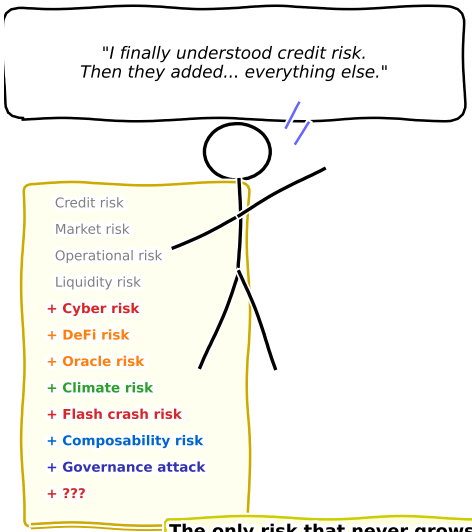
Lesson 4.4: The New Risk Landscape

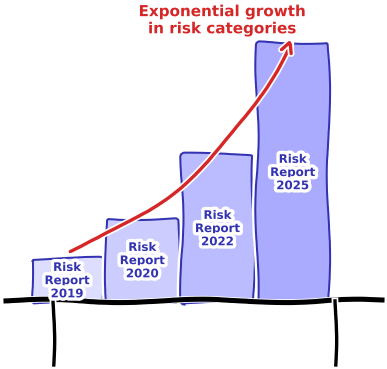
Module 4: The Risk Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

The Risk Manager's Infinite List





The only risk that never grows: the budget for the risk team.

Learning Objectives

After completing this lesson, you will be able to:

1. **Describe** the major categories of cyber threats facing financial institutions and map them to the NIST Cybersecurity Framework [Understand]
2. **Apply** zero-trust principles to a financial network architecture [Apply]
3. **Classify** DeFi-specific risks (composability, oracle, governance) and explain how they differ from traditional finance risks [Analyze]
4. **Interpret** an order book, bid-ask spread, and flash crash dynamics in terms of market microstructure risk [Analyze]
5. **Evaluate** climate-related financial risks using the TCFD framework, distinguishing transition risk from physical risk [Evaluate]

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.

From Frameworks to Frontiers

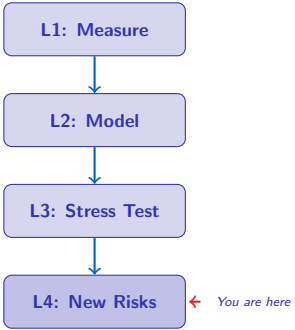
Lessons 4.1–4.3 asked: How do we measure, model, and stress-test risk using established frameworks?

Lesson 4.4 asks: What happens when the **risk landscape itself** changes faster than our models?

Three new frontiers:

- **Cyber risk** — attacks on the digital infrastructure of finance
- **DeFi risk** — composability failures, oracle manipulation, governance attacks
- **Climate risk** — transition costs, physical damage, stranded assets

Common thread: All three are systemic, hard to quantify, and absent from most legacy risk models.



Institutional frameworks exist. But the risk landscape itself is changing.

Definition: Cyber Risk

Cyber risk is the potential for financial loss, operational disruption, or reputational damage caused by failures of, or attacks on, information technology systems.

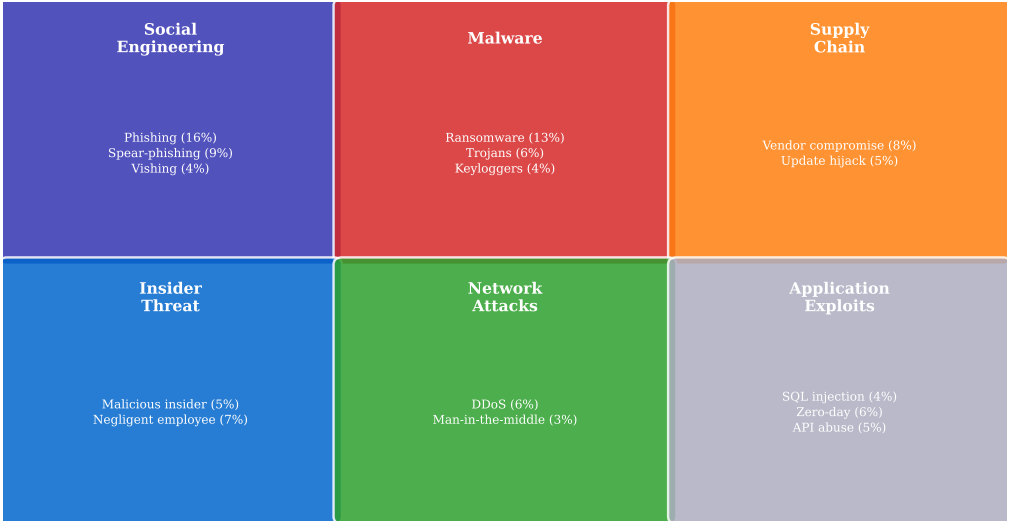
What makes cyber risk unique:

