



CENTRE FOR
CYBERSECURITY
BELGIUM



Cyber Fundamentals

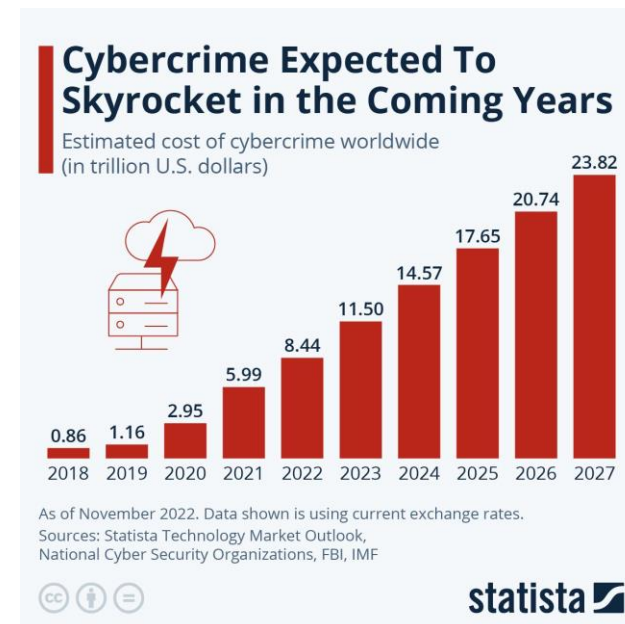
A tool to help closing the Cyber Insurance Protection Gap

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister



Drivers for the Cyber risk protection gap

Cybercrime



Cyberinequity

Cyber resilience:



Companies holding cyber insurance policy:
-24% compared to 2022

In collaboration
with Accenture



Global Cybersecurity Outlook 2024

INSIGHT REPORT
JANUARY 2024

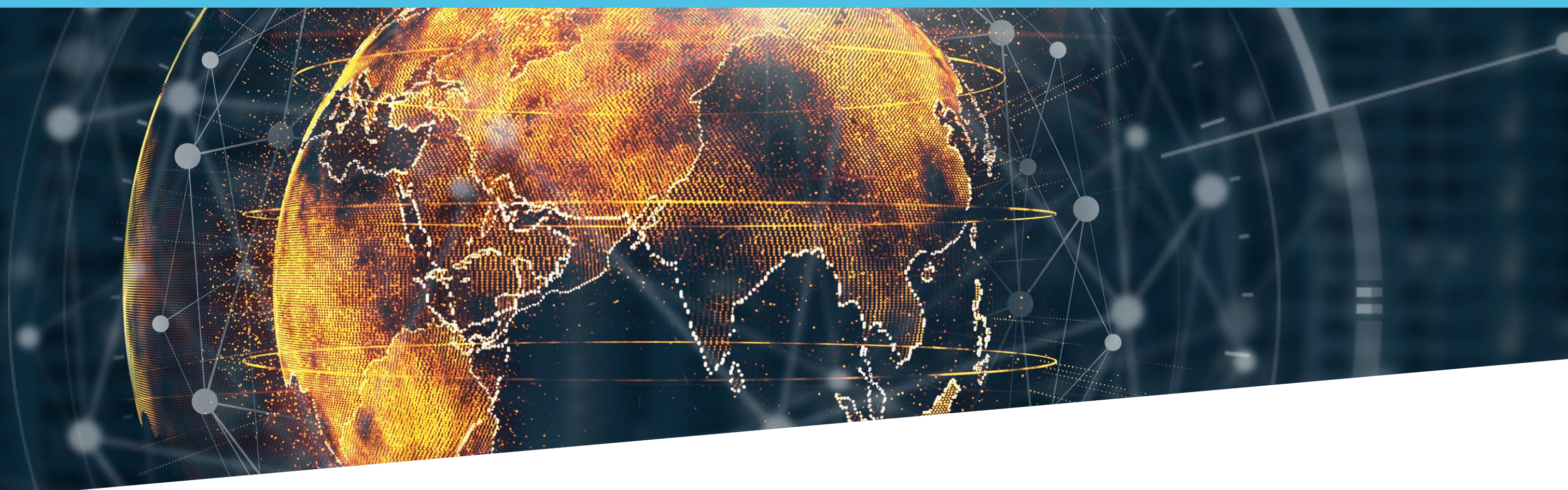
Key elements for solutions:

- Fit for use (large companies /SME's)
- Systemic solution
- Risk-appropriate, affordable
- Public-private cooperation



CENTRE FOR
CYBERSECURITY
BELGIUM

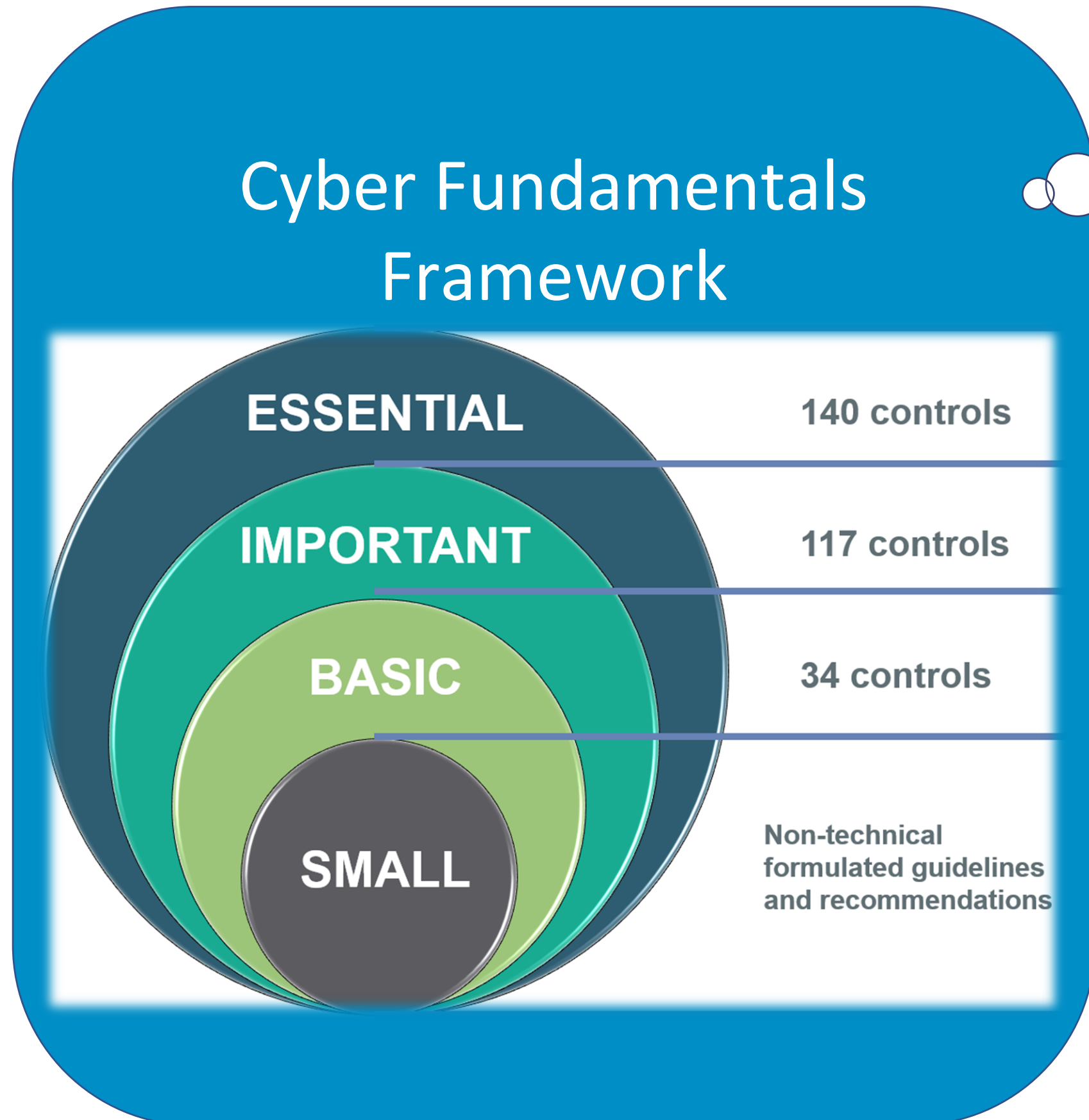
Centre for Cybersecurity Belgium
Under the authority of the Prime Minister



● Cyber Fundamentals

Let's approach cybersecurity as any other security/safety domain

Fit for use & effective



ESSENTIAL: 100 % Attack countered ✓

IMPORTANT: 94 % Attacks countered ✓

BASIC: 82 % Attacks countered ✓

CERT attack profiles (retrofit of successful attacks)

● Systemic solution

Private and public entities:

- Regulatory (NIS2) presumption of compliance
- Supply Chain cybersecurity assurance
- Use to demonstrate the entities resilience to banks, insurance companies
- Voluntary use

Use Certification under accreditation: Cost effectiveness



Accredited once,
Accepted everywhere.

