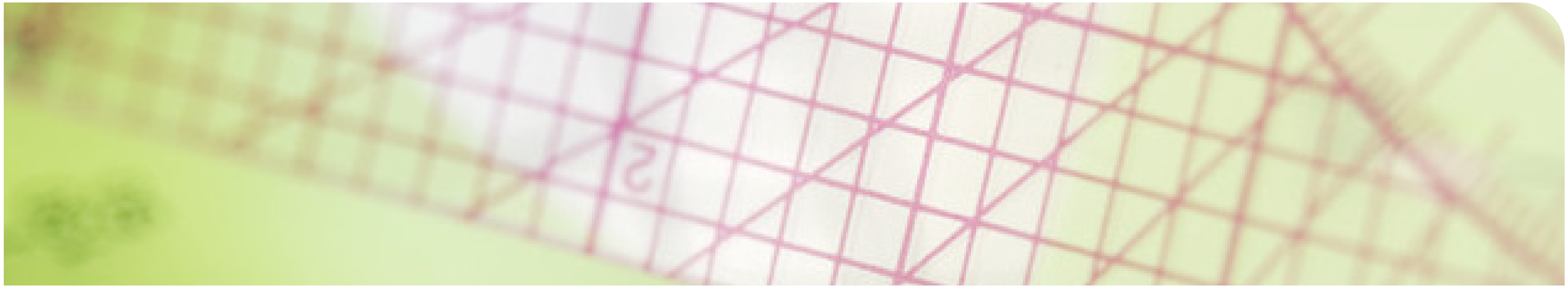


A change for the better

# Deepening the Risk Management Journey

**Scott North**

**Chief Risk Officer**

# Role of the CRO in Mutuals

1. Risk Management Governance

2. Risk Management Framework

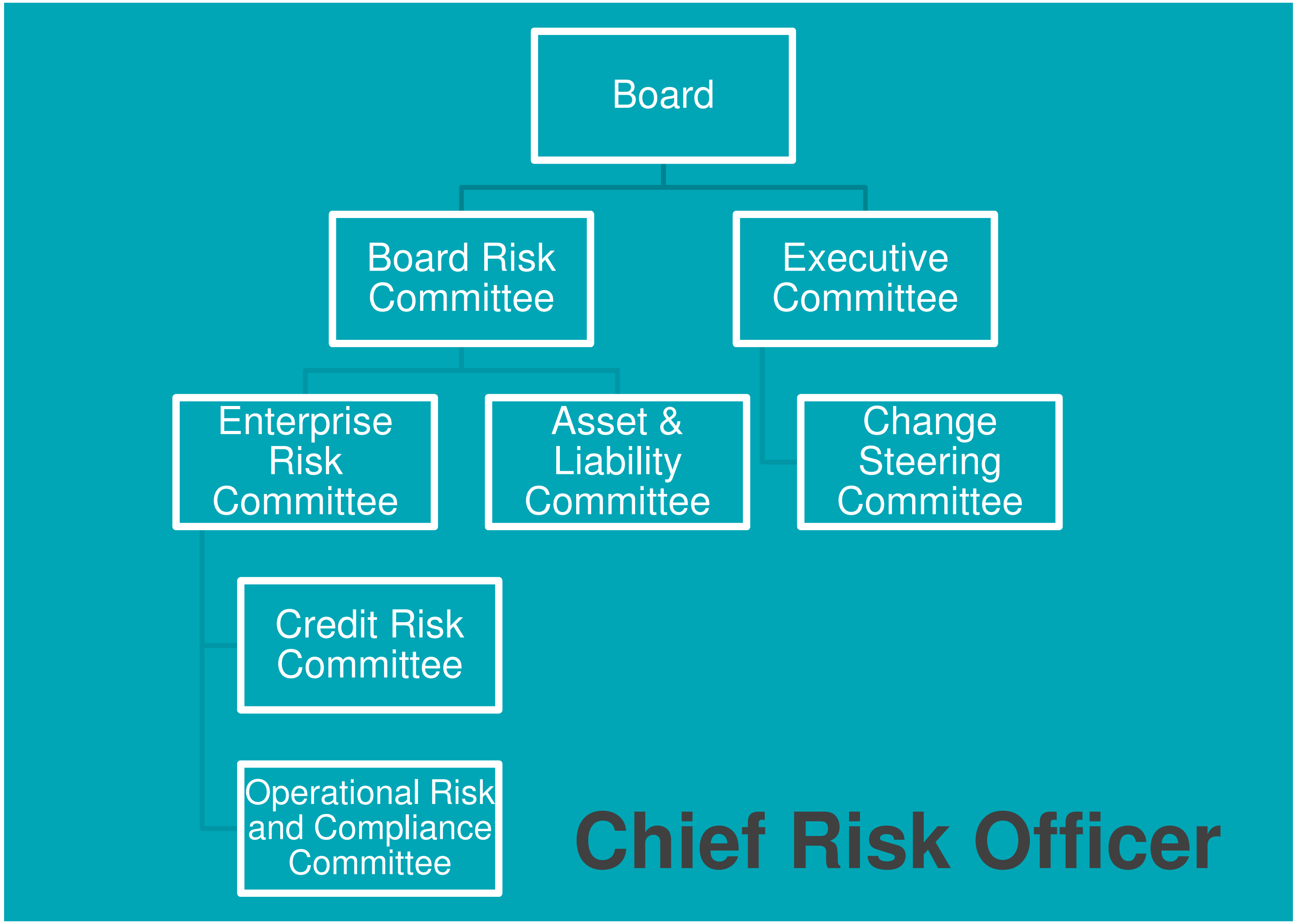
3. Establish Risk Appetite

4. Culture of risk management through 1st and 2nd line of risk

5. Risk assessment, a top down and bottom up philosophy

6. Role of stress testing and scenarios across the portfolio

# 1. Risk Management Governance



Board

Board Risk Committee

Executive Committee

