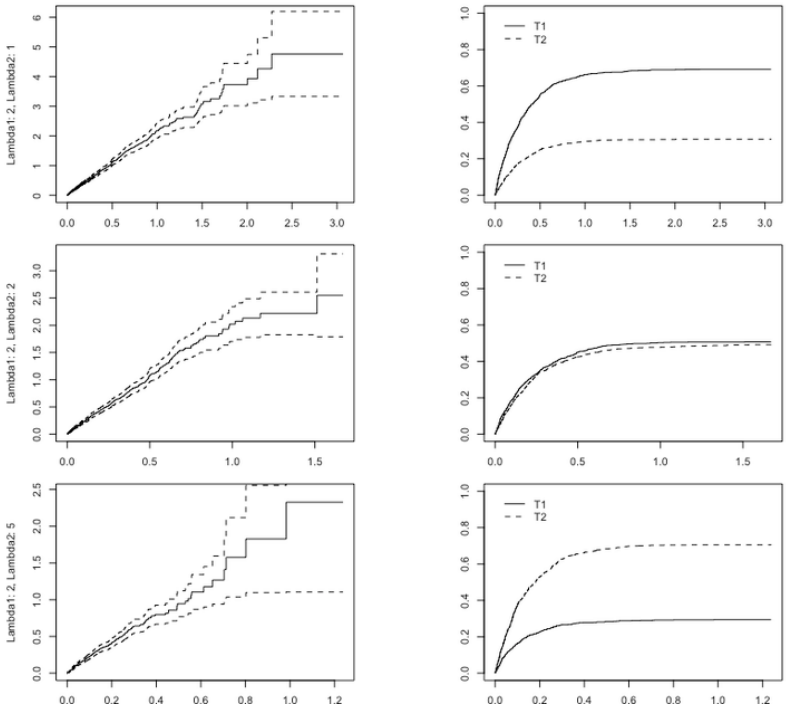
RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

QUANTITATIVE RISK ASSESSMENT

This module introduces the concepts of quantitative risk assessment and associated metrics



QUANTITATIVE RISK ASSESSMENT (QRA)

- Structured approach to assigning numerical values to risk components
  - Enables organizations can measure, compare, and prioritize risks with a degree of mathematical rigor
- QRA attempts to answer three core questions
  - How likely is the risk?
    - Expressed in terms of probability, frequency and rate
  - How much loss will occur if it happens?
    - Expressed in terms of cost, damage, liability and downtime
  - What is the organization's financial exposure?
    - Expressed as Annualized Loss Expectancy or equivalent
- QRA attempts to model uncertainty using numbers instead of categories, aiming for greater objectivity and repeatability

QUANTITATIVE RISK ASSESSMENT (QRA)

- Quantitative risk analysis typically uses the formula
  - Risk = Probability × Impact
- Applied repeatedly over a one-year time horizon, this becomes
  - Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annual Rate of Occurrence (ARO)
    - SLE = cost of one event
    - ARO = number of events per year (or expected frequency)
  - This is then scaled across multiple risks, scenarios, or systems

QUANTITATIVE RISK ASSESSMENT (QRA)

- Key data sources include
  - Historical incident data (internal, industry, insurance)
  - Threat intelligence (malware trends, attack frequency)
  - Actuarial data (claims, premiums, event frequency distributions)
  - Benchmark studies (e.g., Ponemon, Verizon DBIR, Gartner)
  - Operational logs (system outages, fraud cases, processing errors)
- Common statistical models
  - Monte Carlo simulation
  - Bayesian inference
  - Frequency-severity models
  - Regression forecasting

VALIDITY

- Does the quantitative model measure what it claims to measure?
- Challenges with validity
  - Frequency data may not reflect true likelihood
    - For example: many cyber incidents go unreported or undetected
  - Loss data may be incomplete or inconsistent
    - For example: financial impact is often spread across departments
  - Benchmark data may not match the organization's risk profile
    - For example: using Ponemon data for a small credit union
- Improving validity
  - Use scenario-based modeling rather than relying solely on historical data
  - Employ expert judgment to adjust models where data is sparse
  - Validate assumptions by triangulating sources
    - For example: insurance claims, vendors, internal logs

