財團法人住宅地震保險基金　出國報告

Munich Re
Enterprise Risk Management Workshop

出差日期：2013 年 10 月 14 日至 10 月 17 日

派赴地點：德國慕尼黑

報 告 人：陳素惠

2014 年 1 月

目　　錄

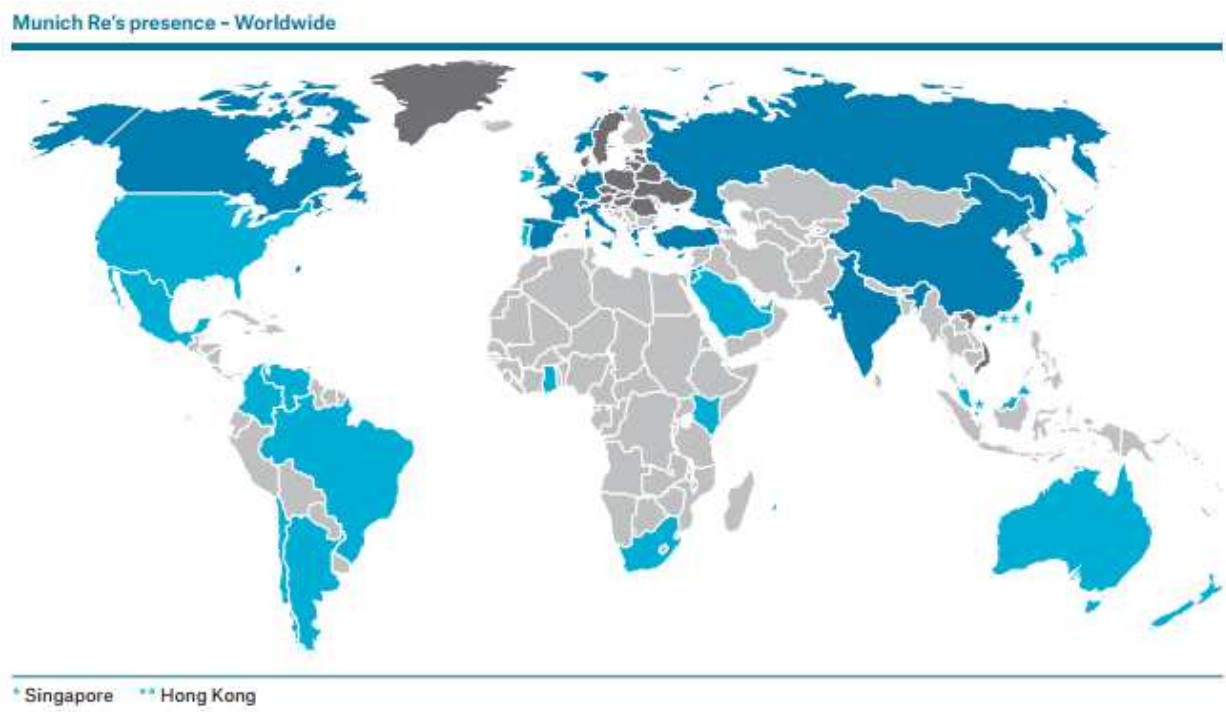
附錄：研討會議程

壹、慕尼黑再保險公司簡介

一、慕尼黑再保險集團

慕尼黑再保險集團於 1880 年成立於德國慕尼黑，總部亦設立於慕尼黑，在全球有 60 處分支機構，正式員工人數約為 45,000 人，2012 年慕尼黑再保險集團保險費收入為 520 億歐元（約新臺幣 2 兆零 8 百億元），獲利為 32 億歐元（約新臺幣 1,280 億元）。

慕尼黑再保險集團之全球分布如下圖：



慕尼黑再保險集團主要包括下列四塊版圖：再保險、保險、健康及資產評估。

(一)再保險

慕尼黑再保險公司為慕尼黑再保險集團最核心之事業單位，員

工人數約 11,000 人，2012 年再保險費收入超過 280 億歐元（約新臺幣 1 兆 1 千 2 百億元）。

(二)保險

慕尼黑再保險集團內最主要的保險公司為 ERGO 保險集團，員工（包括正職及兼職）約有 48,000 人，是德國主要的保險公司，該集團在全世界三十多個國家有分支機構，主要業務集中在歐洲及亞洲， 2012 年 ERGO 保險集團的保費收入約為 180 億歐元（約新臺幣 7 千 2 百億元）。

(三)健康

「慕尼黑健康」係慕尼黑再保險集團成立，為全球保險及再保險公司健康保健知識之品牌，在 2012 年之保費收入為 6.7 億歐元（約新臺幣 268 億元）

(四)資產管理

慕尼黑再保險集團成立 MEAG 以管理該集團全球 2,140 億歐元（約新臺幣 8 兆 5 千 6 百億元）之資產，並為其他公司提供資產管理服務，MEAG 總管理之資產為 2,380 億歐元（約新臺幣 9 兆 5 千 2 百億元）。

二、慕尼黑再保險公司

慕尼黑再保險公司為世界上最主要的再保險人之一其 2013 年 S &P 評等為 AA-，AMBest 評等為 A+。

慕尼黑再保險公司 2008~2012 年再保險業務相關數據如下表：

Reinsurance » Key figures (IFRS) – Reinsurance (XLS, 20 KB)

		2012	2011	2010	2009	2008
Gross premiums written	€bn	28.2	26.0	23.6	21.8	21.9
Investments	€bn	83.8	79.5	83.7	76.8	78.4
Net technical provisions	€bn	61.1	62.7	56.6	53.4	55.8
Large and very large losses (net)	€m	1,799	5,048	2,228	1,157	1,507
Natural catastrophe losses	€m	1,284	4,538	1,564	196	832
Combined ratio property-casualty[5]	%	91.0	113.8	100.5	95.3	99.4

現今世界發展朝向全球化之趨勢，且在資源日漸減少、人口高齡化以及科技與網路技術日新月異的影響下，不論是自然環境、社會環境、經濟環境或是法律環境均可能發生快速而顯著的變化，企業必須建立健全的企業風險管理架構與文化，處理可能面臨之短期及長期、預期與非預期之風險，才能因應挑戰，有效達成經營目標。

有鑑於企業風險管理之重要性，慕尼黑再保險公司特別舉辦 Enterprise Risk Management Workshop，邀請了來自歐洲（法國、葡萄牙、冰島、羅馬尼亞、瑞士、英國）、亞洲（新加坡、臺灣、中國大陸、印度、韓國）及非洲（摩洛哥）等 30 多家保險及再保險公司之人員共同參加本次研討會。

貳、研討會內容摘要

一、企業風險管理介紹（Enterprise Risk Management）

（一）企業風險管理之定義

根據Committee of Sponsoring Organizations of the Treadway Commission（COSO)對「企業風險管理」(Enterprise Risk Management, 以下簡稱ERM）所作之定義，ERM係一種過程，受到該機構董事會、管理階層及所有員工之影響，被應用於企業整體之策略訂定，設計用於辨識可能影響該機構的潛在事件，並且將風險控制在風險胃納範圍內，以提供達成企業目標之合理確信。(Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied to identity potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.）