Enterprise Risk Committee

Asset & Liability Committee

Change Steering Committee

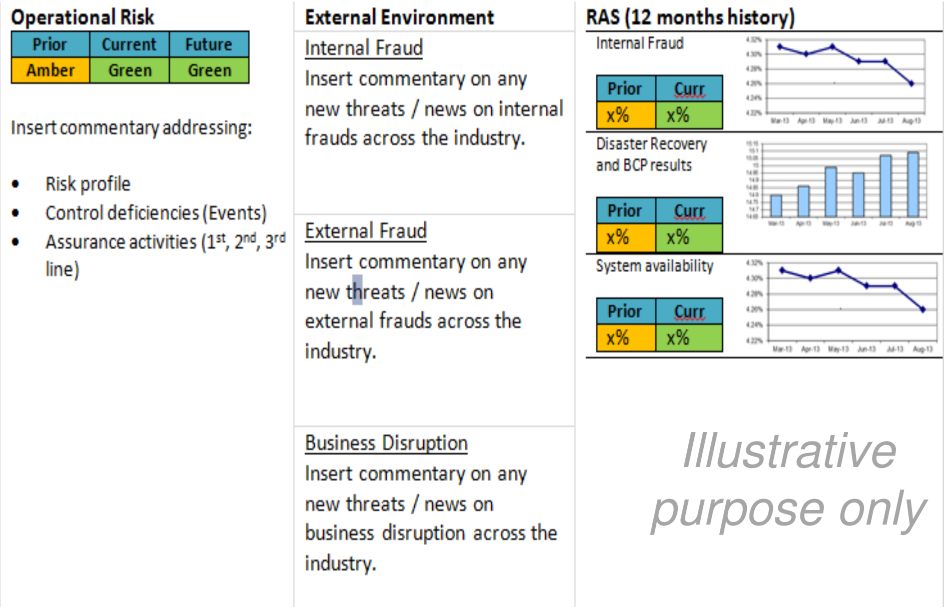
Credit Risk Committee

Operational Risk and Compliance Committee

Chief Risk Officer

# Risk governance and the evolution of risk reporting

- Alignment to risk categories
- Reporting on the risk appetite metrics
- Focus on past and future trends
- Reporting on the internal and external environment
- Promote quality discussion at the executive level
- Alignment of 1st line, 2nd line and 3rd line activities across the risk spectrum



