

# Pool Re Presentation to the ACRSM

Tom Clementi, CEO

*26 July 2023*





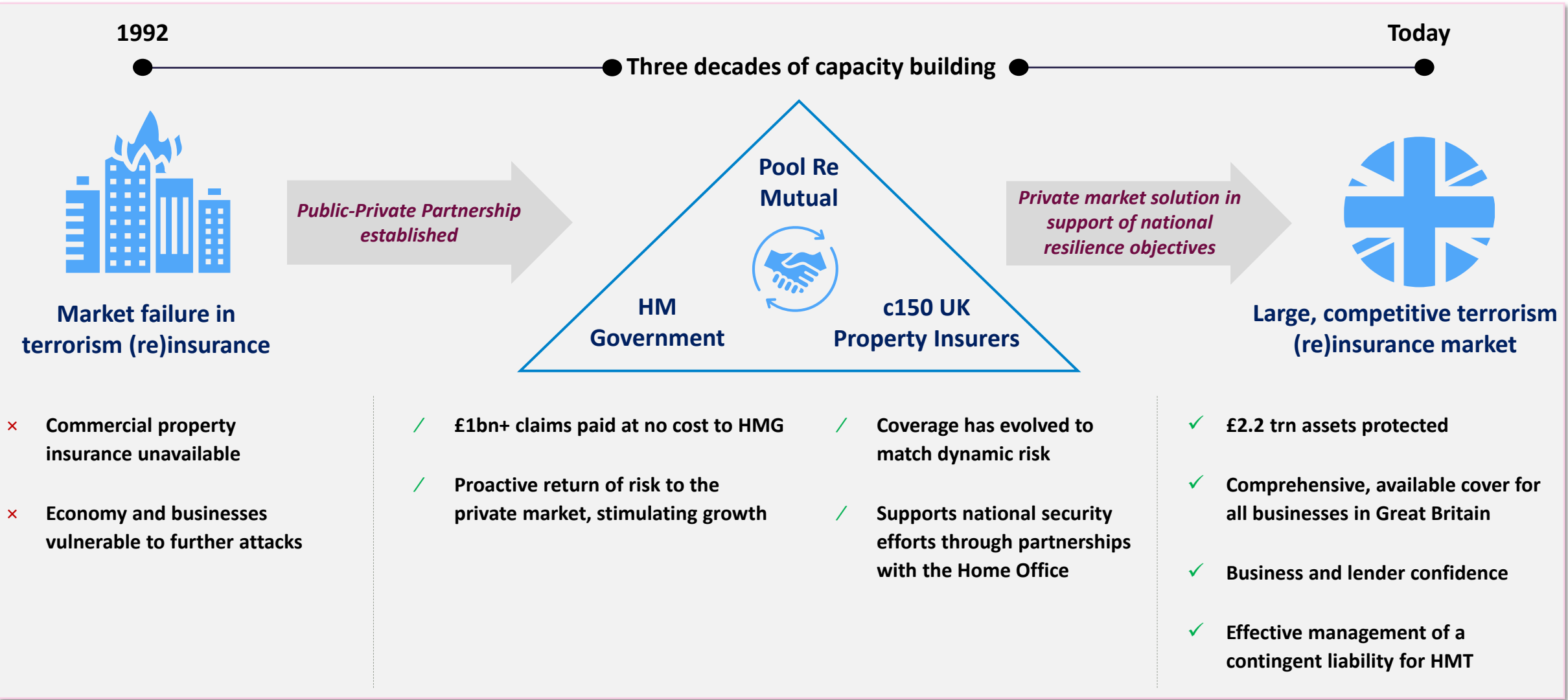
# Contents

---

- 1. Pool Re** (*Overview & Scheme Modernisation*)
- 2. IFTRIP** (*Context and 2023 / 2024 activity*)
- 3. UK Cyber Landscape** (*Assessment of case for greater public/private collaboration*)
- 4. Questions**



# Since its formation, Pool Re has enabled and leveraged the private (re)insurance sector to serve a public policy objective and underpin the UK's economic resilience to terrorism








**Pool Re provides confidence and resilience to the UK economy through a £10bn+ risk financing structure which leverages global reinsurance and capital markets, insulating UK taxpayers from loss**

<b>HM Treasury</b> HM Treasury Funding	
<b>HM Treasury funds to the credit of Pool Re</b> Premium paid to HM Treasury, held to the credit of Pool Re	<b>£1.8bn</b>
<b>Fund</b> Pool Re investment fund	<b>£6.3bn</b>
<b>Retrocession</b> Commercial retrocession & insurance-linked security	<b>£2.4bn</b> £0.1bn
<b>Fund</b> Pool Re investment fund	<b>£0.4bn</b>
<b>Retention</b> Per event Member retention	<b>£0.25bn</b>






# Pool Re is preparing to convert its treaty arrangements with Members from a Facultative Obligatory model to an Aggregate XOL model, incepting in 2025




