A Generalized Framework for Operational Risk Management of Human and Algorithmic Trading

Operational Risk Definition

The risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses.

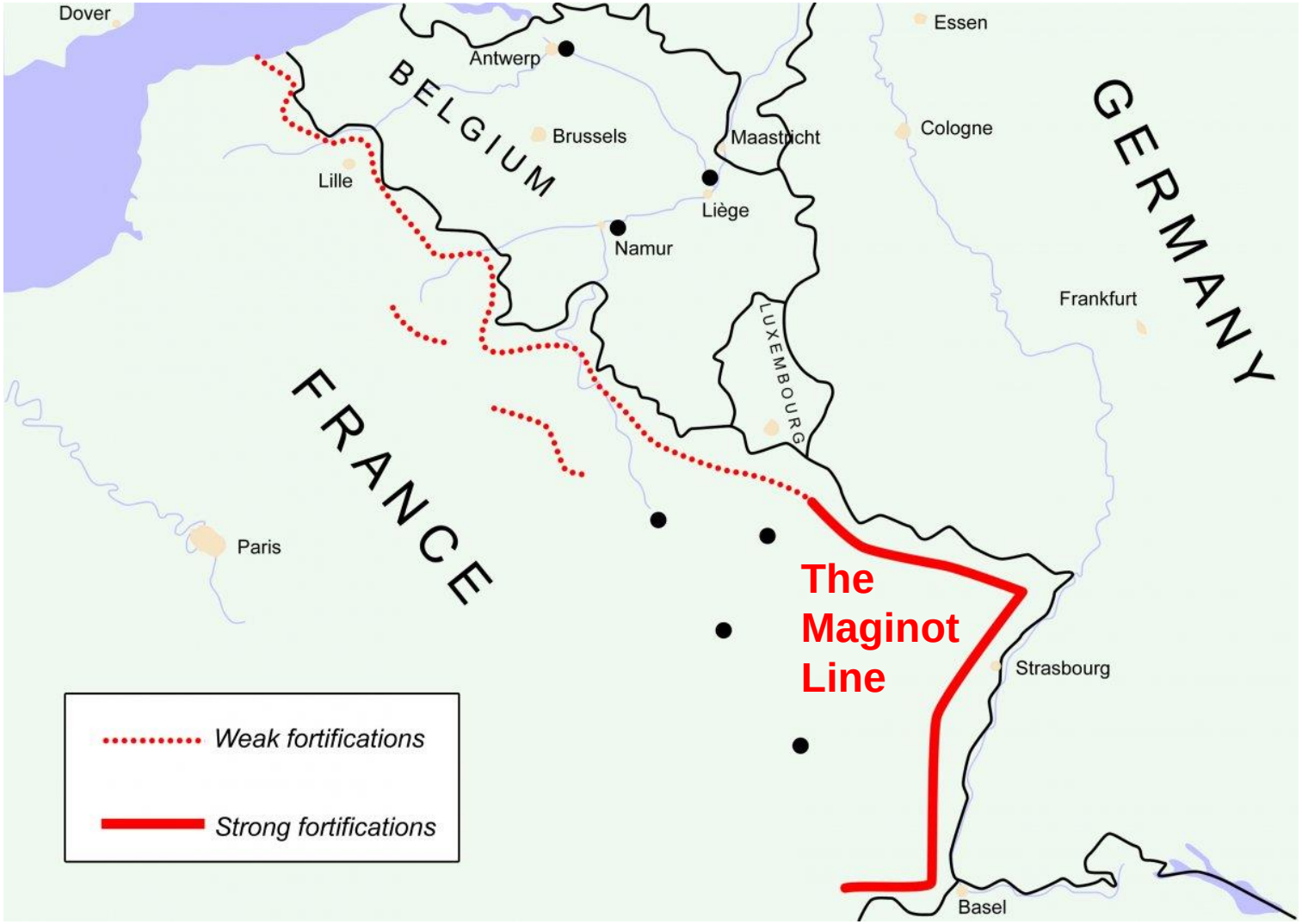
See: Basel II: Revised international capital framework". Bis.org.

See: Solvency II Glossary - European Commission". CEA - Groupe Consultatif.

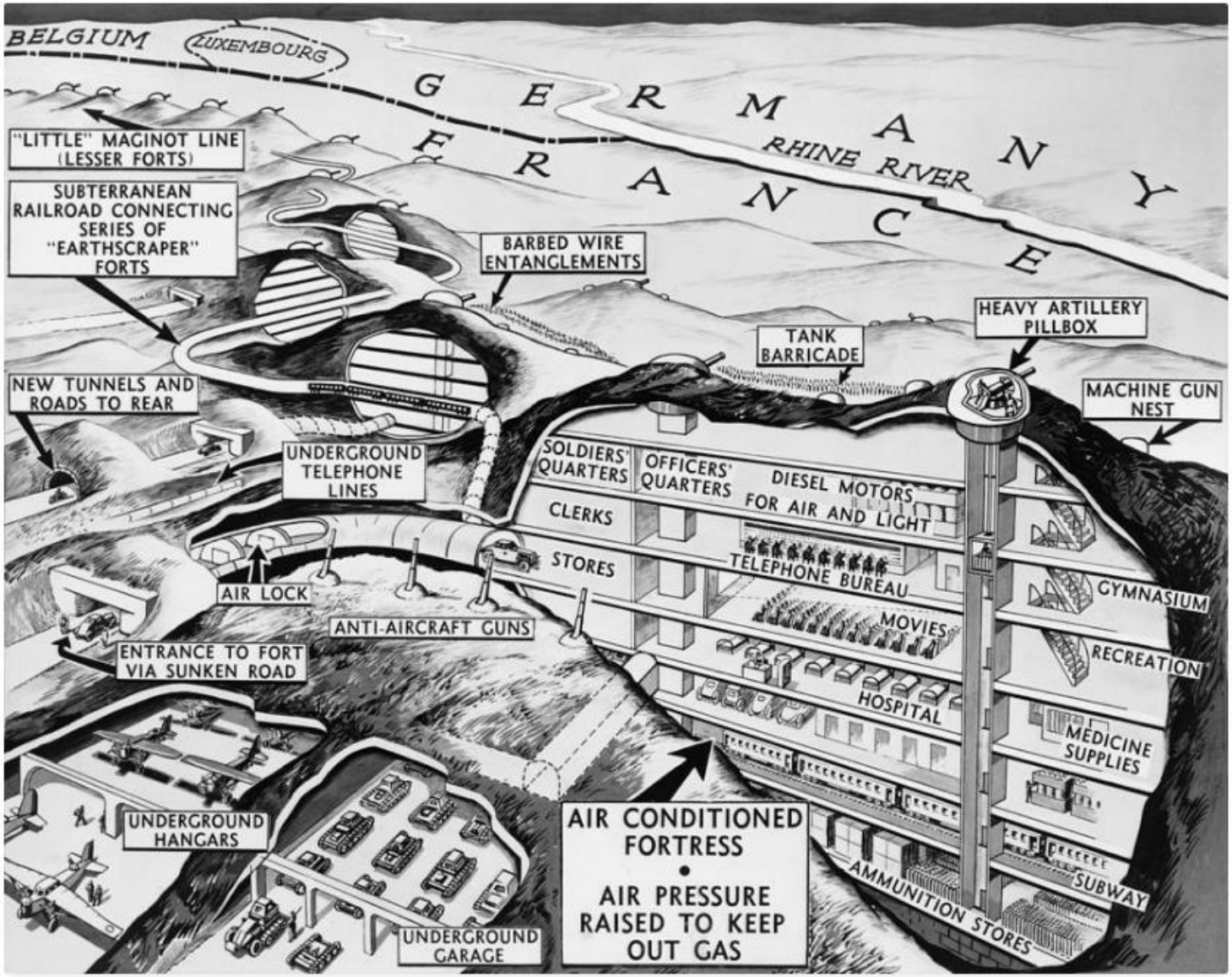
1. A Short History Lesson

Where in the world?