**Operational Risk**

| Prior | Current | Future |
|---|---|---|
| Amber | Green | Green |

Insert commentary addressing:

- Risk profile
- Control deficiencies (Events)
- Assurance activities (1st, 2nd, 3rd line)

**External Environment**

Internal Fraud

Insert commentary on any new threats / news on internal frauds across the industry.

External Fraud

Insert commentary on any new threats / news on external frauds across the industry.

Business Disruption

Insert commentary on any new threats / news on business disruption across the industry.

**RAS (12 months history)**

Internal Fraud

| Prior | Curr |
|---|---|
| x% | x% |

Disaster Recovery and BCP results

| Prior | Curr |
|---|---|
| x% | x% |

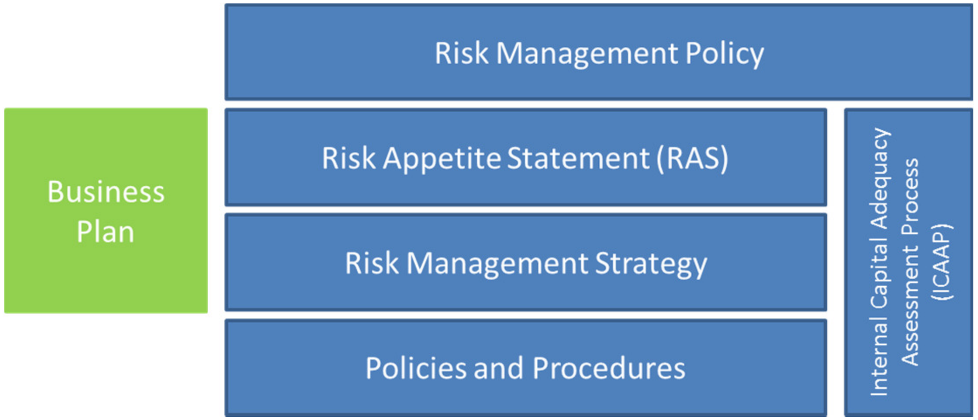
System availability

| Prior | Curr |
|---|---|
| x% | x% |

*Illustrative purpose only*

# 2. Risk Management Policy

- Risk Management policy outlines the requirements for risk management being:
  - a risk appetite;
  - a risk management strategy;
  - a business plan;
  - policies and procedures;
  - a designated risk management function;
  - an Internal Capital Adequacy Assessment Process (ICAAP);
  - a risk information management system (RIMS); and
  - a review process.



Risk Management Policy

Business Plan

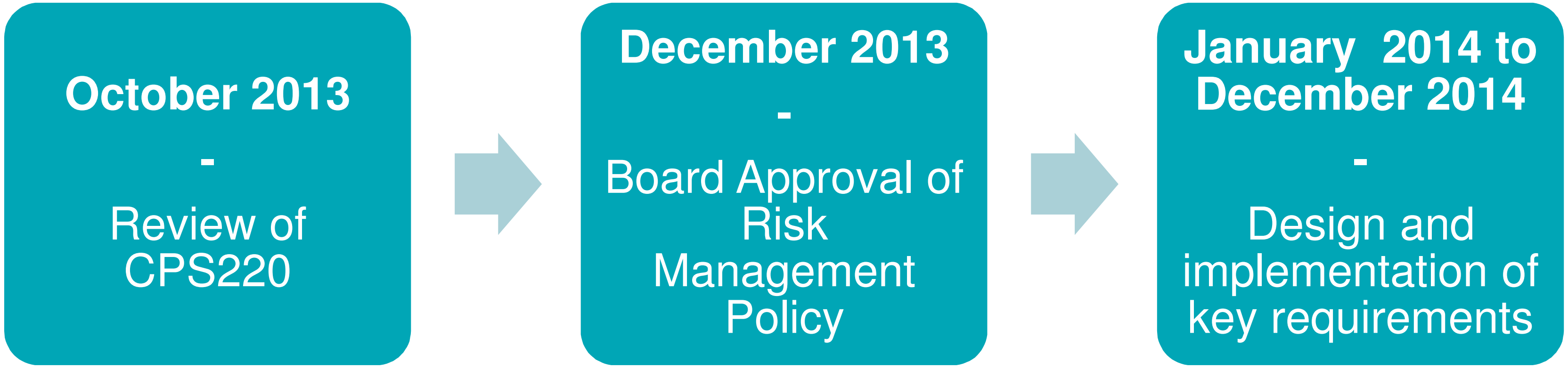
Risk Appetite Statement (RAS)

