Exercises: Lesson 7.2 – RegTech — Automating Compliance at Scale

Module 7: The Compliance Problem

Prof. Dr. Joerg Osterrieder

Exercise 1: False Positive Cost Analysis

A mid-sized bank's transaction monitoring system generates the following monthly statistics:

Metric	Value
Total alerts generated	45,000
False positive rate	96%
Average analyst time per alert	40 minutes
Fully loaded analyst cost	\$55 per hour
SARs filed (from true positives)	720

Tasks:

a) Calculate the number of true positives and false positives per month.

b) Calculate the total monthly cost of investigating all alerts.

c) What percentage of total investigation cost is spent on false positives?

d) An ML system reduces the false positive rate to 55% while maintaining the same 1,800 true positives. Calculate the new total alert volume and the monthly cost savings.

e) If the ML system costs \$1.2 million per year to license and maintain, what is the annual net savings (or cost)?

Exercise 2: ML Model Threshold Tuning

An ML transaction monitoring model scores each transaction from 0 (not suspicious) to 1 (highly suspicious). The compliance team tests three score thresholds:

Threshold	Alerts Generated	True Positives Captured	False Positives
0.4	25,000	1,900	23,100
0.6	12,000	1,750	10,250
0.8	5,000	1,400	3,600

Tasks:

a. Calculate the precision (TP / total alerts) and false positive rate for each threshold.

b. If the bank's analysts can review at most 15,000 alerts per month, which threshold(s) are operationally feasible?

c. Calculate the "cost of missed true positives" for threshold 0.8 vs. 0.4, assuming each missed SAR has an expected regulatory penalty of $50,000.

d. Recommend a threshold and justify your choice, balancing operational capacity, detection rate, and regulatory risk.

e. If the team uses a two-tier system (ML auto-clears scores below 0.4 and prioritizes scores above 0.8 for immediate review), what is the remaining middle-tier volume?

Exercise 3: Regulatory Reporting Error Analysis

A bank submits 120 regulatory reports per quarter. The table below shows error rates before and after implementing an XBRL-based automated reporting system:

Metric	Manual Process	XBRL Automated
Reports requiring restatement	12%	1.5%
Average restatement cost	\$18,000	\$4,000
Staff hours per report	45	8
Staff cost per hour	\$65	\$65
System license (per quarter)	—	\$95,000

Tasks:

a. Calculate the quarterly restatement cost under each approach.

b. Calculate the quarterly staff cost for report preparation under each approach.

c. What is the total quarterly cost (staff + restatement + license) for each approach?

d. Calculate the annual net savings from automation.

e. Beyond cost savings, list two non-financial benefits of XBRL automation.

Exercise 4: Biometric Verification System Evaluation

A neobank is evaluating two identity verification vendors. Each vendor processes 50,000 onboarding attempts per month:

Metric	Vendor A	Vendor B
Document verification accuracy	98.5%	99.2%
Facial match accuracy	99.0%	98.5%
Liveness detection accuracy	97.0%	99.5%
Average verification time	45 seconds	90 seconds
Cost per verification	\$0.80	\$1.40
False rejection rate (legitimate users)	3.5%	1.8%

Tasks:

a. Calculate the combined pass-through probability for a legitimate user under each vendor (multiply accuracies of all three stages).

b. If each false rejection costs the neobank \$25 in customer acquisition loss, calculate the monthly false rejection cost for each vendor.

c. Calculate the total monthly cost (verification fees + false rejection costs) for each vendor.

d. Which vendor would you recommend? Consider cost, security (liveness accuracy), and user experience (speed).

e. A deepfake attack targets 500 onboarding attempts per month. How many would each vendor's liveness detection catch?

Exercise 5: Differential Privacy Budget Allocation

A regulator asks a bank to report the average transaction amount per customer segment. The bank wants to use differential privacy to protect individual records.

Given:

- Number of customer segments: 4
- True average transaction amounts: Retail \$85, SME \$2,400, Corporate \$45,000, High-Net-Worth \$125,000
- Total privacy budget: $\varepsilon = 2.0$
- Noise mechanism: Laplace noise with scale $b = \frac{\Delta f}{\varepsilon}$
- Sensitivity Δf: the maximum change from adding/removing one record (assume \$500 for retail, \$5,000 for SME, \$100,000 for corporate, \$250,000 for HNW)

Tasks:

a. If the bank splits the budget equally across 4 queries ($\varepsilon_i = 0.5$ each), calculate the Laplace noise scale b for each segment.

b. Calculate the expected noise as a percentage of the true average for each segment. Which segment has the worst signal-to-noise ratio?

c. Suggest a non-uniform budget allocation that reduces noise for the most sensitive segment. Justify your allocation.