RELIABILITY

- If we repeat the analysis, do we get the same result?
- Reliability issues
  - Risk frequencies typically fluctuate year to year
  - Threat landscapes evolve quickly which means that past data may not predict future events
  - SMEs give inconsistent estimates when data is sparse.
- Improving reliability
  - Use multi-year averages or parametric distributions instead of single values
  - Use data cleaning to remove outliers that will skew the predictions
  - Document assumptions to ensure repeatability
  - Apply automated statistical methods (e.g., Monte Carlo) to reduce human variability

ACCURACY

- How close are the estimated numbers to the true values?
  - True values are often unobservable, especially for rare events
  - The goal is often reasonable approximation, not perfect precision
- Accuracy limitations
  - Rare or catastrophic risks (black swans) have almost no accurate data
  - Public reports often exaggerate or under report losses
  - Human estimation is error-prone. even when expressed numerically
- Improving accuracy
  - Use wide ranges, not point estimates (e.g., $50k–$300k)
  - Apply repeated statistical simulations to generate a loss distribution
  - Combine internal and external data to reduce estimation variance

STRENGTHS OF QRA

- Supports financial decision-making
  - Because QRA expresses risks in monetary terms, organizations can, for example
    - Compare cost of controls vs. expected losses
    - Justify cybersecurity budgets
    - Support insurance decisions
    - Inform strategic investment decisions
- Enables advanced modeling
  - Monte Carlo and Bayesian techniques allow analysts to
    - Evaluate uncertainty
    - Simulate rare events
    - Model interdependent risks
    - Produce risk distributions rather than one-dimensional scores

STRENGTHS OF QRA

- Reduces subjectivity
  - Numerical inputs minimize the ambiguity of qualitative scales like “High/Medium/Low”
- Enables cost-benefit and ROI calculations
  - For example: ALE (before control) – ALE (after control) = Value of Control
- Standardized and repeatable
  - Once a model is built, new data can be entered consistently over time
- Supports benchmarking and regulatory reporting
  - Many frameworks (NIST CSF 2.0, FAIR, Basel II/III) rely heavily on quantitative risk data

WEAKNESSES OF QRA

- Data scarcity
  - Most organizations lack sufficient:
    - Loss data
    - Frequency data
    - Forensic records
    - Incident cost transparency
  - This can undermine accuracy and reliability
- False precision
  - Numbers give an impression of certainty that usually does not exist.
  - For example: “Probability = 0.13” falsely suggests exactness.