Risk Management Strategy

Policies and Procedures

Internal Capital Adequacy Assessment Process (ICAAP)

# CPS220, High Level Compliance Timeline



**October 2013**

-

Review of CPS220

**December 2013**

-

Board Approval of Risk Management Policy

**January 2014 to December 2014**

-

Design and implementation of key requirements

# 3. Risk Appetite

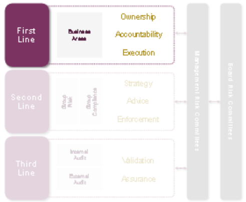
1. Defining clear principles in the setting of risk appetite, including the role of subsidiaries
2. Qualitative and quantitate elements
3. Establish a risk landscape and hierarchy
4. Clearly articulate the risk class, including defining relevant sub classes
5. Establish clear statements of risk appetite
6. Establish reportable risk appetite metrics
7. Detail a linkage to the risk policies in managing the risk appetite
8. Outline the governance / ownership of the risk appetite metric

Key Quantitative Metrics
Key Qualitative Statements

| | Immediate Risk Appetite Metric | Type | Amber | Red |
|---|---|---|---|---|
| Operational Risk Class | Example metric (Reported on Dashboard) | Lead | x% | <x% |

# 4. Risk culture, the 1st line of defence

Risk and control management in 'the Business'.



## Day-to-day ownership and management of risk by each Division Executive and Senior Leaders.

1st line risk manager will support single point of contact for:

- Understanding and applying the various risk/compliance management frameworks.
- Risk identification and assessment.
- Risk control planning and implementation.
- Risk acceptance and monitoring
- Production of risk profiles / footprints and heat maps. (critical and highly rated residual risks)
- Identifying key risk issues.
- Developing, selecting, implementation and monitoring action plans for the management of risks.
- Gathering and collating data for risk indicators.
- Reviewing (via self assessments) control effectiveness.
- Identifying, recording, managing and escalating risk events.
- Embedding risk management into CUA's culture.

The 1st line of defence comprises each of CUA Divisions and their Executives and Senior Leaders. These Executives and Senior Leaders and in some cases managers own and manage CUA's risk. They are also responsible for implementing corrective actions to address process and control deficiencies. They are also responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.

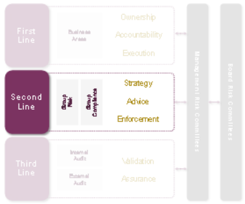
Executives and Senior Leaders must identify, assess, control, and monitor risks. Through a cascading responsibility structure, mid-level managers design and implement detailed procedures that serve as controls and supervise execution of those procedures by their teams.

Executives and Senior Leaders naturally serve as the first line of defence because controls are designed into the systems and processes under their guidance. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events.

***1st line Risk Manager will support in the delivery and management of risk within distinct business areas.***

# Risk culture, the 2nd line of defence

Risk and Compliance specialists.