Risk appropriate

Through the assurance levels based on **cyber risk**

Risk assessment tool to determine the assurance level

Category	Weight	Threat Actor Type	Common skills			Advanced skills			Political Goals		Financial Goals		Score	CyFun Level
Cyber Attack Category	Global or Targeted	Impact	Prof	Mid Level	Adv	Mid/Adv	Prof	Mid Level	Prof	Mid Level	Adv	Mid/Adv		
Subsage/Deception (DDoS,...)	2	High	Low	0	Low	0	Med	10	Med	10	High	40		
Information theft (espionage,...)	2	High	Low	0	Low	0	Low	0	High	40	High	40		
Crime (ransomware,...)	1	High	Low	0	Low	0	Low	0	High	10	Low	0		
Malware (subversion, defacement,...)	1	Med	Low	0	Med	2,5	Low	0	Low	0	Med	2,5		
Disinformation (political influencing,...)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
Total													295	ESSENTIAL

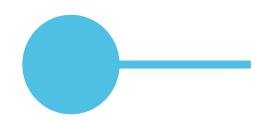
Focus on real **cyber attacks**

➔ **Key Measures**

Conformity thresholds considering the maturity level.

Through **maturity level verification**

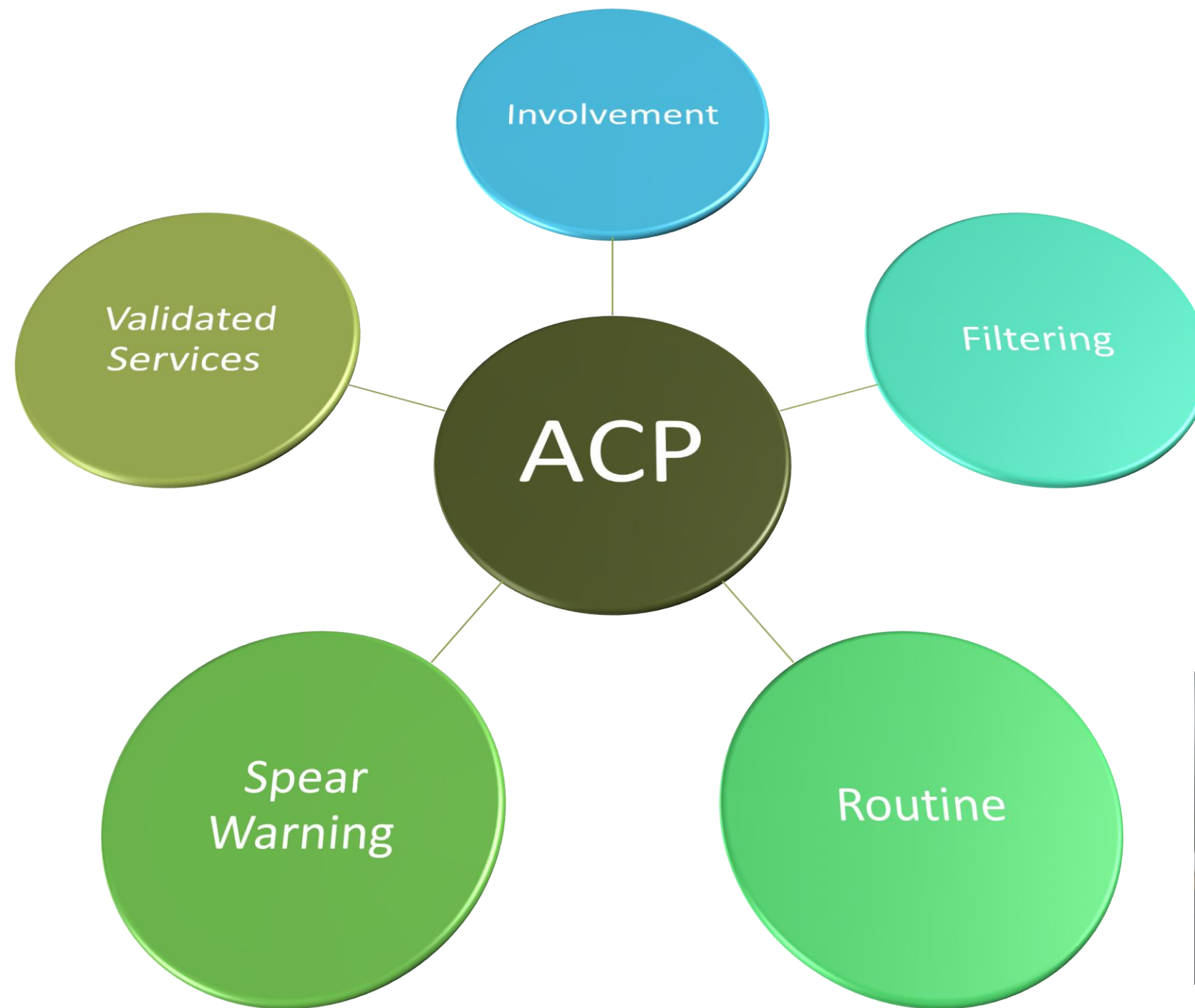
	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity	> 3/5		> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5



Partnership: Active Cyber Protection



suspicious@safeonweb.be



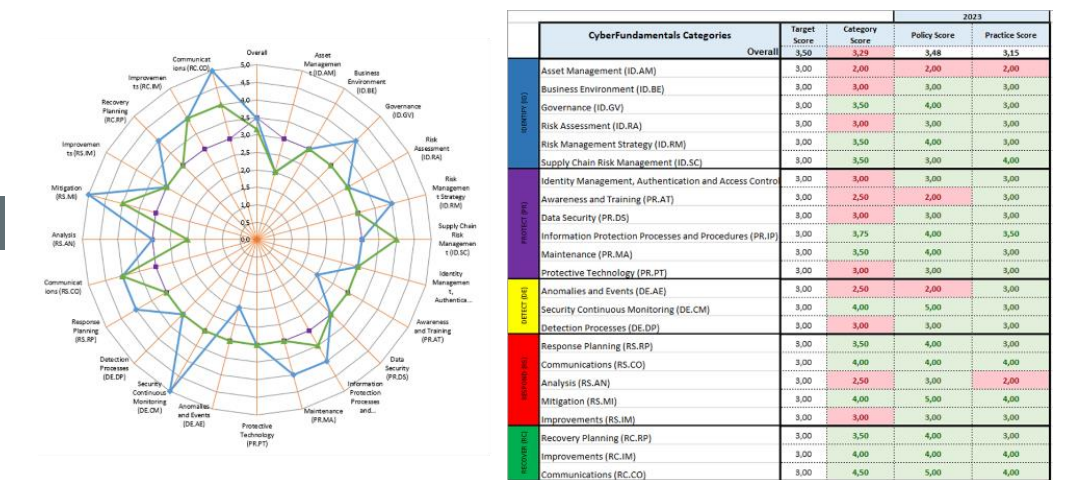
Partnership: CyFun toolbox



CyFun Selection tool
(Risk Assessment)

Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targeted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/Disruption (DDoS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	285	ESSENTIAL

