Risk Management

Continuous Assessment -> Constantly monitoring and evaluating risks in real-time
Ad hoc Assessment -> Conducted after a major security breach, useful for addressing immediate and emerging risks
one-time Assessment -> Conducted only once, usually in response to a specific project or initiative
Recurring Risk Assessment -> Systematic approach (regular intervals -> quarterly or annually) and ensure that changes in the environment, assets, and threat landscape are consistently accounted for and addressed
Asset Value (AV) -> The total value of the asset being evaluated (in monetary terms). In this case, it is $100,000.
Exposure Factor (EF) -> The percentage of the asset's value that would be lost or damaged if a specific threat occurs**.** In this case, it is 40%, or 0.40.
Annualized Rate of Occurrence (ARO) -> The estimated number of times the threat is expected to occur in a year. In this case, it is 2
SLE (Single Loss Expectancy) is the expected loss from a single occurrence of the event.

SLE=AV×EF
SLE=100,000×0.40=40,000
ALE=SLE×ARO
ALE=40,000×2=80,000

Risk Register -> Essential component of effective risk management, serving as a centralized reposition for information, is a document that typically provides a comprehensive view of all identified risks, their status and the mitigation strategies

- Key Risk Indicators (KRI) -> metrics used to measure and monitor the likelihood and impact of risks
- Risk Threshold/Tolerance -> Level of risk that the organization will accept, setting limits on risk
- Risk Appetite -> Amount of risk that an organization is willing to accept in order to achieve its goals and objectives
    - Neutral -> Organization that prefers to maintain its current position and avoid taking unnecessary risks
    - Aggressive/Expansionary -> Organization that is willing to take on high levels of risk in pursuit of aggressive growth and competitive advantages
    - Conservative -> Organization that is very risk-averse and prefers to maintain a low level of risk exposure

- **Risk identification:** This includes the risk name or identification number.
- **Risk description:** This is a brief description of the risk and why it's an issue.
- **Risk category:** Categorizing your risks can help your team identify the risk within the risk register, making it easier to understand who will be responsible for mitigation. For example, you categorize your risk register by departments
- **Risk ownership:** This includes the person or persons who will be responsible for managing and overseeing the risk response.
- **Risk probability:** How likely the risk is to occur. You can categorize each risk as highly unlikely, unlikely, likely, or very likely. You can also use a numerical scale.
- **Risk impact:** This highlights and measures the potential impact of the risk, helping your team understand which risks take precedence. When rating the potential impact, use a simple scale that includes ratings like extremely low, low, medium, high, and extremely high.
- **Risk priority:** This takes risk probability and risk analysis into account to measure the priority level of the risk.
- **Risk response:** Your response or mitigation plan will detail how you plan to handle the risk. Your solution should be clearly outlined.
- **Risk status:** This field of your risk register includes the status of the risk—open, in progress, ongoing, or closed.
- **Notes:** You can also include a notes section to include any additional notes or details that will help team members better understand the risk and mitigation plan.

Risk Avoidance -> Changing plans or procedures to eliminate the risk (eliminating the risk entirely)
Risk Mitigation -> Reduce the likelihood or impact of the risk (not necessarily eliminate the risk entirely)
Risk Transfer -> Sifting the impact of a risk to a third party
Risk Acceptance -> Just accept the risk
Risk Exploitation -> Taking advantage of the potential positive impacts
Risk Reporting -> Communicating information about identified risk

Risk Owner -> Typically responsible for ensuring that risks are addressed in line with the organization's risk strategy and appetite
Risk Assessor -> Identify, assess, and analyze risks within an organization
Risk Communicator -> Effectively communicating risk-related information to stakeholders within the organization

BIA -> How a risk will impact the business

- Maximum Tolerable Downtime (MTD) / Maximum Tolerable Outage (MTO) -> Downtime acceptable before causing irreparable harm
- Recovery Time Objective (RTO) -> Maximum acceptable downtime (This need to be less than MTD/MTO)
- Recovery Point Objective (RPO) -> The maximum acceptable amount of data loss measured in time
- Mean Time to Repair (MTTR) -> Average time taken to repair