- **Asymmetric:** A single attacker can threaten an entire institution
- **Non-stationary:** Attack methods evolve continuously; historical data is a poor guide
- **Correlated:** A zero-day vulnerability can hit thousands of firms simultaneously
- **Hard to insure:** Correlations violate the independence assumptions of insurance pricing
- **Contagious:** Supply-chain attacks propagate through vendor relationships

Key insight: Traditional VaR and ES models assume risk factors are drawn from stationary distributions. Cyber risk violates this assumption fundamentally.

Cyber risk is adversarial, non-stationary, and correlated — it breaks most classical risk models.

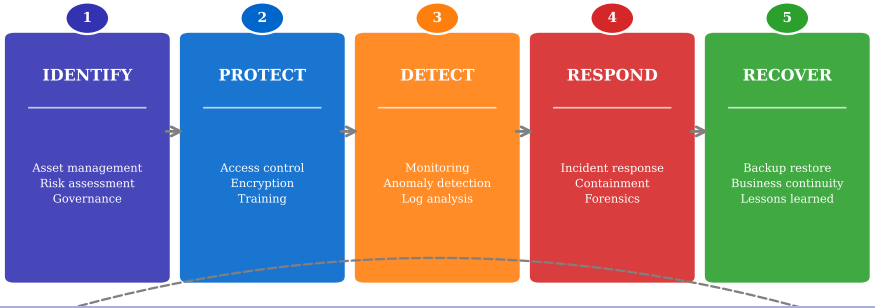
Cyber Attack Taxonomy for Financial Institutions
(synthetic classification, illustrative)



Definition: NIST CSF

The **NIST Cybersecurity Framework** (CSF) is a voluntary guidance framework published by the U.S. National Institute of Standards and Technology. It organizes cybersecurity activities into five core functions: Identify, Protect, Detect, Respond, Recover.

NIST Cybersecurity Framework: Five Core Functions



Definition: Zero Trust

Zero trust is a security model that assumes *no user, device, or network segment is inherently trustworthy*, even if it is inside the corporate firewall. Every access request must be authenticated, authorized, and continuously validated.

Core principles:

1. **Verify explicitly:** Authenticate and authorize every request using all available data (identity, location, device health, anomaly signals)
2. **Least-privilege access:** Grant the minimum permissions needed, for the minimum time
3. **Assume breach:** Design the network so that a compromised component cannot move laterally to other systems

Why finance is adopting zero trust:

- Cloud migration removes the traditional perimeter
- Remote work expands the attack surface
- Regulatory pressure (e.g., DORA in the EU) requires demonstrated resilience

Zero trust replaces "trust but verify" with "never trust, always verify" — a paradigm shift for financial networks.

DeFi Risk Is Structurally Different

Decentralized Finance (DeFi) removes intermediaries but introduces entirely new risk categories:

Risk Dimension	Traditional Finance	DeFi
Counterparty	Known; regulated entities	Pseudonymous; smart contracts
Operational	IT failures, human error	Code bugs, key management
Regulatory	Established frameworks	Unclear, evolving jurisdiction
Systemic	Too-big-to-fail banks	Composability cascades
Governance	Board of directors	Token-weighted voting

Key insight: DeFi does not eliminate risk — it transforms the risk from institutional to technological.

