Date : 08/10/2025

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)

Answer:

Critical Finding 1: API Authentication Bypass

SLE = $5,000,000

ARO= 15% = 0.15

ALE = SLE x ARO = $5,000,000 x 0.15 = $750000

Critical Finding 2: Database Injection Vulnerability

SLE=Number of records at risk x Cost per record =500,000×$250=$125,000,000

ARO= 25%= 0.25

ALE= SLE x ARO=125,000,000×0.25=$31,250,000

Critical Finding 3: Session Hijacking

SLE=Number of records at risk x Cost per record =5000×$1500=$7,500,000

ARO= 40%= 0.40

ALE= SLE x ARO=75,00,000×0.40=$3,000,000

Task 2: Prioritize Risks

Create a risk matrix showing:

- Vulnerability
- SLE
- ARO
- ALE
- Risk Priority Level

Answer:

Vulnerability	SLE	ARO	ALE	Risk Priority level
API Authentication Bypass	$5,000,000	0.15	$750000	Critical
Database Injection Vulnerability	$125,000,000	0.25	$31,250,000	Critical

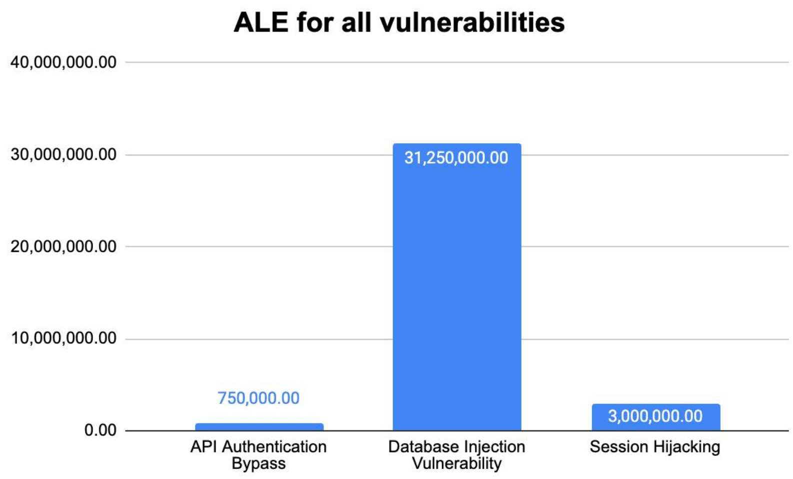
Session Hijacking	$7,500,000	0.4	$3,000,000	Critical

Task 3: Create Risk Visualization

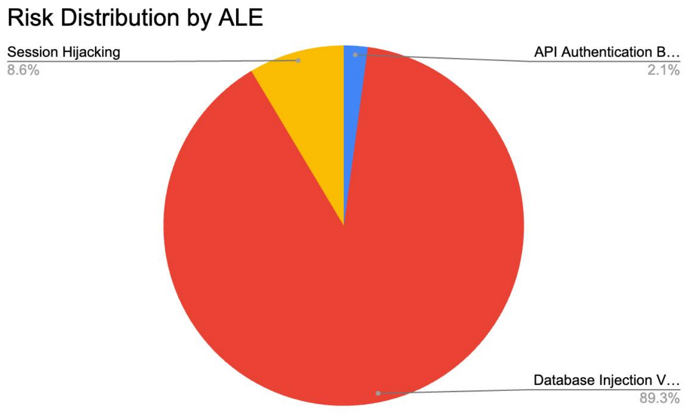
- Generate a bar chart comparing ALE for all vulnerabilities
- Create a pie chart showing risk distribution
- Develop a risk heat map (High/Medium/Low) based on probability and impact

Answer:

Bar Chart for Vulnerabilities



Piechart for Risk Distribution



Determine Risk Level (Matrix Mapping)

Vulnerability	Probability	Impact	Likelihood	Impact	Risk

	(ARO)	(SLE)	Level	Level	Level
API Authentication Bypass	0.15	5,000,000	Low	Low	**Low**
Database Injection Vulnerability	0.25	125,000,000	Medium	High	**High**
Session Hijacking	0.40	7,500,000	Medium	Low	**Medium**

Risk heat map

Impact	5	🟩	🟨	🟥	🟥	🟥
	4	🟩	🟨	🟨	🟥 ●	🟥
	3	🟩	🟨	🟧 ●	🟨	🟨
	2	🟩	🟨	🟨	🟨	🟨
	1	🟩	🟩 ●	🟩	🟩	🟩
		1	2	3	4	5
		Likelihood				

Convention used for the risk matrix above

Scale	Meaning	Risk Level
1	Very Low	Minimal or acceptable risk
2	Low	Manageable risk
3	Medium	Moderate concern
4	High	Significant concern
5	Very High / Critical	Requires immediate mitigation