WEAKNESSES OF QRA

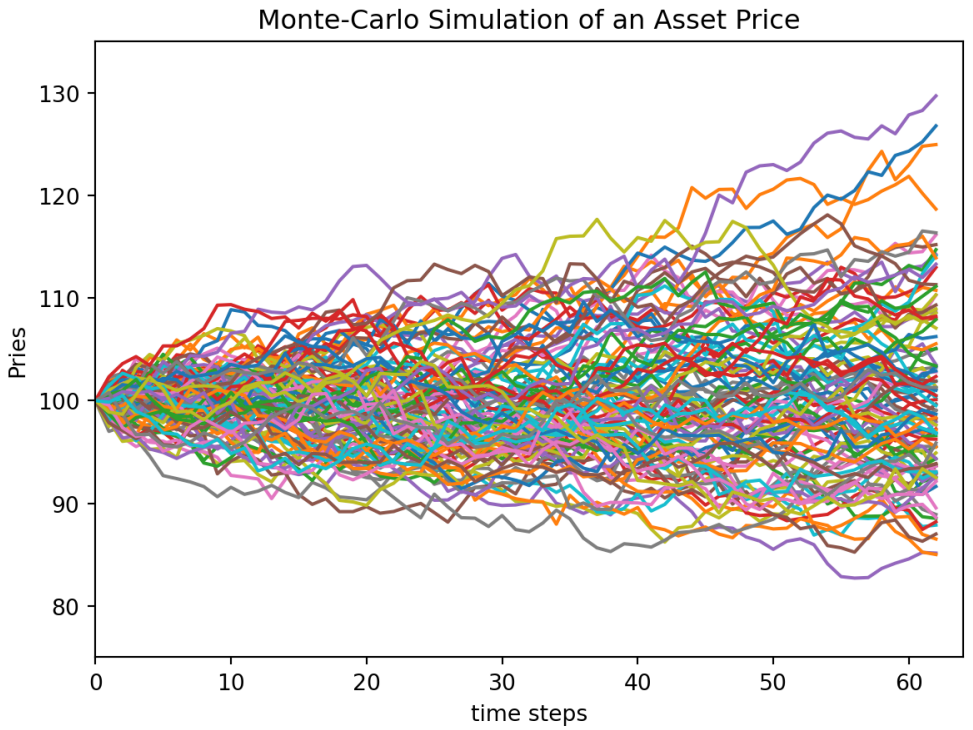
- High reliance on assumptions may be more influential than the data itself
  - Assumptions about
    - Event frequency
    - Control effectiveness
    - Detection rates
    - Recovery times
- Complex modeling may not be understood by decision makers
  - Executives may resist results they cannot interpret, especially Monte Carlo outputs.
- Cannot capture qualitative factors well such as
  - Reputational damage
  - Regulatory backlash
  - Stakeholder trust
  - Organizational culture impacts

WEAKNESSES OF QRA

- Not ideal for entirely novel risks
  - Emerging technology risks (AI misuse, quantum threats) often have no associated data
- Time-consuming
  - Building a reliable quantitative model requires:
    - Data collection
    - Data cleaning
    - Data validation
    - Data modeling
    - Stakeholder review
- Qualitative methods are much faster

MONTE CARLO SIMULATION

- Runs thousands of iterations using ranges or probability distributions
- Produces likelihood curves, heat maps, and loss distributions
- Good for uncertainty and tail risk