DeFi shifts risk from "who do you trust?" to "what code do you trust?"

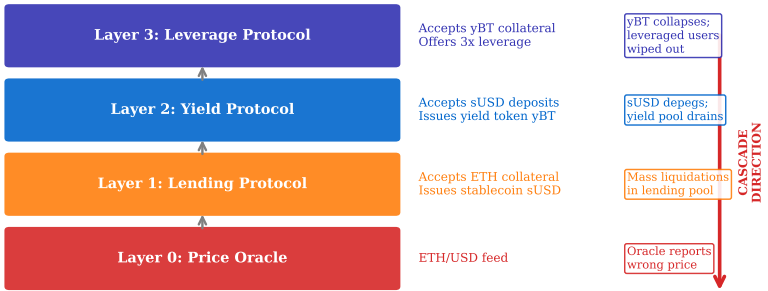
DeFi Risk Taxonomy

Composability Risk: “Money Legos” Can Topple

Definition: Composability Risk

Composability risk arises when multiple DeFi protocols are stacked on top of each other (“money Legos”). A failure in one layer can cascade through every protocol that depends on it.

DeFi Composability Risk: Cascade Through Protocol Stack
(synthetic scenario, illustrative)



Oracle Risk

Definition: Oracle Risk

Oracle risk is the risk that a smart contract receives incorrect external data (e.g., asset prices) from an oracle, leading to unintended liquidations, mispriced trades, or protocol insolvency.

How oracle manipulation works:

1. Attacker manipulates the price on a low-liquidity exchange
2. The oracle reports this manipulated price to the smart contract
3. The smart contract triggers liquidations or allows the attacker to borrow at a distorted collateral ratio
4. The attacker profits; other users suffer losses

Mitigation approaches:

- **Time-weighted average prices (TWAPs):** Smooth price feeds over multiple blocks
- **Multi-source oracles:** Aggregate data from many independent sources
- **Circuit breakers:** Halt protocol execution if price deviates beyond a threshold

---

Oracles are the bridge between the real world and the blockchain — and they are a single point of failure.

Definition: Governance Attack

A **governance attack** occurs when an actor accumulates enough governance tokens (often via a flash loan) to unilaterally pass a malicious proposal — for example, draining the protocol treasury or changing key parameters to their advantage.

Attack pattern:

1. Flash-borrow a large quantity of governance tokens (zero upfront cost)
2. Vote to pass a malicious proposal in a single transaction
3. Execute the proposal before the community can react
4. Return the borrowed tokens and keep the profit

Defenses:

- **Time locks:** Proposals must wait a minimum period before execution
- **Quorum requirements:** A minimum participation threshold must be met
- **Vote-escrow mechanisms:** Only tokens locked for a period can vote (flash loans cannot satisfy this)

Governance attacks exploit the tension between permissionless participation and protocol security.

What Is Market Microstructure?

Definition: Market Microstructure

Market microstructure is the study of how the specific mechanisms and rules of a trading venue affect price formation, transaction costs, and information flow. It examines the "plumbing" of financial markets.

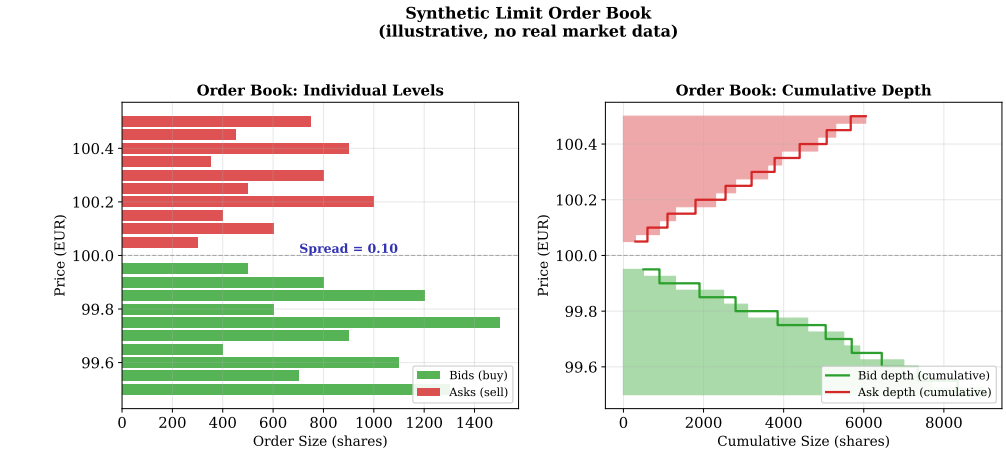
Why risk managers care about microstructure:

- Execution risk: the price you see is not always the price you get
- Liquidity risk: markets can appear deep but evaporate in seconds
- Information asymmetry: some participants have faster access to information
- Technology risk: algorithmic glitches can trigger cascading sell-offs

Key insight: Risk is not just about *what* you hold — it is also about *how* and *where* you trade it.

Market microstructure determines the actual cost and risk of executing trades — the gap between theory and practice.

The Order Book: Where Supply Meets Demand



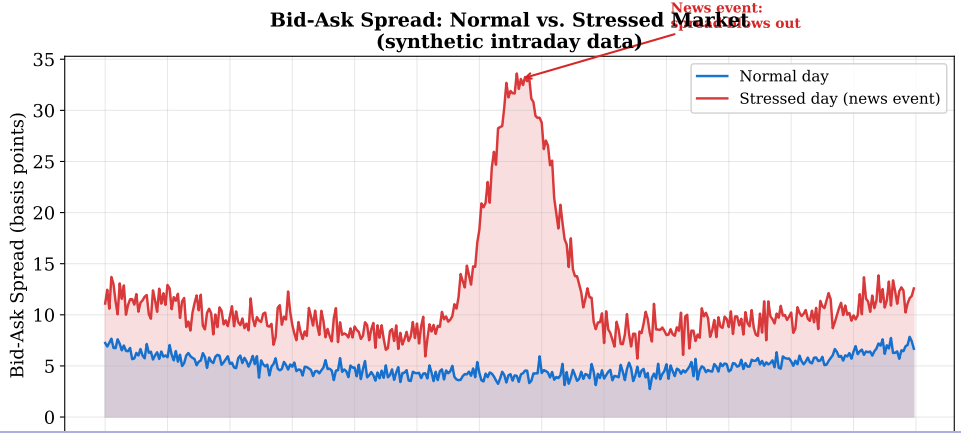
Key components:

- **Bid side (green):** Limit orders to buy at or below a given price
- **Ask side (red):** Limit orders to sell at or above a given price
- **Spread:** The gap between the best bid and best ask

The Bid-Ask Spread: The Cost of Immediacy

Definition: Bid-Ask Spread

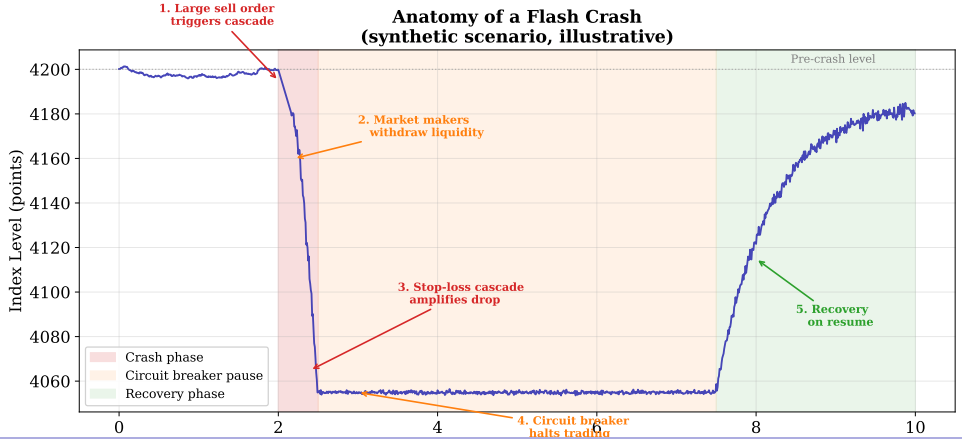
The **bid-ask spread** is the difference between the highest price a buyer is willing to pay (the bid) and the lowest price a seller is willing to accept (the ask). It represents the cost of immediate execution.