## The intended changes to the scheme...

-  Enable Members to **reintroduce terrorism cover as standard** within their 'All Risks' policies
-  **Split retention structure** between CBRN/Cyber and other terrorism perils such that eventually HMG only supports the market in areas of genuine 'failure'.
-  **Operationally simpler scheme** that is fit for contemporary **digital insurance marketplace**

## ... Will lead to beneficial outcomes for HMT, policyholders, and Insurer Members ...

-  **Optimal management of HMT's contingent liability**
-  **Promotes confidence & resilience in the economy and the return of risk to the private market**
-  **Growth & innovation opportunity for UK insurance industry**

## ... And will be facilitated by Pool Re on an ongoing basis

-  Terrorism risk **actuarial, pricing, and exposure management expertise** available to Members
-  Terrorism risk **intelligence, management, and transfer expertise** available to Members
-  **Conduit between HMT, Members, Home Office, and Academia** to align interests, intelligence, and achieve shared national security and resilience objectives



# Pool Re and the FIO are Members of the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP)

## The Value of IFTRIP



## IFTRIP in 2023 / 2024

- × **Only forum of its kind in the world**, with over a dozen members.
- × **Builds international collaboration between national terrorism and disaster insurance programmes**, governments, (re)insurance professionals, academics, and the security community.
- × IFTRIP coordinates and contributes to **international and cross-sectoral working groups** on a variety of topical issues, from cyber terrorism to nuclear pool coverage.
- × **Annual conference** provides a platform for the exchange of experience in mitigation and capacity building against economic loss resulting from terrorism:
 

- 2015: IFTRIP established in London	- 2021: Annual conference held virtually
- 2016: Annual conference in Canberra	- 2022: Annual conference held virtually
- 2017: Annual conference Paris	- 2023: Annual conference held in London (Pools only)
- 2018: Annual conference in Moscow	- <b>May 2024: Next annual conference in Washington</b>
- 2019: Annual conference in Brussels	

- × *Current Chair: ARPC (Australia); Vice Chair: TRIP (US); Secretariat: Pool Re (UK).*
- × **Expectation that US succeeds to Chair at the end of 2023.**
- × At the 2023 Pools meeting, **the US Treasury became a full Member of IFTRIP**, and the following areas were agreed as **focus areas going forward**:
  - a) *Growing the membership of IFTRIP by identifying additional Pools to invite to join the Forum*
  - b) *Thought leadership in the areas of:*
    - I. *The challenges presented by systemic cyber events*
    - II. *Promoting the benefits of Public/Private Partnerships to governments and the global (re)insurance industry*
    - III. *The impact of climate change on terrorism threat*
- × **July 2023 proposed collaboration with private sector partners:**
  - a) **Report on catastrophic cyber risk**
  - b) **Report on CBRN risk**



In 2023, Pool Re has worked with Oliver Wyman and UK industry cyber players to explore the state of the UK's cyber insurance market, and initiatives to increase the UK's overall resilience...

## Our learnings to date include:

### 1. Market growth:

- × *The global cyber insurance market has been one of the fastest-growing over the last decade, with premiums more than doubling since 2015.*
- × *The UK cyber insurance market has seen significant growth in recent years. **The global cyber insurance market was estimated to have reached ~\$12BN in 2022, of which the UK market represents ~\$660MM.***
- × ***Both the global and UK markets are expected to grow at more than 20% per annum to 2025, with the global market forecast to reach \$22BN by 2025, and the UK market to reach between £1.3BN and £1.5BN by 2027.***

### 2. Protection gap:

- × ***Annual economic losses from cyber incidents globally are estimated at over \$0.9trn.** There is no definitive figure for total cyber losses, as not all incidents are reported and quantified by businesses and national institutions*
- × ***Global claims paid annually by insurers: \$6bn** (extrapolated from USA loss ratios of 65%)*

### 3. Penetration & cyber-attacks:

- × ***5% of UK businesses have a specific cyber security insurance policy** and 38% have cyber security as part of a wider insurance policy.*
- × ***39% of all UK businesses reported a cyber breach or attack in 2022***

### 4. There are clear market failures preventing a narrowing of the protection gap for cyber insurance.

*We can distinguish between **demand side failures, which impact mostly SMEs, and supply side failures, which impact mostly large corporates:***

- × *Many SMEs have a low level of cyber awareness and consequently are not well prepared for cyber events when they occur – both in terms of **risk mitigation** and in terms of their **purchase of cyber insurance***
- × *Large corporates are **unable to obtain covers proportionate to the material threat** which cyber poses to their businesses*

***These market failures could lead to catastrophic damage to UK businesses and the economy in a systemic event.***

***We see a strong case for pre-emptive, public-private efforts to mitigate the risk.***



## We have formulated a set of recommendations for consideration for each of our potential initiatives – *focused on strengthening demand*

