0,50	\$5,750
Virus	Database	\$8,900	70.00%	\$6,230	0,80	\$4,984
Insider Theft	Credit card data	\$325,500	83.00%	\$270,165	0,65	\$175,607

The fire to a facility and a facility has a TCO value set at \$560,000. This might also be what is represented as the value of it on an insurance policy. Our exposure factor is 40% that means that the fire has caused a 40% loss to the building and that might represent a claim value, translating to

\$224,000 of a **Single Loss Expectancy**. Our **Frequency of Occurrence** is 0.25 which means that once in four years a loss of this magnitude occurs that calculates to a \$56,000 annualized loss.

The theft of a trade secret where the trade secret itself by some calculation is valued at \$43,500. 92% of that value is lost probably through some form of exploitation. So our **Single Loss Expectancy** is \$40,000 and change. This happens 0.75 which means it happens three times in four years. Now, to be clear, that could mean that it happens three times in one year and then not again for another three years or it could happen one time each of three years in a four year period or some other combination. But our **Annualized Loss Expectancy** is \$30,015.

In some cases as with a file server the loss is 100% so that the **Single Loss Expectancy** is the assessed value of the server itself. This should include the value of the data that might be lost on the server as well. 0.50 simply means it happens every other year.

The insider threat, the data is valued at \$325,500, 83% exposure factor might mean that 83% was in an exploitable condition and was in fact exploited in some way by the insider. Possibly sold to a third party who might be hacking into it. For a **Single Loss Expectancy** of \$270,000, a frequency of occurrence 0.65 which means that in a 10 year period, it happens six plus times, for an **Annualized Loss Expectancy** of \$175,000.


The **ALE** values that are shown in this table would be used to put together a budget that would then be expended on various types of controls, changes in procedure, different kinds of employee training perhaps but a mixture of these things and this money would be spent to stop these losses from happening. Or reduce the losses from occurring if there is no way to effectively stop them from occurring.


Whenever we're considering controls, there is never a time we're going to consider controls that are not operationally effective, in achieving the desired results. So, the **cost/benefit analysis** is always done on the controls that will produce that result.


The annualized cost of these safeguards to protect the threats is going to be compared to the expected cost of the potential loss itself.

If a server worth \$10,000 and one suggested security safeguard, would cost a company 12,000 to protect that one server that would not be a cost effective comparison. The server itself is 10,000, a solution proposed at \$12,000 is worth 20%, more than the server itself is worth, nothing cost effective about that.


Exercises:

1. A web server earns you \$25,000 per hour. The likelihood that the web server will fail at least once in a year is estimated as 25%. Server recovery time is 3 hours. The cost of recovery is \$5000. Calculate ALE 


2. The server is worth \$ 32,000, its exposure factor to DoS attacks is 0.25. Likelihood of such incident happening once a year in the industry is estimated as 30%. What is the value of ALE? 


3. The reliability of the local corporate network is 75%. The profit from the use of it is \$20,000 per hour. It requires \$ 3,000 to restore the network after an incident and it takes 1 hour. Likelihood of such incident happening once a year in the industry is estimated as 30%. Calculate ALE. 

4. You are the administrator of a research firm and work in one project of data collection and their placement on a single web-server. The estimated value of each research project is about \$100,000. The exposure factor is 90%, which means that at any time the attacker can steal no more

than 90% of the data. Likelihood of such incident happening once a year in the industry is estimated at 33%. Calculate ALE. 

5. Resistance to failures of equipment worth \$8000 is 75%. Likelihood of an incident is once every four years. What is the value of ALE? 

6. Due to equipment failure, the probability of data loss is 0.35. Likelihood of an incident is twice a year. The value of the assets is estimated as \$30,000. What is the value of ALE? 

7. You work in technical support in a small company. One of the most common incidents is the recovery of data accidentally deleted by users. This happens once a week. If a user creates a file on the server and then deletes it (70% of incidents), it can be restored instantly with a shadow copy and the data is rarely lost. If a user creates a file on their workstation and then deletes it (30% of incidents), the file cannot be recovered and the user needs about 2 hours to create the file again. The cost of file creation is estimated as \$12 per hour. What is the value of ALE? 

Example:

Here's a fictional scenario to help you practice calculating an ALE and using it in a business decision. Note that this is a very simplified calculation that considers just one threat to one information asset.

Let's say that your organization is considering investing in a solution that can help you to discover malicious insider actions on your file servers to reduce the risk of losing a particular piece of intellectual property (IP). Here's how you could determine if investing in a particular security solution is justified:

Determine the **AV**. Let's say that the IP asset of interest has a value of \$75,000.

Calculate the **EF**. Let's assume it is 0.75 (75%).

Calculate the **SLE** by multiplying the AV by the EF, which yields an SLE of \$56,250.

Determine the **ARO**. Let's assume it's 0.95 (meaning there's a 95% chance of malicious insider activity occurring in any given year).

Calculate the ALE: $\$56,250 \text{ (SLE)} \times 0.95 \text{ (ARO)} = \$53,357.50 \text{ (ALE)}$.

Compare the ALE to the cost of each of the software solutions you're considering. If the license fee exceeds your ALE (\$53,357.50), the solution is not a worthwhile investment.

$\text{SLE} = \text{AV} \times \text{EF} = \$75,000 \times 0.75 = \$56,250$

$\text{ALE} = \text{SLE} \times \text{ARO} = \$56,250 \times 0.95 = \$53,357.50$