Lesson 4.4 Exercises: The New Risk Landscape

Module 4: The Risk Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Exercise 1: NIST Framework Mapping

Scenario: A mid-size European bank experiences the following cybersecurity events during a single quarter:

1. An employee clicks a phishing link, installing malware on their workstation
2. The bank's intrusion detection system flags unusual outbound traffic from the infected machine 4 hours later
3. The incident response team isolates the workstation and blocks the command-and-control IP address
4. A forensic investigation determines that no customer data was exfiltrated
5. IT restores the workstation from a clean backup and patches the vulnerability

Tasks:

a) Map each event (1–5) to the appropriate NIST CSF function (Identify, Protect, Detect, Respond, Recover). Justify each mapping in one sentence.

b) Which NIST function **failed** in this scenario? What specific control could have prevented the initial compromise?

c) The bank has no formal asset inventory. Explain how this gap in the Identify function could make events 2–5 *more difficult or less effective*.

Difficulty: Introductory — tests understanding of the NIST CSF lifecycle.

Exercise 2: Order Book and Execution Cost

Scenario: The following synthetic order book is displayed for stock XYZ at 10:00 AM:

Bids (Buy)		Asks (Sell)	
Price (€)	**Qty (shares)**	**Price (€)**	**Qty (shares)**
49.95	500	50.05	300
49.90	800	50.10	600
49.85	1,200	50.15	400
49.80	600	50.20	1,000

Tasks:

a. What is the current bid-ask spread (in € and in basis points relative to the midpoint)?

b. A trader submits a **market sell order** for 1,500 shares. Walk through the execution step by step: how many shares fill at each bid level? What is the volume-weighted average execution price (VWAP)?

c. Compare the VWAP to the midpoint price. Express the execution cost (slippage) in € per share and as a percentage.

d. If the trader instead used an **iceberg order** (hidden quantity) to sell 1,500 shares in batches of 200, what is the likely impact on execution quality?

Difficulty: Intermediate — requires arithmetic and microstructure reasoning.

Exercise 3: Physical vs. Transition Risk Classification

Scenario: A bank's credit portfolio includes loans to the following borrowers. For each, determine whether the primary climate-related risk is **physical**, **transition**, or **both**.

Borrower	Description
A	A coastal hotel chain in Southeast Asia
B	A German coal-fired power plant operator
C	An agricultural cooperative in sub-Saharan Africa
D	An electric vehicle manufacturer
E	A commercial real estate developer in a flood-prone European city
F	A diversified oil & gas major with a renewables division

Tasks:

a. Classify each borrower (A–F) as primarily facing physical risk, transition risk, or both. Justify each in one sentence.

b. For borrower F, explain why a 1.5°C scenario might actually *benefit* part of the business while harming another part.

c. Which borrower faces the highest risk of holding **stranded assets**? Explain using the carbon budget concept.

Difficulty: Introductory — tests classification of climate risk channels.

Exercise 4: DeFi Composability Cascade

Scenario: Consider the following DeFi stack:

1. **Base layer:** A lending protocol (Protocol A) accepts ETH as collateral and issues a synthetic stablecoin (sUSD)
2. **Layer 2:** A yield farming protocol (Protocol B) accepts sUSD and issues yield tokens (yBT)
3. **Layer 3:** A leveraged trading protocol (Protocol C) accepts yBT as collateral for leveraged positions

Tasks:

a) Draw a dependency diagram showing which protocol depends on which.

b) Suppose the ETH price drops 25% in 10 minutes. Trace the cascade: what happens at each layer? Be specific about liquidation triggers and collateral shortfalls.

c) Now suppose the oracle feeding ETH/USD prices to Protocol A goes offline for 5 minutes during the crash. How does this **worsen** the cascade?

d) Propose two design changes (one at the protocol level, one at the ecosystem level) that could reduce the severity of this cascade.

Difficulty: Advanced — requires tracing multi-layer DeFi dependency chains.

Exercise 5: Flash Crash Mechanism

Scenario: At 14:32:00, a synthetic stock index is trading at 4,200 points. The following sequence of events occurs:

1. 14:32:05 — A large algorithmic sell order of 50,000 contracts is submitted
2. 14:32:06 — Market makers absorb the first 10,000 contracts; index drops to 4,180
3. 14:32:08 — Market makers pull remaining quotes (liquidity withdrawal)
4. 14:32:10 — Stop-loss orders at 4,175 are triggered, adding 30,000 sell contracts
5. 14:32:15 — Index reaches 4,050 (a 3.6% drop in 10 seconds)
6. 14:32:30 — The exchange activates a circuit breaker; trading pauses for 5 minutes
7. 14:37:30 — Trading resumes; index recovers to 4,185 within 3 minutes

Tasks:

a) Identify the three feedback loops that amplified the initial sell order into a flash crash.

b) Explain why the market makers withdrew quotes at step 3. Use the concept of adverse selection.

c) A trader had a stop-loss at 4,175. Their order executed at 4,080 (95 points of slippage). Explain why the execution price was so far from the trigger price.

d) Evaluate the circuit breaker: did it help or merely delay the problem? What are the trade-offs?

