Hedge Funds News, January 2025

The "as-a-Service" (aaS) model has revolutionized how businesses deliver and monetize products and services by shifting from traditional ownership to subscription-based access.

Initially popularized in the tech industry (Software-as-a-Service - SaaS), the model has expanded across sectors, offering new ways to sell products and services in a scalable, customer-centric manner.

There are several benefits. Customers access the service or product whenever needed. Services can scale up or down based on customer requirements. Also, the provider maintains, updates, and supports the service.

Unfortunately, cybercriminals have also adopted the "as-a-Service" business model to scale their operations and monetize their skills. This approach mirrors legitimate subscription-based services, allowing criminals to offer tools, infrastructure, and expertise on a pay-as-you-go or subscription basis. The Cybercrime-as-a-Service (CaaS) economy has become a multi-billion-dollar industry, fueling the global rise in cybercrime.

In Cybercrime-as-a-Service, tools, platforms, and services for conducting cyberattacks are sold or rented to others in exchange for payment. It enables even non-technical individuals to execute sophisticated cyberattacks by outsourcing expertise.

In Malware-as-a-Service, malware developers create and sell malicious software to others. In Ransomware-as-a-Service, platforms offer ready to use ransomware kits. In Phishing-as-a-Service, platforms provide phishing kits, email templates, and hosting services, including pre-built phishing pages resembling legitimate websites, and email

delivery infrastructure to evade spam filters.

In DDoS-as-a-Service, cybercriminals offer botnets to conduct Distributed Denial-of-Service (DDoS) attacks. Pricing is based on attack duration and scale.

In Access-as-a-Service, cybercriminals offer access to compromised systems, networks, or credentials. It includes access to corporate networks, and admin accounts. Often includes information from high-profile breaches.

In Spyware-as-a-Service, cybercriminals offer spyware tools for monitoring devices, stealing data, or tracking individuals. They offer tools disguised as legitimate apps, used in corporate espionage.

Hedge funds, as custodians of highly sensitive financial data, trading strategies, and substantial assets, are prime targets for cybercriminals. Access-as-a-Service (AaaS) and Spyware-as-a-Service (SaaS) pose unique and significant threats to these entities. Attackers steal proprietary trading algorithms, investment strategies, or insider information. Competitors or hostile actors use this information to gain market advantage. Breaches undermine client trust, resulting in investor withdrawals and regulatory scrutiny.

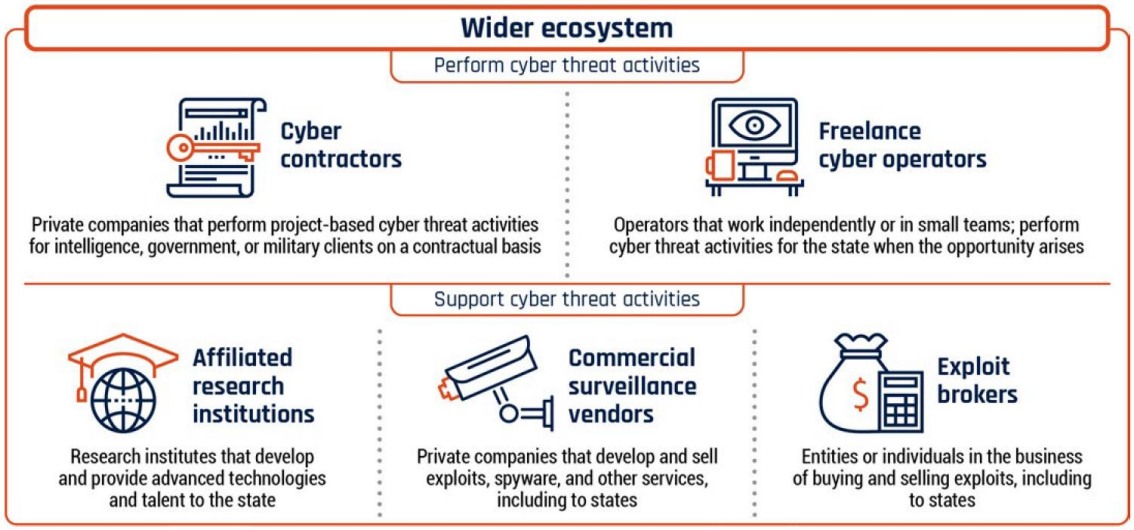
Today we will start with a very interesting paper:

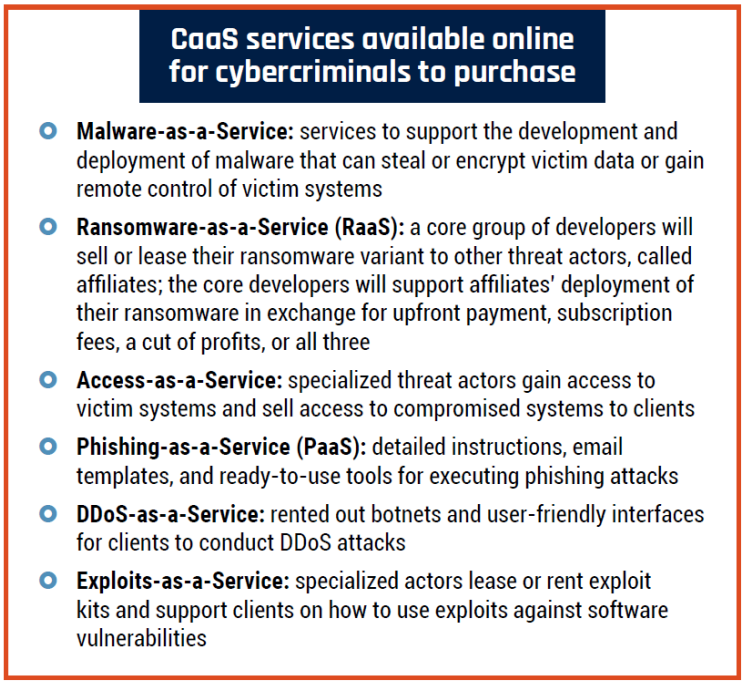
The National Cyber Threat Assessment 2025-2026 (NCTA 2025-2026)

Canadian Centre for Cyber Security

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada
Canadian Centre for Cyber Security | Centre canadien pour la cybersécurité

Note: The Canadian Centre for Cyber Security (Cyber Centre) is Canada's technical authority on cyber security. Part of the Communications Security Establishment Canada (CSE), it is the single unified source of expert advice, guidance, services, and support on cyber security for Canadians and Canadian organizations. The Cyber Centre works in close collaboration with Government of Canada departments, critical infrastructure, Canadian businesses, and international partners to prepare for, respond to, mitigate, and recover from cyber events.