（二）ERM之功能

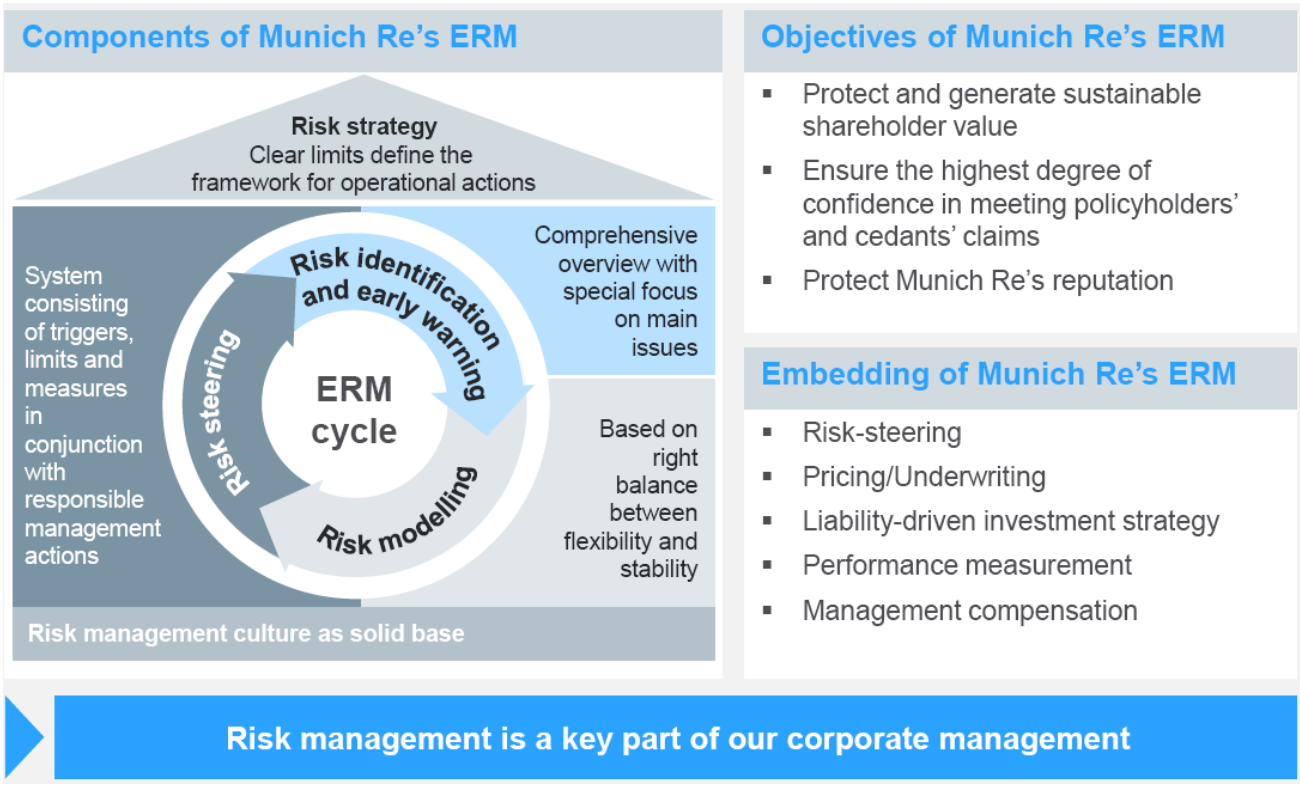
企業經營需要面對來自不同面向之利害關係人（如客戶、通路、主管機關、內部員工、股東及社會大眾)各自不同之期待，以保險公司為例，可能需要面對外來的事故（如天災）發生而對保戶產生之理賠責任、主管機關之監理要求及公司股東對於持續運作及獲利之要求等等，不同的利害關係人其對企業之期待均有所不同，董事會希望透過極大化風險報酬以提高股東價

值；經理人及員工希望藉由創造股東價值，保障其工作並獲得更好之薪酬與獎勵；保險客戶希望公司穩健經營；評等機構希望公司有一定透明度使其能提供正確資訊；監理機關希望公司運作均符合相關法規，有足夠清償能力，避免系統性問題發生，而如何在不同利害關係人利益相互衝突的要求之間取得企業經營之平衡，即是 ERM 要達成之目標。

根據 IAIS 所訂定之 ERM 準則，保險公司應建立健全的 ERM 架構，且應該在該架構下經營其業務，而該架構應考量保險公司本身業務風險的性質、規模及複雜程度，並將 ERM 架構視為整體公司治理結構的一部分。ERM 架構應結合保險公司的業務經營及公司文化，並依據實際建置的風險管理政策，處理保險公司所有合理預期及具攸關性的重要風險。

（三）經營策略觀點下的 ERM

下圖係慕尼黑再保險以其公司為例，說明 EMR 如何結合經營策略在企業內運作之組成架構：



ERM 應以企業之風險管理文化為基礎，並在風險策略中清楚地定義各種經營活動之風險限額，以作為企業運作之架構。ERM 作業循環則包括風險辨識、風險模型及風險管控。風險辨識應在綜合檢視企業內各種風險後，著重於顯著風險上；風險模型之設計應在作業彈性及經營穩健之間取得正確的平衡；而風險管控應結合負責管理作為，並在系統中設定風險觸發事件（risk trigger）、限額（limit）及衡量指標（measures）。慕尼黑再保險將 ERM 之觀念納入企業內之主要活動，如：風險管控、承保與定價、投資策略、績效評量及經理人薪酬等，均與 ERM 相結合，期能達成保障與永續股東價值、確保清償能力符合客戶理賠需求、保護公司信譽等 ERM 之目標。

（四）風險策略之訂定

Structure of Munich Re's risk strategy

Munich RE

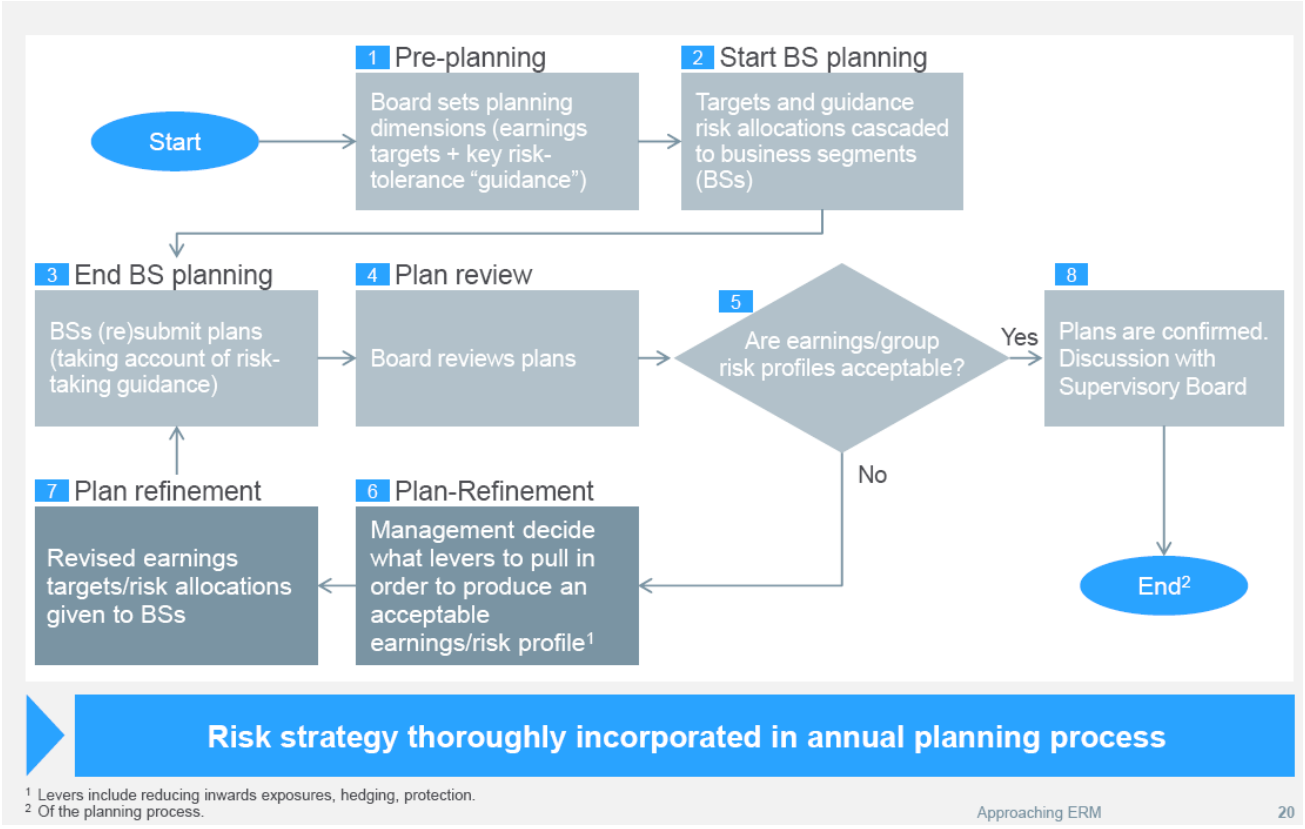
Category	Risk criteria	Measure	Objective of criterion	ERM objective addressed
Whole-portfolio criteria	**Financial strength**	▪ ERC ▪ Rating ▪ Solvency	To maintain sufficient excess capital and limiting frequency of negative economic results of Munich Re's **entire risk portfolio**	Maintaining Munich Re's financial strength, thereby ensuring that all liabilities to our clients can be met
	Avoiding financial distress	Probability of breaching financial strength criterion		
Supple-mentary criteria	▪ **Acc. risk management** ▪ Individual NatCat perils ▪ Financial sector limit ▪ Terrorism ▪ Pandemic ▪ Longevity ▪ **ALM limits** ▪ **Liquidity**	VaR limits ▪ as % of AFR or ▪ maximum exposure figure Stress-testing	To limit losses from **individual risks** or **accumulation exposure** and **liquidity risks** that could endanger Munich Re's survival capability	Protecting and increasing the value of our shareholders' investment
Other criteria	▪ Counterparty credit risk ▪ Single risks ▪ Alternative investments ▪ Non-investment-grade investments ▪ …	Individual risk limits	To limit risks that could cause long-term damage to **stakeholders' confidence in Munich Re**	Safeguarding Munich Re's reputation, thus perpetuating future business potential