CyFun Self-Assessment tool



CyberFundamentals
Conformity Assessment
Scheme for CAB's



CyberFundamentals
Framework mapping

CyberFundamentals Toolbox is **publicly available** → www.cyfun.eu



Cyber Fundamentals Summary



Systemic solution

*Multi-standards framework, international references
Based on accreditation (competence & independence)*

**Accredited once,
Accepted everywhere.**

Risk-appropriate

Assurance level approach – Key Measures – Maturity to demonstrate resilience

Affordable, Fit for use (micro entities – SME's - large companies)

Voluntary: assurance level approach

Legal obligation: upgrading according to public interest (NIS2)

Limited conformity assessment cost (basic-important: appr 1.000 Euro/yr)

Public-private cooperation

Scheme maintenance with stakeholders

Part of the CCB Active Cyber Protection program



CENTRE FOR
CYBERSECURITY
BELGIUM



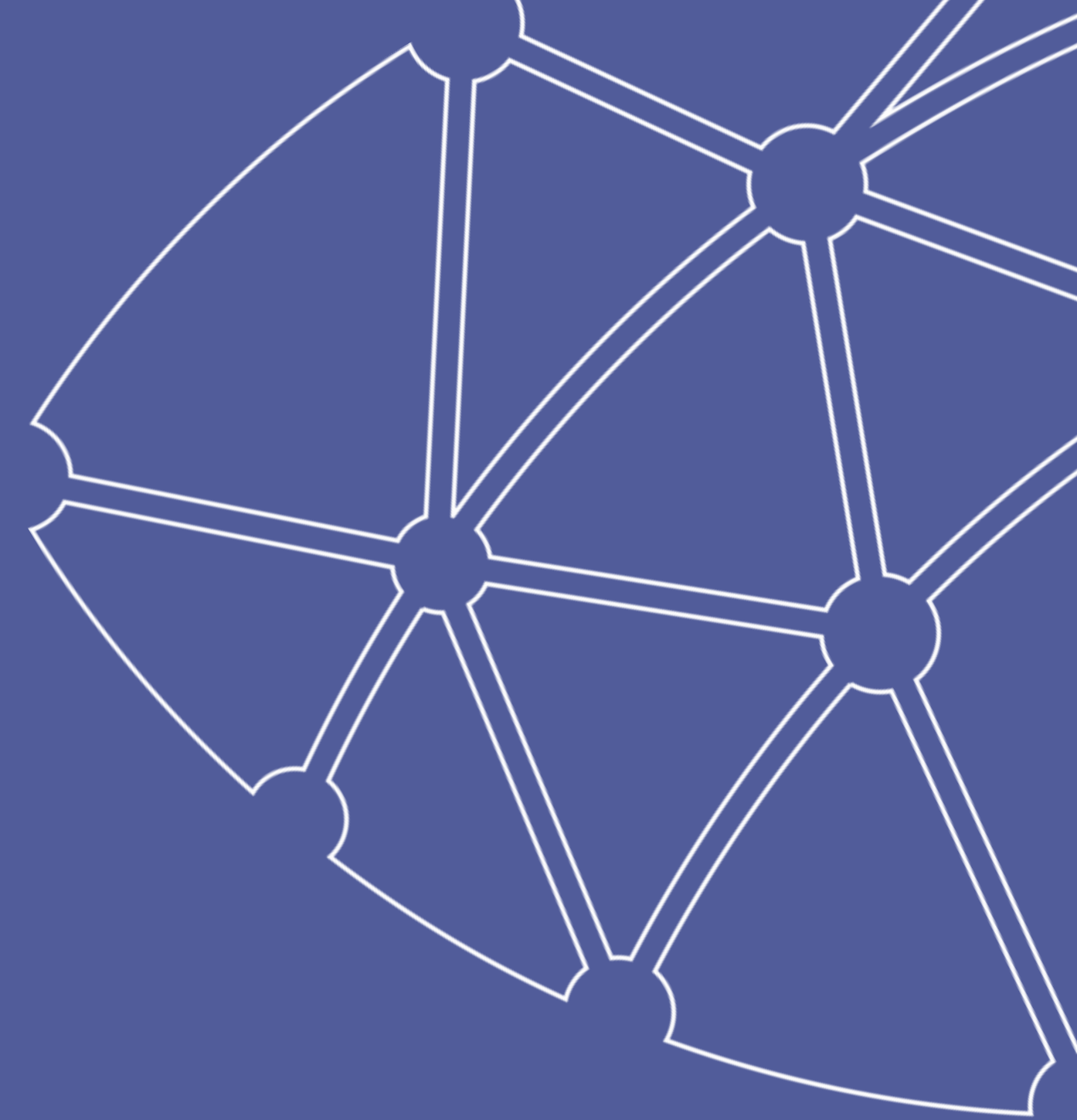
Johan Klykens

Director Cybersecurity Certification Authority

Centre for Cybersecurity Belgium

Under the authority of the Prime Minister

certification@ccb.belgium.be

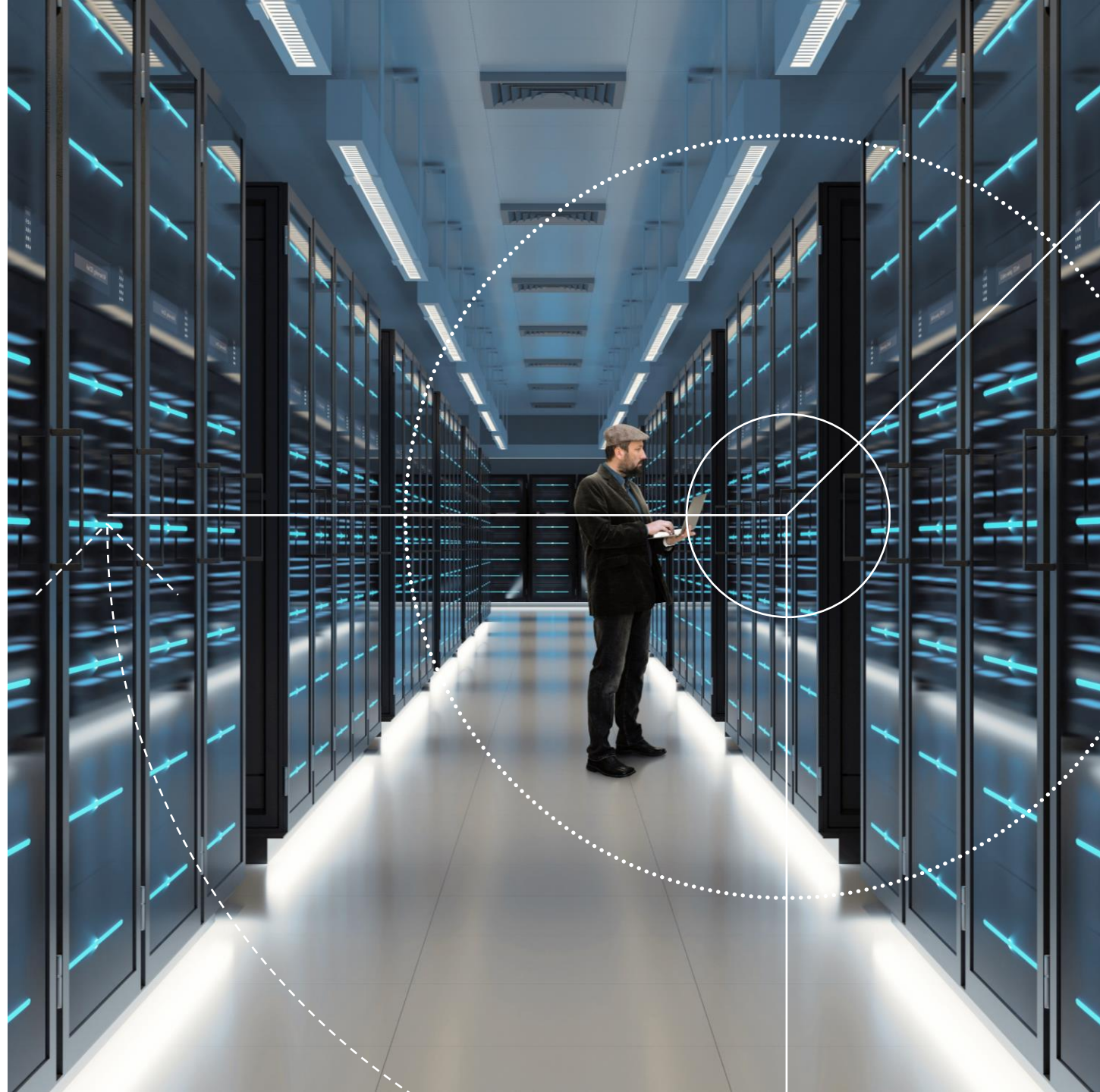




Insuring Cyber Risks

Insurance solutions to address the cyber risk
protection gap

Allianz Commercial Brussels
Cyber | Elisabeth Van Rompay February 26, 2024



Content / topics

1 Introduction

3 Cyber Risk Protection Gap

2 Cyber Risk Landscape

4 Insurance Solutions to address the gap

Providing peace of mind through Allianz's financial stability

 Allianz Commercial global business 2022 (EUR)

> €19bn
Gross premium



Allianz Group key figures 2022 (EUR)



Allianz Commercial remains **one of the highest rated** global Property & Casualty insurers.