Introduction

Canada has entered a new era of cyber vulnerability where cyber threats are ever-present, and Canadians will increasingly feel the impact of cyber incidents that have cascading and disruptive effects on their daily lives.

Advancements in communications and computing technologies have ushered in a world of ubiquitous connectivity for Canadians.

In this environment, online platforms and digital technologies continue to shape and mediate Canadians' interactions with the physical world—the way we work, shop, travel, socialize, get informed, and access critical services.

These systems record and process vast amounts of data about us, often over poorly secured or untrustworthy digital networks.

These systems are also interconnected and fragile: cyber incidents, from cyber attacks to flawed software updates, can knock airlines, hospitals, banks, and retailers around the world offline.

CSE and its partners in Canada and across the Five Eyes are attuned to the cyber threats to Canada from state and non-state cyber threat actors and are tracking them as they evolve.

NCTA 2025-2026 provides the Canadian public with CSE's current insights on the state and non-state cyber threat actors conducting malicious cyber threat activity against Canada and how we assess the cyber threat landscape will evolve in the next two years.

This assessment is divided into three sections that are designed to stand independently and together.

Section 1—Cyber threat from state adversaries: introduces the state cyber threat ecosystem and discusses the cyber threats to Canada.

Section 2—Cybercrime threats: discusses the interconnectivity of the Cybercrime-as-a-Service (CaaS) ecosystem and the cybercrime threats facing Canada, specifically from fraud, scams, and ransomware. This section also highlights the ransomware threat to Canada's critical infrastructure.

Section 3—Trends shaping Canada's cyber threat landscape: identifies five trends that will shape Canada's cyber threat landscape and drive cyber threat activity impacting Canadians up to 2026.

The rise of AI-generated websites

Foreign states are creating fake news websites masquerading as real news outlets as part of their disinformation campaigns. Many of the sites are designed to look like local news outlets that have closed down and rely on AI-generated content.[142]

Trend 3: Geopolitically inspired non-state actors are creating unpredictability

Geopolitical conflicts and tensions are inspiring disruptive cyber threat activity from non-state groups, commonly referred to as hacktivists. Geopolitically motivated hacktivists typically conduct attacks to gain attention, such as DDoS attacks, website defacements, and data leaks. Some groups have elevated the impact of their activity by opportunistically targeting and disrupting vulnerable critical infrastructure, such as municipal water systems, risking serious harm to the public.[153]

Geopolitically motivated hacktivism is surging around military conflicts. Hacktivist groups have carried out campaigns related to Russia's invasion of Ukraine in 2022 and the Israel-Hamas war in 2023.[154] Diplomatic tensions are also inspiring hacktivist activity. After Canada accused India of involvement in the killing of a Canadian citizen, a pro-India hacktivist group claimed to have defaced and conducted brief DDoS attacks against websites in Canada, including the public-facing website of the Canadian Armed Forces.[155]

This non-state ecosystem is dynamic and unpredictable. Some hacktivists are genuinely motivated by a mix of patriotism, ideology, or a political cause, but others opportunistically take advantage of conflicts for personal benefit or notoriety. New groups regularly appear and established groups dissolve and re-emerge with new names. Actors shift their focus and motivations. Different groups coordinate and collaborate, including across multiple conflicts.[156] Although hacktivist activities can sometimes align with an adversarial state's interests, the relationship, if any, between a hacktivist and the state can be difficult to discern.

To read more: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

SEC Approves 2025 PCAOB Budget and Accounting Support Fee

U.S. Securities and Exchange Commission

The Securities and Exchange Commission voted to approve the 2025 budget of the Public Company Accounting Oversight Board (PCAOB) and the related annual accounting support fee.

The 2025 PCAOB budget totals $399.7 million. The accounting support fee totals $374.9 million, of which $346.1 million will be assessed on public company issuers and $28.8 million will be assessed on registered broker-dealers.

“Well-functioning financial markets are built on trust,” said SEC Chair Gary Gensler. “Critical to such trust are disclosures – including financial statement disclosures made by issuers and broker-dealers to the investing public. I have seen since the passage of Sarbanes-Oxley 22 years ago the importance of that law in promoting trust in public company figures. This trust, though, can easily be taken for granted. The PCAOB – an important reform of the George W. Bush Administration – writes the standards for auditors and audits the auditors. That’s the core of what it does, and it’s every bit as important now and into the future.”

“I am confident in the Board’s ability to continue to act as a diligent and responsible steward of publicly sourced accounting support fees, as evidenced by their accomplishments this past year,” said SEC Chief Accountant Paul Munter.

The Sarbanes-Oxley Act of 2002, which established the PCAOB, provides the Commission with oversight responsibility over the PCAOB. This includes reviewing and approving the PCAOB’s budget and accounting support fee annually.

To read more: https://www.sec.gov/newsroom/press-releases/2024-204

Chair Williams’ Statement Before the SEC Open Commission Meeting on the PCAOB’s Proposed 2025 Budget

Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams

Thank you, Paul [Munter] and Caryn [Kauffman], and good morning, Chair Gensler and Commissioners Peirce, Crenshaw, Uyeda, and Lizárraga. It is great to be with you today, and I want to thank you for the opportunity to present the PCAOB’s 2025 Budget for your consideration.

I am obligated to note that I am here today in my capacity as Chair of the PCAOB and my comments do not necessarily reflect the views of other Board Members or PCAOB staff.

Before I start, I want to take a few minutes at the beginning of our time together today to acknowledge that this is likely my last meeting with both Chair Gensler and Commissioner Lizárraga, and I want to thank you both, not only for your support for the PCAOB, but for your decades of public service on behalf of investors.

Chair Gensler, your history with the PCAOB goes back to your work for Senator Paul Sarbanes and helping to craft the Sarbanes-Oxley Act, which as we know, created the PCAOB. As you have said before, "It matters who sets the standards. It matters who 'audits the auditors.'"

I couldn't agree more.

Thank you for your many years of dedicated, steadfast work in support of our mission.

Commissioner Lizárraga, I want to thank you, and also your staff, for your commitment to serving hardworking people who are saving for a better future. I wish you, your wife, and your family all the best in the days ahead.