Difficulty: Advanced — requires dynamic analysis of microstructure feedback loops.

Exercise 6: Supply-Chain Cyber Attack

Scenario: A major financial software vendor (used by 200 banks globally) is compromised. The attacker inserts a backdoor into a routine software update. Within 48 hours, 200 banks have installed the malicious update.

Tasks:

a) Classify this attack using the cyber attack taxonomy: what type of attack is this (phishing, ransomware, supply-chain, insider, DDoS)?

b) Explain why this attack type is **particularly dangerous** for the financial system (think: correlation, contagion, detection difficulty).

c) Map the ideal response to NIST CSF functions. For each of the five functions, describe one specific action the affected banks should take.

d) A risk model treats cyber events as independent across banks. Explain why this supply-chain attack violates the independence assumption and what this means for systemic risk estimation.

Difficulty: Intermediate–Advanced — applies NIST CSF to a systemic cyber scenario.

Exercise 7: Evaluating a TCFD Disclosure

Scenario: A large European bank publishes the following TCFD-aligned climate risk disclosure excerpt:

> *"The Board reviews climate risks annually. Our strategy includes a commitment to net-zero financed emissions by 2050. We assess climate risk using qualitative expert judgment. Our Scope 1 and 2 emissions declined 15% last year. We do not currently measure Scope 3 financed emissions."*

Tasks:

a. Map each sentence of the disclosure to a TCFD pillar (Governance, Strategy, Risk Management, Metrics & Targets). Note any pillar that is missing or inadequately addressed.

b. The bank uses "qualitative expert judgment" for risk assessment. Critique this approach: what are its limitations compared to quantitative scenario analysis (e.g., NGFS scenarios)?

c. The bank omits Scope 3 (financed emissions). For a bank, which scope typically dominates total emissions? Why is this omission problematic?

d. Draft two specific recommendations for improving this disclosure, citing the TCFD guidance.

Difficulty: Advanced — requires critical evaluation of a real-world-style disclosure.

Exercise 8: Compound Risk Scenario Design

Scenario: You are a risk manager at a bank with exposure to:

- A DeFi lending platform (through a subsidiary)
- A portfolio of fossil fuel corporate bonds
- Heavy reliance on a single cloud provider for core banking

Tasks:

a. Design a "compound stress scenario" that involves *all three* new risk types (cyber, DeFi, climate) materializing in a correlated sequence. Describe the triggering event, the transmission channels, and the expected portfolio impact.

b. For each leg of your scenario, identify which traditional risk category (market, credit, operational, liquidity) it maps to. Show that a single new risk event can trigger losses across multiple traditional categories.

c. Explain why a siloed risk management approach (separate cyber, climate, and DeFi risk teams) would **underestimate** the total loss in your compound scenario.

d. Propose three concrete actions the bank's risk committee should take to prepare for compound risk scenarios. For each, specify the responsible function (CRO, CISO, Board, etc.).

Difficulty: Advanced–Integrative — synthesizes all lesson concepts into a scenario design.

Answer Key

Exercise 1:

(a) (1) Protect failed (email filtering/training); (2) Detect (IDS flagged anomaly); (3) Respond (isolation, blocking); (4) Respond/Recover (forensics confirmed no breach); (5) Recover (restoration from backup).

(b) Protect failed — a phishing-aware email gateway or mandatory security awareness training could have prevented the initial click.

(c) Without an asset inventory (Identify), the team cannot determine which systems the infected workstation had access to, what data was at risk, or whether the forensic scope was complete. Detection is slower, response is less targeted, and recovery may miss affected systems.

Exercise 2:

(a) Spread $= €50.05 - €49.95 = €0.10$. Midpoint $= €50.00$. Spread in bps $= 0.10/50.00 \times 10{,}000 = 20$ bps.

(b) Fill 500 at €49.95, 800 at €49.90, 200 at €49.85. VWAP $= (500 \times 49.95 + 800 \times 49.90 + 200 \times 49.85)/1{,}500 = e\,49.907$.

(c) Slippage $= 50.00 - 49.907 = e\,0.093$/share $= 0.186\%$.

(d) An iceberg order would reveal only 200 shares at a time, reducing information leakage and potentially achieving better average execution as other participants do not see the full order size.

Answer Key (continued)

Exercise 3:

(a) A: Physical (coastal flooding, storm damage). B: Transition (carbon regulation, stranded plant). C: Physical (drought, temperature stress). D: Transition (benefits from it — but supply-chain disruption possible). E: Both (flood damage = physical; building codes tightening = transition). F: Both (fossil fuel arm = transition risk; renewables arm = transition opportunity).

(b) In a 1.5°C scenario, aggressive carbon pricing harms the fossil fuel division (stranded reserves), but accelerates demand for renewables, benefiting the renewables division. The net effect depends on the relative size of each business unit.