## Risk management framework, systems and monitoring by centralised risk and compliance functions.

2nd line risk team will

- Develop and maintain principle based policies and management standards for all risk types.
- Develop and maintain risk management frameworks.
- Identify known and emerging risk management issues.
- Identify and articulate shifts in CUA's risk appetite.
- Assist the 1st Line Risk Manager in the development of processes and controls to manage risks.
- Provide guidance and training on risk management processes.
- Monitor and report on the implementation and ongoing management of effective risk management practices by 'the Business'.
- Advise management and the Board on emerging internal and external issues and changing regulatory and risk environments.
- Monitor the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

The 2nd line of defence develops, aligns and maintains risk management frameworks through policies, standards, procedures, tools and training. They are also responsible for identifying the right risk management practices for CUA and supporting the proper implementation of risk management policies and for monitoring the outcomes.

The 2nd line includes:

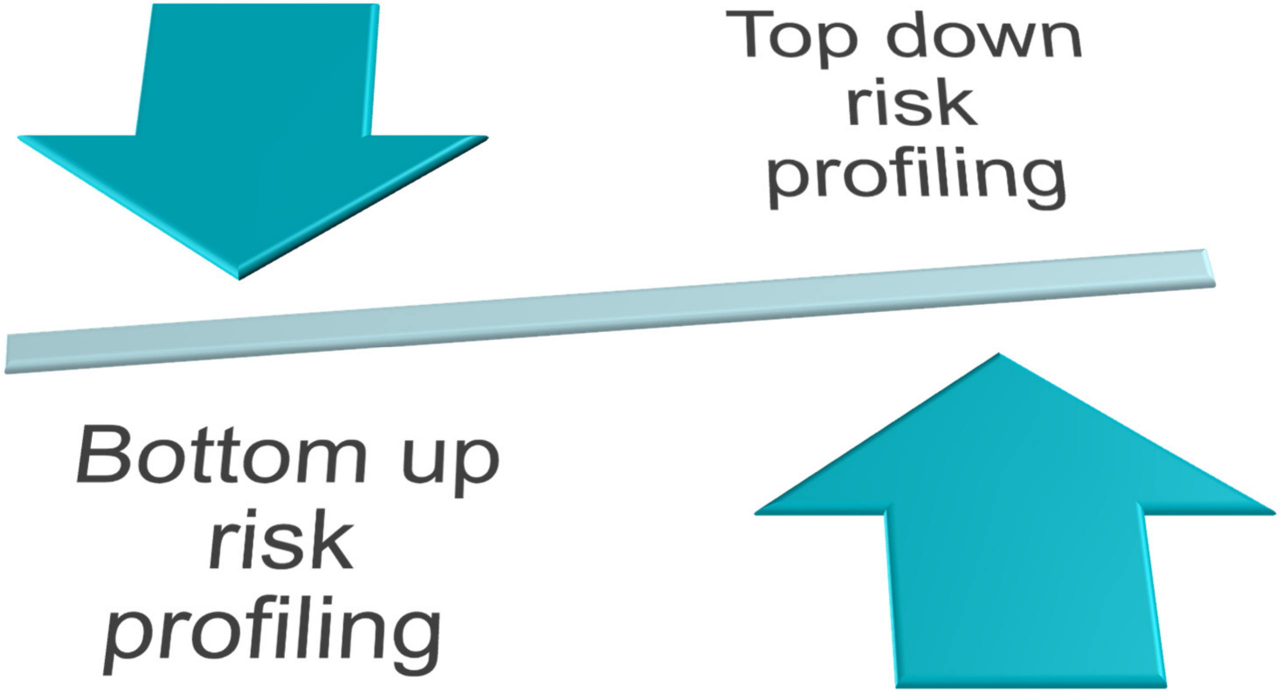
- A risk management function and committees that facilitate and monitor the implementation of effective risk management practices by the 1st line along with the provision of adequate risk-related information and analysis throughout the organisation.
- A compliance function that monitors the specific risk of non-compliance with applicable laws and regulations.

The 2nd line ensures that the 1st line of defence is properly designed, in place, and operating as intended. The 2nd line has some degree of independence from the 1st line of defence, but it is by nature a management function. As a management function, the 2nd line may intervene directly in modifying and developing the internal control and risk systems.