Europe 1940: The Maginot Line

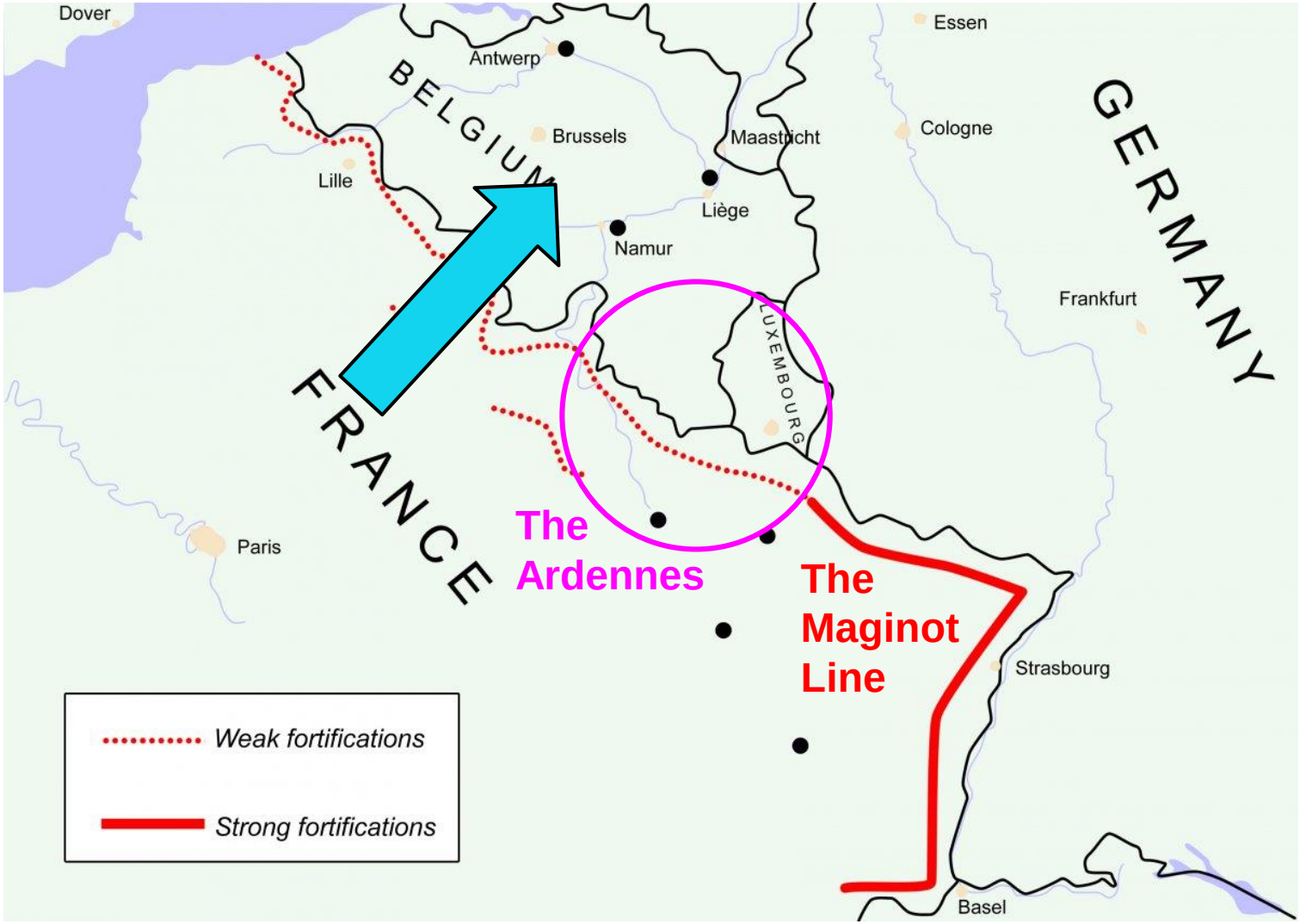


A Maginot Line fortress

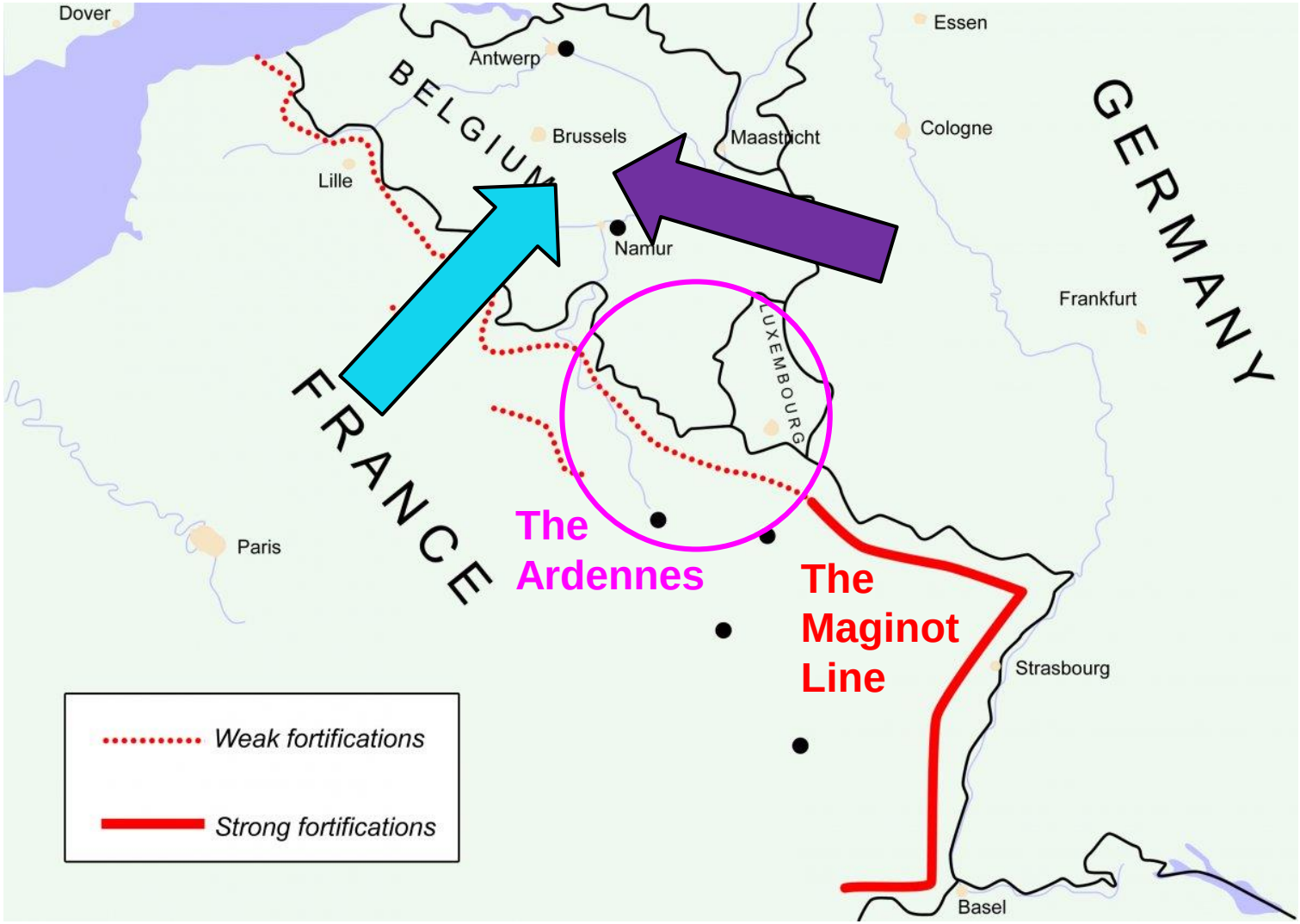


The Ardennes forest: A natural line of defense

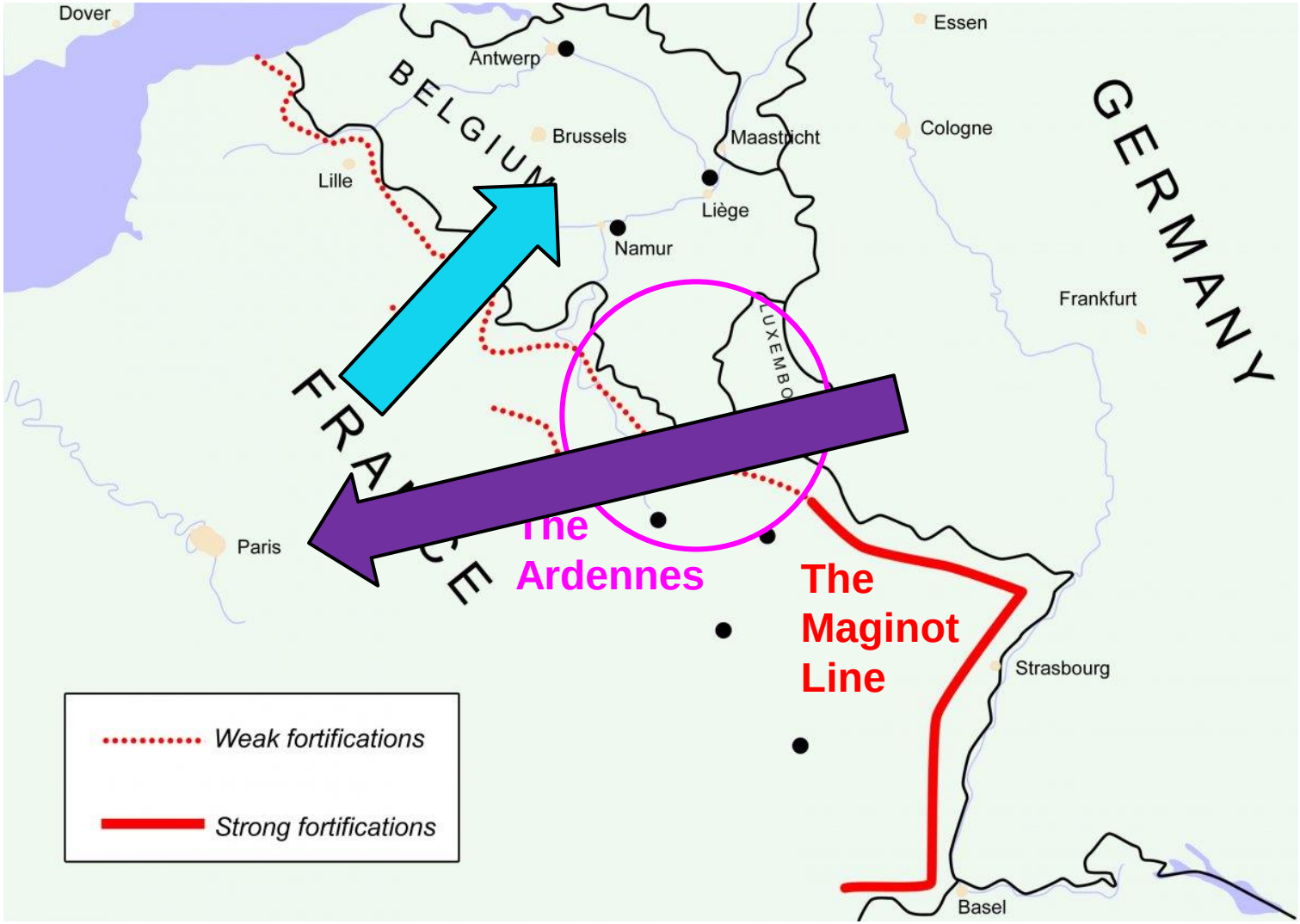
The French battle plan



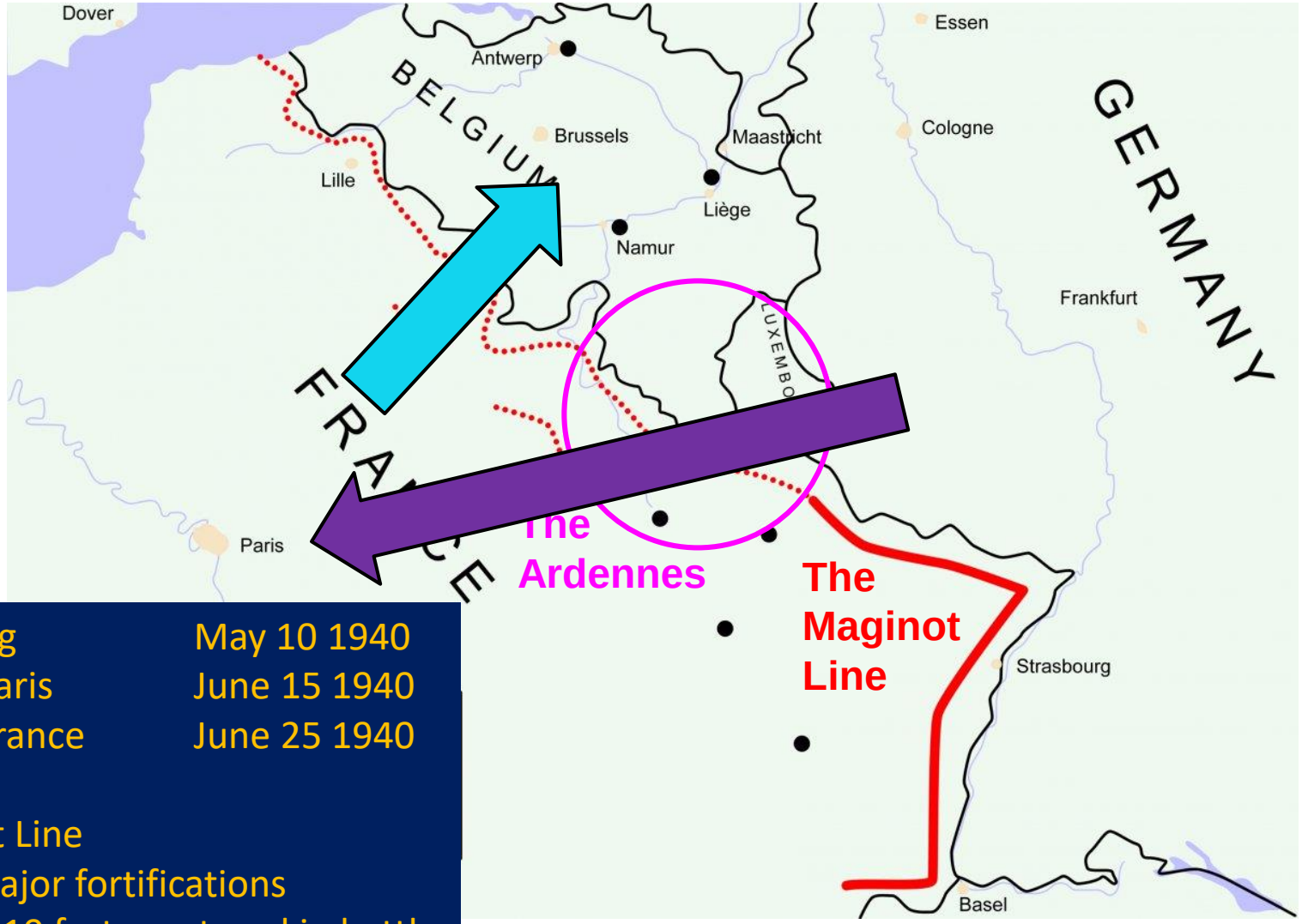
The French battle plan



The German battle plan



The German battle plan



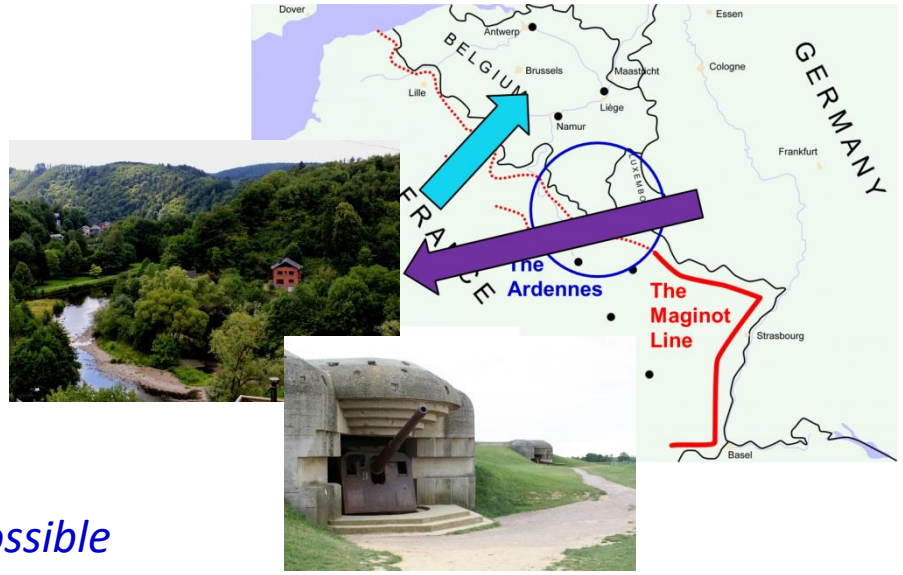
Blitzkreig	May 10 1940
Fall of Paris	June 15 1940
Fall of France	June 25 1940

Maginot Line

- 58 major fortifications
- Only 10 forts captured in battle

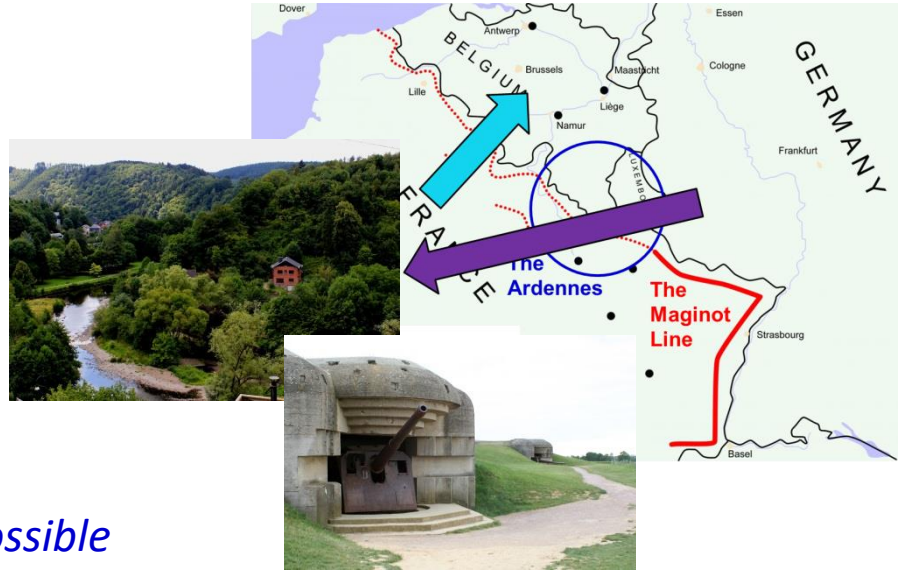
What can we learn about lines of defense?

- Static lines of defense are inflexible
