

Qualitative and Quantitative Assessments

THREAT MANAGEMENT

Qualitative vs Quantitative

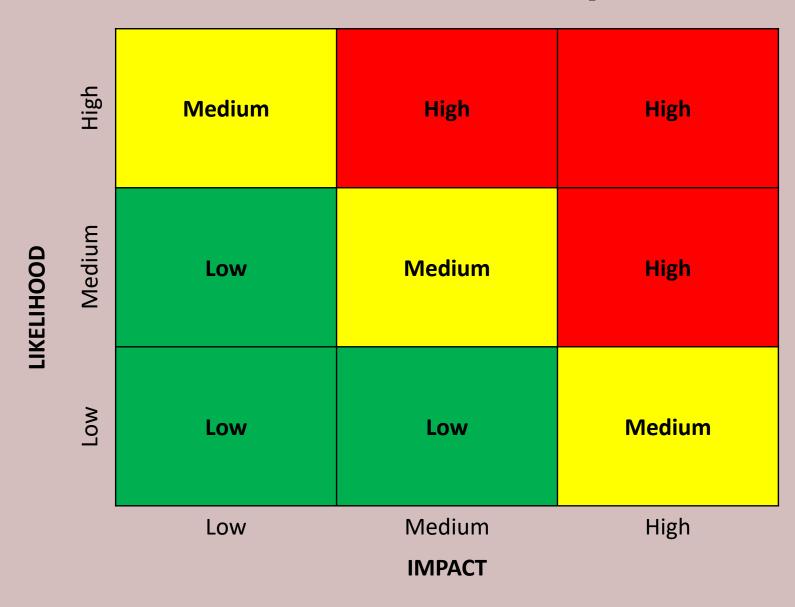
Qualitative measurement is subjective

Quantitative is based on numbers

 For the CompTIA CSA+ exam, you do not need to understand quantitative assessments, but they are covered on exams like CASP and CISSP.



Qualitative Example

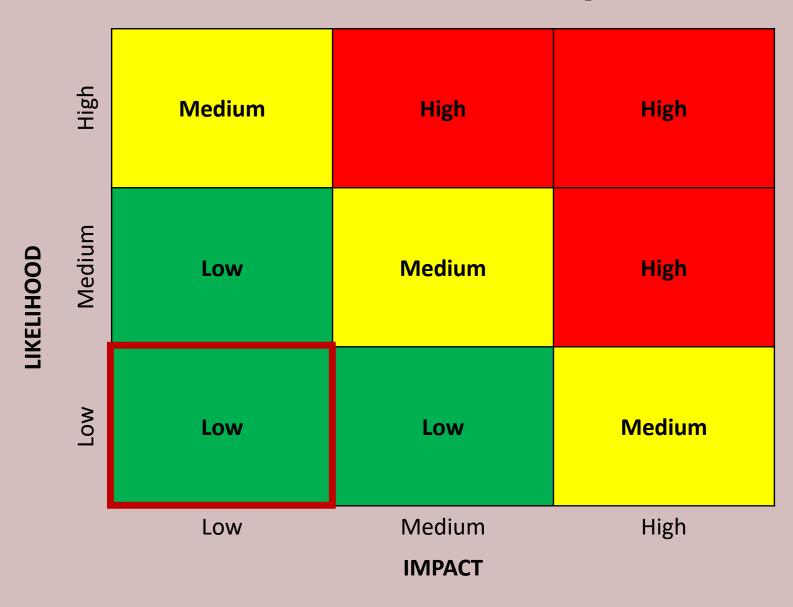




TRAINING THE CYBER SECURITY WORKFORCE



Qualitative Example

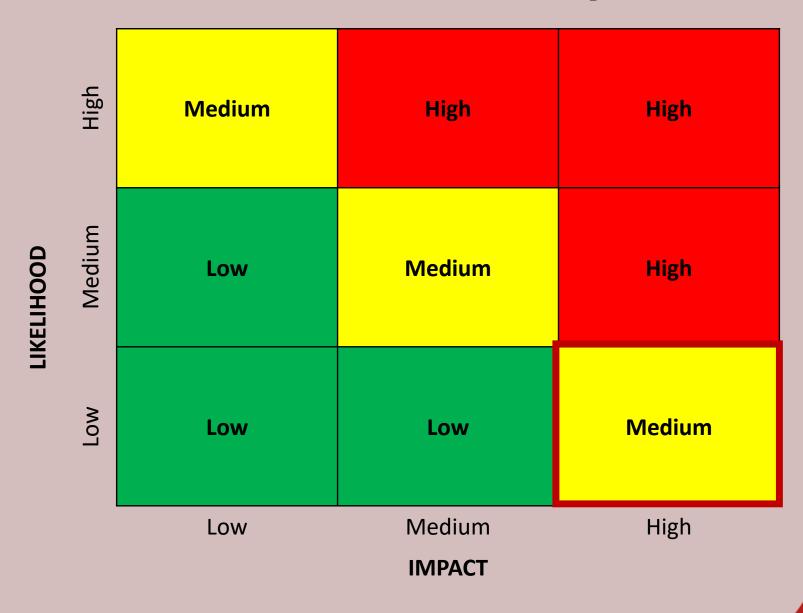




TRAINING THE CYBER SECURITY WORKFORCE



Qualitative Example





TRAINING THE CYBER SECURITY WORKFORCE



ANNUAL LOSS EXPECTANCY (ALE)

Common calculation to determine the cost associated with risk

 Aids in determining when to accept, avoid, transfer, or mitigate the risk

If a risk would be actualized 3 times a year, then Occurrences equals 3.0.

If a risk would be actualized once ever 3 years, then Occurrences equals 0.33.

ANNUAL LOSS EXPECTANCY (ALE)

Assume a theft of customer information costs a company \$1 million per occurrence, and risk is large and expected to occur 5 times per year... ... Then, it makes sense to spend up to \$5 million to mitigate this risk!

ANNUAL LOSS EXPECTANCY (ALE)

But, if a theft of customer information costs a company \$1 million per occurrence, and the risk that it occurs is only once every 5 years...

...Then, it would make sense to only spend up to \$200,000 to mitigate this risk!

** If it costs >\$200,000 to mitigate, just accept the risk and pay \$200k each time **