Flash Crash Anatomy

Definition: Flash Crash

A **flash crash** is an extremely rapid, deep, and short-lived drop in asset prices, typically caused by algorithmic trading feedback loops, liquidity withdrawal, or erroneous orders.

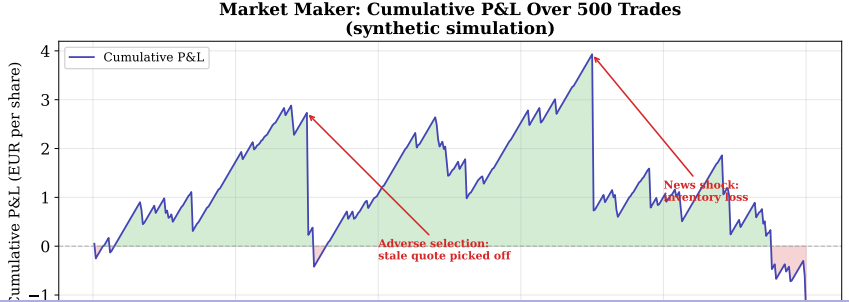


Definition: High-Frequency Trading (HFT)

HFT refers to algorithmic trading strategies that use extremely fast execution speeds (microseconds), co-located servers, and high message rates to capture small per-trade profits at massive scale.

The market-making business model:

- Continuously post bid and ask quotes on both sides of the order book
- Earn the spread on each round-trip (buy at bid, sell at ask)
- Manage inventory risk: avoid accumulating a large net position



Microstructure Risk: Why It Matters for Risk Management

Microstructure Risk	Consequence for Risk Management
Liquidity illusion	The order book may look deep but evaporates under stress — VaR assumes you can sell at current prices
Execution slippage	Large orders move the market; realized loss exceeds model predictions
Flash crash	Intraday losses can far exceed daily VaR; stop-loss orders trigger cascades
HFT withdrawal	Market makers may pull quotes in volatile periods, amplifying price swings
Cross-venue fragmentation	Liquidity is split across exchanges; consolidated book may not exist

Key insight: Risk models that ignore microstructure assume frictionless trading. Real markets have friction, and that friction spikes in exactly the moments when risk matters most.

Microstructure risk is highest precisely when you need liquidity most — during market stress.

Climate Risk Enters Finance

Climate change creates material financial risks:

- The Bank of England's 2015 speech by Mark Carney ("Tragedy of the Horizon") placed climate on the financial risk agenda
- The Financial Stability Board created the **Task Force on Climate-Related Financial Disclosures (TCFD)** in 2015
- As of 2024, climate risk disclosure is mandatory or recommended in over 40 jurisdictions

Two fundamental channels:

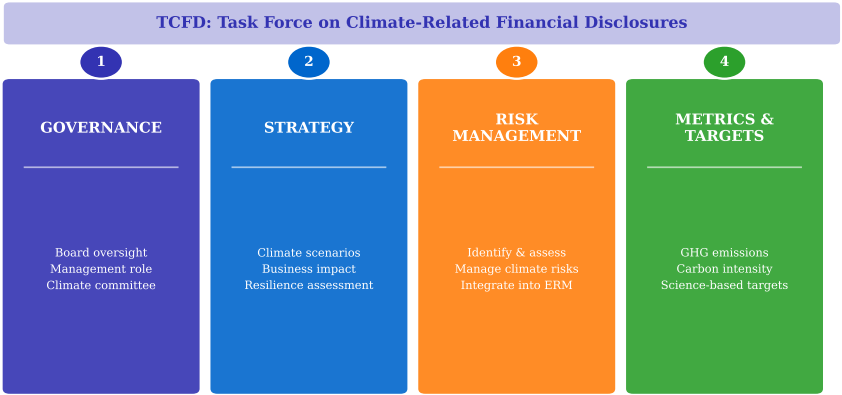
1. **Physical risk:** Direct damage from extreme weather, sea-level rise, and chronic temperature shifts
2. **Transition risk:** Financial impact of moving to a low-carbon economy — policy changes, technology shifts, stranded assets

Key insight: Climate risk is not a distant future problem. It is repricing assets *today* through insurance costs, regulatory requirements, and investor expectations.