Allianz SE Ratings*	S&P	Moody's	A.M. Best
Insurer financial strengths rating	AA stable outlook (affirmed 06/26/2023)	Ao2 stable outlook (upgraded 09/26/2023)	A+ stable outlook (affirmed 03/08/2023)

*Includes ratings for securities issued by Allianz Finance II B.V. and Allianz Finance Corporation.

Our regional set-up

Asia: China, Hong Kong, India, Indonesia, Japan, Malaysia, Sri Lanka, Singapore, South Korea, Laos, Thailand

Australia: Australia

Benelux & Nordics: Belgium, Netherlands, and Nordic countries

Central & Eastern Europe: Austria, Poland, Hungary Czech Republic, Slovakia, Bulgaria, Romania, Croatia, Slovenia & Ukraine.

France: France, South Africa

Germany & Switzerland: Germany & Switzerland, Liechtenstein

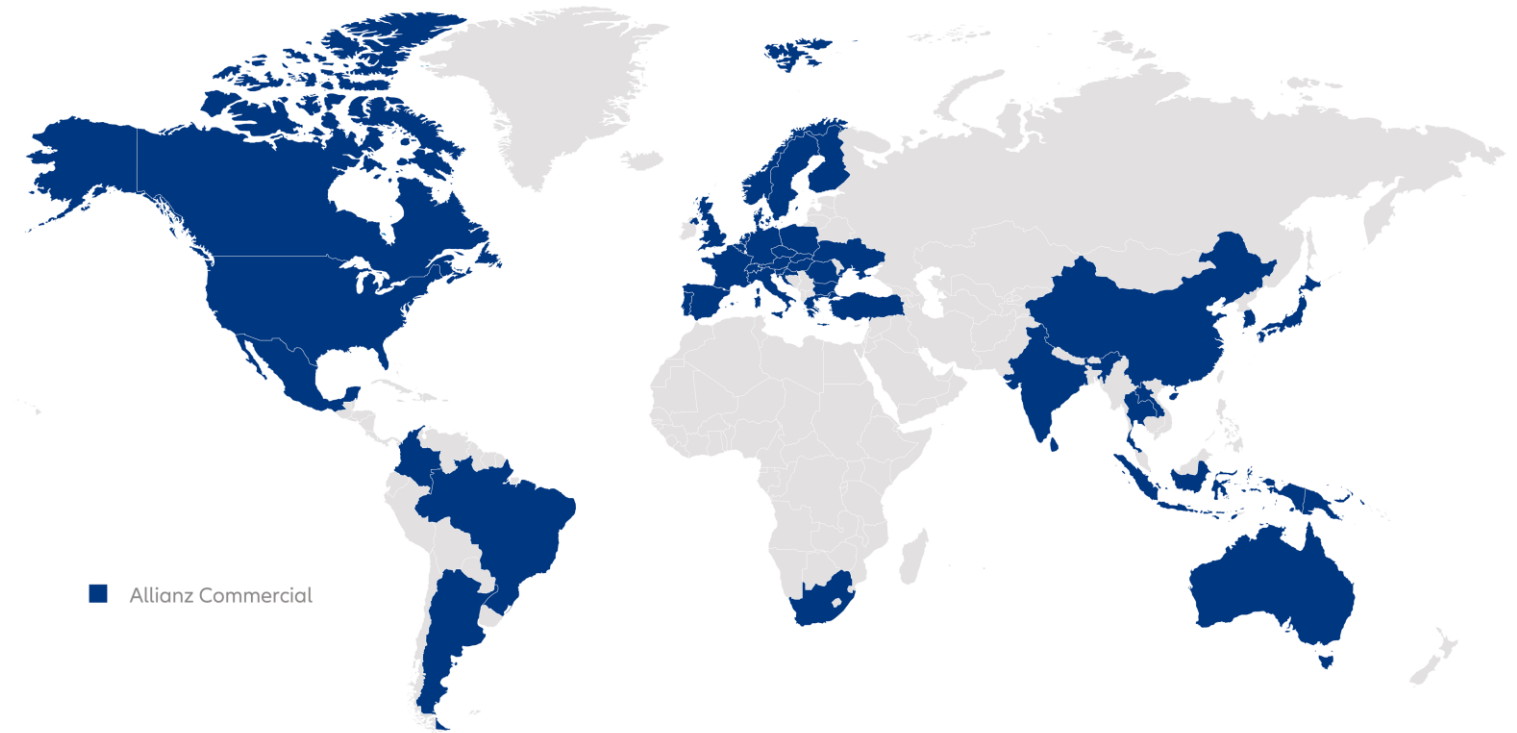
Iberia: Spain & Portugal

Latin America: Argentina, Brazil, Colombia, Mexico

North America: Bermuda, Canada, USA

Southern Europe: Greece, Italy, Turkey

United Kingdom: United Kingdom





Cyber at a glance

What you can expect from across Allianz Commercial

Claims experts: We are there when you need us most. Our 600+ global experts have 10+ years average claims adjusting experience and handle 125,000+ claims per year. Within the Claims team, Allianz Commercial has value driving experience handling claims for many years with access to top tier partners for incident response and other immediate measures. Allianz Commercial makes average annual claims payments of over €4 billion.

Multinational specialists: 900 dedicated multinational underwriters and 1,500+ multinational service experts are there to build your bespoke global programs.

Dedicated Risk Consultants: Combining industry-knowledge with an average of 10 years of experience, our 250+ global risk consultants from industry backgrounds understand the key risks and challenges you face.

Alternative Risk Transfer: We specialize in helping clients mitigate their most complex, broad-ranging risks by leveraging our expertise in alternative risk transfer and the global capabilities of the Allianz Group.

Allianz Commercial will consider every risk on its own merit. Capacity and Coverage offered to individual clients subject to hazard, Nat Cat exposure, grading, terms & conditions.

Actively growing

- Selective growth appetite across virtually all industries, but with focus on per-account risk quality
- Preference for excess positions.

Coverage

- Primary stand-alone cyber
- Excess cyber
- Technology PI
- Media PI

Capacity

Up to €10m
Up to €10/15m
Up to €15m
Up to €15m

Restricted

- Cryptocurrency
- Payment processors
- Pay day loan companies
- Air traffic controllers
- Adult entertainment
- Online gambling
- Central reserve banks

Contact

Scott Sayce
Global Head of Cyber
+44 203 451 3414
scott.sayce@allianz.com

Marek Stanislawski
Global Cyber Underwriting Lead
+46 8 5050 2106
marek.stanislawski1@allianz.com



Why choose us?