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

Answer:

1) Advanced API Security Gateway

- Current Risk (ALE) = $750,000
- Effectiveness = 90% = 0.90

  New Risk = 750,000 × (1 − 0.90) = 750,000 × 0.10 = $75,000

  Risk Reduction = 750,000 − 75,000 = $675,000 (annual)

  Initial Investment = $350,000

  Annual Maintenance = $50,000/year

ROI = (Benefit − Cost) ÷ Cost × 100
= (675,000 − 350,000) ÷ 350,000 × 100
= 325,000 ÷ 350,000 × 100 = **92.86%**
Payback Period = Initial Investment ÷ Risk Reduction
= 350,000 ÷ 675,000 = 0.5185 years ≈ 0.52 years ≈ 189 days (~6.2 months)

2) Web Application Firewall (WAF)

- Current Risk (ALE) = $31,250,000
- Effectiveness = 75% = 0.75

  New Risk = 31,250,000 × (1 − 0.75) = 31,250,000 × 0.25 = $7,812,500

  Risk Reduction = 31,250,000 − 7,812,500 = $23,437,500 (annual)

  Initial Investment = $150,000

  Annual Maintenance = $25,000/year

ROI = (23,437,500 − 150,000) ÷ 150,000 × 100
= 23,287,500 ÷ 150,000 × 100 = **15,525%**
Payback Period = 150,000 ÷ 23,437,500 = 0.0064 years ≈ 2.34 days

3) Multi-Factor Authentication (MFA) Enhancement

- Current Risk (ALE) = $3,000,000
- Effectiveness = 95% = 0.95

  New Risk = 3,000,000 × (1 − 0.95) = 3,000,000 × 0.05 = $150,000

  Risk Reduction = 3,000,000 − 150,000 = $2,850,000 (annual)

  Initial Investment = $200,000

  Annual Maintenance = $30,000/year

ROI = (2,850,000 − 200,000) ÷ 200,000 × 100
= 2,650,000 ÷ 200,000 × 100 = **1,325%**
Payback Period = 200,000 ÷ 2,850,000 = 0.0702 years ≈ 25.6 days

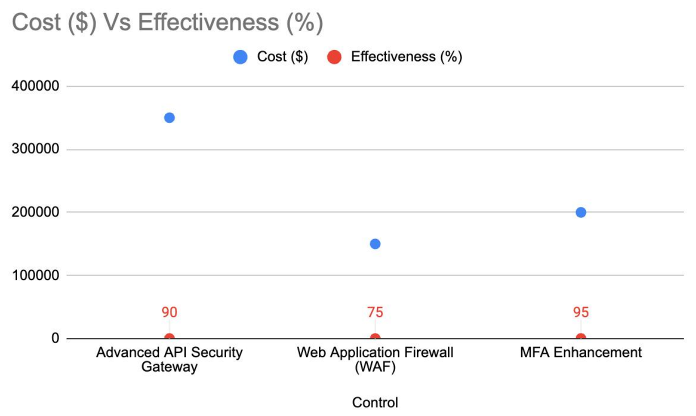
Task 5: Control Selection Analysis

- Create a scatter plot showing cost vs. effectiveness of controls
- Generate a bar chart comparing ROI for all controls

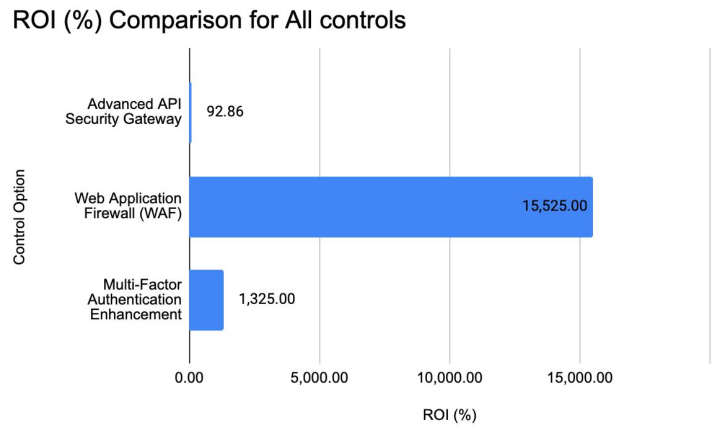
- Develop a line graph showing risk reduction over time

Answer:

Control	Cost ($)	Effectiveness (%)
Advanced API Security Gateway	350,000	90
Web Application Firewall (WAF)	150,000	75
MFA Enhancement	200,000	95