Exercise 6: Federated Learning vs. Centralized Training

A consortium of three banks considers two approaches to training a shared AML detection model:

Bank	Transactions/month	SARs filed/month	SAR rate
Bank A	12,000,000	3,600	0.030%
Bank B	3,000,000	1,200	0.040%
Bank C	800,000	480	0.060%

Tasks:

a. If all data were pooled (centralized), calculate the combined SAR rate.

b. In federated learning, each bank trains locally and sends gradients. If Bank C's local model achieves 85% recall (true positive rate) alone but the federated model achieves 92%, how many additional true SARs does Bank C detect per month?

c. What privacy risk exists in centralized training that federated learning eliminates?

d. Identify one weakness of federated learning when banks have very different transaction profiles.

e. If Bank B leaves the consortium, estimate the impact on the federated model's ability to detect cross-bank layering schemes.

Exercise 7: RegTech Return on Investment

A bank is evaluating a RegTech platform that consolidates transaction monitoring, regulatory reporting, and KYC into a single system. Current and projected costs:

Cost Category	Current Annual	With RegTech
Compliance staff (FTE $\times$ salary)	\$8,500,000	\$4,200,000
Legacy system licenses	\$1,800,000	\$0
RegTech platform license	\$0	\$2,400,000
Implementation (Year 1 only)	\$0	\$1,500,000
Regulatory fines (3-year avg.)	\$3,200,000	\$800,000
Training and change management	\$0	\$350,000

Tasks:

a. Calculate the total cost of ownership (TCO) for Year 1 under each scenario.

b. Calculate the TCO for Years 2–3 (assume no implementation or training costs).

c. Calculate the 3-year cumulative savings.

d. Calculate the simple payback period (months until cumulative savings exceed cumulative implementation and transition costs).

e. List two risks that could reduce the actual ROI below the projected figures.

Exercise 8: Secure MPC for Sanctions Screening

Two banks want to check whether any of their customers appear on the other bank's internal watchlist, without revealing their full customer lists.

Setup:

- Bank X has 2,000,000 customers
- Bank Y has 1,500,000 customers
- They use a Private Set Intersection (PSI) protocol (a form of secure MPC)
- PSI reveals only the intersection (common entries), not the non-matching records
- Computational cost: 0.002 seconds per comparison pair
- The naive approach compares every customer in X against every customer in Y

Tasks:

a. How many comparison pairs would the naive approach require? Estimate the total computation time.

b. A hash-based PSI optimization reduces comparisons to $O(n + m)$ rather than $O(n \times m)$. Calculate the new number of operations and computation time.

c. If the match rate is 0.05%, how many shared customers are expected?

d. What information does each bank learn from the PSI result? What information remains hidden?

Answer Key (1/3)

Exercise 1:

(a) TP: $45{,}000 \times 0.04 = 1{,}800$. FP: $45{,}000 \times 0.96 = 43{,}200$.

(b) Cost: $45{,}000 \times (40/60) \times 55 = 45{,}000 \times 36.67 = \$1{,}650{,}000$/month.

(c) FP cost share: $43{,}200/45{,}000 = 96\%$ of total cost = $\$1{,}584{,}000$.

(d) New total: $1{,}800/(1 - 0.55) = 4{,}000$ alerts. New cost: $4{,}000 \times 36.67 = \$146{,}667$. Savings: $\$1{,}650{,}000 - 146{,}667 = \$1{,}503{,}333$/month.

(e) Annual savings: $\$1{,}503{,}333 \times 12 = \$18{,}040{,}000$. Net: $\$18{,}040{,}000 - 1{,}200{,}000 = \$16{,}840{,}000$.

Exercise 2:

(a) 0.4: precision = $1{,}900/25{,}000 = 7.6\%$, FPR = 92.4%. 0.6: $1{,}750/12{,}000 = 14.6\%$, FPR = 85.4%. 0.8: $1{,}400/5{,}000 = 28.0\%$, FPR = 72.0%.

(b) 0.6 and 0.8 (both $\leq 15{,}000$).

(c) Missed TPs at 0.8 vs. 0.4: $1{,}900 - 1{,}400 = 500$. Cost: $500 \times 50{,}000 = \$25{,}000{,}000$.

(d) 0.6 recommended: feasible volume (12,000), captures 1,750 TPs (92% of max), balanced risk.