  - → *Build adaptive defenses*
- Single lines of defense are vulnerable
  - → *Layered defense in depth*
  - → *Mobile reserve*
- The enemy is wily and determined
  - → *Difficult attack vectors are not impossible*
  - → *Learn to think like the enemy…*



What can we learn about lines of defense?

- Static lines of defense are inflexible
  - → *Build adaptive defenses*
- Single lines of defense are vulnerable
  - → *Layered defense in depth*
  - → *Mobile reserve*
- The enemy is wily and determined
  - → *Difficult attack vectors are not impossible*
  - → *Learn to think like the enemy…*



Homework: Please research these cases

John Rusnak	Nick Leeson	Jerome Kerviel	Anonymous, Lizard Squad	Kweku Adoboli
				
				
Fancy Bear	Knight Trading		?	

Think about….

- Insider threats *vs* outsider threats
- White hat actors *vs* criminal actors *vs* chaos actors *vs* espionage actors
- Human actors *vs* machine actors
- Velocity of disaster
- Potential countermeasures

2. Organization

The three (or possibly four) lines of defense

- Principles for the Sound Management of Operational Risk
  (BIS / Basel Committee on Banking Supervision, June 2012)

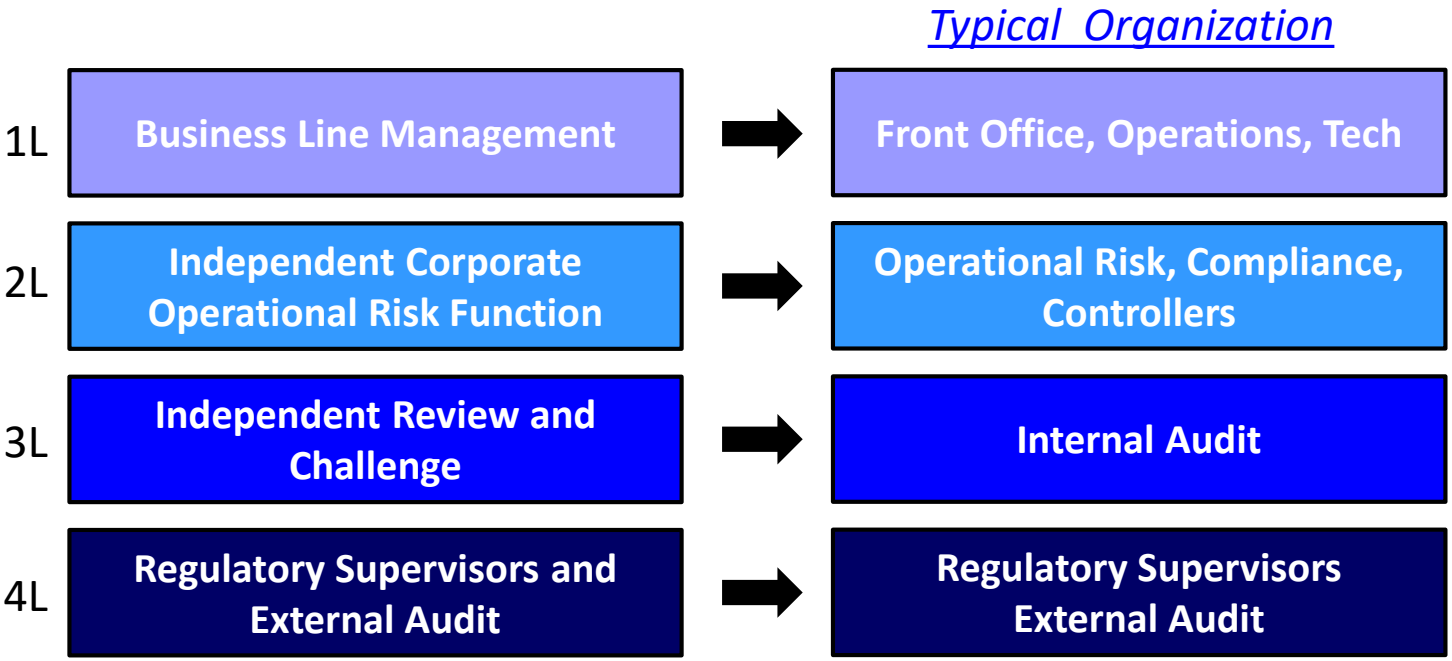
- Occasional Paper No. 11: The "four lines of defence" model for financial institutions
  (BIS / Financial Stability Institute, December 2015)