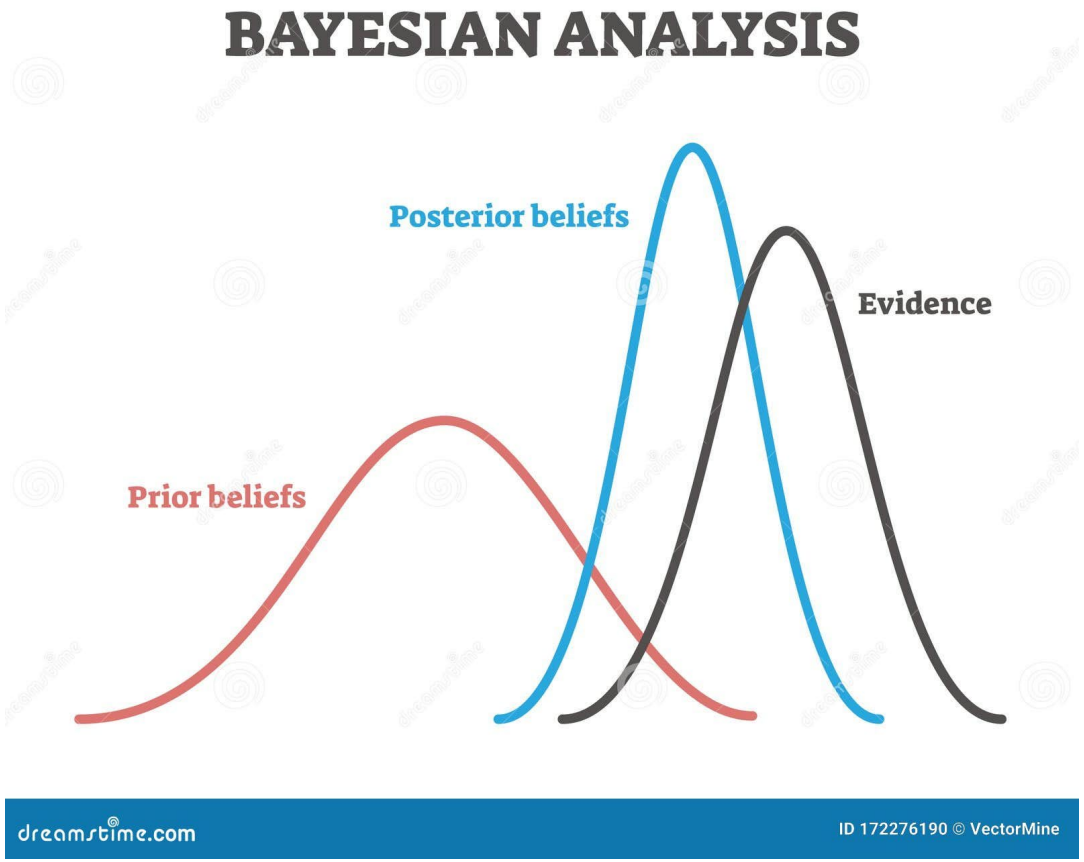


BAYESIAN SIMULATION

- Bayesian modelling represents unknown parameters as probability distributions (priors), observe data and update the priors to posterior distributions using Thomas Bayes' theorem:

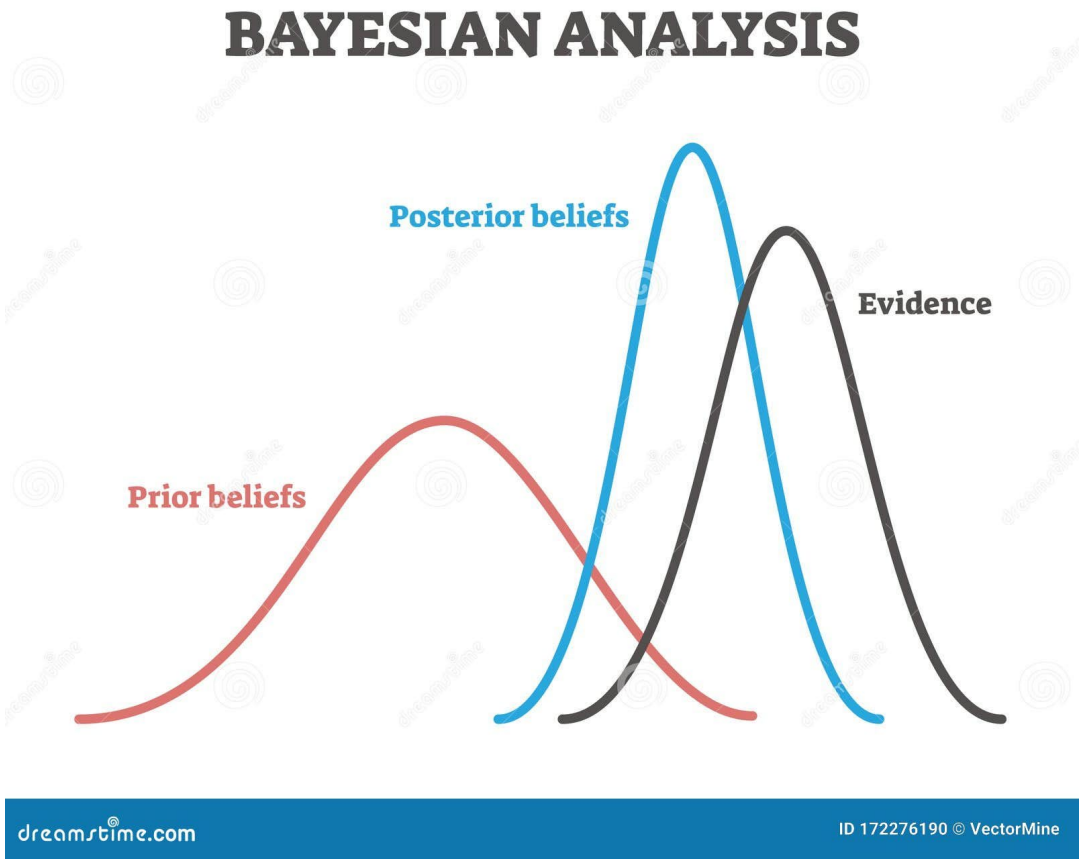
$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