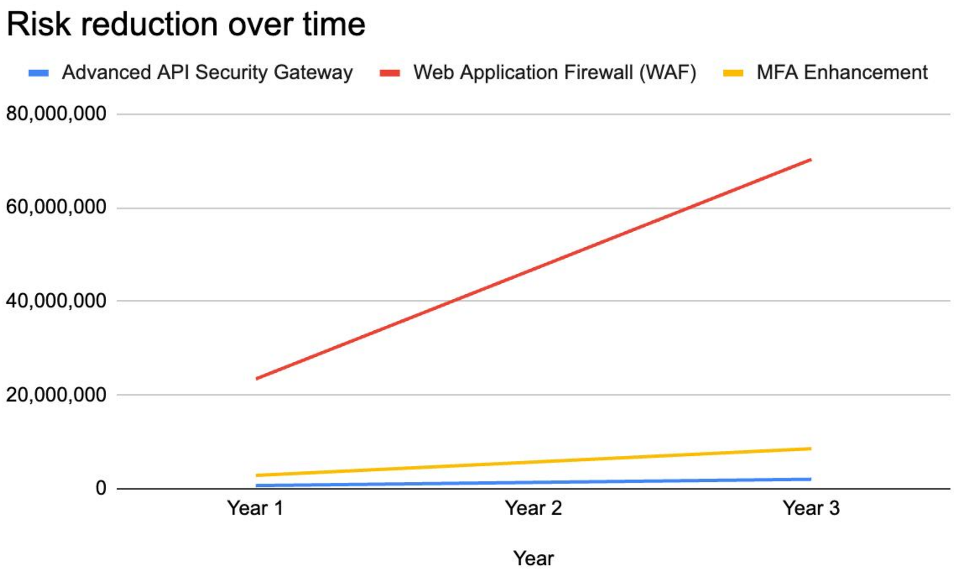


Control Option	ROI (%)
Advanced API Security Gateway	92.86
Web Application Firewall (WAF)	15,525.00
Multi-Factor Authentication Enhancement	1,325.00



Year	Advanced API Security Gateway	Web Application Firewall (WAF)	MFA Enhancement

Year 1	675,000	23,437,500	2,850,000
Year 2	1,350,000	46,875,000	5,700,000
Year 3	2,025,000	70,312,500	8,550,000



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)

Answer:

Executive Summary

1. Top 3 Risks with Financial Impact

Risk	Systems Affected	ALE (Current Annual Loss Expectancy)	Potential Impact
Database Injection Vulnerability	Customer Database	**$31,250,000**	Data breach (PII + financial data)
Session Hijacking	User Sessions	**$3,000,000**	Account Takeover
API Authentication Bypass	API Gateway	**$750,000**	Unauthorized Access

2. Recommended Controls & Costs

Control Option	Initial Cost ($)	Annual Maintenance ($)	Effectiveness (%)	New ALE ($)	Risk Reduction ($)
Advanced API Security Gateway	350,000	50,000	90%	75,000	**675,000**
Web Application Firewall (WAF)	150,000	25,000	75%	7,812,500	**23,437,500**
Multi-Factor Authentication (MFA) Enhancement	200,000	30,000	95%	150,000	**2,850,000**

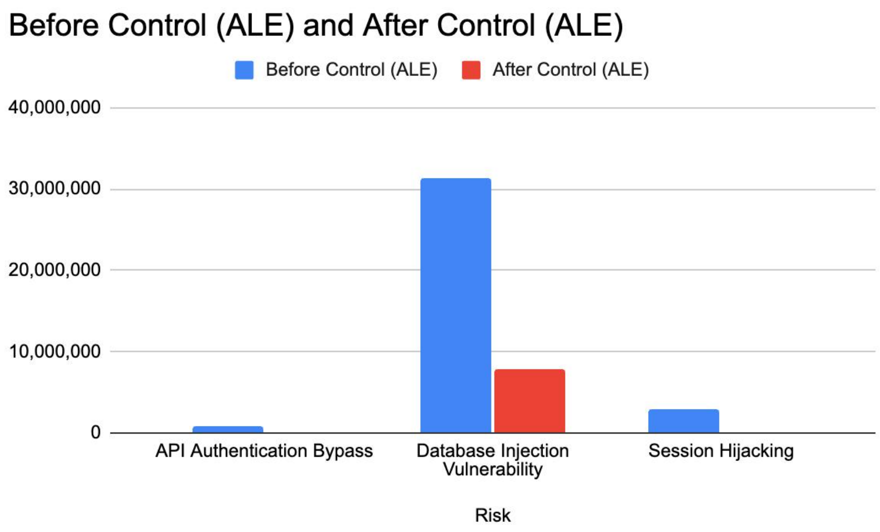
3. ROI Calculations & Payback

Control Option	ROI (%)	Payback Period
Advanced API Security Gateway	**92.86%**	**0.52 yrs (≈189 days)**
Web Application Firewall (WAF)	**15,525%**	**0.0064 yrs (≈2.3 days)**
Multi-Factor Authentication Enhancement	**1,325%**	**≈0.07 yrs (≈25 days)**