The 2025 Budget is $399.7 million and funds 945 positions across the PCAOB—which is one less position than was assumed in the 2024 Budget. It results in a projected Accounting Support Fee or ASF of $374.9 million, comprised of $346.1 million for issuers and $28.8 million for broker-dealers. While the 2025 budget assumes a necessary increase in the ASF overall, we anticipate the smallest billable issuers will see no increase, while the median difference per bill for issuers will likely be only $100.

The PCAOB's 2025 Budget reflects the resources required to carry out our statutorily mandated responsibilities and protect investors in U.S. markets by continuing to achieve our strategic goals.

Under this Board, we have made significant progress against our goals, and the 2025 Budget will enable the organization to build upon this success through the dedicated efforts of the PCAOB's talented and experienced staff.

Inspections

Our inspections program is one of the most important tools we have to protect investors, and more than half of our staff are in our Division of Registration and Inspections. Most of these individuals have decades of experience, and they are serving, quite literally, on the frontlines of audit quality as they build upon our accomplishments.

Specifically, the 2025 Budget will enable our 430 staff in the Firm Inspections Group to continue their outstanding work in conducting domestic and international inspections, including approximately 30 staff that will be executing inspections in Mainland China or Hong Kong.

By the end of 2024, our staff will have inspected 232 audit firms and more than 920 audits across domestic annual, domestic triannual, international, and broker-dealer audits.

These numbers include 79 international inspections of firms and more than 220 audits, including audits of firms in Mainland China and Hong Kong.

We have also made significant improvements this year in issuing our inspection reports in a timelier manner. Prior to this Board taking shape in early 2022, there was a significant backlog of inspection reports from prior years.

In our first year, this Board approved more than 280 inspection reports, representing a 73% increase over the prior year, and the most reports the Board has approved in any given year. I am pleased to report that we have resolved the backlogs and are working to get the inspections reports into the hands of investors and other stakeholders as quickly as possible.

We published the 2023 inspections reports for annually inspected firms in August of 2024–six months faster than last year, and nearly all of the reports for triennially inspected firms were published within six months of the completion of those inspections.

In 2025, we will strive to continue to improve on these results to provide this critical information to the public even faster, so they have the information they need to confidently participate in the markets.

In 2024, we continued to use every tool available to us to drive audit quality, including remediation.

When PCAOB inspectors identify deficiencies in a firm's quality control systems, firms can take advantage of the remediation process, which gives them a year to correct or remediate the problems before they are made public.

We recently published a supplement to our remediation staff guidance, providing additional direction to firms to facilitate improvements in their remediation activities. The 2025 Budget enables our staff to continue to focus on remediation and engage with firms as they improve their quality control systems.

To further increase our efforts to provide even more information to investors and others, we added charts to our website this year to make it easier to understand and compare inspection results both across firms and over time.

Under this Board, we have also more than doubled the number of staff Spotlight reports which provide valuable insights into how to improve, including highlighting key risks and examples of good practices to follow.

And we recently published the first two installments of "Audit Focus," a new PCAOB staff publication series aimed at auditors who typically audit smaller public companies. "Audit Focus" highlights applicable auditing standards and provides reminders and good practices specific to auditors of smaller public companies.

This year, our inspectors are seeing significant improvements in the aggregate Part I.A deficiency rate from the largest firms, which we expect to be reflected in our inspection reports next year. Based on these results, it appears the work that I just described is bringing about positive change in audit quality. The resources reflected in this budget will provide our staff with the ability to continue their great work in this area.

Standards and Rules

Moving to standard setting and rulemaking, we continue to focus on modernizing our standards and rules and to assist firms in their implementation of them.

This Board has issued proposals or adopting releases to update 20 standard-setting or rulemaking projects, including four proposals and seven adopting releases this year alone—many of which had not been substantially updated in two decades.

This Board has taken more formal actions to modernize standards and rulemaking this year than any year since 2003 when the PCAOB was established.

The 2025 Budget provides the necessary resources for us to continue this important work and help firms prepare for the implementation of recently updated standards and rules.

As we finalize our standard-setting and rulemaking projects, we are committed to providing firms with resources to help them update their methodologies and train their staff for the upcoming changes. We have proven this commitment in 2024 by issuing multiple new resources for firms related to our new quality control standard, QC 1000.

Although the responsibility for preparing for the upcoming changes falls on firms, we recognize the need for such resources and plan to issue additional materials in 2025.

Enforcement

We also continue to strengthen our enforcement program to ensure accountability, promote deterrence, and protect investors. Our Division of Enforcement and Investigations staff continues to focus on cases with significant audit violations, failures to comply with auditor independence rules, and matters threatening the Board's oversight activities, such as non-cooperation with PCAOB inspections and investigations.

This year, we revoked the registration status of a China-based firm for repeated violations of PCAOB rules and for failing to cooperate with an investigation into those violations.

Separately, we barred two partners of a China-based firm from practicing and imposed practice limitations on another partner of the same firm for violating PCAOB standards. We also concluded major enforcement matters involving exam cheating at audit firms and lying to PCAOB investigators.

All of these violations put investors at risk.

We explore all aspects of a case to determine the appropriate form of relief including where appropriate, revoking firms' registration status and issuing bars like in the previous examples out of China, requiring functional changes to a firm's supervisory structure, and requiring firms to retain an independent monitor to drive improvements.

This budget provides us with the resources to continue to hold bad actors accountable on behalf of the investors we serve.

Organizational Effectiveness

Finally, we continue to be good stewards of the fees collected to fund the PCAOB. We do this by evaluating not only our oversight activities, but also our outreach to stakeholders, internal processes, and information technology capabilities.

In 2024, we expanded our outreach to, and support for, smaller audit firms by organizing a nationwide series of in-person and virtual forums for auditors of smaller businesses and broker-dealers, with each event hosted by a different Board Member. The forums provide the PCAOB an opportunity to share valuable resources and information with small firms to help them improve audit quality, while also giving us a chance to hear from them directly about their unique needs and challenges.

We also enhanced our outreach activities with investors. Our Office of the Investor Advocate issued seven Investor Advisories and Bulletins this year. These publications provide critical information to deepen investors' understanding of the PCAOB's work.

In addition, we continue to focus on improving our well-functioning internal processes and information technology capabilities, while investing in our highly skilled staff. I am proud to share that our internal surveys show significant increases in staff satisfaction under this Board.

More than 80 percent of PCAOB employees who participated in our most recent employee engagement survey said they would recommend the PCAOB as a great place to work, an increase of nearly 30 percentage points from our first survey.