Market leading capacity to handle the largest risks



Network to service clients in 200+ countries and territories



Financial strength backed by strong ratings: AA Standard & Poor's A+ A.M. Best



Manager of 2,800+ global programs, spanning 21,000+ local policies, via our Multinational capabilities



4,000+ employees in 50 offices worldwide



We insure over three quarters of the Fortune 500®



ESG integrated into our underwriting via industry-leading rules and tools



Allianz Group is committed to decarbonize its insurance and investment portfolios by 2050 in close partnership with clients



Part of the wider Allianz Group, one of the leading integrated financial services providers worldwide

Cyber Risk Landscape

Cyber threats and impact of cyber incidents on business





Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)



Business interruption

(incl. supply chain disruption)



Natural catastrophes

(e.g., storm, flood, earthquake, wildfire, extreme weather events)



Changes in legislation and regulation¹

(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)



Macroeconomic developments²

(e.g., inflation, deflation, monetary policies, austerity programs)



Fire, explosion



Climate change

(e.g., physical, operational, and financial risks as a result of global warming)



Political risks and violence

(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)



Market developments

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)



Shortage of skilled workforce

- **Cyber Risks** ranked as top concern across all company sizes
- **Ransomware** on the rise.
- **Data** privacy claims
- **Critical** infrastructure
- **AI** may power ransomware attacks
- **Shortage** of global talent in cybersecurity .

Key

- Risk higher than in 2023
- ↓ Risk lower than in 2023
- No change from 2023
- (5%) 2023 risk ranking %

- ¹ Changes in legislation and regulation ranks higher than macroeconomic developments based on the actual number of responses
- ² Macroeconomic developments ranks higher than fire, explosion based on the actual number of responses

Source: Allianz Commercial

Figures represent how often a risk was selected as a percentage of all survey responses Respondents: 3,069. Figures don't add up to 100% as up to three risks could be selected

NEW New entry in the top 10 risks

The increasing sweet spot for Cybercriminals SMEs



Cybercriminals are turning to SMEs

Increase in cyber attacks and data breaches

Cyber threats increase

Due to shift to remote work and outsourcing

Hard recovery

From business interruption

Cyber Risk Protection Gap

The discrepancy between potential losses incurred due to cyber threats and the level of insurance protection in place



Cyber Risk Protection Gap

1. **Underestimation** of cyber risks
2. **Lack** of cyber risk awareness
3. **Inadequate** risk assessment and management
4. **Evolving** cyber threats
5. **Complexity** of cyber incidents
6. **Historical data** is limited
7. **Quantification** of risk remains difficult



Insurance Solutions

Addressing the cyber risk gap through insurance solutions is crucial in today's digital landscape, where businesses face ever evolving threats



Insurance Solutions

Customers' perspective



Tailored Coverage

Tailored policies ensure that businesses have the right protection in place to address their vulnerabilities



Risk Assessment

By identifying businesses and understand their cyber risks , insurers enable organizations to implement proactive measures to reduce vulnerabilities, e.g. Allianz CyberSafe Scan

<https://allianz.be/nl/ondernemers/cyberscan.html>



Incident Response assistance

Insurers work with forensic experts and legal firms to navigate the aftermath of a cyber incident and to facilitate a swift recovery



Financial Protection

Adequate financial support helps business manage the consequences of a cyber incident



Continuous Coverage Adaption

Insurance solutions can adapt to emerging risks



Education

By empowering organizations with knowledge, insurers contribute to closing the gap in managing risks effectively

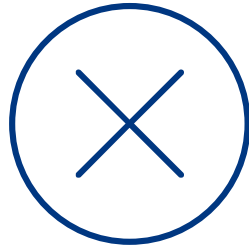
Insurance Solutions

Insurers' perspective



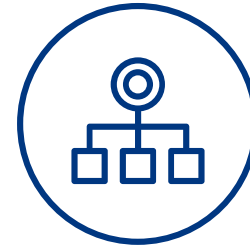
Diversification of portfolios

- Diverse range of business and industries
- Mitigating risks
- To reduce impact of catastrophic event



Setting Policy Limits and Deductibles

- Deductibles are based on unique profile of policyholder
- Appropriate limits to control potential exposure
- Deductibles to share the financial burden of smaller incidents with policyholders
- Co-insurance with policyholders as an incentive to improve their risk quality



Risk Pooling and Reinsurance

- Insurers utilize reinsurance mechanisms to spread the financial impact
- Transfer of portion of risk
- Manage financial implications of a catastrophic cyber event

Closing Cyber Risk Gap

Closing the gap

By offering tailored coverage, supporting risk management efforts, providing financial protection, insurance can close the gap

Business that leverage comprehensive cyber insurance policies can significantly enhance their resilience against cyber threats and navigate the complex challenges posed by the digital environment

Thank you!





Closing the Insurance Protection Gap

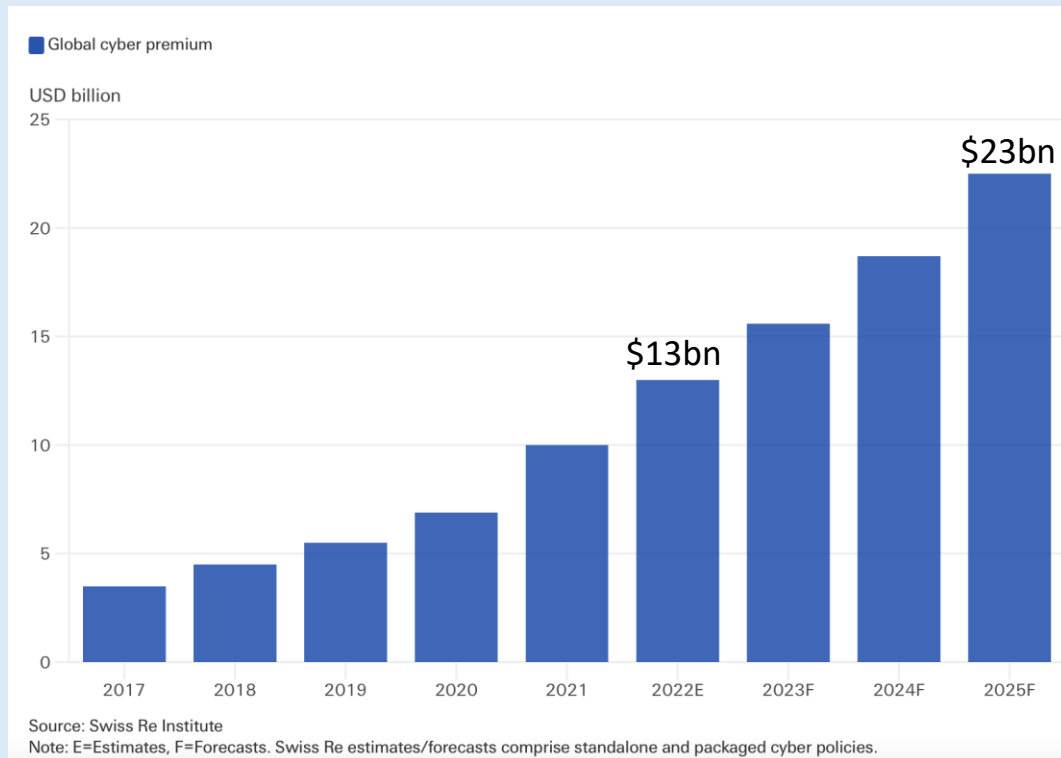
*Cyber risk dynamics and
views from an international perspective*



Cyber insurance in numbers

A very young insurance market with the first cyber policy in 1999

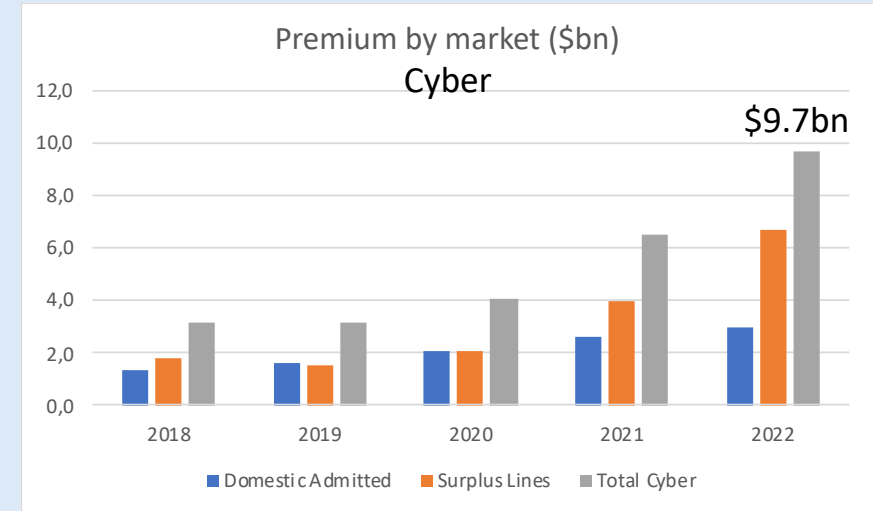
The vast majority of the premium and the available data come from the US
In part segmented, in other aspects, existence of a federal consolidated view



