Lab 3b: Advanced Cybersecurity Risk Quantification

1. Introduction
Welcome to the Cybersecurity Risk Quantification Lab. As a GRC professional, you must translate technical vulnerabilities into business impact. This lab will challenge you to perform end-to-end risk analysis for a critical business system.

2. Scenario
You are the lead GRC analyst at "SecureBank Financial." The CISO has provided you with data from a recent penetration test and vulnerability assessment of your new mobile banking platform. Your task is to quantify the financial risk, evaluate control options, and prepare an executive briefing.

3. Learning Objectives

- Calculate risk exposure using quantitative methods
- Perform cost-benefit analysis for security controls
- Create data-driven recommendations
- Develop executive-level risk reporting with visualizations

4. Dataset: Mobile Banking Platform Assessment

System Context:

- Platform: "SecureMobile" banking application
- User Base: 500,000 active customers
- Average Transaction: $2,500
- Daily Transactions: 50,000

Vulnerability Assessment Results:

Critical Finding 1: API Authentication Bypass

- Exploit Probability: 15%
- Systems Affected: Transaction processing system
- Potential Impact: Unauthorized fund transfers
- Maximum Single Incident Loss: $5,000,000
- Estimated Detection: 48 hours

Critical Finding 2: Database Injection Vulnerability

- Exploit Probability: 25%
- Systems Affected: Customer database
- Potential Impact: Data breach (PII + financial data)

- Records at Risk: 500,000 customer profiles
- Cost per Record: $250 (regulatory + notification)

Critical Finding 3: Session Hijacking

- Exploit Probability: 40%
- Systems Affected: User sessions
- Potential Impact: Account takeover
- Accounts at Risk: 5,000 simultaneous sessions
- Average Loss per Account: $1,500

Control Options:

1. **Advanced API Security Gateway**
   - ➢ Cost: $350,000
   - ➢ Effectiveness: 90% reduction in API vulnerabilities
   - ➢ Maintenance: $50,000/year
2. **Web Application Firewall (WAF)**
   - ➢ Cost: $150,000
   - ➢ Effectiveness: 75% reduction in web vulnerabilities
   - ➢ Maintenance: $25,000/year
3. **Multi-Factor Authentication Enhancement**
   - ➢ Cost: $200,000
   - ➢ Effectiveness: 95% reduction in account takeover
   - ➢ Maintenance: $30,000/year

Phase 1: Risk Exposure Calculation

Task 1: Calculate Annualized Loss Expectancy (ALE)
For each vulnerability, calculate:

- Single Loss Expectancy (SLE)
- Annual Rate of Occurrence (ARO)
- Annualized Loss Expectancy (ALE)

Task 2: Prioritize Risks
Create a risk matrix showing:

- Vulnerability

- SLE
- ARO
- ALE
- Risk Priority Level

Task 3: Create Risk Visualization

- Generate a bar chart comparing ALE for all vulnerabilities
- Create a pie chart showing risk distribution
- Develop a risk heat map (High/Medium/Low) based on probability and impact

Phase 2: Control Evaluation

Task 4: Cost-Benefit Analysis
For each control option, calculate:

- Initial Investment
- Annual Maintenance
- Risk Reduction (in $)
- Return on Investment (ROI)
- Payback Period

Task 5: Control Selection Analysis

- Create a scatter plot showing cost vs. effectiveness of controls
- Generate a bar chart comparing ROI for all controls
- Develop a line graph showing risk reduction over time

Phase 3: Executive Reporting

Task 6: Create Executive Dashboard
Develop a one-page executive summary containing:

- Top 3 risks with financial impact
- Recommended controls with costs
- Expected risk reduction
- ROI calculations

Required Visualizations:

- Risk exposure before/after controls (double bar chart)
- Control investment breakdown (stacked bar chart)

- ROI comparison across controls (horizontal bar chart)

Task 7: Risk Treatment Timeline
Create a Gantt chart showing:

- Immediate actions (first 30 days)
- Short-term controls (90 days)
- Long-term strategy (1 year)

Deliverables

1. **Completed Risk Calculations**

- ➢ ALE for all vulnerabilities
- ➢ Risk prioritization matrix

2. **Control Analysis Worksheet**
    - ➢ Cost-benefit analysis for each control
    - ➢ ROI calculations
3. **Graphical Representations**
    - ➢ Risk exposure chart (Bar/Pie)
    - ➢ Control effectiveness comparison (Scatter Plot)
    - ➢ ROI visualization (Horizontal Bar Chart)
    - ➢ Risk reduction timeline (Line Graph)
    - ➢ Investment breakdown (Stacked Bar Chart)
    - ➢ Risk heat map (Matrix Visualization)
4. **Executive Briefing Package**
    - ➢ One-page dashboard with integrated visuals
    - ➢ Risk treatment plan with Gantt chart
    - ➢ Financial justification with graphs

Graph Requirements:

- All graphs must have proper titles, axis labels, and legends
- Use appropriate colors for different risk levels
- Ensure all financial figures are properly formatted
- Graphs must be professional and executive-ready

Bonus Challenge:
Create a combined risk-control matrix that shows:

- Current risk exposure vs. residual risk after controls
- Control cost vs. risk reduction benefit
- Optimal control selection based on budget constraints

Lab Duration: 3 hours
Tools Required: Calculator, Spreadsheet Software, Presentation Software, Graphing Tools

Note: Show all calculations and maintain proper documentation for your risk decisions. Your work will be reviewed by the CISO and CFO.