Before turning back over to you, Chair Gensler, and the Commissioners for any questions you may have, I want to add that I am incredibly honored to lead our talented staff and learn from them every day. When I took over as Chair of this organization just about three years ago, I empowered the staff to challenge existing processes and to work together to develop innovative approaches to achieve our goals.

As demonstrated by their numerous achievements, PCAOB staff have more than risen to the occasion. Investor protection is strong because of their tremendous efforts.

This budget enables us to both provide our staff with competitive compensation that acknowledges their extraordinary work on behalf of investors and retain them, as well as attract new, expert talent to help us meet our investor-protection mission.

I would like to thank the Commissioners and the staff of the Securities and Exchange Commission, including in the Office of the Chief Accountant, Paul Munter, Natasha Guinan, Anita Doutt, Shehzad [Shaz] Niazi, and Taylor Pross as well as in the Office of Financial Management, Caryn Kauffman.

I would also like to thank my fellow PCAOB Board members, and our dedicated PCAOB staff. I would now be happy to answer any questions you may have.

To read more: https://pcaobus.org/news-events/speeches/speech-detail/chair-williams--statement-before-the-sec-open-commission-meeting-on-the-pcaob-s-proposed-2025-budget

The 2024-2029 Commission

The Commission is composed of the College of Commissioners from 27 EU countries. They are assigned responsibility for specific policy areas by the President. As the treaty says, each Member of the College is equal – and each Commissioner has an equal responsibility to deliver on the priorities. That means that all Commissioners must work together.

A new era for European Defence and Security

The last few years have been a sharp reminder of how fragile peace is. This is why the Commission will continue investing in European security by:

- Building a true Defence Union to strengthen the defence industrial base, innovation and the Single Market
- Developing a Preparedness Union Strategy to ensure we're ready to respond quickly to any crisis
- Building a safer and more secure Europe to have the means to deal with threats and fight crime, so people can feel safe
- Strengthening our common borders to make them more secure and to make the EU the most advanced travel destination in the world

- Managing migration to open up legal pathways to migration, and address it fairly and effectively

The 4 pillars of the EU Security Union Strategy

The strategy lays out the tools and measures to be developed over the next five years to ensure security in our physical and digital environments. It is composed of four strategic priorities for action at EU level and will draw heavily on the work of the EU agencies.

Fighting terrorism and organised crime

To step up the fight against terrorism and organised crime by strengthening existing instruments and providing new tools for effective law enforcement.

A future-proof security environment

To protect public spaces and critical infrastructure -physical or digital. This includes addressing cybersecurity threats.

Building a strong security ecosystem

To better exchange information between national authorities and EU agencies and to use research & innovation to counter current and future threats.

Tackling evolving threats

To equip national authorities with the right tools to detect and combat hybrid threats, cybercrimes and illegal content online, taking account of technological developments.

Pillars and key action areas of the European Security Union Strategy

To read more: https://ec.europa.eu/stories/2024-2029-commission/

Faster digital payments: global and regional perspectives

BIS Papers No 152, December 2024

Abstract

Digital payments are a promising tool to improve people's payment experience and financial health. This is especially true for fast payments, which allow for immediate availability of final funds to the beneficiary.

Often combined with new functionalities, fast payments can offer enhanced convenience compared with other payment instruments. They can also be cheaper for individuals and businesses, especially when provided by or in collaboration with the public sector and on a cost recovery basis.

This chapter provides a high-level overview of key insights and issues discussed at the Workshop on "Fast payments in Latin America" organised by the Bank for International Settlements and the World Bank and held in Mexico City in May 2024.

In particular, it draws out some common themes on financial inclusion, the role of central banks, domestic and cross-border interoperability and new functionalities, and gives an overview of the other chapters in this volume.

Overview of FPS implemented in LAC, selected jurisdictions — Table 1

	Name of FPS[1]	Launch date	Payment initiation methods			
			Account details[2]	QR codes[3]	Email[4]	Mobile number[5]
Argentina	Transferencias 3.0	Dec 2020	X	X		
Bolivia	QR BCB Bolivia	Dec 2022		X		
Brazil	Pix	Nov 2020		X	X	X
Chile	Transferencias Electronicas de Fondos	2008	X			
Colombia	Transfiya	Dec 2019				X
	Entre-cuentas	Jan 2023		X		
Costa Rica	SINPE Móvil	May 2015				X
El Salvador	Transfer 365	Jun 2021	X			
	Transfer 365 – Móvil	Jun 2022				X
Mexico	SPEI	Aug 2004	X			
	CoDi	Sep 2019		X		
	DiMo	Feb 2023				X
Peru	Transferencias Interbancarias Inmediatas	Nov 2020	X			X
	Yape	Feb 2017		X		X
	Plin	May 2020		X		X
Uruguay	Toke	Sep 2024		X		

[1] The use of the term "fast payment systems", or FPS, can vary. See footnote 2. [2] End users can transfer funds using bank account details. [3] End users can pay by scanning QR codes. [4] End users use an email address to send and receive money. [5] End users send or receive money using their mobile phone numbers.

Introduction

The retail payments landscape in Latin America and the Caribbean (LAC) is going through revolutionary changes. At the heart of this revolution is the introduction of fast payment systems (FPS) and the adoption of fast payments (Randall et al (2024)).

Fast payments, also referred to as instant, real-time, immediate or rapid payments, allow for transaction messages to be transmitted and final funds to become available to the beneficiary in real time or near real time, and as near as possible to 24 hours a day and 365 days a year (24/365) (CPMI (2021); World Bank (2021a)).

FPS enable swift processing of retail transactions to ensure the immediate availability of funds for the recipient. In this chapter, we use "FPS" as an umbrella term that encompasses the underlying technical infrastructure, participating payment service providers (PSPs), end user-facing services and underlying rules that govern the processing and delivery of fast payments (Frost et al (2024)).

Over 15 jurisdictions have implemented an FPS in LAC (see Table 1 for some examples).

Brazil's Pix was implemented in November 2020 and is a notable example of a central-bank owned FPS (Duarte et al, 2022); over 90% of the adult population in Brazil received or initiated a Pix transaction between July 2023 and July 2024.

Costa Rica has seen a similar success story with SINPE Móvil, which was implemented in May 2015, with nearly 80% of adults using it by August 2024.