慕尼黑再保險以自己集團為例說明風險策略之架構。該公司之風險策略係配合經營策略而訂定，其目的係為達成下列三項目標： 1.在財務面確保清償能力符合客戶理賠需求、2.在風險管理面保護及永續創造股東價值、3.保護公司信譽。

1.在財務面，財務能力可透過如：評等、清償能力等項目做為衡量指標，並評估各種損害財務能力之項目發生之可能性，避免財務困難，以保持資產超過整體風險組合及降低虧損之頻率，確保清償能力符合客戶理賠需求。

2. 在風險管理面，可分為三方面：(1)針對天災風險事故、恐怖攻擊、流行病、長壽風險等累積風險進行風險管理、(2)資產負債管理（Asset and Liability Management）、(3)流動性風險（Liquidity Risk）管理，透過風險值（VaR）限額及壓力測試等方式進行風險管控，將單一風險、累積風險及流動性風險控制在限額內，避免危及公司存續的資本及股東的投資，以保護及永續創造股東價值。

3. 就其他如信用風險、另類投資、非投資等級之高風險投資等風險，應就個別風險訂定限額，避免該類風險日後可能破壞股東之信心，以保護公司信譽，延續未來業務潛力。



在實務作業面上，風險策略之訂定，應整合於年度營業計畫訂定之流程中。首先由董事會訂定獲利目標及主要風險容忍指標，再由各部門依預訂獲利目標及主要風險容忍指標訂定營業計畫草案，營業計畫草案應提報董事會通過。

二、ERM 實務

ERM 在實務上可依下列的步驟進行，首先實施風險管理職責制度，接著進行風險盤點、建立風險報告及風險管控機制，重點在由上而下傳達風險容忍度，由下而上揭露風險暴露。

（一）實施風險管理職責制度（Implementation of a risk management function）

企業首先應建立風險監控制度，依企業組織架構及各個風險管理職責之角色與責任不同，區分為下列三個層級（如下圖）：

1. 第一層：管理階層

管理階層之風險管理職責為：訂定經營策略及風險策略、訂

定風險胃納及風險承受能力、定期控管風險概廓(profile)、建立早期警示系統、訂定統一之風險管理準則。

2. 第二層：風險管理人員與業務單位人員

(1) 風險管理人員

風險管理人員之風險管理職責為：進行風險之辨識、評估與風險累積之分析、發展風險評估與控管之方法與流程、風險報告、提供有關風險限額之建議、控管公司所有作業均在風險限額內進行。

(2) 業務單位人員

業務單位包括承保、定價、理賠及投資等部門之人員，其風險管理職責為：對業務單位內部顯著之風險進行辨識、分析與管理。

3. 第三層：內部稽核人員

內部稽核人員之風險管理職責為:獨立檢視風險管理目標之實施，並直接對管理階層報告。

（二）風險盤點（risk register）

風險盤點係指就公司所有種類之風險包括承保面、投資面、資金面、策略面、信譽面、操作面等風險，進行風險辨識及風險分級。

1.風險盤點作業應至少包括下列所有種類之風險：

(1)承保面風險，應包括公司經營之所有險種之風險。

(2)投資面風險，應包括如損益管理、市場風險與信用風險等。

(3)資金面風險，應包括如資金之流動與集中度及保額累積之集中度之分析等。

(4)策略面風險，應包括如經濟策略與內部策略等風險之分析。

(5)信譽面風險，應考慮如影響企業傳統及永續經營等風險。

(6)操作面風險，如作業流程、資訊系統、人員及委外人員等可能產生之風險。

2. 風險辨識

依風險之類別進行分類，並描述風險之情境/事件、造成原因、影響、最高風險之擁有者（topic owner）與風險承擔者（risk taker）等等相關資訊。進行風險辨識時，其分類應儘量完全、深入但不要過於細瑣。

3. 風險分級

將風險分為低、中、高三級，例如可就風險對財務之衝擊，依 IFRS 之標準進行分級：財務衝擊高於 15%者為高風險、財務衝擊在 5~15%之間者為中風險、財務衝擊低於 5%者為低風險；亦可依風險之發生頻率進行分級，如影響三年內經營計畫者為高風險、影響十年內經營計畫者為中風險、影響長於十年之經營計畫者為低風險。風險評估應依專家之判斷進行評估，而非僅依據數量評估。

4. 風險盤點之優點與挑戰

(1)風險盤點之優點

進行風險盤點可使企業獲得整體且全面之風險概觀，做

為風險管理細部構成之良好起點，且在引進風險盤點時所花費之人力、成本及風險管理專業知識之門檻需求相對較低，並可透過風險盤點之同時，改進企業之風險文化。

(2)風險盤點之挑戰

惟在進行風險盤點時，仍可能面臨下列之挑戰：

a. 風險細節在風險分類架構上須定位在對的層次。舉例來說，某一風險係所有部門之共通風險或僅特定部門存在該風險？

b. 在風險的質化評估僅能以相對比較標準，依低、中、高分級，如此所謂風險高低的判斷，會受該企業內風險概廓（risk profile）中風險之性質、規模及複雜程度之影響，無法有絕對的量化標準。

（三）風險報告（Risk Reporting）

風險報告可大致分為下列三類

1. 定期報告：依企業內部或外部之需求定期提供整體風險狀況及經濟觀點，內容包括顯著及異常之風險。

2. 臨時報告：即風險限額、風險觸發事件（risk trigger）報告及缺失稽查報告。

3. ORSA 報告：Solvency II 要求企業應實施 ORSA（Own Risk Solvency Assessment，有關 ORSA 之介紹詳第三點）。ORSA 綜整了經營策略、風險策略及資本策略，強化了企業對顯著風險的意識及內部模型與定價之適當性，故企業需要更適當

地配置其資本，以增進永續經營之獲利能力。

4.建立風險報告機制時，應注意下列事項：

(1)風險報告應獲得高階管理階層之協助，歌功頌德並非風險報告之重點，需透過公司高層（如董事會）對風險報告的重視，將風險報告視為對公司有用且具有價值之項目，風險報告製作者應被授權可得知必要之機密事項，且有權詢問關鍵問題，才能讓風險報告之內容真實呈現。

(2)風險報告不用在一開始建制初期即追求完美，初期的報告應概述未來的架構，將可取得之資訊納入報告中，每季定期補充新資訊。

(3)風險報告使用之文字應明確易懂，報告內容儘量簡潔，但應涵括所有已知之顯著風險，且應說明風險間之交互影響。

(4)業務部門之最高風險擁有者，因其對風險了解最深，若能獲得其協助風險管理部門者進行風險報告之撰寫，能使風險報告之內容更貼近實務。

（四）風險管控（Risk Governance）與風險模型（Risk Modeling）

1.風險管控

風險管控應由董事會由上而下進行風險之控管，企業內的人員依架構及其責任，可區分為三道防線（如下圖）：

(1)第一道防線：風險承擔者（Risk takers）

風險承擔者係指業務單位，業務單位於實施風險辨識、分析及管理時，負責及時處理及控管業務單位之顯著風險，並向獨立的風險管理窗口（independent risk management function）報告。

(2)第二道防線：ERM 窗口（ERM functions）

ERM 窗口之職責為：進行獨立的風險之辨識及累積風險分析，檢視風險策略及作成風險決策，建議風險限額並控管業務單位在風險限額內進行各項業務，設計並實施風險管控流程。