(c) Borrower B (coal plant). Coal has the highest carbon intensity per MWh. Under a 1.5°C carbon budget, most coal reserves cannot be burned, making the plant a stranded asset.

Exercise 4:

(a) Protocol C depends on yBT from Protocol B, which depends on sUSD from Protocol A, which depends on ETH collateral value and oracle price feeds.

(b) ETH drops 25% $\longrightarrow$ Protocol A liquidates undercollateralized positions $\longrightarrow$ sUSD supply shrinks or depegs $\longrightarrow$ Protocol B's collateral (sUSD) loses value $\longrightarrow$ yBT devalues $\longrightarrow$ Protocol C liquidates leveraged positions $\longrightarrow$ forced selling amplifies ETH price decline.

(c) Without oracle updates, Protocol A cannot trigger liquidations, allowing positions to become deeply undercollateralized. When the oracle comes back, a sudden batch of liquidations hits simultaneously, causing a sharper cascade.

(d) Protocol-level: implement dynamic collateral ratios that increase during volatility. Ecosystem-level: create cross-protocol risk monitoring dashboards or inter-protocol circuit breakers.

Answer Key (continued)

Exercise 5:

(a) (1) Liquidity consumption: the initial sell exhausts top-of-book liquidity. (2) Liquidity withdrawal: market makers pull quotes, creating a vacuum. (3) Stop-loss cascade: triggered stops add sell volume, further depressing prices.

(b) Market makers withdrew because the large sell order signaled either a better-informed counterparty or a structural shift. Continuing to buy exposes them to adverse selection — buying at a price that is about to fall further.

(c) The stop-loss triggered at 4,175, but with market makers absent and order flow overwhelmingly one-sided, there were no bids near 4,175. The order "gapped" through the empty book and executed at the next available bid (4,080).

(d) The circuit breaker halted the cascade and allowed participants to reassess. The recovery to 4,185 suggests the crash was driven by a liquidity vacuum, not fundamentals. Trade-off: circuit breakers may trap liquidity providers in losing positions and create uncertainty about when trading resumes.

Exercise 6:

(a) Supply-chain attack: the compromise occurs at a trusted third-party vendor, not at the target banks.

(b) Correlation: all 200 banks are compromised simultaneously through the same vector. Contagion: the shared vendor creates a single point of failure for the entire system. Detection: the malware arrives via a trusted update channel, bypassing standard defenses.

(c) Identify: inventory all systems using the vendor's software. Protect: segment networks to limit lateral movement. Detect: scan for indicators of compromise associated with the backdoor. Respond: isolate affected systems, revoke the update. Recover: restore from pre-update backups, patch independently.

(d) The supply-chain vector introduces perfect positive correlation across all 200 banks. Independence-based models would estimate the probability of 200 simultaneous breaches as astronomically low, when in reality the shared vector makes it a single event affecting all.

Answer Key (continued)

Exercise 7:

(a) "Board reviews annually" → Governance. "Net-zero by 2050" → Strategy. "Qualitative expert judgment" → Risk Management. "Scope 1&2 declined 15%" → Metrics & Targets. Risk Management is inadequately addressed (no quantitative methodology). Metrics & Targets is incomplete (no Scope 3).

(b) Qualitative judgment is subjective, non-reproducible, and cannot be stress-tested. It provides no quantitative loss estimates, cannot be compared across institutions, and does not explore tail scenarios. NGFS scenarios provide standardized, quantitative pathways that can be integrated into existing risk models.

(c) For banks, Scope 3 (financed emissions from lending and investment portfolios) typically represents >95% of total emissions. Omitting Scope 3 means the bank's climate impact is massively understated, and its transition risk exposure is unquantified.

(d) (1) Adopt quantitative scenario analysis using NGFS scenarios to assess transition and physical risk impacts on the loan portfolio. (2) Begin measuring and disclosing Scope 3 financed emissions using the PCAF standard, with interim targets for high-carbon sectors.

Exercise 8:

(a) Example compound scenario: A heatwave (physical climate risk) strains the cloud provider's data center cooling, causing an outage (operational/cyber). Simultaneously, the heatwave triggers agricultural commodity price spikes, which are fed to the DeFi lending platform via oracle, causing a composability cascade (DeFi risk). Meanwhile, a policy announcement on carbon pricing reprices the fossil fuel bond portfolio (transition risk).

(b) Cloud outage = operational risk. DeFi liquidation = market + credit risk. Bond repricing = market risk. Liquidity squeeze from simultaneous selling = liquidity risk. One triggering event (heatwave + policy) cascades into all four traditional categories.

(c) Siloed teams would estimate each risk independently and sum the losses. But the scenario creates *reinforcing* feedback: the cloud outage prevents the bank from managing its DeFi exposure during the cascade, amplifying losses beyond the sum of parts.

(d) (1) CRO: conduct annual compound stress tests that explicitly combine cyber, DeFi, and climate scenarios. (2) CISO: ensure disaster recovery for cloud infrastructure includes geographically diverse backup during extreme weather. (3) Board: require integrated risk reporting that shows cross-risk correlations, not just siloed metrics.