- Key features
  - Explicitly encode prior beliefs (or lack thereof) about parameters
  - Update beliefs in light of new data.
  - All parameters and predictions are treated probabilistically, not just point estimates



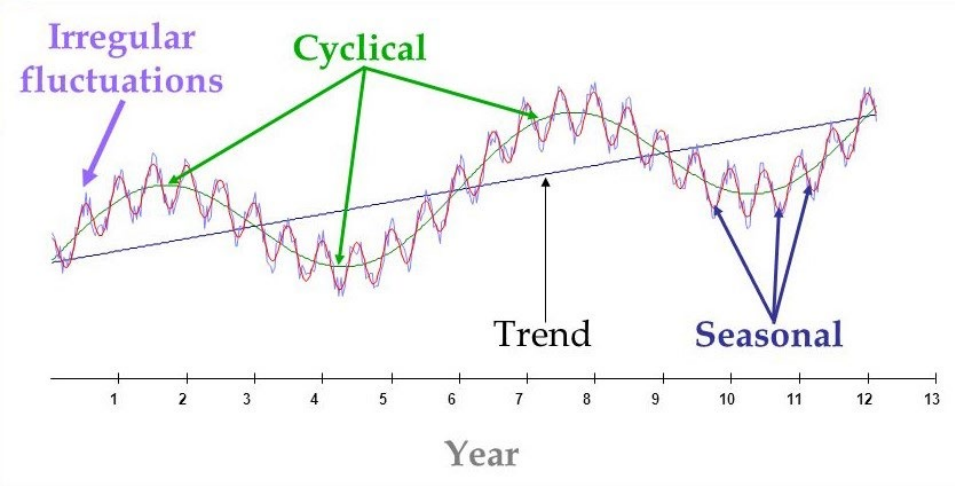
BAYESIAN SIMULATION

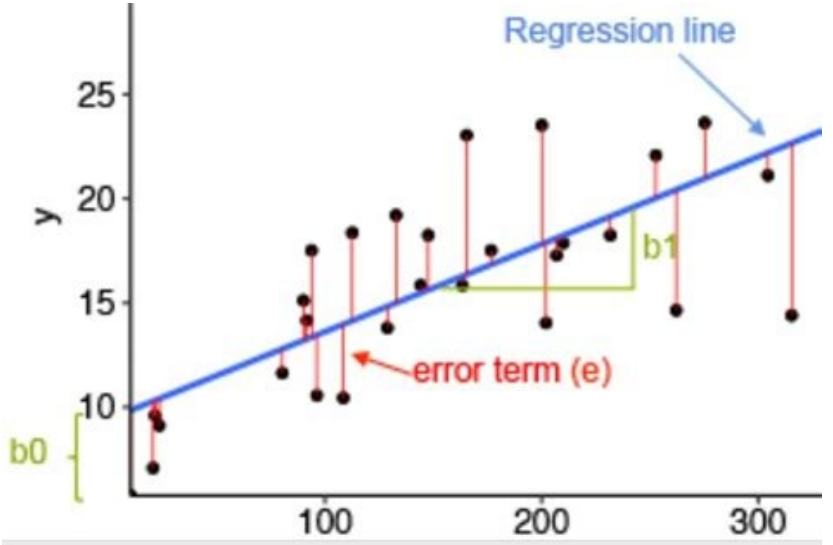
- Suitable for hierarchical models, uncertainty quantification, small-sample scenarios, and modelling complex structure
- Strengths include
  - Better handling of uncertainty
  - Ability to incorporate prior knowledge, and natural fit with modern computational methods
- Limitations include
  - Computational cost
  - Sensitivity to prior choices
  - Potential difficulty in interpretation for non-statisticians.