(3) 第三道防線：內部稽核人員

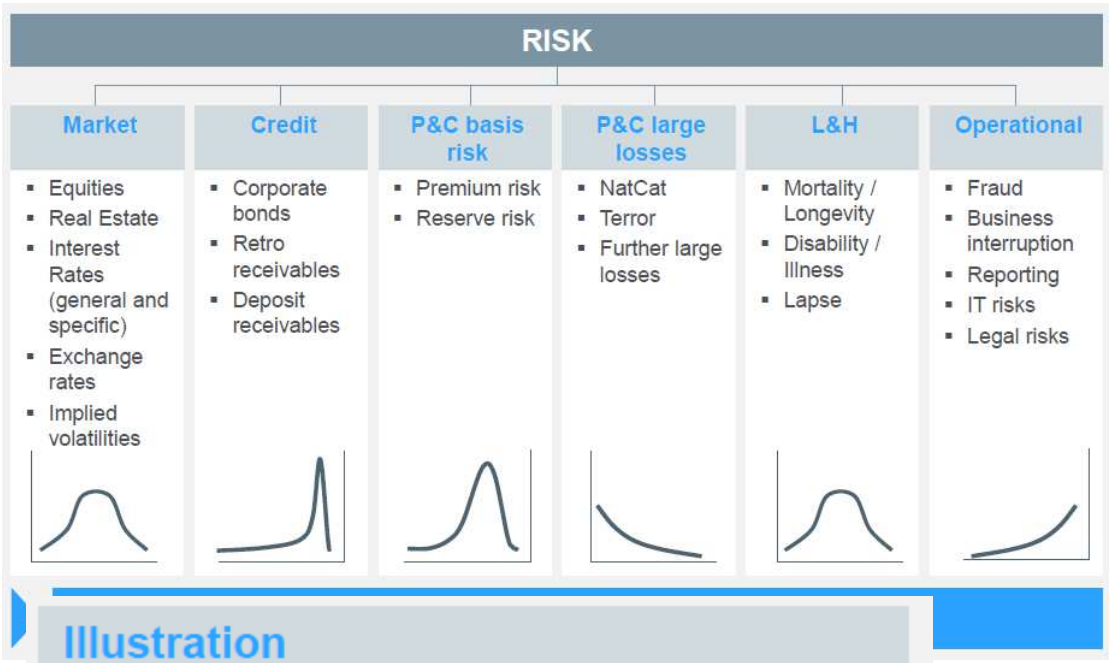
獨立驗證風險管控之有效性及相關作業運作順利與否。

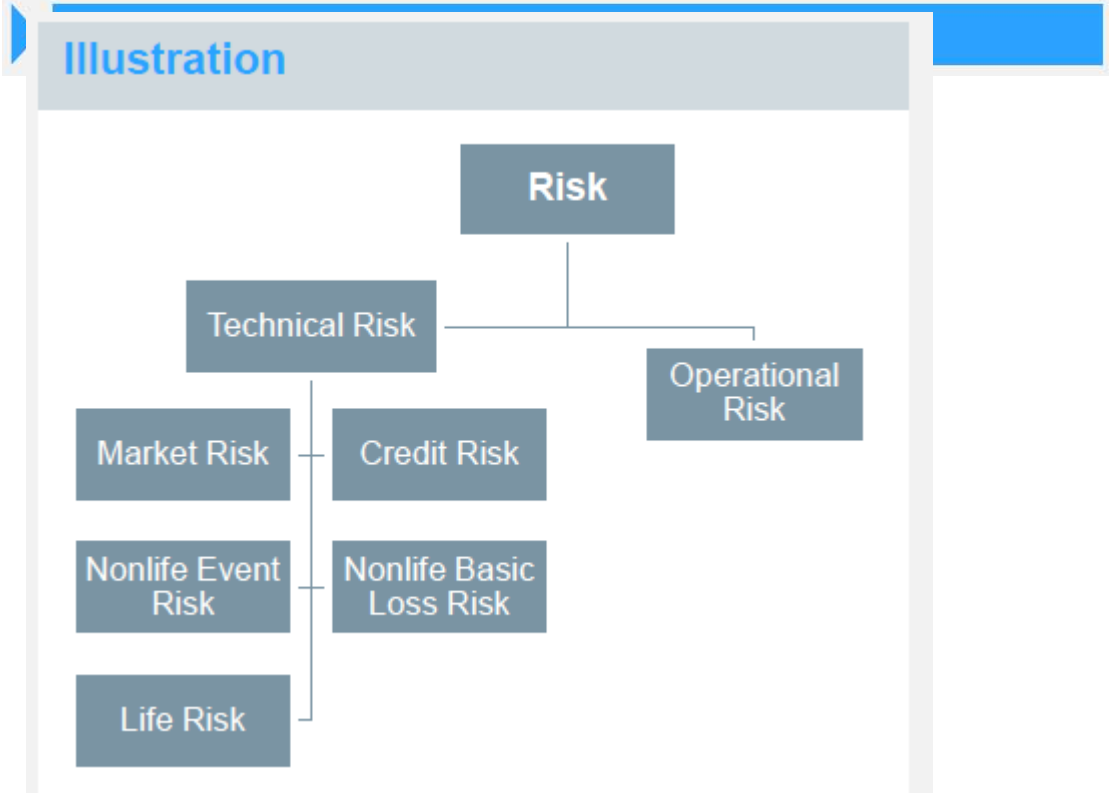
2. 風險模型

建置風險模型可協助以量化之方式進行風險管控，以慕尼黑再保險公司為例，其風險模型包括：資本配置、資產與負債

管理、風險管控與承擔、訂價、績效評估與薪酬、風險減低與評估及法規遵循等事項，風險模型在其風險管控流程之發揮重要功用。

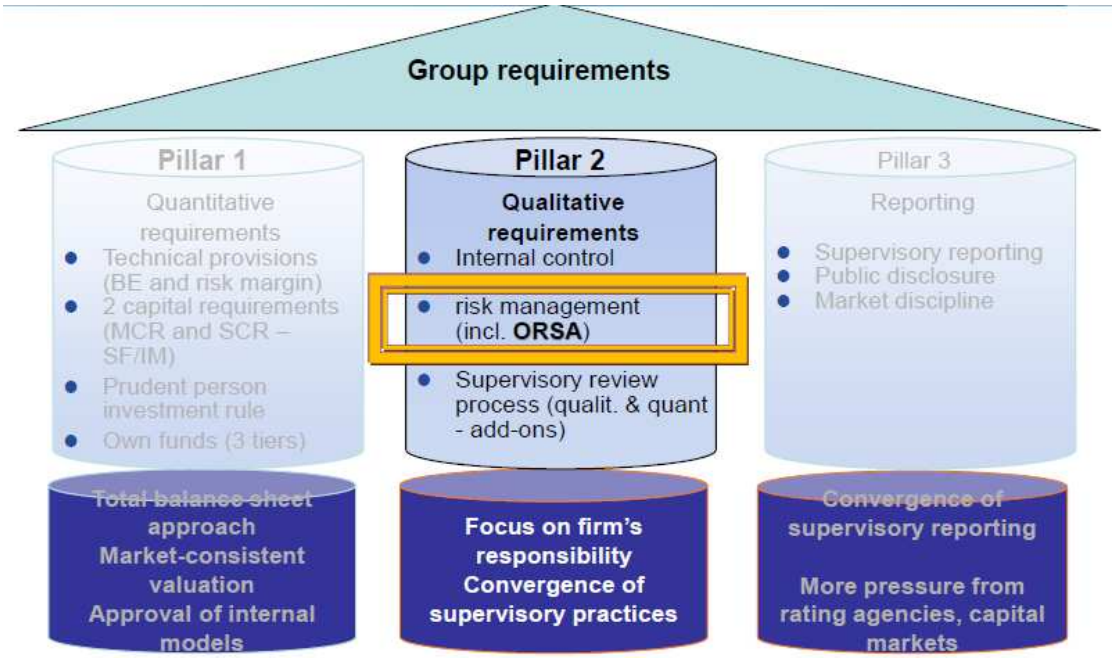
慕尼黑再保險公司針對市場風險、信用風險、財產保險之天災風險、財產保險非天災風險、人身保險風險及操作風險等不同風險分別建立獨立之風險模型，再就個別風險間之風險累積及交互影響進行分析。





三、自我風險及清償能力評估(Own Risk Solvency Assessment)介紹

歐盟（EU, European Union）所研擬的 Solvency II，係針對保險產業的清償監理制度，而 Solvency II 之監理架構可分為三大支柱：第一支柱為量化(quantitative)的要求(包括資本計提計算)、第二支柱為質化（qualitative）的要求（包括內部控管、風險管理及監理檢視流程)、第三支柱為報告（reporting）的要求（包括監理機關通報、公開揭露及市場紀律等)。而自我風險及清償能力評估(Own Risk Solvency Assessment,以下簡稱 ORSA)，即是 Solvency II 第二支柱中風險管理部分之核心。



資料來源：European Insurance and Occupational Pensions Authority, EIOPA 網站

（一）ORSA 之定義

ORSA 根據 CEIOPS（Committee of European Insurance and Occupational Pensions Supervisors）之定義，係指

它可以被定義為用來的識別、評估、監控、管理和報告公司面臨或可能面臨之短期及長期風險之過程和程序的全部，以及確定公司必要之自有資金可承擔任何時間點之整體清償能力之需求。

（ORSA can be defined as the entirety of the processes and procedures employed to identity, assess, monitor, manage and report short and long-term risks which a company faces or may face and determine the own funds necessary to cover the overall solvency needs at all times.）（CEIOPS Issues Paper on ORSA, 27 May 2008）