Focus on the US

Role of the Surplus Lines market, rate increases and losses ratios

Bn USD	2018	2019	2020	2021	2022
Domestic Admitted	1,4	1,6	2,0	2,6	3,0
Surplus Lines (Domestic & Aliens)	1,8	1,5	2,0	3,9	6,7
Total Cyber	3,1	3,1	4,1	6,5	9,7
% Surplus Lines	57%	48%	50%	60%	69%
*Of which Alien Surplus Lines	1,1	0,9	1,3	1,7	2,4
Total domestic	2,0	2,3	2,8	4,8	7,2
Total domestic loss ratio (first 20 Cies)				66%	45%



More than 50% reinsured

Limited number of increase in policies (excluding Aliens)

	2018	2019	2020	2021	2022
Total Policies in Force	2,996,820	3,314,005	4,019,428	3,747,986	3,913,123
% Change - PIF	15.1%	10.6%	21.3%	-6.8%	4.4%

=> Significant rate increases

Surplus lines (all risks – “freedom of rate & form”) represent:

- 22% of US commercial lines (\$515bn) vs. 11% in 2002 and 13% in 2012
- 11% of total P&C lines (\$881bn) vs. 6% in 2002 and 7% in 2012



*Source: NAIC's report on the Cybersecurity Insurance Market – Nov 2023

A strongly dynamically evolving risk

Cyber: increased maturity but still in *infancy*

2023 marks a different development stage in the market

But the protection gap is still massive

With: **3tn** losses in 2015, **8tn** losses expected in 2023, **11tn** in 2025*

Signs of increased maturity

Attack vectors in Cyber crime

- Cyber attacks
- System errors
- Human errors
- Physical attacks
- Supply chain attacks

Investments in

- Prevention
- Quantification
- Protection
- Detection
- Crisis management
- Incident response/Recovery

Many actions from most stakeholders

Underwriters and reinsurers: better understanding, improved questionnaires, underwriting tool adaptation: deductibles, limits, exclusions such as warfare, losses stemming from key players in the IT supply chain, attacks on critical infrastructure that lead to wide range cyber loss

Proven recipes

- Patch external vulnerabilities
- Control remote access
- Deploy multi factor authentication
- Use offline backups (making sure they work)
- Migrate email to the cloud vs. on premises and constant training on the threat of phishing
- Cyber insurance and ransomware risk

Innovation

Cyber risk management vendors (incl. InsurTech): support in cyber loss quantification, EDR (Endpoint Detection Response) monitors your network for signs of suspicious activity and provides the tools to promptly identify and respond to data breaches

Regulators: cyber event reporting (SEC), cyber incident data repository...

Innovation

Governments: alerts, investments in tech, High Impact Operations, increased collaboration

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

Feb 20, 2024



But still a long way ahead

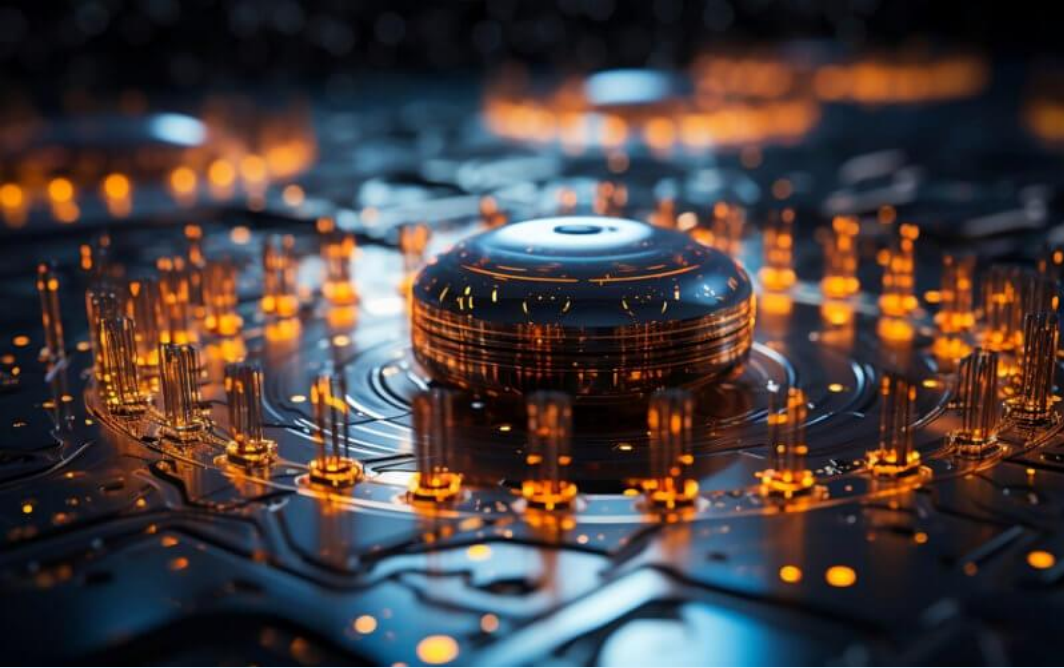
- Barely 20 years of observations
 - Improved data on occurrence
 - Struggling on quantification
 - Pricing still based on scenario modelling
 - Low penetration rate limiting data availability and mutualization
 - Systemicity
 - No coverage for the “Big One”
- Supporting parametrics

What lies ahead of us?/ What are the latest trends?

The double edge sword of progress







A new 're' encryption programmes era?