1.Double Bar Chart – Risk Exposure Before & After Controls

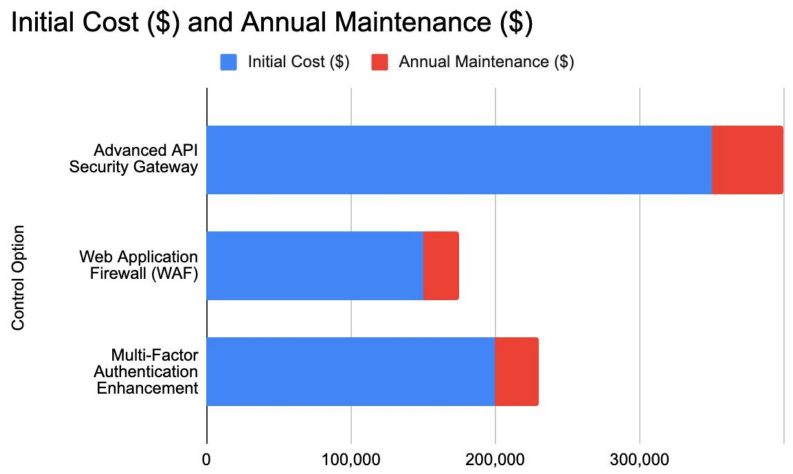
Risk	Before Control (ALE)	After Control (ALE)

API Authentication Bypass	750,000	75,000
Database Injection Vulnerability	31,250,000	7,812,500
Session Hijacking	3,000,000	150,000



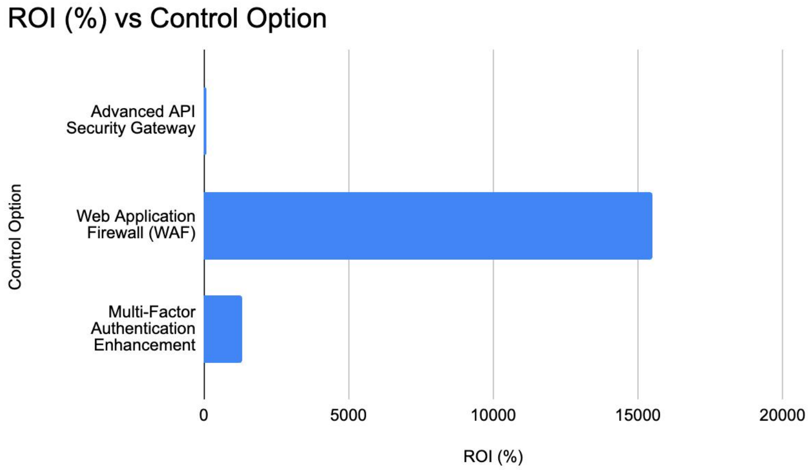
2. Stacked Bar Chart – Control Investment Breakdown

Control Option	Initial Cost ($)	Annual Maintenance ($)
Advanced API Security Gateway	350,000	50,000
Web Application Firewall (WAF)	150,000	25,000
Multi-Factor Authentication Enhancement	200,000	30,000



3. Horizontal Bar Chart – ROI Comparison Across Controls

Control Option	ROI (%)
Advanced API Security Gateway	92.86
Web Application Firewall (WAF)	15,525
Multi-Factor Authentication Enhancement	1,325



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)

Answer:

Task / Control	Category	Start Date	End Date	Duration (Days)	Phase
Conduct immediate API vulnerability patch	Risk Mitigation	01-Oct-2025	30-Oct-2025	30	Immediate
Deploy Web Application Firewall (WAF)	Control Implementation	01-Nov-2025	31-Jan-2026	90	Short-term
Implement Multi-Factor Authentication (MFA) enhancement	Control Implementation	15-Nov-2025	15-Feb-2026	90	Short-term
Deploy Advanced API Security	Infrastructure	01-Dec-	28-Feb-	90	Short-

Gateway	Security	2025	2026		term
Perform security awareness training for staff	Risk Awareness	01-Jan-2026	31-Dec-2026	365	Long-term
Conduct periodic audits and vulnerability scans	Risk Monitoring	01-Mar-2026	31-Dec-2026	300	Long-term
Implement continuous monitoring (SOC integration)	Strategic Initiative	01-Apr-2026	30-Sep-2026	180	Long-term

Gantt Chart link :
https://docs.google.com/spreadsheets/d/1wo8WukdeOoMkVLJRhhAMYNenkbnlkQwXE-fOqFnWtrw/edit?usp=sharing

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.