（二）ORSA 之內容

ORSA，Own Risk Solvency Assessment

1.Own，指由公司自己本身的角度來看自己本身的風險。

2.Risk，指公司現在面臨或未來可能面臨之所有風險。

3.Solvency，指確定自有資金足可因應公司依預訂之營業計畫運作及發生潛在不可預期之不利狀況下均有足夠之清償能力。

4.Assessment，指進行自我風險管理程序，以識別、評估、監控、管理和報告短期及長期風險之有效性。

（三）ORSA之主要流程

ORSA之主要流程，可分為5個步驟，分別為：風險辨識、風險評估、風險管理、風險報告及風險監控，茲分述如下：

1.風險辨識

辨識所有顯著風險，包括承保風險、市場風險、信用風險、作業風險、流通性風險、信譽風險、策略風險及新興風險等，並須一併考慮外部因素，例如經濟情況（如利率及國內生產毛額等）、法律環境（如稅法及行政機關命令之改變等）、保險市場變動（如新產品的開發、併購及保險市場趨勢等）。

2.風險評估

根據上述已辨識之風險，依風險優先性、風險來源、風險發生可能性、風險發生頻率、風險暴露、風險交互影響性及風險對資產負債表之衝擊等進行評估，並依風險發生頻率高低

及影響程度大小分級。

風險評估亦可以壓力測試之方式進行，測試方式有：

(1) 敏感度分析（Sensitivity Analysis)，係指檢驗單一風險因子 （例如利率、匯率、或資產價格等）或是一小組彼此高度相關風險因子，在所有其他不確定因素保持在定值的條件下，變動該項目的不確定性對目標之影響程度為何。

(2) 情境模擬分析（Scenario Analysis)，係指由某種可引發多種風險的背景環境事件出發，設想各種風險變動結果之過程。

(3) 反向壓力測試（reverse stress test)，即給定某程度嚴重損失後，假設可能造成該嚴重損失的壓力事件。反向壓力測試的重點在於評估什麼樣的壓力事件或是壓力事件到底要有多嚴重，才能造成給定的損失水準。

3.風險管理

風險管理之重點在管理顯著風險,風險管理係以達成營業策略為目標,其內容包括訂定風險容忍度內之風險胃納、訂定風險限額及風險觸發事件、評等之優化及法令遵循等。

風險管理之方法包括：再保險、資本市場工具、降低資產或負債風險、資產證券化、避險工具及風險移轉等。

4.風險報告

ORSA 之政策包括：訂定集團適用之準則、連結至現有之作

業程序、建立負責窗口及年度檢視。

企業無需為 ORSA 另行製作一套新的報告或文件，但應保留 ORSA 及結果之內部文件或適當之證明。

年度 ORSA 報告應包括下列內容：

(1) 風險概廓。

(2) 營業策略及風險策略。營業策略應包括營業目標及營業策略；風險策略應包括風險分類之定義、實施過程及結果等。

(3) 資本管理，應包括如清償能力、可用資本、資本適足評估、資本管理策略等。

(4) 風險容忍度。

5.風險監控

風險監控之內容包括：

(1) 持續監控風險限額及風險觸發事件。

(2) 當發生超過風險門檻（risk threshold）情形時，即應啟動相關程序。

(3) 監控自有資金是否足以因應該風險。

四、風險複雜性及交互影響（Risk Complexity and Interdependencies）

（一）風險之複合性

近十幾來的重大事件除了單獨事件所造成之鉅額保險損失，尚引發了其他事件之發生造成了重大的經濟損失，如世貿大

樓的恐怖攻擊（2011.9.11）影響美國航空及旅遊相關產業，對美國短期經濟造成震撼性影響；颶風 Katrina（2005.8.29），迫使美國墨西哥灣沿海地區的油井、煉油廠關閉，影響美國煉油 1/4 生產量，墨西哥灣沿海港口及碼頭受損或關閉，影響進、出口貿易，並使全球原物料短期上漲；冰島火山爆發（2010.3.25）使歐洲實施大範圍空中管制，致航空業遭受重大經濟損失，並使依賴航空運輸之旅遊、物流等相關產業也受到嚴重波及；東日本大地震（2011.3.11）造成日本福島第一核電廠受損因而發生輻射洩露事件，核能輻射洩露事件除持續影響日本福島當地人身安全健康、農產品滯銷外，本(2013)年 8 月尚發生輻射水外洩至太平洋之事件，此事件對洋流沿岸之國家可能造成之影響如何，至今仍待觀察；泰國水災（2011 年 8 月~10 月）嚴重影響電子、汽車業，尤其是對在泰國設廠之全球化企業造成重大之營業中斷損失。

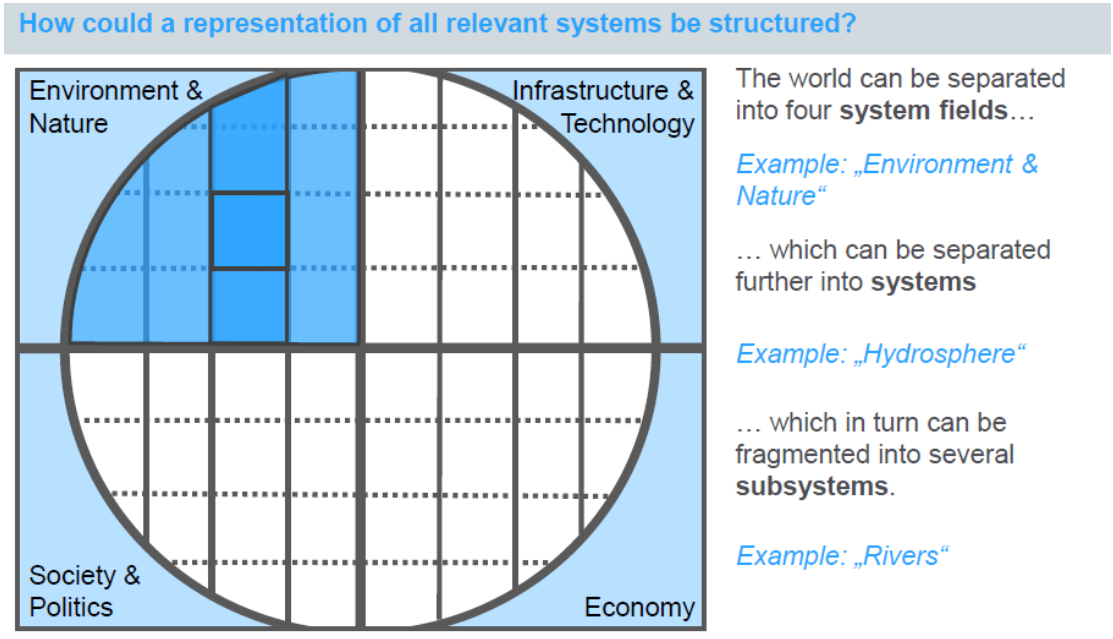
現今科技發展快速、全球化、都市化、資源日漸稀少、氣候變遷、法規數量增加，相關監理日益嚴格、人口數量增加等，都在在使世界發生結構性的變化，亦大幅增加了風險複雜性及其交互影響，增加風險值（VaR）正確預估之困難度。