REGRESSION AND TIME-SERIES

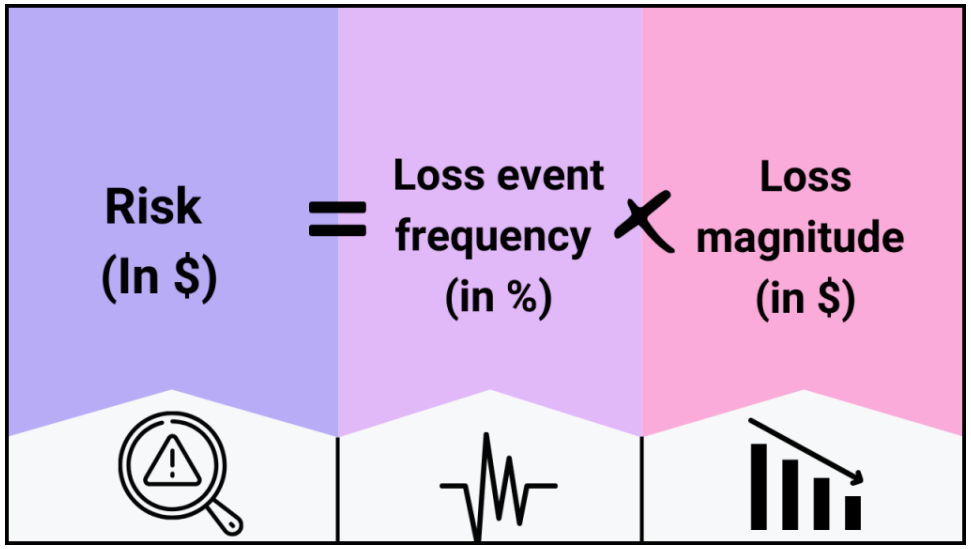
- Predicts frequency/severity trends
- A sequence of observations recorded at successive points in time
  - Example: daily stock prices, hourly sensor readings, monthly sales numbers, annual climate measurements, etc.
- The central idea is that past patterns help explain or predict future behavior
- Time series help identify long-term movements in data
- Regression is used to fit a curve to existing data that can be used for future predictions





FAIR MODEL

- Factor Analysis of Information Risk
- Decomposes risk into frequency + magnitude components
  - Widely used in cybersecurity
  - Provides repeatable numerical estimates



WHEN QRA WORKS BEST

- Quantitative methods excel when
  - A large volume of high-quality, consistent data exists
  - Risks have measurable financial impacts
  - The organization has mature incident reporting
  - The objective is budgeting, prioritization, or insurance
  - Top leadership prefers evidence-based decision-making
- Ideal domains
  - Cybersecurity
  - Fraud and financial loss forecasting
  - Operational risk (Basel frameworks)
  - Business continuity and disaster recovery
  - Insurance and actuarial sciences

INTEGRATION

- Most modern ERM programs use a hybrid approach
  - Qualitative to identify and explore risks
  - Quantitative to measure and justify decisions
  - Scenario analysis to fill gaps where data is scarce
  - Dashboards combining both for executives

STANDARD QUANTITATIVE RISK METRICS

- Single Loss Expectancy (SLE)
  - SLE estimates the financial loss from a single occurrence of a risk event.
  - Formula: SLE = Asset Value (AV) × Exposure Factor (EF)
    - AV = monetary value of the asset
    - EF = % of the asset lost in the event (0–1)
  - Example
    - Asset value: $500,000
    - Exposure factor: 0.25 (25% damage)
    - SLE = 500,000 × 0.25 = $125,000

STANDARD QUANTITATIVE RISK METRICS

- Annualized Rate of Occurrence (ARO)
  - Represents how often an event is expected to occur per year.
  - Sources for ARO:
    - Historical logs
    - Industry databases (ISACA, Ponemon, Verizon DBIR)
    - Threat modeling
    - Expert estimation
    - Statistical frequency data
  - Example
    - If phishing incidents occurred 10 times in 5 years:
    - ARO = 10 / 5 = 2
    - Expect 2 phishing events per year.