In Mexico, the central bank launched Cobro Digital (digital collection, "CoDi") and Dinero Móvil (mobile money, "DiMo") in 2019 and 2023 respectively, building upon the large-value Sistema de Pagos Electrónicos Interbancarios (Interbank Electronic Payments System, "SPEI"). By September 2024, the number of validated CoDi accounts had grown to 20.3 million.

In Peru, the Automated Clearing House (ACH) implemented a fast payment service in November 2020. This happened in parallel with the rise of digital wallets (eg Yape and Plin), which also allow immediate transfer of funds. These developments have boosted the uptake of fast payments in Peru, which reached 157 such payments per adult in 2023. In Bolivia, the central bank implemented QR BCB Bolivia – a standardised and interoperable QR code – for fast payments in 2022.

In December 2020, the Central Bank of Argentina launched Transferencias 3.0, which comprises different fast payment services provided by the private sector, including payments initiated with QR codes.

End users in Uruguay have been able to send and receive fast payments using "Toke", which is also based on QR codes, since September 2024.

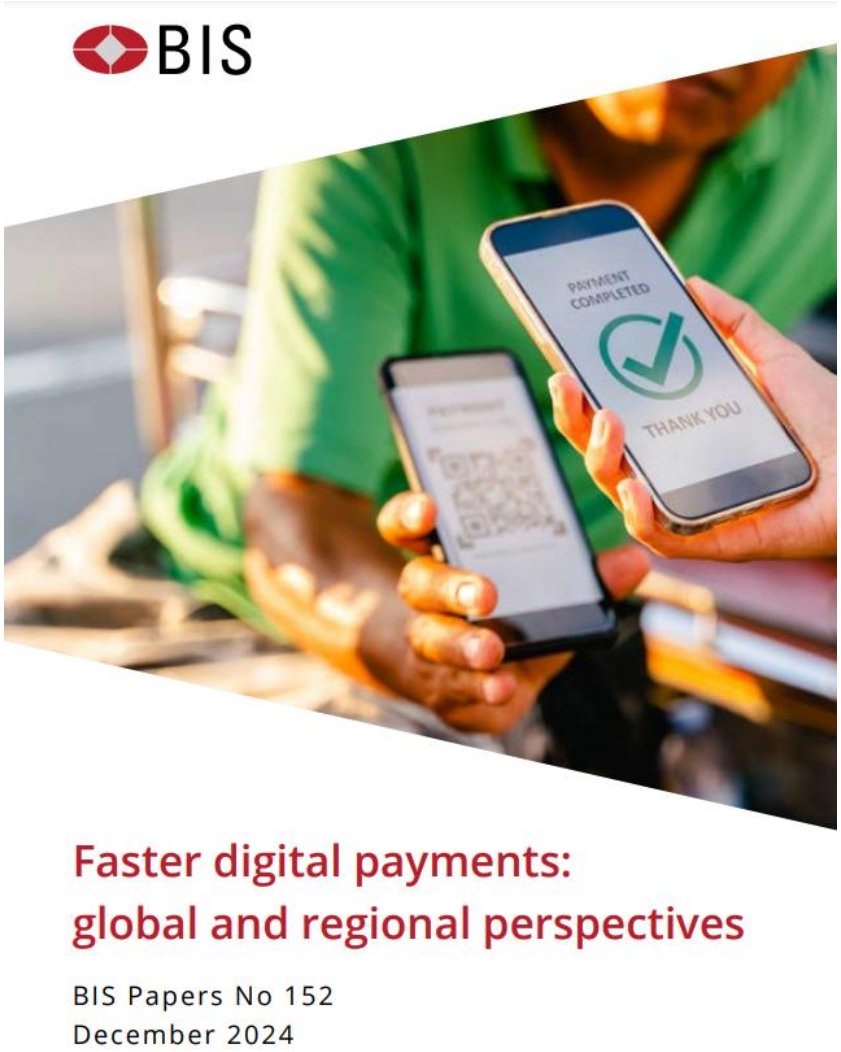
In 2025, Colombia plans to implement "Bre-B", which is a new central bank-owned service that interconnects financial institutions offering fast payments, such as institutions using the (private sector) FPS Transfiya and Entre-cuentas.

In Central America, the countries of Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras and Nicaragua have seen a rapid increase in digital cross-border payments, thanks to their regional real-time gross settlement (RTGS) system, Sistema de Interconexión de Pagos (System of Payment Interconnection, "SIPA") and the Transfer 365 FPS.

What has been driving these developments? In LAC, the implementation of FPS is often viewed as a tool to achieve public policy objectives. Fast payments have the potential to drive financial inclusion, reduce transaction costs and stimulate economic activity by providing individuals and businesses with convenient and affordable payment solutions and faster and cheaper access to funds (Aguilar et al (2024)).

The implementation of an FPS has also been associated with improved access to credit (Aurazo and Franco (2024)). Through these and other benefits, greater use of fast payments could also improve financial health, which is defined as the extent to which a person or family can successfully manage their financial obligations and have confidence in their financial future (Cantú et al (2024)). In particular, it could give users the ability to pay and be paid more efficiently, save for the future and thus better withstand shocks.

To read more: https://www.bis.org/publ/bppdf/bispap152.pdf



ECB and EIOPA propose European approach to reduce economic impact of natural catastrophes

This paper proposes a possible EU-level solution to address the widening gap in natural catastrophe insurance protection in Europe. Increased economic exposure and the growing frequency and severity of natural catastrophes linked to climate change have been driving up the cost of natural catastrophes in Europe.

Pillar 1: EU reinsurance scheme		Pillar 2: EU disaster fund
Increase insurance coverage and supply	Goal	Incentivise risk mitigation and limit public outlays
(Re)insurers and national schemes	Participants	Governments
Public-private	Set-up	Public
Voluntary	Membership	Mandatory
Risk-based premia from participants (and capital market funding incl. cat bonds)	Funding	Risk-adjusted contributions from governments (and possibly debt issuance)
Payout according to contract conditions	Payouts	Payout calibrated to event and dependent on implementation of national plans

Between 1981 and 2023, natural catastrophes caused around €900 billion in direct economic losses within the EU, with one-fifth of these losses having occurred in the last three years alone. However, over the same period, only about a quarter of the losses incurred from extreme weather and climate-related events in the EU were insured – and this share is declining.

This "insurance protection gap" is expected to widen further due to the increasing risk posed by climate change. Europe is the fastest-warming continent in the world and increasing climate risk is likely to have implications for both the supply of and demand for insurance if no relevant measures are in place.