		Typical Activities
1L	**Business Line Management**	Trading, asset management, sales, client relationship management, operations
2L	**Independent Corporate Risk Functions**	Risk management, compliance, finance, risk control, model validation
3L	**Independent Review and Challenge**	Audit (internal), management assurance
4L	**Regulatory Supervisors and External Audit**	Audit (external), supervisory oversight

The three (or possibly four) lines of defense

- Principles for the Sound Management of Operational Risk
  (BIS / Basel Committee on Banking Supervision, June 2012)

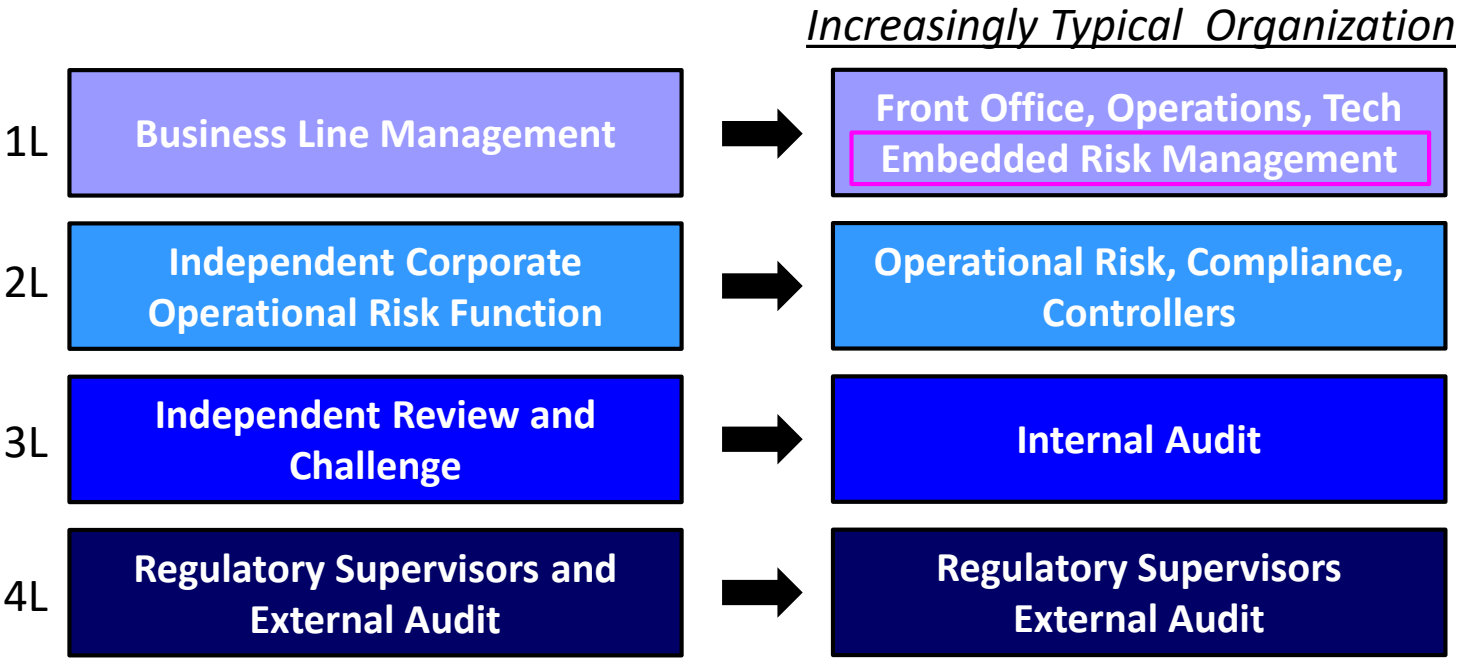
- Occasional Paper No. 11: The "four lines of defence" model for financial institutions
  (BIS / Financial Stability Institute, December 2015)



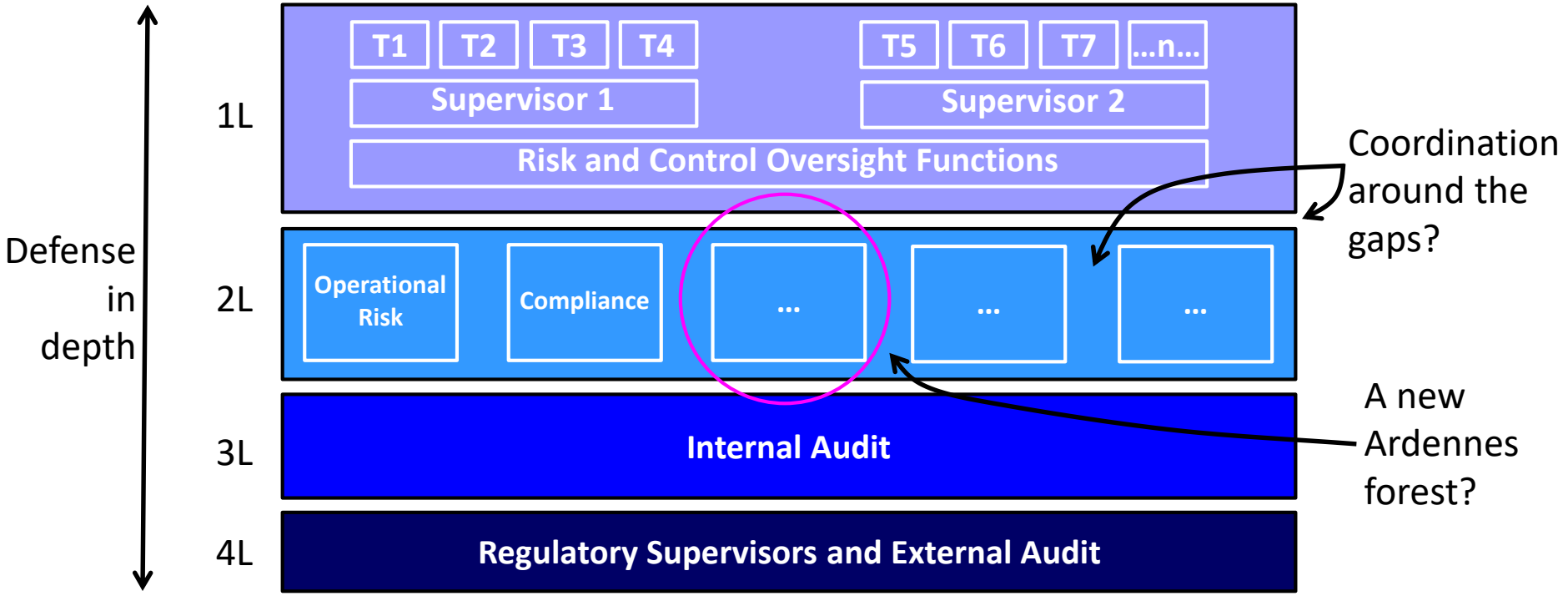
The three (or possibly four) lines of defense