Climate risk has moved from an ESG footnote to a core pillar of financial risk management.

Definition: TCFD

The **Task Force on Climate-Related Financial Disclosures (TCFD)** provides a framework for companies and financial institutions to disclose climate-related risks and opportunities. It is structured around four pillars: Governance, Strategy, Risk Management, and Metrics & Targets.



Definition: Physical Risk

Physical risk is the financial risk arising from the direct impacts of climate change, including acute events (storms, floods, wildfires) and chronic shifts (rising temperatures, sea-level rise, changing precipitation patterns).

Financial transmission channels:

- **Real estate:** Flood-zone properties face declining values and rising insurance premiums
- **Agriculture:** Crop yields decline with temperature and water stress
- **Infrastructure:** Ports, power grids, and transportation networks face physical damage
- **Insurance:** Rising claims erode underwriting profitability
- **Sovereign risk:** Countries with high exposure face fiscal strain from disaster recovery

Challenge for risk models: Historical loss data underestimates future physical risk because the climate system is non-stationary — past frequency and severity of events do not predict the future.

Physical risk turns climate science into balance-sheet impact — through asset damage, insurance losses, and credit downgrades.

Definition: Transition Risk

Transition risk is the financial risk arising from the process of adjusting to a low-carbon economy. It includes policy changes (carbon taxes, emissions caps), technological disruption (renewables replacing fossil fuels), market shifts (changing consumer preferences), and reputational effects.

Key drivers:

- **Policy:** Carbon pricing, emissions trading schemes, fossil fuel subsidy removal
- **Technology:** Rapid cost declines in solar, wind, batteries; electric vehicle adoption
- **Market:** Investor divestment from fossil fuels; green bond issuance growth
- **Reputation:** Public pressure on banks financing high-carbon activities

The paradox: An orderly transition (gradual policy tightening) creates moderate, predictable transition risk. A disorderly transition (sudden policy shock) creates severe transition risk. Inaction creates severe physical risk. There is no zero-risk path.

Transition risk penalizes delay: the longer the transition is postponed, the more abrupt and costly it becomes.

Stranded Assets

Definition: Stranded Assets

Stranded assets are assets that suffer unanticipated or premature write-downs, devaluations, or conversion to liabilities, before the end of their expected economic life. In climate finance, this typically refers to fossil fuel reserves that cannot be burned if climate targets are to be met.

The "carbon budget" argument:

- To limit warming to 1.5°C, only a fraction of known fossil fuel reserves can be burned
- Reserves on corporate balance sheets may therefore be overvalued
- This creates a potential "carbon bubble" in equity and debt markets

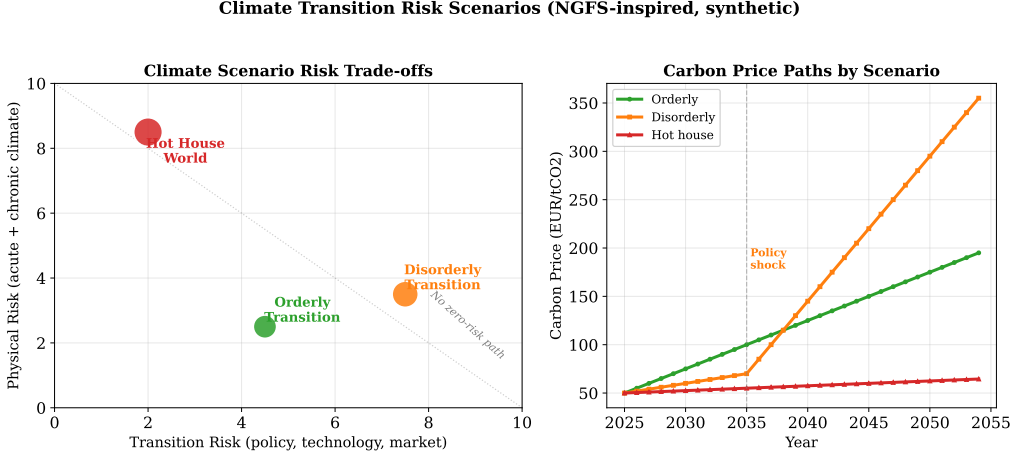
Financial implications:

- Coal, oil, and gas companies face asset impairment
- Banks with large fossil fuel loan books face elevated credit risk
- Pension funds with fossil fuel equity exposure face long-term value erosion

---

Stranded assets illustrate how climate policy can transform a resource from a balance-sheet asset into a liability.