（二）風險交互影響分析

1.列出可能發展成系統性風險之獨立的風險

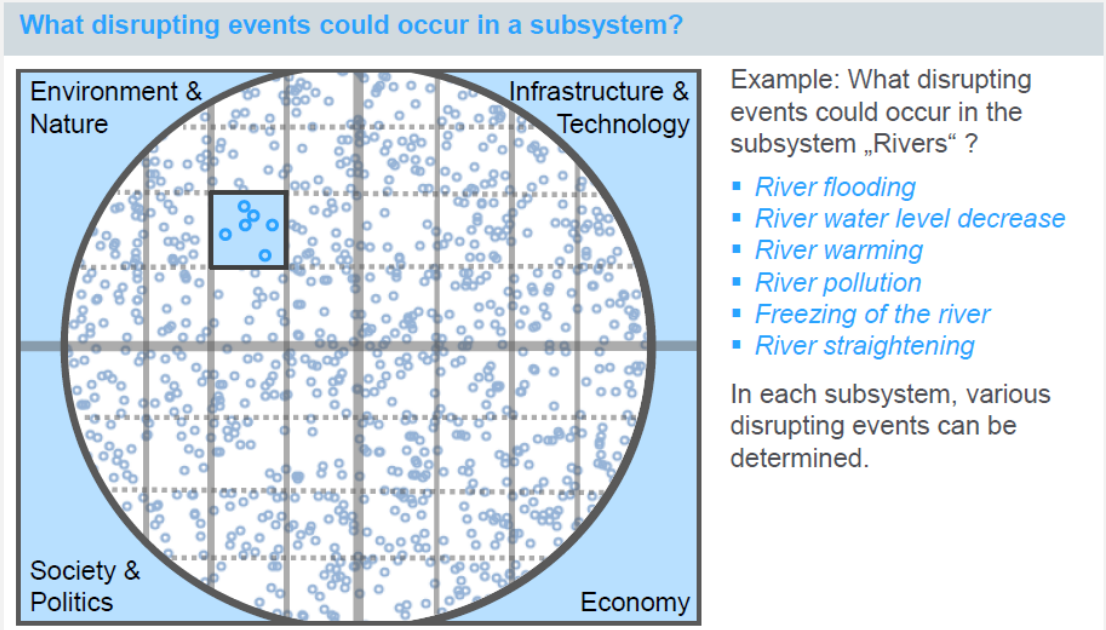
(1)首先將自然環境、社會政治、科技與基礎建設及經濟列為同一張圖之四個象限。

(2)再試列出可能發展為系統性風險之獨立的風險，例如：水資源（hydrosphere），再將水資源細為幾個子項，列出可能較為硬弱的環節，如：河流。



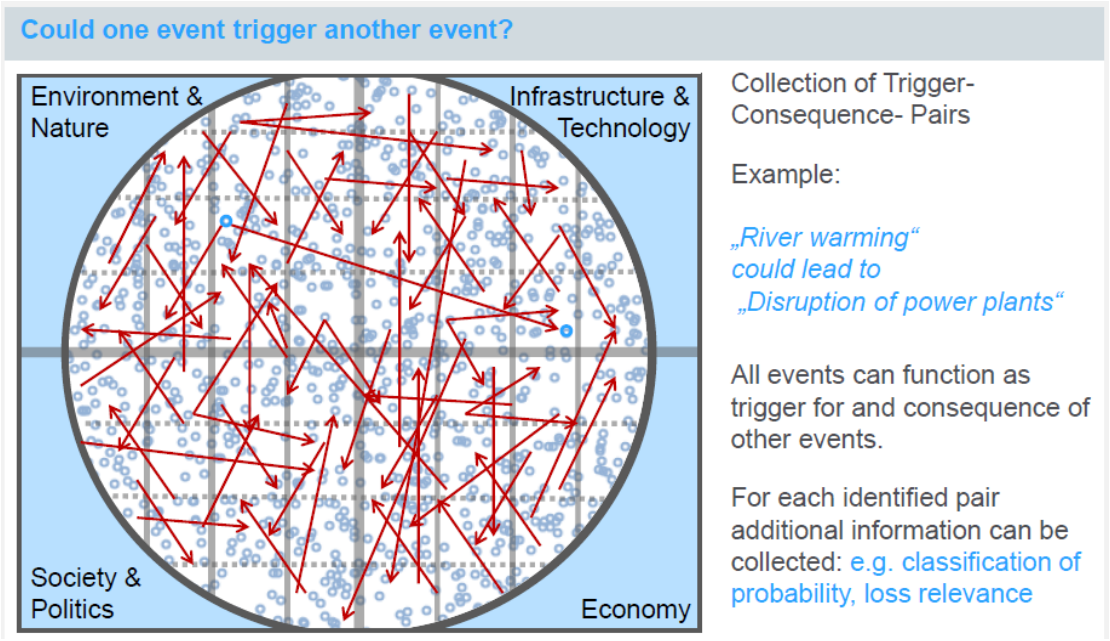
2. 辨識相關事件

確認何種破壞事件可能會發生在「河流」這個子項中？如：河水泛濫、河水面高度下降、河水溫度變高、河水污染、河流結冰、河流河道變直…..等。



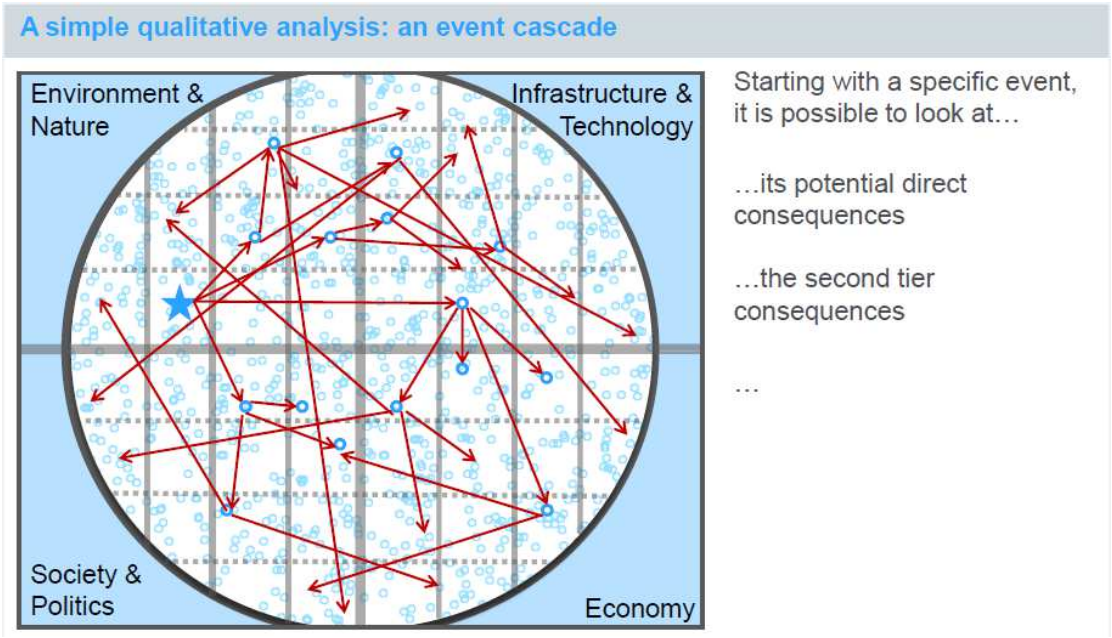
3. 辨識風險之關連性

將彼此間可能具有關連性之事件連結組合起來，例如：「河水溫度升高」可能造成「發電廠運作中斷」，並將所有可能具有關連性之事件組合依損失概率（probability）及損失金額（loss relevance）等相關數據分類。