As the frequency and severity of climate-related events grow, (re)insurance premiums are expected to rise. This will make insurance less affordable, particularly for low-income households.

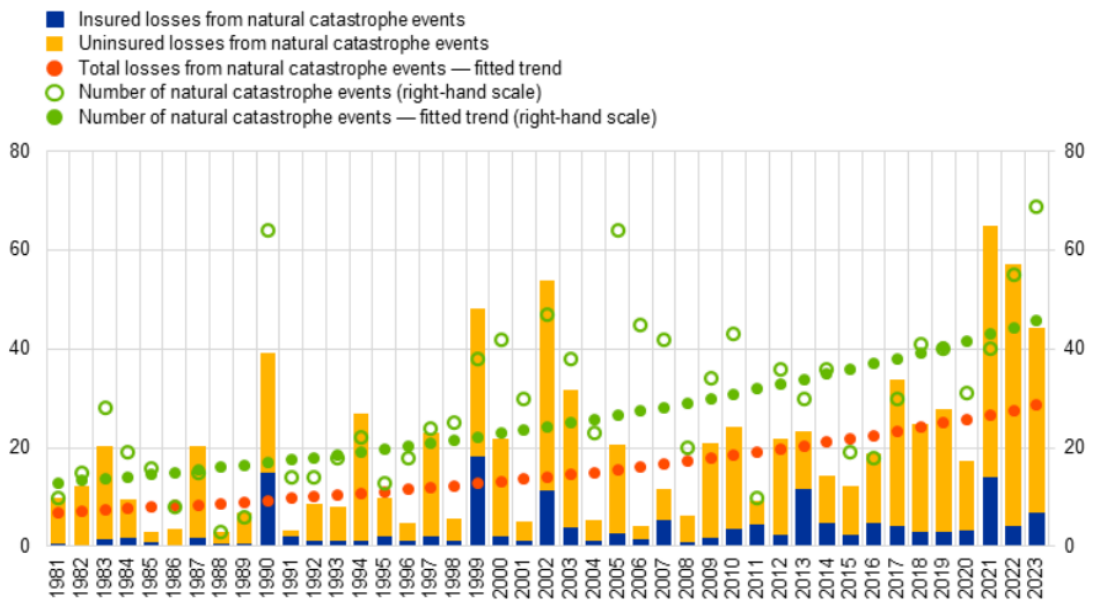
Climate change also increases the unpredictability of these events, which may prompt insurers to stop offering catastrophe insurance in high-risk areas. At the same time, low risk awareness and reliance on government disaster aid further dampen insurance uptake by households and firms.

In April 2023 the European Central Bank (ECB) and the European Insurance and Occupational Pensions Authority (EIOPA) published a joint discussion paper on addressing this growing protection gap.

Chart 1

Economic losses from and number of natural catastrophes in the EU

(1981-2023; EUR billions as measured in 2023 values, number of events)



Sources: CATDAT (Risklayer GmbH – Europe Climate related impact Analysis Project), EIOPA's Dashboard on insurance protection gap for natural catastrophes – European Union (europa.eu) and EM-DAT.
Notes: The two fitted trends depict exponential trends fitted to the annual time series of the number of and the total losses (insured and uninsured) from natural catastrophe events. (Initially, two types of linear regressions were fitted, one for the original data and one for logs of the original data: since better fits – as measured by R-squared – were obtained for the logs of the original data, the estimated coefficients from these regressions were used to depict the exponential trends). The trend fitted to total losses remains upward-sloping when total losses are scaled by GDP. Natural catastrophes include both geological catastrophe events (e.g. earthquakes, volcanic eruptions) and climate-related catastrophe events (droughts, extreme temperatures, floods, mass movements, storms and wildfires). The frequency of geological catastrophe events (as opposed to that of all natural catastrophe events or climate-related catastrophe events) is not upward-trending.

The paper provided evidence showing the economic significance of this gap, including its implications for the macroeconomy, the financial system and fiscal budgets. It showed, for instance, that the lack of insurance can slow down economic recovery, increase banks' exposures to credit risk and weaken the fiscal position of governments when they step in to cover uninsured losses.

To help reduce the gap, it advocated for a ladder approach to natural catastrophe insurance, calling for a multi-layered approach involving both the private and public sectors at national and EU-level. Following its release, the paper received responses from various stakeholders, which motivated this follow-up work.

Recent events, such as the 2024 flooding in central and eastern Europe and in Spain, have further illustrated the challenges that extreme weather events can pose for the EU and its Member States. These events highlight the importance of emergency preparedness, risk mitigation, and adaptation efforts to prevent and/or minimise the losses from natural disasters, as well as the relevance of national insurance schemes in reducing the economic impact of natural catastrophes. They also bring to the fore the importance of addressing the insurance protection gap and the associated burden on public finances.

The EU Solidarity Fund, which aims to support governments in the wake of severe disasters, has proved to be too small to provide meaningful support for reconstruction efforts. Following the floods in central and eastern European

countries, the European Commission thus proposed that the affected countries receive €18 billion from the EU cohesion funds to support their recovery efforts.

However, these funds are not intended for responding to specific disasters, they are not available to all EU Member States and they have no mechanism for ensuring that Member States address natural disaster risk pre-emptively or increase private insurance coverage.

Table 1

Factors negatively affecting insurance demand and supply in the context of natural catastrophe coverage

	Factors lowering insurance demand	Factors lowering primary insurance supply
Risk identification	Low level of risk awareness Underestimation of the likelihood of being affected by natural catastrophes	Uncertainty and unpredictability of evolution of risks (e.g. due to lack of (granular) data, modelling complexity)
Scope of coverage	Incorrect knowledge or assumptions on the scope of coverage for natural catastrophes (e.g. due to unclear terms and conditions in insurance contracts)	Challenges in diversifying risks at national or regional level
Cost of (re)insurance	Unaffordability of premiums or high perceived cost of insurance	Reduction in reinsurance capacity
Moral hazard	Expectation of government support in case of disaster	Expectations of government support in case of disaster
Other factors	Lack of (regulatory) incentives for risk prevention Previous negative experience with insurance claims (lack of trust) Perception that taking out insurance is complex and time-consuming Lack of understanding of insurance products Lack of insurance distribution channels (access)	Lack of (regulatory) incentives for risk prevention Lack of private (re)insurance market competition

Sources: Largely based on EIOPA Staff Paper on Measures to address demand-side aspects of the NatCat protection gap[26], the EIOPA Report on non-life underwriting and pricing in light of climate change[27] and the Climate Resilience Dialogue Final Report of July 2024.[28]