STANDARD QUANTITATIVE RISK METRICS

- ALE estimates annual financial loss due to a given risk.
  - Crucial for comparing the cost of mitigation vs. expected loss.
  - Formula: ALE = SLE × ARO
  - Example
    - SLE = $125,000
    - ARO = 0.5 (every two years)
    - ALE = 125,000 × 0.5 = $62,500 per year

QUALITATIVE VS. QUANTITATIVE

- Risk assessment methods fall on a spectrum from qualitative to quantitative
  - Each approach has strengths, weaknesses, and preferred use cases
  - Modern Enterprise Risk Management (ERM) frameworks increasingly leverage hybrid approaches that combine the advantages of both

QUALITATIVE RISK ASSESSMENT

- Uses descriptive, non-numeric scales to evaluate likelihood, impact, and priority
  - Relies heavily on expert judgment, interviews, and subjective evaluations
- Characteristics
  - Uses words or discrete categories (e.g., low, medium, high)
  - Often includes ordinal scales (e.g., 1–5), risk matrices, and heat maps
  - SME input is central to identifying emerging risks, understanding context, and assessing controls
  - Useful when numerical data are scarce or uncertainty is high

QUALITATIVE RISK ASSESSMENT

- Strengths
  - Fast and easy to perform
  - Works well with ambiguous, emerging, or strategic risks
  - Encourages discussion among stakeholders and SMEs
  - Helps uncover hidden issues and process weaknesses
  - Minimal data requirements.

QUALITATIVE RISK ASSESSMENT

- Limitations
  - Highly subjective
    - Influenced by cognitive biases (anchoring, availability, groupthink)
  - Inconsistent results across teams, interviews, or time periods
  - “High/Medium/Low” categories oversimplify uncertainty
  - Heat maps can create false precision or distort comparisons
  - Difficult to justify risk decisions to regulators, auditors, or executives seeking numeric analysis

QUALITATIVE RISK ASSESSMENT

- Best use cases
  - Early-stage risk identification
  - Strategic, reputational, cultural, or political risks
  - Areas with incomplete or low-quality data
  - Rapid assessment workshops or preliminary scans

QUANTITATIVE RISK ASSESSMENT

- Assign numeric values to likelihood and impact and use mathematical models to estimate financial exposure
- Characteristics
  - Uses probability values, frequencies, ranges, and distributions
  - Produces monetary loss estimates (e.g., ALE = ARO × SLE)
  - Incorporates statistical techniques such as Monte Carlo simulation, Bayesian models, and regression
  - Draws from loss data, benchmarks, actuarial sources, and threat intelligence

QUANTITATIVE RISK ASSESSMENT

- Strengths
  - Produces replicable, evidence-based results
  - Enables financial decision-making (ROI on controls, capital planning, insurance)
  - Quantifies uncertainty using ranges and distributions
  - Supports advanced modeling of rare/complex events
  - Critical for operational risk, cyber risk, and enterprise decision-making

QUANTITATIVE RISK ASSESSMENT

- Limitations
  - Requires high-quality, consistent data is often missing
  - Can create false precision (“probability = 0.23”)
  - Dependent on assumptions and model calibration
  - Computationally and conceptually more complex for stakeholders
  - Not ideal for emerging risks with no historical data

QUANTITATIVE RISK ASSESSMENT

- Best use cases
  - Financial, cyber, and operational risk
  - Cost-benefit analysis of controls
  - Capital adequacy / reserve calculations
  - Insurance underwriting
  - Strategic budgeting and scenario analysis