***2nd line Risk Management will maintain and monitor the management of risk across CUA.***

# 5. Risk profiling

A top down and bottom up philosophy



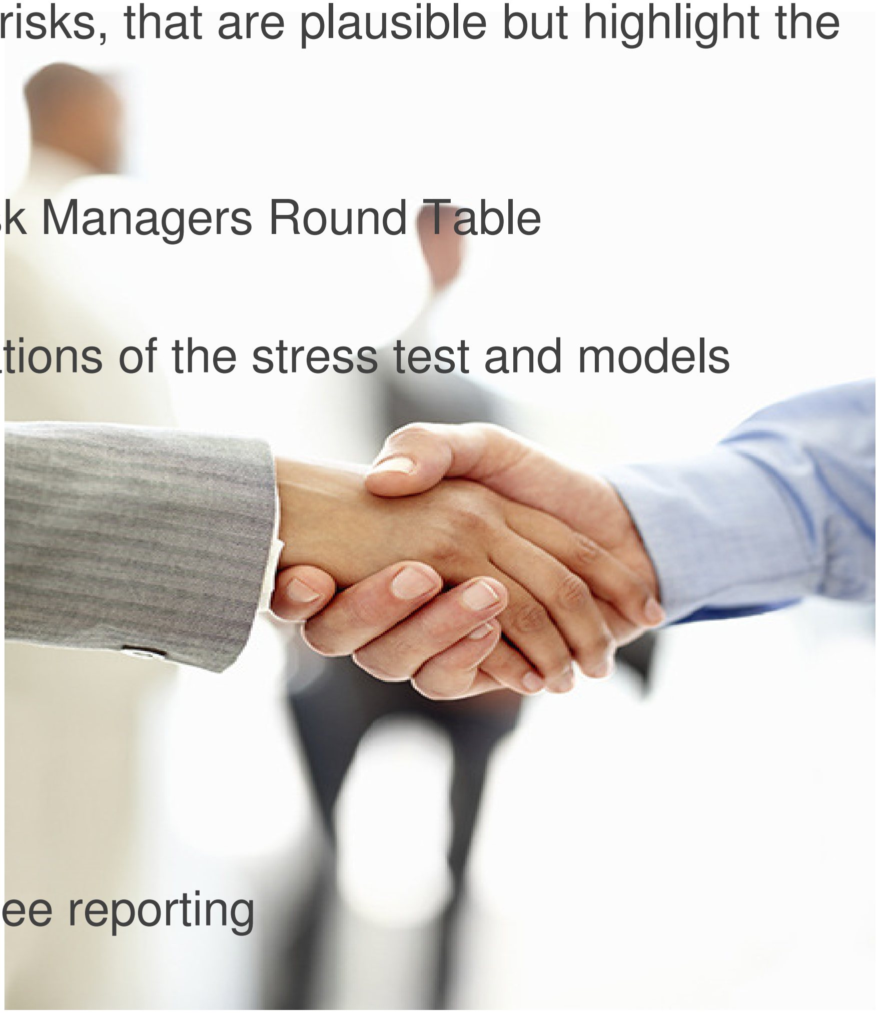
Top down risk profiling

Bottom up risk profiling

# 6. Stress testing and scenarios

## Assessing the potential future in the present

- Determine stress tests that impact cross-risks, that are plausible but highlight the impacts in a severe downturn
- Leverage external data, such as from Risk Managers Round Table
- Clearly document assumptions and limitations of the stress test and models
- Determine the capital and risk weighted assets impacts
- Ensure that the stress test results in a "so what does this mean"
- Follow up stress test results with committee reporting and actions



# Summary highlights

1. It all starts with clear risk management governance
2. Underpin risk management with a clear risk management policy, living CPS220
3. Embed in the business a board approved risk appetite statement
4. Have a robust 1st and 2nd line of risk management
5. Make risk assessment a top down and bottom up philosophy
6. Leverage stress testing and scenarios across the portfolio