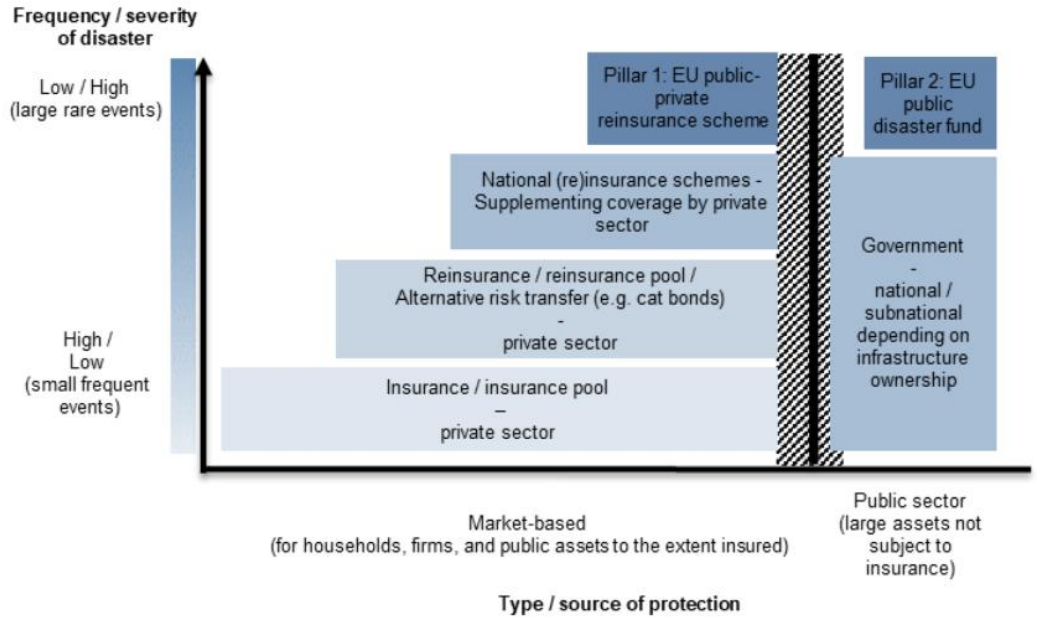
This paper analyses 12 existing national natural catastrophe insurance schemes and how they employ private and public funds to address the protection gap. The paper finds that the existence of such schemes in European countries correlates with higher insurance coverage.

National schemes aim to broaden insurance coverage and encourage risk prevention. Typically, they do so by setting up risk-based (re)insurance structures involving public-private sector coordination for multiple perils (e.g. floods, drought, fires and windstorms).

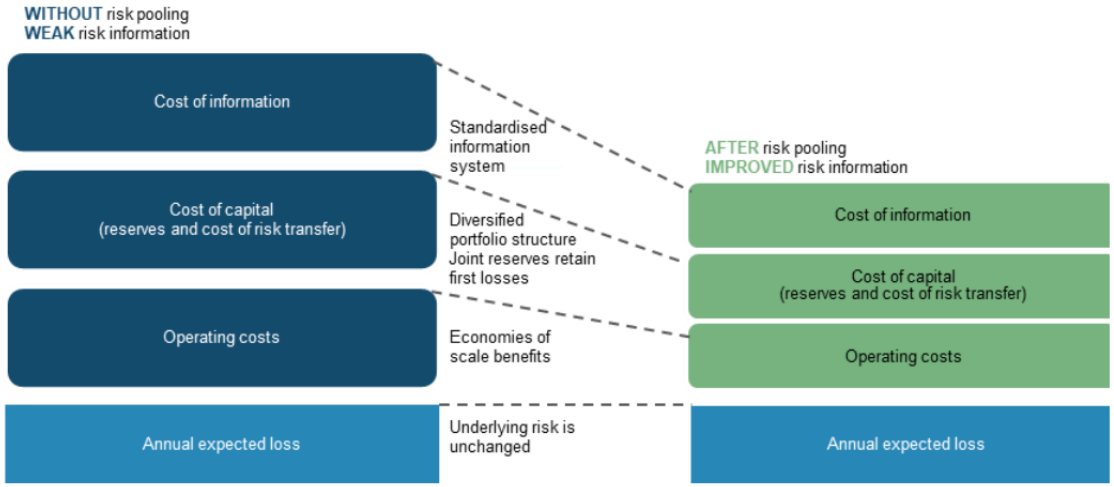
Some of the schemes further support the availability of insurance through mandatory insurance coverage and improve the affordability of insurance through national solidarity mechanisms. At the same time, there are fewer risk diversification opportunities at national than at EU level and reliance on both national and EU public sector outlays has been growing. Therefore, it is beneficial to discuss at EU level how adaptation measures can help in proactively reducing disaster losses and how the sharing of losses between the public and private sectors can help in raising risk awareness and improving risk management before disasters occur.

Figure 2

Ladder of intervention with EU components



Stylised decomposition of the catastrophe risk insurance premium



Source: World Bank (2017) Sovereign climate and disaster risk pooling: World Bank Technical Contribution to the G20.

To read more:
https://www.ecb.europa.eu/pub/pdf/other/ecb.climateinsuranceprotectiongap_EIOPA202412~6403e0de2b.it.pdf

EIOPA's stress test shows EU insurers can handle surging geopolitical risks but at a heavy price

European Insurance and Occupational Pensions Authority

The 2024 stress test exercise tested the resilience of the European insurance industry against the uncertainty deriving from the economic consequences of a re-intensification or prolongation of geopolitical tensions.

Figure 1: Structure of the exercise

Capital Component	Liquidity Component

• Combined scenarios with Market and Insurance specific shocks
• Approach:
  • Instantaneous shocks
  • Fixed balance sheet (no reactive Management Actions)
  • Constrained balance sheet (with guided reactive Management Actions)
• Metrics:
  • Balance sheet based (Excess of Assets over Liabilities)
  • Solvency based (OF, SCR)
	• Approach:
	  • Instantaneous shocks
	  • Fixed balance sheet (no reactive Management Actions)
	  • Constrained balance sheet (with guided reactive Management Actions)
	  • Stylised flow based evaluation
	  • Stock based evaluation
	• Time Horizon:
	  • 90 days
	• Metrics:
	  • Liquidity sources / Liquidity needs

MAIN FINDINGS

Owing to their **strong initial capital position**, reflected in an aggregate solvency ratio of 221.8%, insurers had **sufficient resources to withstand the shocks** of the extreme but plausible stress test scenario.