COMPARISON

Dimension	Qualitative	Quantitative
Primary Input	Expert judgment, interviews	Data, distributions, statistical models
Output Type	Categories (High/Med/Low)	Numeric (e.g., $250k expected loss)
Accuracy	Lower, depends on SME consistency	Potentially high, data-dependent
Reliability	Variable between assessors	Repeatable if assumptions documented
Validity	Good for context & narrative	Better for measurable financial loss
Complexity	Low to moderate	Moderate to high
Bias Sensitivity	High (anchoring, optimism)	Reduced but still subject to assumptions
Decision Support	Strategic, exploratory	Financial allocation, quantifying tradeoffs

HYBRID RISK ASSESSMENT

- Combine strengths of both qualitative and quantitative methodologies
  - Produces a balanced, defensible, and flexible risk analysis
  - Increasingly popular in ERM, cyber risk, and operational risk programs
- Why hybrid approaches are used
  - Qualitative methods provide context and identification
  - Quantitative methods provide measurement and justification
  - Many risks require both narrative context and financial modeling
  - Data may be available for some components but not others
  - Hybrid methods allow analysts to blend SME insight with data-driven rigor

TYPES OF HYBRID APPROACHES

- Qualitative identification followed by quantitative measurement
  - The most common approach
  - Steps:
    - SMEs identify risks through interviews/workshops
    - Analysts quantify key risks using QRA models
    - Leadership receives both descriptive and numeric insights.
  - Example: ERM programs prioritizing top 10 risks for capital planning

TYPES OF HYBRID APPROACHES

- Quantitative inputs embedded in qualitative models
  - A qualitative heat map supplemented with:
    - Actual loss data
    - Industry benchmarks
    - Threat intelligence
    - Control failure rates
  - Improves validity but keeps the model simple for executives
  - Example: Cyber risk dashboards in IT governance

TYPES OF HYBRID APPROACHES

- Weighted scoring models (semi-quantitative)
  - Ordinal scales are assigned numeric values but weighted:
    - Likelihood scored 1–5
    - Impact scored 1–5
    - Weighted using factors (e.g., 30% frequency, 70% magnitude)
  - Not fully quantitative, but offer more granularity than pure qualitative methods
  - Example: Operational risk committees comparing non-financial risks

TYPES OF HYBRID APPROACHES

- Bayesian/Monte Carlo overlays
  - SME judgments are converted into probability ranges rather than categories
  - Then used in quantitative models
  - Example:
    - SME belief a risk is “likely” is mapped to a probability distribution of 0.3–0.6
    - Monte Carlo simulation produces a distribution of expected loss.
  - Example: Cybersecurity, insurance, business continuity simulations

TYPES OF HYBRID APPROACHES

- FAIR-based hybrid models
  - FAIR decomposes qualitative SME insights into quantitative elements:
    - Threat event frequency
    - Vulnerability
    - Loss magnitude
    - Control strength
  - SMEs give ranges; models convert them to distributions
  - Example: Quantifying cyber risks where data is sparse but SMEs have rich contextual knowledge

STRENGTHS OF HYBRID APPROACHES

- Balanced: context + numbers
  - Provides rich narrative and measurable evidence
- Flexible with data availability
  - Works with both robust datasets and SME estimates
- Reduced bias
  - Quantitative elements counterbalance SME subjectivity
- Better stakeholder communication
  - Qualitative summaries for executives, quantitative details for analysts
- High validity and reliability when designed well
  - Cross-verification strengthens the final result

WEAKNESSES OF HYBRID APPROACHES

- Potential inconsistency
  - Poorly integrated models can blend incompatible scales
- Can become overly complex
  - More components mean heavier documentation and governance
- Requires multidisciplinary skill sets
  - Analyst must understand psychology, qualitative interviewing, and statistics
- Risk of double counting
  - Mixing multiple inputs can overweight certain variables

Q&A AND OPEN DISCUSSION