- Principles for the Sound Management of Operational Risk
  (BIS / Basel Committee on Banking Supervision, June 2012)

- Occasional Paper No. 11: The "four lines of defence" model for financial institutions
  (BIS / Financial Stability Institute, December 2015)

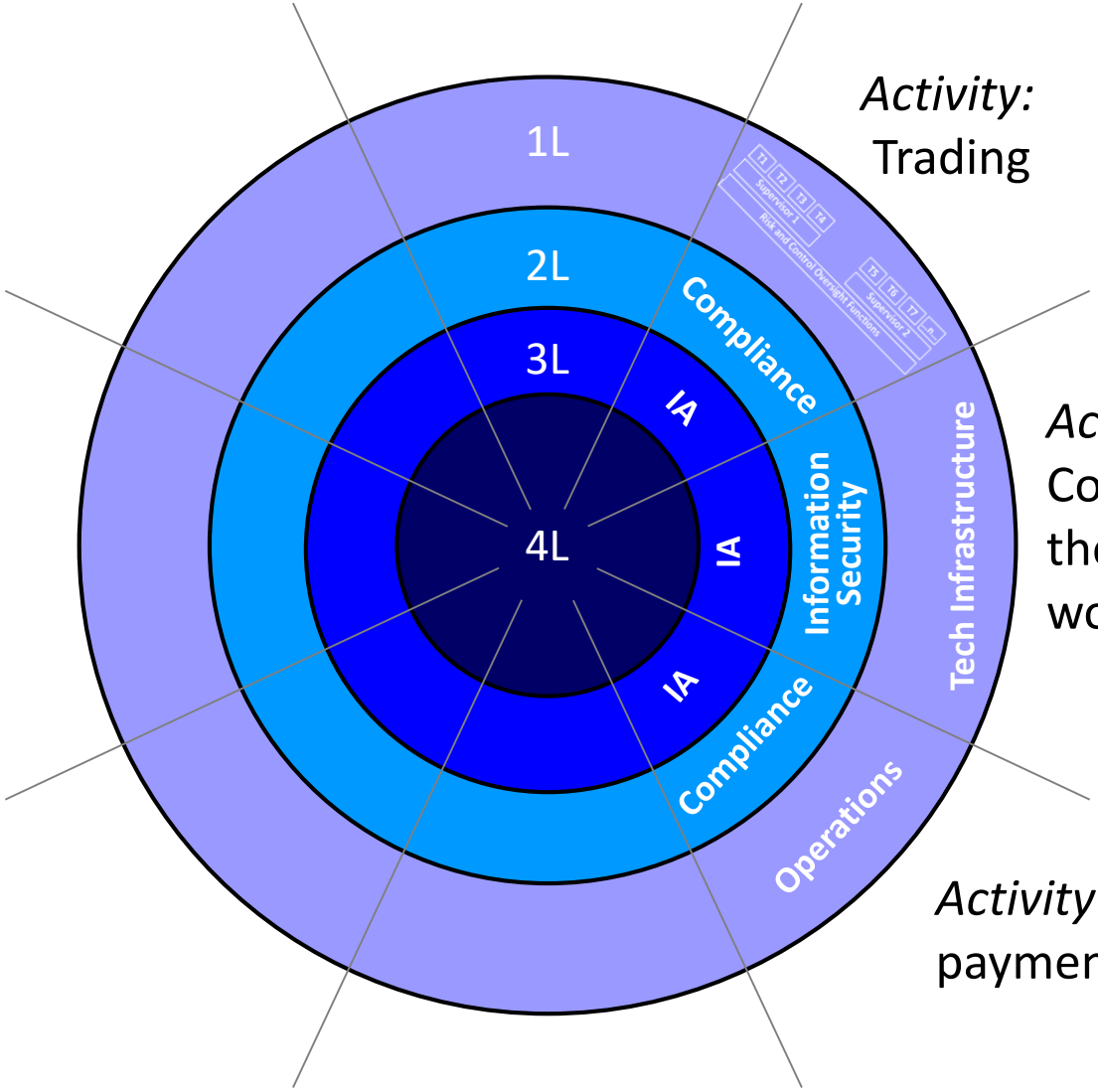


A new Maginot Line?



Too inflexible?