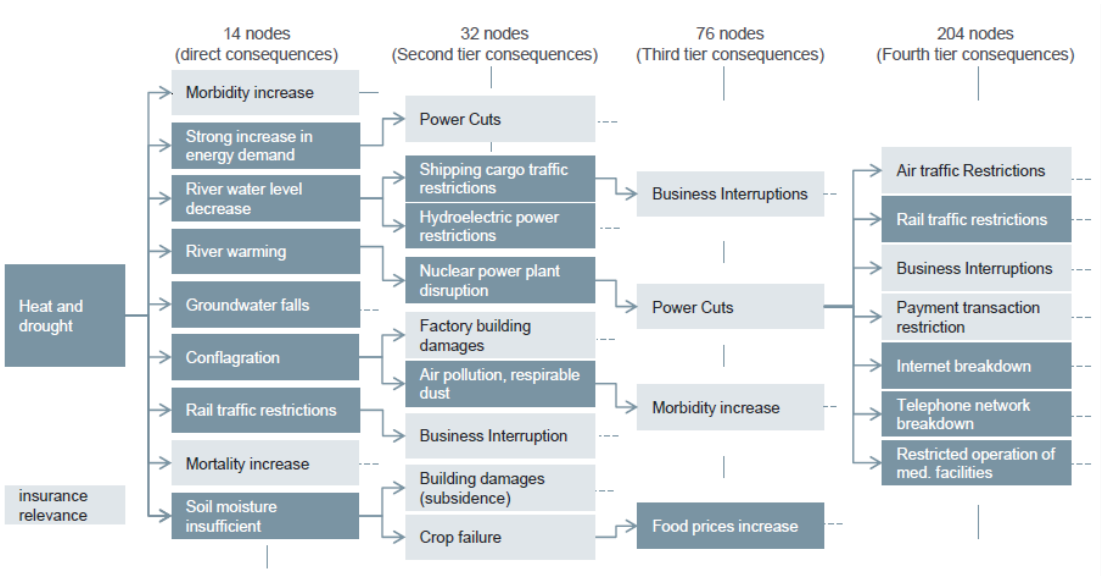
4. 分析

依據相關資料進行量化及質化分析，例如：將關連性之事件依可能發生之時間順序串連起來。



5. 將潛在之損害結果依發生之遠近順序分析

例如以天氣高溫與乾旱為例，依影響因素與損害結果間之遠近順序列出可能造成之情境如下圖：



(1)直接造成損害結果之可能情境，例如：因天氣高溫與乾旱造成死亡及生病人數增加。

(2)經過二層因素而產生損害結果之可能情境，例如：因缺

乏水力發電而造成電力中斷、發生火災然因缺乏水源滅火而使工廠廠房損壞、因乾旱造成土壤乾燥而致使農作物欠收…等。

(3)經過三層因素而產生損害結果之可能情境，例如：因河水水面降低影響貨物之水路運送而造成營業中斷、因河水水溫升高造成核電廠故障而導致電力中斷…等。

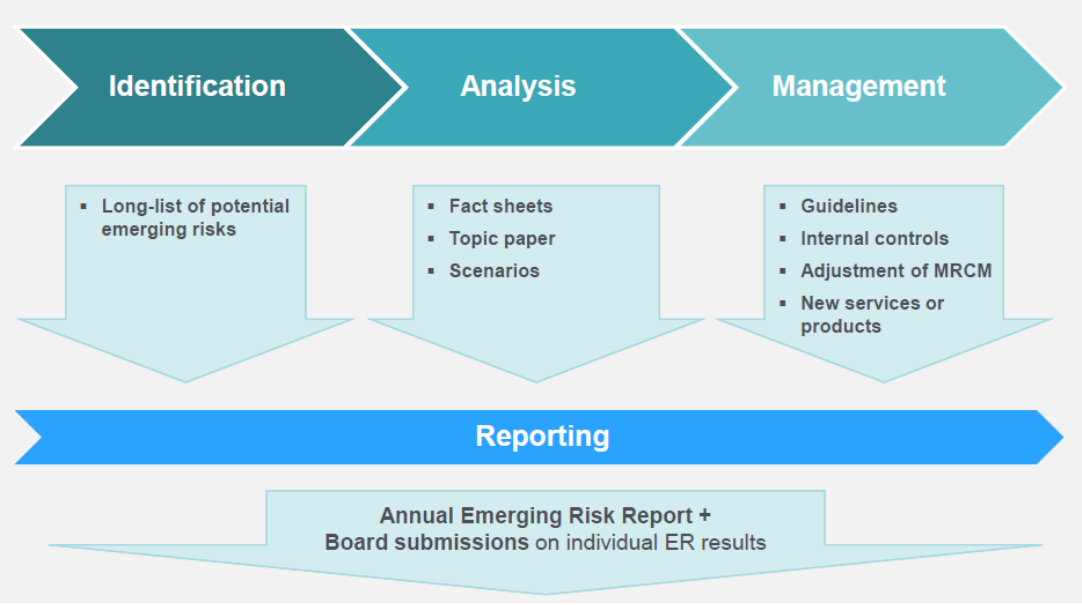
(4)經過四層因素而產生損害結果之可能情境，例如：因河水水溫升高造成核電廠故障、導致電力中斷而致使空運交通受限、網路及通訊中斷、影響醫院設施運作…等。

五、新興風險-以網路風險為例

（一）新興風險

1. 如何辨識新興風險

辨識新興風險之流程包括：新興風險之辨識、分析與管理，最後針對獨立之新興風險製作年度報告，其概略流程如下圖：



(1) 新興風險辨識：列出潛在之新興風險名單。

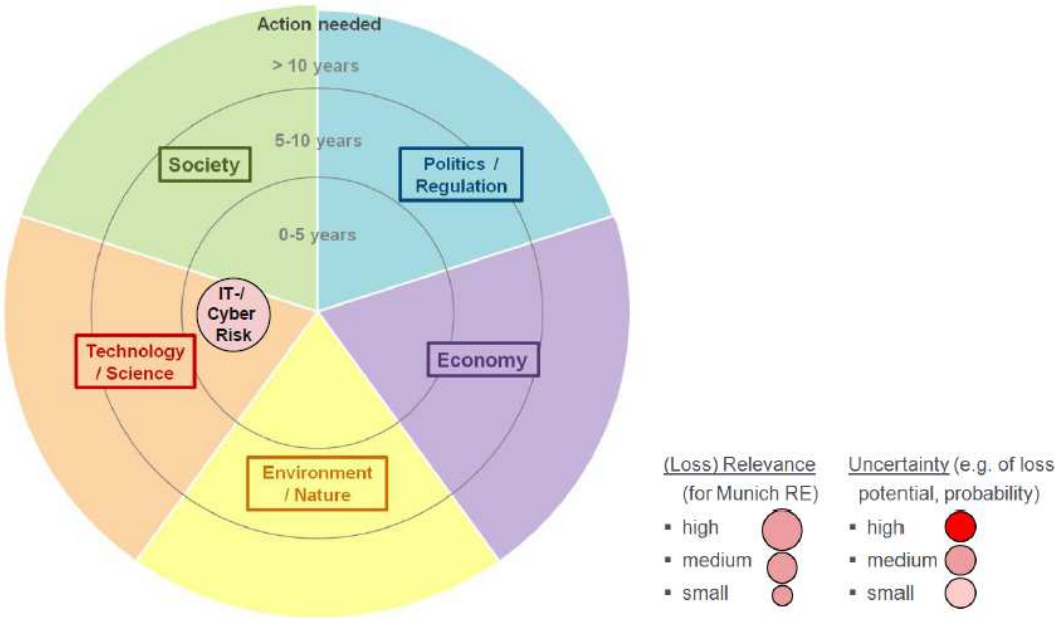
(2) 新興風險分析：製作新興風險清冊、新興風險主題報告及情境模擬分析。

(3) 新興風險管理：製作新興風險準則、內部控制制度、調整內部模型參數、採用新服務或採購新產品因應新興風險。

(4) 新興風險報告：針對獨立之新興風險製作年度新興風險報告，並提報董事會。

2. 風險雷達圖

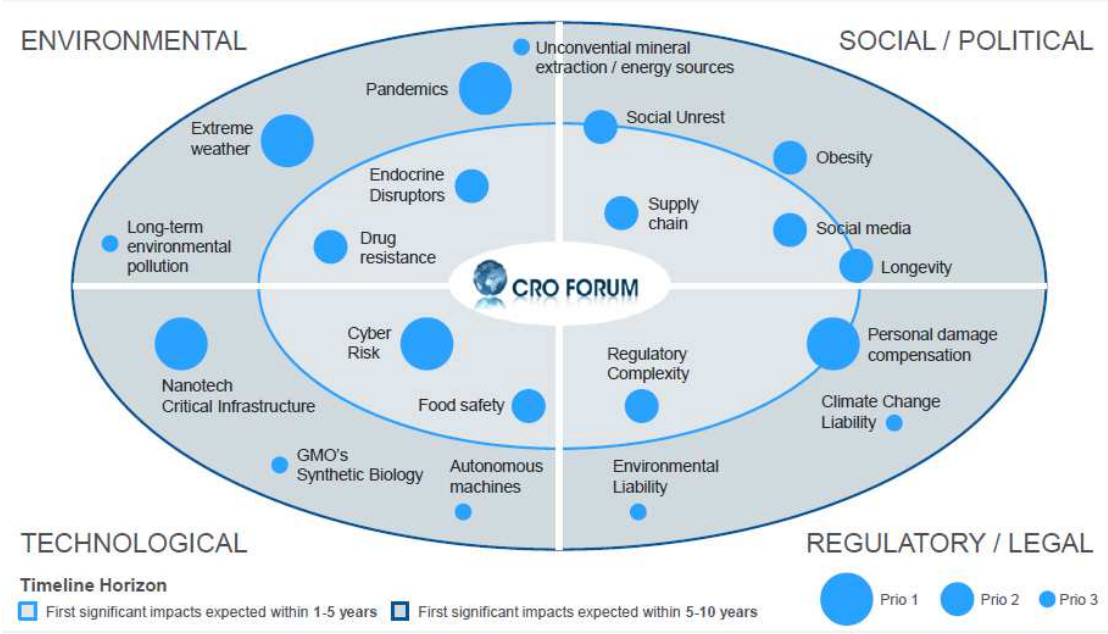
企業可將已辨識出之新興風險，依其種類區分為數個大類，如政策及法規面、經濟面、自然環境面、科學科技面、社會面，再依各個新興風險需採取行動之因應時程，分為 5 年內、5~10 年及長於 10 年。然後依上述分類及因應時程，可畫出風險雷達圖如下：



各個新興風險尚可分別依損失之相關性，由高至低以符號大小標示，及損失發生之可能性，由高至低以顏色深淺標示。如此則越接近雷達中央、符號越大、顏色越深者，即表示需特別注意之新興風險。