Transition Risk Scenarios



Scenario analysis is the primary tool for assessing climate risk because historical data is insufficient — the climate transition has no precedent.

Climate scenario analysis replaces backtesting: we cannot rely on history for a risk that has never materialized at this scale.

Integrating New Risks into Enterprise Risk Management

How do institutions incorporate these emerging risks?

	Cyber Risk	DeFi Risk	Climate Risk
Data	Incident databases, threat intel	On-chain analytics, audit reports	Climate models, emissions data
Modeling	Scenario-based, red-team exercises	Simulation, formal verification	NGFS scenarios, integrated assessment
Governance	CISO, NIST CSF, DORA	Smart-contract audits, multi-sig	Board oversight, TCFD disclosure
Regulation	NIS2, DORA, SEC	MiCA, travel rule	ISSB, EU Taxonomy

Common challenge: All three risk types suffer from limited historical data, fat-tailed loss distributions, and deep uncertainty about future states.

Enterprise risk management must expand from market/credit/operational to include cyber, DeFi, and climate as first-class risk categories.

Interconnections: When New Risks Combine

These risks do not exist in isolation:

- **Cyber + Climate:** A cyberattack on a power grid during a heatwave compounds physical risk with operational disruption
- **DeFi + Cyber:** Smart-contract exploits are a form of cyber risk applied to decentralized financial infrastructure
- **Climate + DeFi:** Tokenized carbon credits create new DeFi-native climate instruments — with oracle risk on the carbon price
- **All three + Microstructure:** In a crisis, liquidity dries up across all venues; algorithmic market makers withdraw; flash crashes amplify any shock

Systemic risk amplifier: The correlation between these risk types *increases* under stress — exactly when diversification is needed most. **Key insight:** A modern risk manager must think in terms of **risk networks**, not independent risk silos.

The most dangerous scenarios involve multiple new risk types materializing simultaneously.

Key Takeaways

1. **Cyber risk** is adversarial, non-stationary, and correlated; the NIST CSF (Identify–Protect–Detect–Respond–Recover) provides a structured management framework
2. **Zero trust** replaces perimeter-based security with continuous verification — essential as finance migrates to the cloud
3. **DeFi risk** includes composability cascades, oracle manipulation, and governance attacks — structurally different from traditional counterparty risk
4. **Market microstructure** determines real execution costs; the order book, bid-ask spread, and flash crash dynamics are critical for risk managers
5. **Climate risk** splits into physical risk (direct damage) and transition risk (policy, technology, stranded assets); the TCFD framework structures disclosure
6. **Scenario analysis** replaces backtesting for risks with no historical precedent
7. These risks are **interconnected and correlated under stress** — risk management must move from silos to networks

---

The new risk landscape demands new tools: scenario analysis, network thinking, and continuous adaptation.

Summary / Next Lesson Preview

This lesson: We explored three frontiers of the new risk landscape — cybersecurity, DeFi, and climate — plus market microstructure risk, and examined how they interconnect.

Key vocabulary:

- Cyber risk
- NIST Cybersecurity Framework
- Zero-trust architecture
- Composability risk
- Oracle risk
- Governance attack
- Market microstructure
- Order book, bid-ask spread
- Flash crash
- High-frequency trading (HFT)
- TCFD framework
- Physical risk vs. transition risk
- Stranded assets
- Carbon budget

Next lesson (M4L5): *Risk in Practice: Case Studies and Integration* — We apply the frameworks from Lessons 4.1–4.4 to real-world scenarios, integrating measurement, modeling, stress testing, and new risk categories into a unified enterprise risk view.

Review: Can you explain the difference between physical and transition risk, and why composability is both DeFi's strength and its systemic weakness?