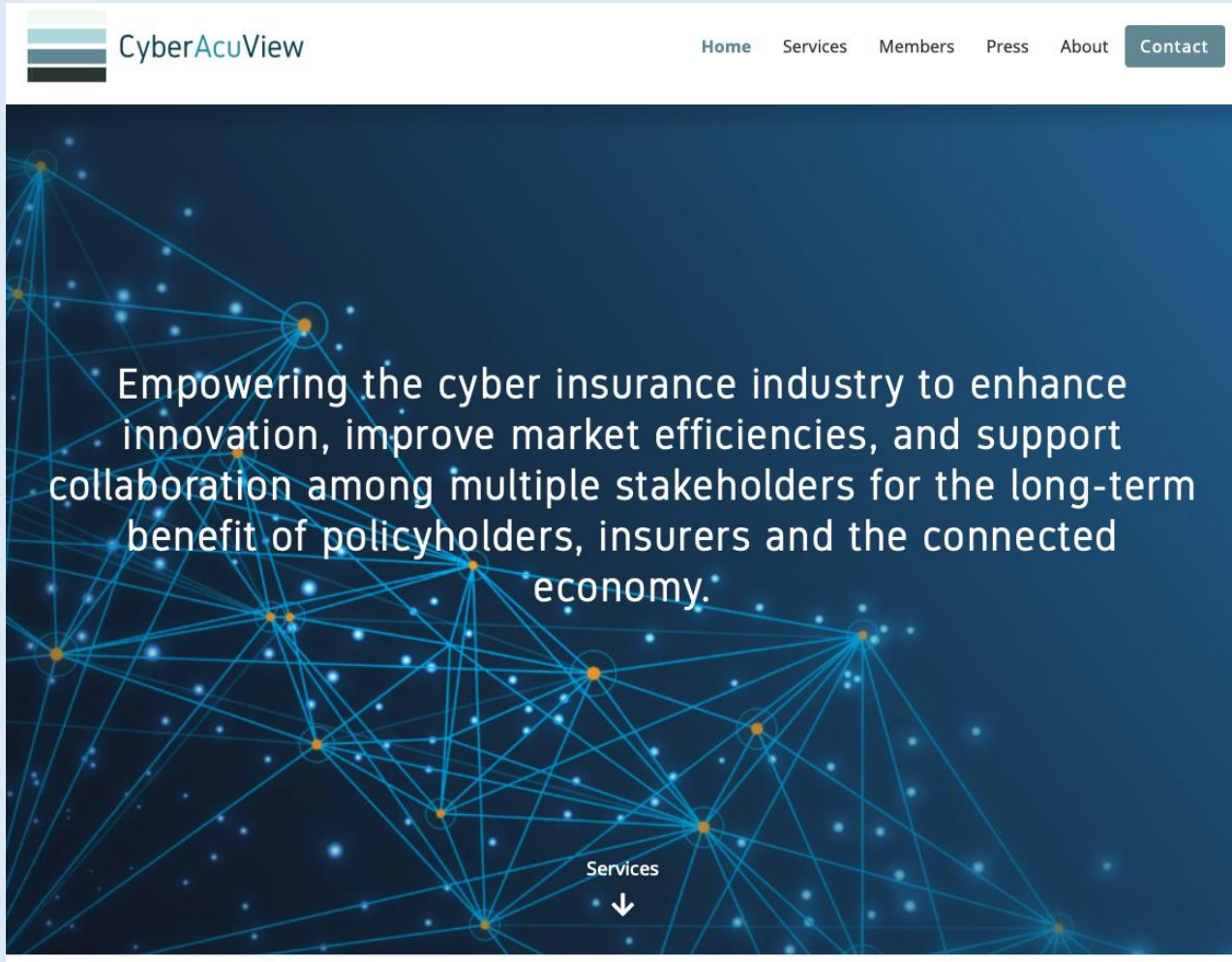
Quantum computing

Break existing encryptions?



Data

Eventually, some did it: data sharing and collaboration



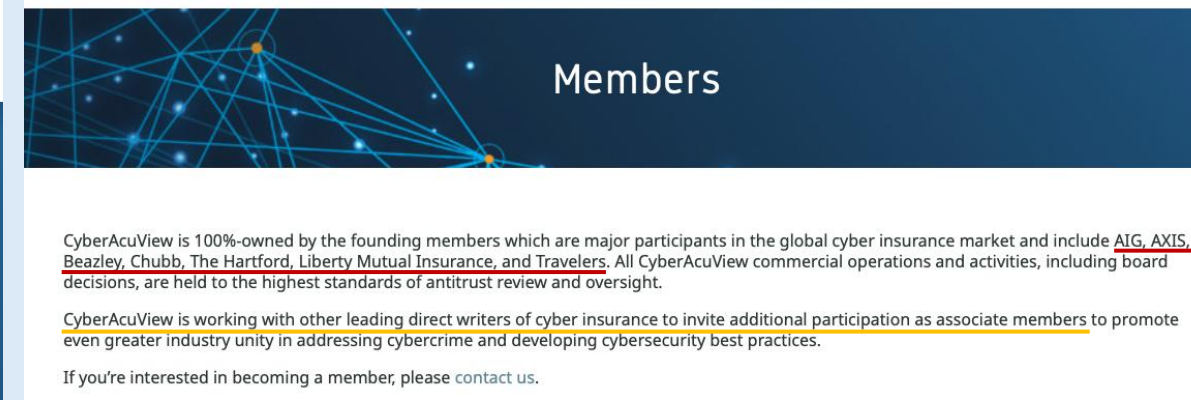
The image shows the top portion of the CyberAcuView website. At the top left is the CyberAcuView logo, consisting of three horizontal bars in shades of blue and green. To the right of the logo is the navigation menu with links for Home, Services, Members, Press, About, and a Contact button. The main content area features a dark blue background with a network of glowing blue nodes and lines. Overlaid on this background is the text: "Empowering the cyber insurance industry to enhance innovation, improve market efficiencies, and support collaboration among multiple stakeholders for the long-term benefit of policyholders, insurers and the connected economy." At the bottom right of this section, the word "Services" is written with a downward-pointing arrow.

CyberAcuView

Home Services Members Press About Contact

Empowering the cyber insurance industry to enhance innovation, improve market efficiencies, and support collaboration among multiple stakeholders for the long-term benefit of policyholders, insurers and the connected economy.

Services ↓



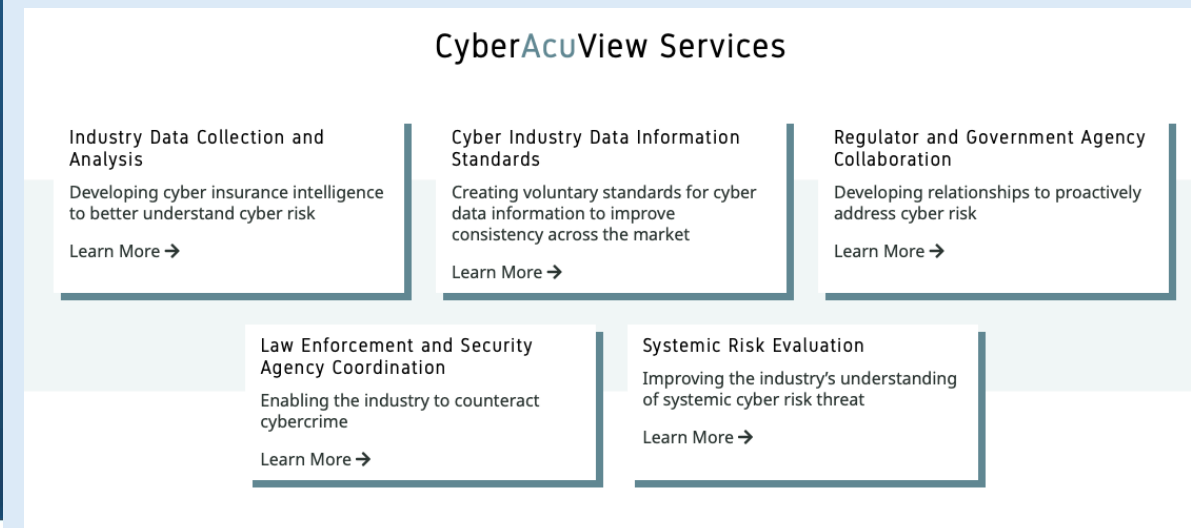
The image shows the "Members" section of the CyberAcuView website. It has a dark blue header with the word "Members" in white. Below the header is a paragraph of text: "CyberAcuView is 100%-owned by the founding members which are major participants in the global cyber insurance market and include AIG, AXIS, Beazley, Chubb, The Hartford, Liberty Mutual Insurance, and Travelers. All CyberAcuView commercial operations and activities, including board decisions, are held to the highest standards of antitrust review and oversight." This is followed by another paragraph: "CyberAcuView is working with other leading direct writers of cyber insurance to invite additional participation as associate members to promote even greater industry unity in addressing cybercrime and developing cybersecurity best practices." The final sentence reads: "If you're interested in becoming a member, please contact us."

Members

CyberAcuView is 100%-owned by the founding members which are major participants in the global cyber insurance market and include AIG, AXIS, Beazley, Chubb, The Hartford, Liberty Mutual Insurance, and Travelers. All CyberAcuView commercial operations and activities, including board decisions, are held to the highest standards of antitrust review and oversight.

CyberAcuView is working with other leading direct writers of cyber insurance to invite additional participation as associate members to promote even greater industry unity in addressing cybercrime and developing cybersecurity best practices.

If you're interested in becoming a member, please contact us.



The image shows the "CyberAcuView Services" section of the website. It features a light blue header with the title "CyberAcuView Services". Below the header are five service cards, each with a title, a brief description, and a "Learn More" link with a right-pointing arrow.