Four Adaptive Lines of Defense



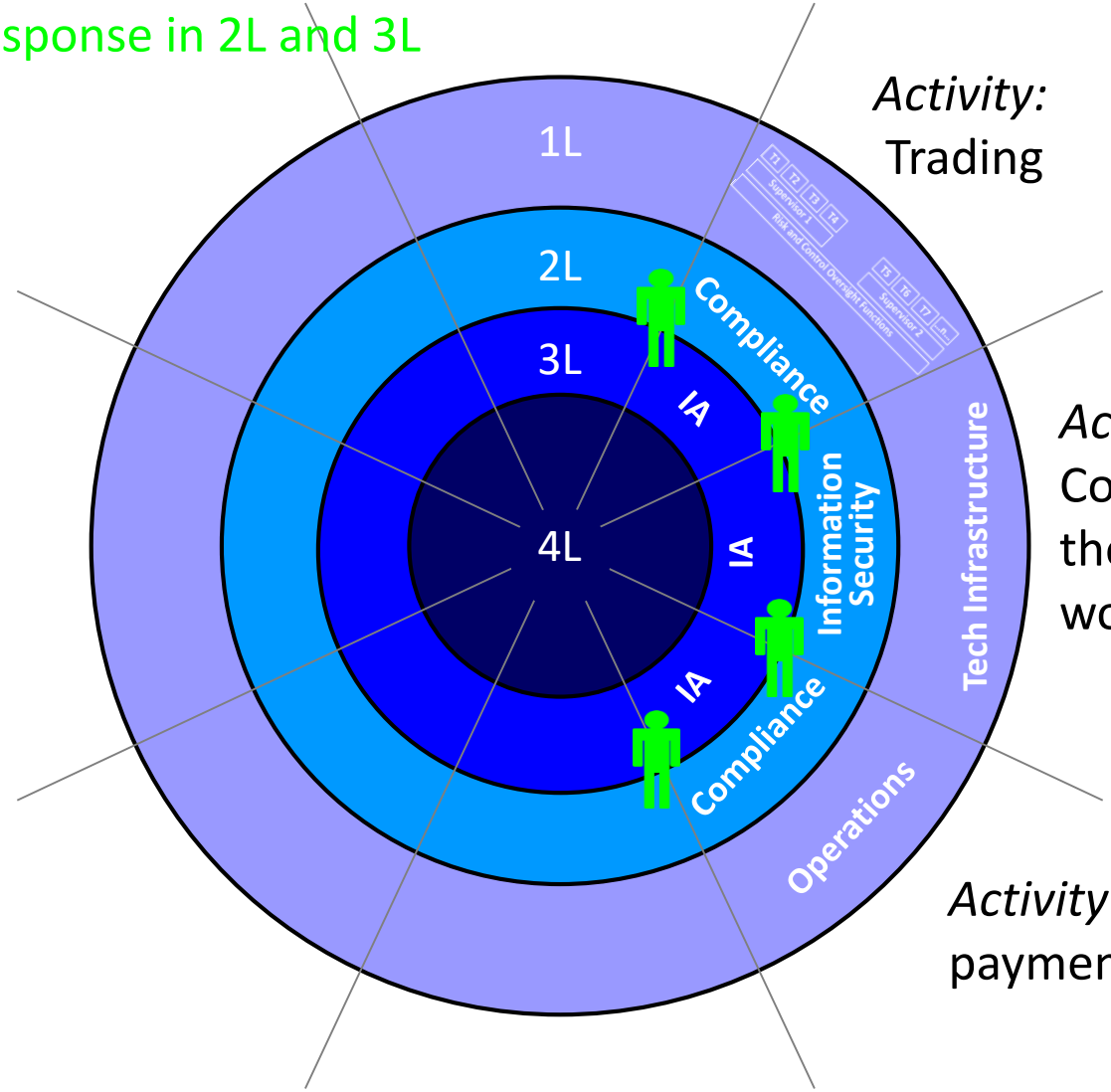
Activity: Trading

Activity: Connecting to the outside world

Activity: Making payments

Four Adaptive Lines of Defense

+ Flexible response in 2L and 3L



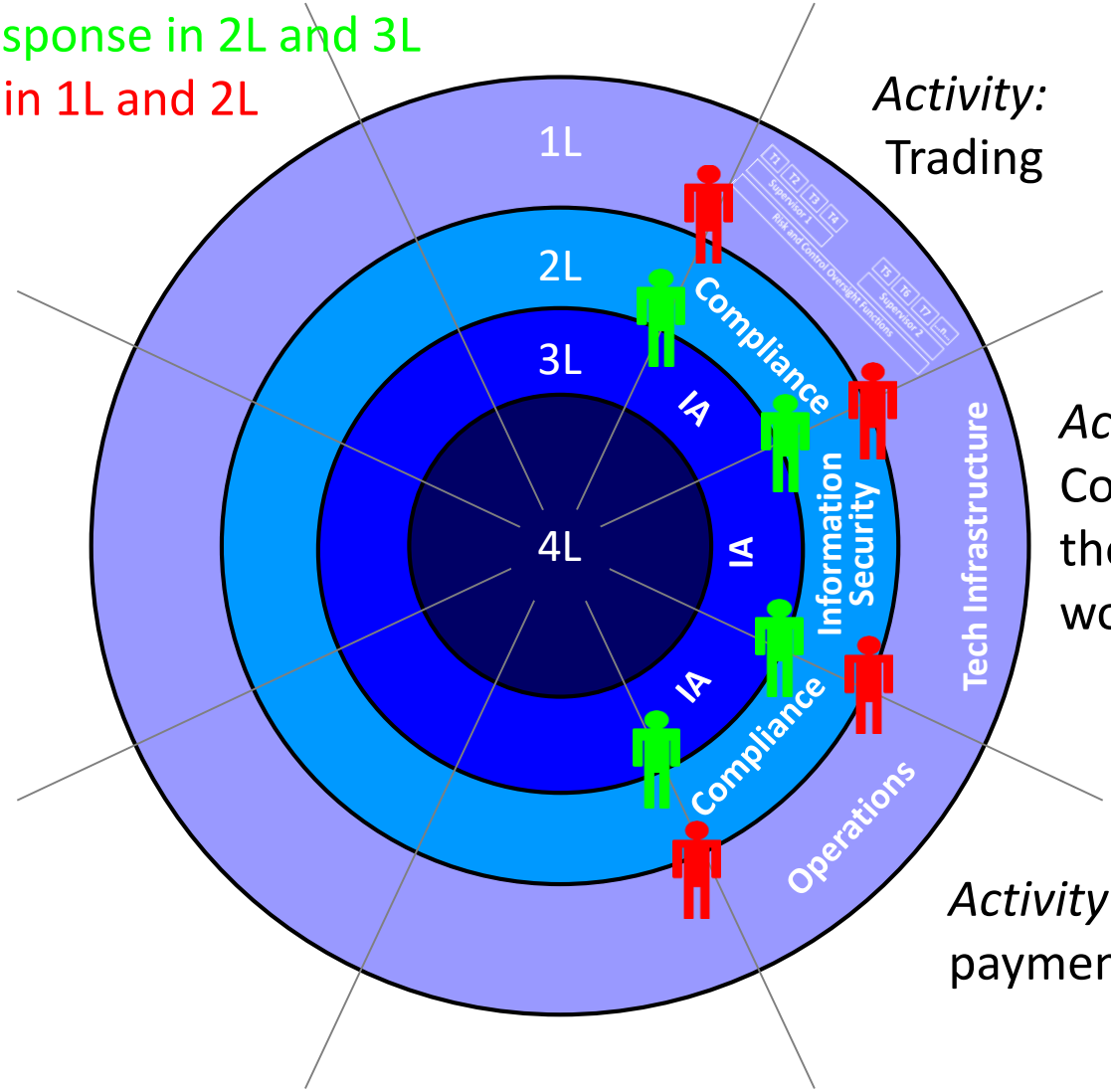
Activity: Trading

Activity: Connecting to the outside world

Activity: Making payments

Four Adaptive Lines of Defense

+ Flexible response in 2L and 3L
+ Red Team in 1L and 2L



Activity: Trading

Activity: Connecting to the outside world

Activity: Making payments

3. Methodology

8 elements of operational risk management

1. Risk identification
2. Risk assessment (“Inherent Risk”)
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing (“Residual Risk”)
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

1. Risk Identification

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

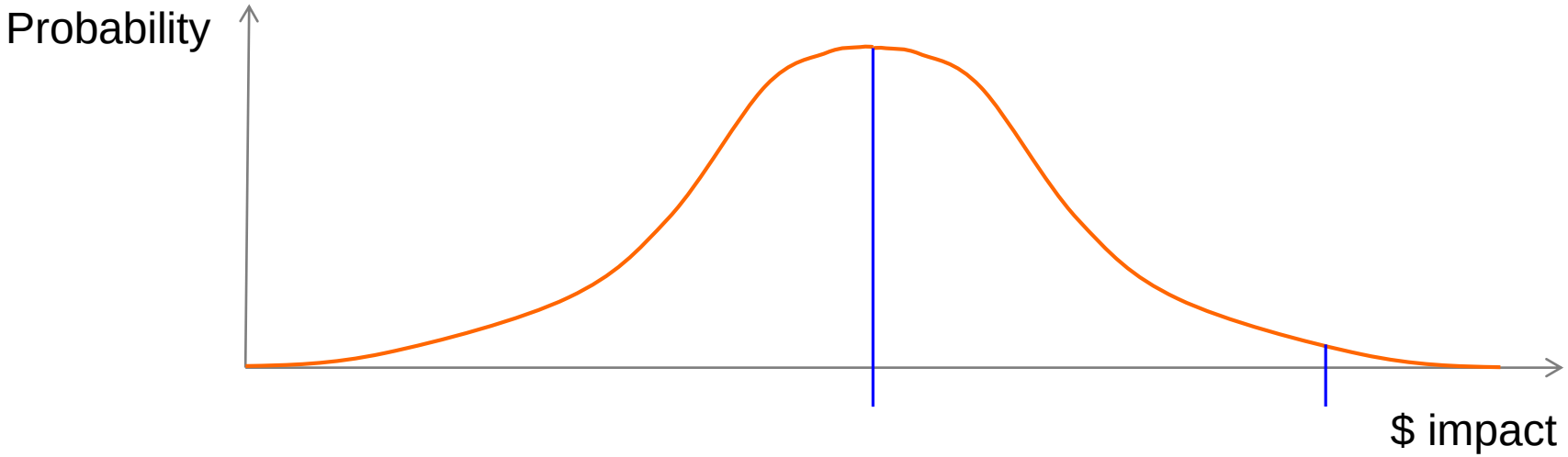
- What could go wrong?
  - Human factors
  - Environment / infrastructure
  - Information
  - Software / Algos
  - Fraud
  - Threat actors
- Balance between standardized risks and specific risks
- A commercially useful list, for example
  - Trades could be entered with excessive size
  - Unauthorized persons may access sensitive data or code
  - Sensitive information may be sent to unintended external persons
  - Flooding in New York may disrupt trading operations
- Non-financial risks must be included

2. Risk Assessment

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

- Inherent Risk

  What could go wrong if there were no controls?