Potential Initiatives	Recommendations	How could HMG support?
<p><b>1</b> Raise awareness, Education and skill level on cyber risks &amp; best practices</p>	<ul style="list-style-type: none"> <li>• <b>Establish a cyber security education hub</b> providing businesses with educational material on cyber threats, mitigants and insurance options (e.g., guidance on mitigating malware and ransomware attacks, event response and recovery, etc.)</li> <li>• <b>Create a wide-reaching communications</b> strategy to promote cyber awareness and skills across UK businesses (esp. SMEs)</li> </ul>	<p><i>Encourage the insurance industry to provide input on cyber risk management for existing platforms, and collaborate on opportunities to achieve consistency of guidance provided to businesses. Magnify the reach of this guidance via various government touchpoints with businesses.</i></p>
<p><b>2</b> Support firms to take timely action via Early warning mechanisms</p>	<ul style="list-style-type: none"> <li>• Launch an <b>early warning system that proactively distributes information on emerging cyber threats</b> to businesses (focusing on SMEs) to enable them to take pre-emptive action to address vulnerabilities</li> <li>• This mechanism could be established as part of the above cyber security education hub or through the National Cyber Security Centre's (NCSC) existing activities</li> </ul>	
<p><b>3</b> Improve uptake &amp; raise standards of Cyber certifications</p>	<ul style="list-style-type: none"> <li>• Given the promising results to date, <b>continue enhancing the existing Cyber Essentials</b> scheme (e.g., encouraging a more aspirational posture around cyber culture, cyber event response and planning, etc.) and focus on <b>increasing uptake</b></li> <li>• Explore options for <b>insurers to better integrate cyber certifications into the underwriting process</b></li> </ul>	<p><i>Encourage collaboration between the insurance industry and the NCSC on enhancements to the Cyber Essentials scheme</i></p>
<p><b>4</b> Incentivise uptake of cyber insurance</p>	<ul style="list-style-type: none"> <li>• Explore the case for requiring <b>cyber insurance as part of corporate commitments for major government outsourcing contracts</b> (similar to the requirement for net zero commitments from businesses bidding for government contracts worth more than £5MM)</li> <li>• Explore the case and feasibility of encouraging the uptake of cyber insurance by firms via <b>sector regulation, corporate procurement, bank lending</b>, and other touchpoints</li> </ul>	<p><i>Review public procurement requirements, and explore the case for encouraging regulators, corporates, and banks to promote uptake of cyber risk mitigants and insurance</i></p>





## We have formulated a set of recommendations for consideration for each of our potential initiatives – *focused on strengthening supply*

Potential Initiatives	Recommendations	How could HMG support?
<p><b>5</b> Improve sharing of cyber data in the insurance industry</p>	<ul style="list-style-type: none"> <li>Encourage <b>increased sharing of aggregated data and insights by insurers to raise market-wide standards for risk modelling</b></li> <li><b>Create a central body for producing aggregate insights</b> from granular event data</li> <li>Collaborate across the industry and government to <b>quantify cyber catastrophe risks</b></li> </ul>	<p><i>Endorse the initiative, facilitate appropriate information sharing, and engage the insurance industry on government-led efforts to quantify cyber risk</i></p>
<p><b>6</b> Create a shared cyber event declaration and Classification mechanism</p>	<ul style="list-style-type: none"> <li><b>Create a size/scale-based event classification system</b> which will support insurers to draw boundaries between attritional and systemic losses and <b>provide a clear understanding of losses that can be covered in the commercial market.</b> The criteria should be as objective as possible, in order to support speed of determination and minimise uncertainty and disagreements</li> <li><b>Establish or identify an independent body to be responsible for event declaration and classification.</b> Although a mechanical outcome, an appointed body would still be required to officially declare the event; it is also essential that the body is able to identify and classify emerging risks quickly and reliably</li> </ul>	<p><i>Consider government's role with respect to declaring cyber events, in particular whether it should be responsible for officially declaring events in line with the framework (analogous to the role Treasury plays for Pool Re)</i></p>
<p><b>7</b> Establish a cyber catastrophe reinsurance scheme with a Government backstop</p>	<ul style="list-style-type: none"> <li>Consider a programme of work to design and set up a public-private cyber catastrophe reinsurance scheme with a government backstop. Solution design should holistically consider a broad set of dimensions, seeking to bolster the UK's resilience to systemic cyber events whilst enabling insurance innovation</li> <li>The different stakeholders that will need to be engaged in this work include: <ul style="list-style-type: none"> <li>– <b>Government:</b> Ensure the design aligns with objectives, notably on contingent liabilities and protecting public finances</li> <li>– <b>Insurance industry:</b> Ensure the scheme addresses private sector coverage gaps, and industry can effectively implement changes required to enable distribution, underwriting and claims payments</li> <li>– <b>Businesses:</b> Understand how the design can impact willingness to adopt risk mitigants and purchase cyber insurance</li> </ul> </li> <li>A clear definition of what is covered and how this is determined will be pivotal to the establishment of a cyber catastrophe reinsurance scheme, and as such initiative 6 is a requirement for this scheme</li> <li>This is not a completely novel initiative as it <b>builds on previous successful government interventions on hard to insure risks</b>, notably Pool Re for terrorism (with a government backstop) and Flood Re for flood</li> </ul>	<p><i>Support with the design of the scheme and agree to providing the backstop</i></p>



# Questions