CyberAcuView Services

- Industry Data Collection and Analysis**
Developing cyber insurance intelligence to better understand cyber risk
Learn More →
- Cyber Industry Data Information Standards**
Creating voluntary standards for cyber data information to improve consistency across the market
Learn More →
- Regulator and Government Agency Collaboration**
Developing relationships to proactively address cyber risk
Learn More →
- Law Enforcement and Security Agency Coordination**
Enabling the industry to counteract cybercrime
Learn More →
- Systemic Risk Evaluation**
Improving the industry's understanding of systemic cyber risk threat
Learn More →

PERILS and CyberAcuView US Cyber Industry Loss Index gains early traction with use in ILS and ILW transactions

Zurich (Switzerland) and Lakewood Ranch (Florida, USA), 12 February 2024 – PERILS, the independent Swiss-based organisation providing industry-wide catastrophe insurance data, and CyberAcuView, the independent US-based organisation set-up by leading cyber insurers for the benefit of the cyber insurance market, have today announced the use of their US Cyber Industry Loss Index in the first cyber insurance risk transactions.

The US Cyber Industry Loss Index, launched in September 2023, reports affirmative US primary cyber market losses resulting from systemic cyber incidents affecting more than one insurer and policyholder for events exceeding USD 500 million industry loss. As the risk of systemic cyber losses continues to grow, the index is designed to provide an independent cyber industry loss estimate arising from US systemic loss events for use in alternative capital transactions.

The index is used to produce an index value to determine the payouts of the protection under Insurance Linked Securities (ILS) and Industry Loss Warranty (ILW) contracts. The cyber industry losses are based upon loss data collected from US cyber insurers by CyberAcuView with subsequent industry-level calculations jointly signed-off by CyberAcuView and PERILS. All data services are conducted under strict antitrust supervision.

Since its launch in September, PERILS and CyberAcuView have actively engaged with major stakeholders in the industry to raise awareness and acceptance of the loss index. This extensive work culminated in the first cyber 144a ILS being placed using an industry loss trigger (sponsored by Swiss Re) as well as an ILW reinsurance contract which was completed using the index.



**Feb 12, 2024
Press Release**

PERILS and CyberAcuView announce the first two transactions using the US Cyber Industry Loss Index.

Commenting on the announcement, Christoph Oehy, CEO of PERILS, said: “We are very pleased our loss index has been used in transactions so soon after launch. In recent months, we have engaged closely with the market, while risk protection sellers and buyers have undertaken extensive due diligence on the index. It is clearly a very positive development to see its acceptance by the industry as demonstrated by these placements. As the risk of systemic cyber loss events grows, it is increasingly important to ensure sustainable capacity is available to support the US cyber sector. We believe our loss index can play an important role in enabling the expansion of the cyber-ILS and ILW markets by providing independent systemic loss estimates.”

Mark Camillo, Chief Executive of CyberAcuView, added: “We are very excited by the level of interest in the index since launch. CyberAcuView’s original mission was to make available reliable US cyber insurance industry data which can be used to better understand cyber risk. In recent months, there has been various discussions with industry players regarding key industry topics such as event definitions and war exclusions. I personally found this engagement very positive and it highlights the need for the industry to cooperate closely to expand capacity. It also became evident during this process there is an increasing interest in cyber risk by many protection sellers which we hope presents opportunities for the index to be used in future transactions.”

Nick Meuli, Head Capacity and Platform Management at Swiss Re commented, “We are pleased to have worked with PERILS and CyberAcuView on the world’s first 144a Cyber index cat bond. Independent indices are an important aspect in bringing more alternative capital into the market, something we believe is key for the further growth of the cyber market.”

ILS & the like

Innovation

Towards a PPP for Cyber as part of the US National Cybersecurity strategy?

*U.S. Treasury has reached a “tentative conclusion” that **a potential federal cyber insurance backstop** will be focused on catastrophic cyber risk.*

*“We will remain focused on the policy options for **some kind of public-private sector collaboration or other federal response** that cabins catastrophic risk alongside the existing and expanding commercial cyber insurance market,” said Graham Steele, assistant secretary for financial institutions at the Treasury Department.*

The challenge, acknowledged Steele, is the fact that unlike natural catastrophes, there is limited historical data on catastrophic cyber losses in order to model projections. Plus, potential catastrophic losses can transcend geographic boundaries as well as industries and an organization’s size.

“Waiting until after a catastrophic cyber incident occurs is sub-optimal for everyone, including private sector firms, the government that bears the responsibility for stabilizing the economy, and ultimately the taxpayers,” Steele said.

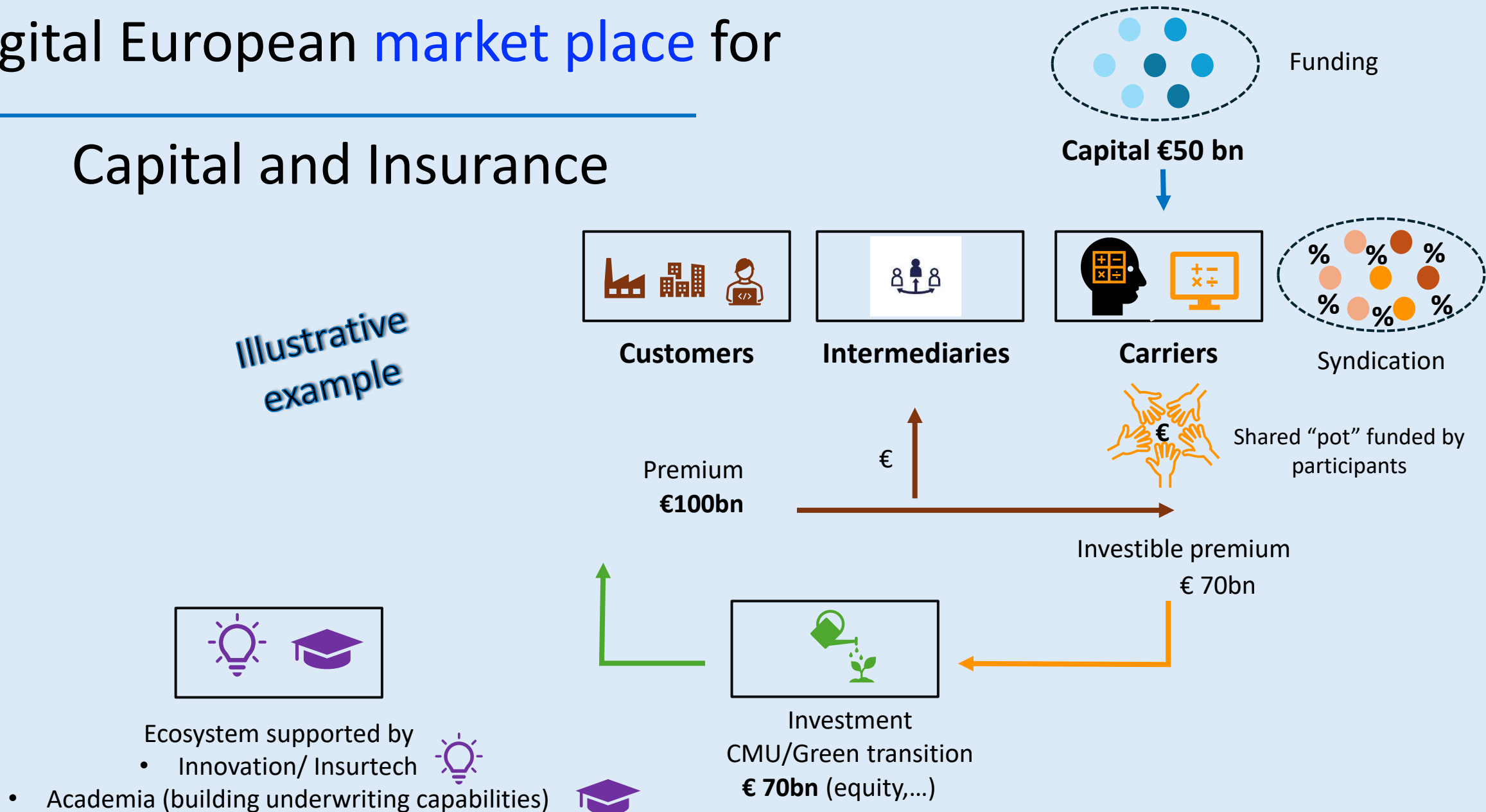
What about us?



A digital European market place for

Capital and Insurance

Illustrative example



The way forward

Increase the private sector cover via a European market place