- Consider both Expected case and Stressed case

→ *Low probability, high impact events prove to be the most harmful (look back to the Rogues Gallery on page 15)*

→ *Is some level of "shrinkage" acceptable?*

3. Control Identification

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

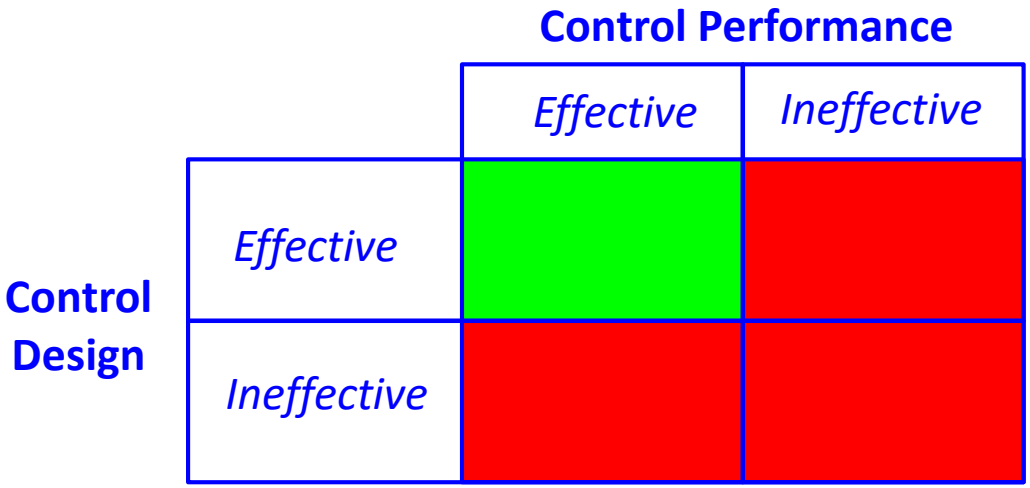
- Consider:
  - Automated controls
    - eg: Fat finger controls
    - Message rate controls
  - Human controls
    - eg: Reconciliation between reports
    - Supervisor sign off
  - Preventative vs detective controls
    - eg: Cannot enter a value > $50 billion in a field
    - Values > $50 billion appear in an exception report
  - Environmental controls
    - eg: Heartbeat check between processes
    - Physical access controls to hardware
    - Redundancy of pathways
  - Exogenous controls
    - eg: Exchange message rate controls
    - Exchange credit limits

- Key controls only

4. Control Assessment

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

- Is a control Effective or Ineffective?
- Both control <u>design</u> and control <u>performance</u> are critical:

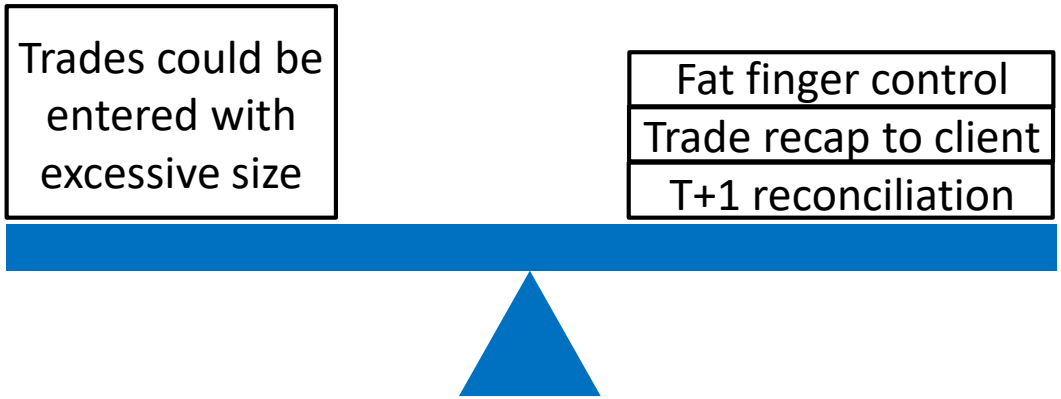


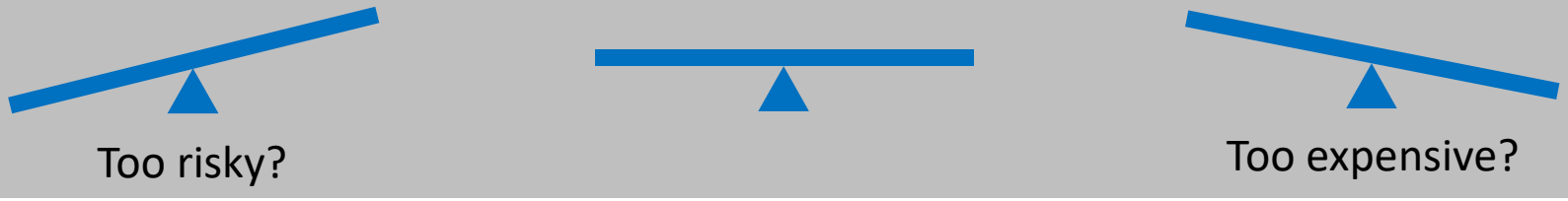
5. Risk and Control Balancing

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

Inherent Risk – Control Effectiveness = Residual Risk

- For example:





And what about Stressed cases?

6. Risk Appetite Assessment

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

Risk Appetite = *f* (Severity, Probability, Regret*, Capital)

- If you have $100 of capital, how much risk are you willing to assume?
- For each legal entity, as a function of capital, determine risk appetite on the following dimensions:

		Single Event	*Cumulative*
Risk Assessment	*Expected* • *Inherent* • *Residual*		
	Stressed		

- If Risk > Appetite, the options are:
  - → *Treat the risk (and make a plan to do so)*
  - → *Accept the risk (and document why)*
  - → *Transfer the risk to somebody else*
  - → *Stop doing the thing which creates risk*

*Seeing Tomorrow: Rewriting the Rules of Risk, Ron S. Dembo, Andrew Freeman, Wiley

7. Event Collection and Back-Testing

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

- Event detection / collection network which:
  - Spans the entire enterprise
  - Operates close to real time
  - Is easy to use

- Use past events to challenge forward risk assessments

8. Event Remediation

1. Risk identification
2. Risk assessment ("Inherent Risk")
   a) Expected
   b) Stressed
3. Control identification
4. Control assessment
5. Risk and Control Balancing ("Residual Risk")
6. Risk Appetite Assessment
7. Event collection and back-testing
8. Event remediation

- This isn't academic! The objective is to fix things

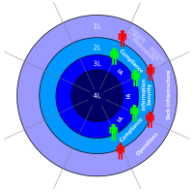
- Process
  - Event collection
  - Triage
  - Emergency remediation
  - Long-term remediation where commercial to do so

To conclude…

Know your enemy

Know your weak spots

Don’t build defenses that can only face in one direction



Build layered, adaptable defense in depth

Know your appetite for risk

Understand the balance of risks and controls

If it’s broken, fix it. Properly.

Thank you…

Questions?