3. 未來 1~10 年需優先注意之新興風險

2013 年 3 月慕尼黑再保險公司主辦之 CRO FORUM 即提出依優先順序於 1~5 年及 5~10 年內在環境面、科技面、社會政治面、法規面可能發生之新興風險雷達圖。CRO FORUM 認為在 1~5 年需優先注意之新興風險為網路風險（Cyber Risk）及個人權利保護與損失填補（Personal damage compensation）；而在 5~10 年內需優先注意之新興風險為傳染病（Pandemics）、極端氣候（Extreme weather）及奈米科技之關鍵基礎建設（Nanotech Critical Infrastructure）等。



（二）網路風險

新興風險中最需優先注意者，非網路風險莫屬，茲簡要說明網路風險如下：

1.網路風險之定義

(1) Committee on National Security Systems of the US 認為：網站風險係指透過利用系統弱點對資訊系統造成特定威脅之可能。(Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability)

(2) ISO International Organization for Standardization 認為：網站風險係指，一個特定威脅利用資產組合的漏洞對組織造成損害之潛在可能。(the potential that a given threat will exploit vulnerabilities of an asset of group of assets and thereby cause harm to the organization)

(3) Information Systems Audit and Control Association (IACA)認為：網站風險係指透過在企業中使用、擁有、經營、參與、影響及採用資訊系統而產生之營業風險。(The business risk associated with the use, ownership, operation involvement, influence and adoption of IT within an enterprise.)

2.網路風險之趨勢與威脅

現今科技、外部網路、現代化的基礎建設越來越進步，在

全球化的影響下，網路風險相關之立法、監理及法律遵循的控管也越來越受到重視，此為網路風險之趨勢。

隨著委外業務、雲端服務逐漸發展，服務業的文化也逐漸改變，從固定的服務時間到隨時（24hrs/7days）都在網路上提供服務，網路風險之威脅也隨之增加，除了系統遭到駭客入侵可能對商譽造成風險外，隨著網路使用率的增加，也提高了非惡意造成之事件或系統當機之造成之衝擊。

3.網路風險之概廓

網路風險之影響範圍可大概區分為安全、法律、責任及商譽等下列四個方面：

(1)安全面：可能發生如服務中斷、駭客勒索、網路蓄意破壞（Electronic Vandalism）、資料失竊、電腦病毒等風險。

(2)法律面：網路風險可能導致企業違反民法、個人資料保護法等相關法令。

(3)責任面：倘發生資料失竊事件，可能發生智慧財產權侵害、個人資料洩露等賠償責任，還有無法提供客戶服務可能亦需負擔之責任。

(4)商譽面：倘發生網路中斷、網站資料遭人竄改或資料洩露等網路風險事件，可能導致商譽受損。

4.降低網路風險之建議方案

為降低網路風險，企業可以考慮採行下列方案：

(1)提升安全性，如提升軟、硬設備之安全等級等，以及建

立持續性的風險管理架構，如資料加密等。

(2)評估、分類及保障公司之資產，如營業及市場資訊，尤其是敏感性資料，如健康及信用等個人資料等。

(3)為意外事件做好準備，如事先列出顧問清單及因應媒體之策略。

(4)法律保障，如訂定保密條款、依法律之規定對個資遭到洩露事件之當事人於時限內進行告知等。

(5)檢視包商及合作對象之安全等級，特別是委外業務之廠商及雲端服務廠商。

(6)關注報紙及媒體登載之相關新聞。

(7)進行員工教育訓練，以能對風險保持警覺。

(8)購買網路風險保險。

參、心得

ERM 是近年來風險管理領域發展出之新型態管理方式。現今企業面臨的風險型態日益複雜，企業經營之不確定性增加，來自外界如監理機關、信評公司、投資人及消費者的監督力量，亦不斷增加，對企業形成不小之壓力，除了傳統各種險種如財產、人身或責任等風險外，尚包括財務、作業、策略、法令遵循、商譽等類型之風險，某些風險難以量化，亟需適當之管理方式，且各項風險並非獨立存在，而有是交互牽動、影響，為因應當前所面臨之環境日益複雜，因而形成 ERM 之概念，由企業整體經營及運作之角度，同時考慮到各種風險間之相關性，將企業所面臨之所有風險全部納入管理。

隨著現今世界環境變化快速，且在全球化的連結下，極可能產生牽一髮而動全身的蝴蝶效應，企業隨時都需面對新興風險發生之可能，或維持運作之基礎可能日漸在改變，而其不自知，而 ERM 即可幫助企業早期發現新興風險存在並做好因應之準備。

本報告於說明 ERM 時，為行文簡便，採行 ERM 之主體大多以「企業」為主詞，然 ERM 之觀念對於非屬營利單位之組織，如本基金，亦可比照適用。本次整理 ERM 研討會報告資料的同時，再對照本基金為因應個人資料保護法施行所採行之相關風險管理措施，時心有戚戚焉，本基金在因應個資法施行之處理上，實已採行了 ERM 之概念。本次慕尼黑再保險所舉辦之 ERM 研討會，理論面與實務面均有清楚之說明，深覺獲益良多。

附錄：研討會議程

Programme

Monday, 14 October 2013

ERM – definition, requirements, assessments

9.00 a.m.	**Welcoming address, programme, introduction of participants** *Patrik Asselmann, Dr. Thomas Schaffrath-Chanson, Evelyn Wild, Cora Ziegler-Bohr*
10.00 a.m.	Break
10.30 a.m.	**CRO view on Enterprise risk management** *Jo Oechslin*
11.30 a.m.	**Approaching ERM** *Dr. Jürgen Dümont*
2.00 p.m.	**Building the ERM house: Group work on requirements, benefits and effort required**
3.15 p.m.	**Presentation of group work results and plenum discussion**
4.00 p.m.	End of programme

Tuesday, 15 October 2013

Risk identification, strategy, modelling, capital allocation and risk reporting

9.00 a.m.	**ERM in practice: functions, identification and risk reporting** *Ulrike Licht*
10.00 a.m.	Group photo session and break
10.30 a.m.	**From business to risk strategy, from limits to triggers** *Alexander von Borries*
11.30 a.m.	**Risk modelling and governance at Munich Re** *Robert Lempertseder*
12.30 p.m.	Buffet lunch
2.00 p.m.	**Risk radar:** **Group work on strategic, reputational, operational and liquidity risks**
3.00 p.m.	Break
3.15 p.m.	**Presentation of group work results and plenum discussion**

4.15 p.m.	**All eyes on the medical crystal ball: Meta trends and their impact on the insurance industry** *Dr. Karsten Filzmaier*
5.15 p.m.	End of programme
5.30 p.m.	**The inner way: Discovering Munich Re's art and buildings (optional)**
6.45 p.m.	End of guided tour

Wednesday, 16 October 2013

ERM and value based management, special topics, tools, financial management

9.00 a.m.	**Return versus risk? Economic performance** *Silke Habenicht*
10.00 a.m.	Break
	Breakout sessions: Please choose which you wish to attend
10.30 a.m.	**Reinsurers' capital strength – increasing impact on balance sheet** *Dr. Manijeh Mc Hugh, Lars Moormann*
	or
10.30 a.m.	**Organising ORSA – preconditions, workflows, assessments** *Patrik Asselmann,* *Dr. Thomas Schaffrath-Chanson*

2.00 p.m.	**Introducing NATHAN: Around the globe in one hour** *Bernd Wagner*
	or
2.00 p.m.	**KEYFUN – key function requirements under ERM** *Norman Ducoffre, Dr. Thomas Schaffrath-Chanson*
4.00 p.m.	Break
4.15 p.m.	**Never-ending euro crisis? Capital management in turbulent times!** *Dr. Jürgen Callies*
5.15 p.m.	End of programme
5.30 p.m.	Meeting place: Walking Man Leopoldstrasse 36, 80802 München
6.00 p.m.	**Special tour through BMW Welt** **Am Olympiapark 1, 80809 München**

Thursday, 17 October 2013

Beyond ERM – emerging and cyber risks, business model stress and innovation

9.00 a.m.	**Risk identification, complexity and interdependencies** *Dr. Markus Wadé*
10.00 a.m.	Break
10.30 a.m.	**Cyber risks – findings, challenges and solutions** *Heidi Strauß*
12.00 noon	**Business model stresses in the era of change** *Rudolf Schmid*
12.30 p.m.	Buffet lunch
2.00 p.m.	**Is your business model @ risk? Group work on taking ERM to the business level** *Rudolf Schmid*
4.00 p.m.	Break
4.15 p.m.	Wrap-up and participants' feedback
4.30 p.m.	End of seminar