(e) Middle tier (0.4–0.8): $25{,}000 - 5{,}000 = 20{,}000$. But auto-cleared below 0.4, so middle = scores 0.4–0.8 = $25{,}000 - 5{,}000 = 20{,}000$ alerts requiring standard review.

Answer Key (2/3)

Exercise 3:

(a) Manual: $120 \times 0.12 \times 18{,}000 = \$259{,}200$. Auto: $120 \times 0.015 \times 4{,}000 = \$7{,}200$.

(b) Manual: $120 \times 45 \times 65 = \$351{,}000$. Auto: $120 \times 8 \times 65 = \$62{,}400$.

(c) Manual total: \$610,200. Auto total: $62{,}400 + 7{,}200 + 95{,}000 = \$164{,}600$.

(d) Quarterly saving: \$445,600. Annual: \$1,782,400.

(e) (i) Faster regulatory response time. (ii) Audit trail with machine-validated data lineage.

Exercise 4:

(a) A: $0.985 \times 0.990 \times 0.970 = 94.56\%$. B: $0.992 \times 0.985 \times 0.995 = 97.22\%$.

(b) A: $50{,}000 \times 0.035 \times 25 = \$43{,}750$. B: $50{,}000 \times 0.018 \times 25 = \$22{,}500$.

(c) A: $50{,}000 \times 0.80 + 43{,}750 = \$83{,}750$. B: $50{,}000 \times 1.40 + 22{,}500 = \$92{,}500$.

(d) Vendor B recommended despite higher total cost: 99.5% liveness accuracy is critical for fraud prevention; 1.8% false rejection is significantly better UX; 90-second verification is still fast.

(e) A: $500 \times 0.970 = 485$ caught. B: $500 \times 0.995 = 498$ caught. B catches 13 more deepfake attacks.

Answer Key (3/3)

Exercise 5:

(a) $b = \Delta f / \varepsilon_i$. Retail: $500/0.5 = 1{,}000$. SME: $5{,}000/0.5 = 10{,}000$. Corp: $100{,}000/0.5 = 200{,}000$. HNW: $250{,}000/0.5 = 500{,}000$.

(b) Noise/avg: Retail $1{,}000/85 = 1{,}176\%$. SME $10{,}000/2{,}400 = 417\%$. Corp $200{,}000/45{,}000 = 444\%$. HNW $500{,}000/125{,}000 = 400\%$. Retail has worst ratio.

(c) Allocate more budget to high-sensitivity segments. E.g., Retail $\varepsilon = 0.2$, SME $\varepsilon = 0.4$, Corp $\varepsilon = 0.6$, HNW $\varepsilon = 0.8$ (total $= 2.0$). HNW noise: $250{,}000/0.8 = 312{,}500$ (vs. 500,000). Retail noise: $500/0.2 = 2{,}500$ (still high, but retail has lower regulatory sensitivity).

Exercise 6:

(a) Combined: $(3{,}600 + 1{,}200 + 480)/(12M + 3M + 0.8M) = 5{,}280/15{,}800{,}000 = 0.0334\%$.

(b) Extra TPs: $480 \times (0.92 - 0.85) = 480 \times 0.07 = 33.6 \approx 34$ additional SARs/month.

(c) Centralized training requires raw data pooling, exposing all customer records to a shared environment.

(d) Model may overfit to large-bank patterns; small-bank typologies underrepresented.

(e) Reduced ability to detect layering patterns that involve Bank B as an intermediary.

Exercise 7: (a) Current Y1: $8.5M + 1.8M + 3.2M = \$13.5M$. RegTech Y1: $4.2M + 2.4M + 1.5M + 0.8M + 0.35M = \$9.25M$. (b) Current Y2–3: $\$13.5M \times 2 = \$27.0M$. RegTech Y2–3: $(4.2M + 2.4M + 0.8M) \times 2 = \$14.8M$. (c) 3-yr savings: $(13.5M + 27.0M) - (9.25M + 14.8M) = \$16.45M$. (d) Monthly savings Y1: $(13.5M - 9.25M)/12 = \$354K$/mo. Payback $\approx$ 5–6 months. (e) Implementation delays; vendor lock-in increasing future license costs.

Exercise 8: (a) $2M \times 1.5M = 3 \times 10^{12}$ pairs. Time: $3 \times 10^{12} \times 0.002 = 6 \times 10^{9}$ sec $\approx$ 190 years. (b) $O(n + m) = 3.5M$ ops. Time: $3.5M \times 0.002 = 7{,}000$ sec $\approx$ 2 hours. (c) $\min(2M, 1.5M) \times 0.0005 = 750$ shared customers. (d) Each bank learns only the 750 matched identities; all non-matching customers remain hidden.