The exercise confirmed the **sector's sensitivity to simultaneously rising risk premia and interest rates** (i.e. higher yields).

The stress test showed that a re-intensification or prolongation of geopolitical tensions could have a **significant impact on insurers**, resulting in a drop of capital of over €270 billion in the scenario tested.

That said, insurers showed they **have the ability and tools to cope with such a severe drop of capital**. With reactive management actions, they significantly improved their post-shock results vis-á-vis the fixed balance sheet approach.

The exercise did not reveal vulnerabilities in the liquidity position of the participants. Although insurers' cash holdings do fully not cover outflows, they **hold sufficient liquid assets** to meet the liquidity needs generated by the shocks.

This sixth Union-wide exercise ran by EIOPA covers a representative sample of 48 participants from 20 countries covering around 75% of the European Economic Area market (EEA) and it comprises of a capital as well as a liquidity component.

The exercise has a non pass-fail nature and has a primary micro-prudential objective, in line with the previous stress test exercises. In addition, it contains macro-prudential elements which allow to infer potential spill-over effects from the insurance industry to other sectors.

The severe but plausible scenario, developed in cooperation with the European Systemic Risk Board (ESRB), elaborates over the intensification of geopolitical tensions and envisages a widespread resurgence of supply chain disruptions leading to lower growth and higher inflation.

What is a stress test?

A stress test is an important risk management and supervisory tool. It is used by financial institutions, micro-prudential and macro-prudential supervisors to explore vulnerabilities and assess the resilience of financial institutions (e.g. insurers, banks) and of the respective sectors as a whole to severe but plausible shocks. For example, a stress test provides an indication of the impact and potential losses upon the materialization of the risks envisaged in the scenario and help to indicate areas where further supervisory actions might be needed.

Is the EIOPA stress test a pass-fail exercise?

The EIOPA stress test exercises have never been characterised by a pass-fail nature and this also holds for the 2024 stress test. No potential weakness in the post-stress position of the participants shall automatically trigger actions aimed at strengthening the financial position of the insurers. Information collected and produced under the stress test process is used in an aggregated way to issue recommendations to the National Competent Authorities (NCAs). Individual results are only used as a basis for follow-up dialogues between EIOPA and supervisors, as well as between the supervisor and the participant.

What are the objectives of the exercise?

Given its non pass-fail nature, the 2024 exercise has the primarily microprudential objective of assessing the capability of the participants to sustain the adverse conditions depicted in the stress test scenario, both from a capital and liquidity perspective.

The post-stress individual positions are eventually aggregated to infer the overall resilience of the insurance industry.

The 2024 insurance stress test enhances the macroprudential dimension first introduced in 2021. As in the 2021 stress test, the standard fixed balance sheet approach is complemented with a constrained balance sheet approach where participants are allowed to apply reactive management actions in the calculation of their post-stress position (i.e. fixed balance sheet). For the capital component of the 2024 exercise the application of such actions are linked to the risk management framework of the participants and not only to the fulfilment of the regulatory solvency ratios. For both capital and liquidity component, the results after the reactive management actions are used to identify potential spill-over effects on other markets.

Second-round effects stemming from a wage-price spiral would further exacerbate inflationary pressures, ultimately leading to a re-appraisal of market expectations of interest rates across tenors and currencies.

Despite expectations of decreasing inflationary pressures over time, growth will continue to be adversely affected. The resulting tightening of financing conditions would heterogeneously increase government bond rates and would weigh on corporate profitability, widen credit spreads and have a negative impact across other asset classes.

The market shocks are complemented by a set of relevant insurance specific shocks given the context of the scenario. The results show that the overall European insurance industry is well capitalised.

This strong starting position provides enough capital to withstand the materialization of the tail events embodied in the extreme but plausible scenario of the stress test. The aggregate solvency ratio drops by 98.5 p.p., from 221.8% reaching the level of 123.3% in the post stress, increased to 139.9% after the reactive management actions. The total drop of capital without the application of management actions exceeds EUR 270 bn.

The number of participants that apply reactive management actions is 26, many of them applying more than one resulting in a total of 95 actions. Both eligible own funds (EOF) and solvency capital requirement (SCR) contributed to the reduction of the aggregate solvency ratio, with the former reduced by 40.3% and the latter increased by 7.4%.

These effects are more severe against the 2021 stress test (38.2% and 7.1%, respectively), although the comparison is under the caveat of different scenario, scope and basis. Also, due to a methodological enhancement for the application of reactive management actions, namely, to consider the risk management frameworks of the participants and not only to the fulfilment of the regulatory solvency ratio, the number of participants applying them increased from 19 in 2021 to 26.

Besides this aggregate effect, for 8 participants the post stress capital requirement is not met in the fixed balance sheet (i.e. before reactive management actions). However, both for these and the rest of the participants the assets remain enough to cover the obligations to policyholders.

All 8 participants with solvency ratio below 100% applied reactive management actions showing their ability to restore their positions above 100%.

As noted above, more participants apply reactive managements actions, although the 100% solvency ratio is not breached to ensure that their internal risk management framework remains relevant.

Overall, no substantial externalities emerged by the application of the reactive management actions, under the caveat that the embedded actions could not be controlled for this.

Transitional measures contribute to maintain position above the regulatory requirements under post-stress scenario, with 7 more undertakings falling below regulatory requirements under fixed balance sheet assumption when such measures are removed.

The application of the shocks reduces the assets over liabilities ratio by 4.0 p.p. (3.7 p.p., when reactive management actions are allowed). However, the post-stress AoL remains above 100% for all the participants also when removing transitional measures.

Regarding the liquidity component, the results show the importance of the ample availability of liquid assets, needed to meet the increased liquidity needs of the scenario.

The adverse scenario generated material liquidity needs, stemming mainly from the need to pay for surrenders. The aggregate liquidity position (net cashflows plus cash and equivalent) was not enough and resulted in a shortfall of EUR 40.9 bn.

This led insurers to take reactive management actions, mainly redirecting investments and effectively becoming net seller of EUR 305.9 bn of assets. As a result of all the actions taken (embedded and reactive), the liquidity position improved to a level of EUR 61.1 bn on aggregate.

Regarding the contribution of margin call flows to the liquidity position, on aggregate they account for EUR -2.1 bn in the baseline, turning EUR -5.9 bn in the stressed scenario.

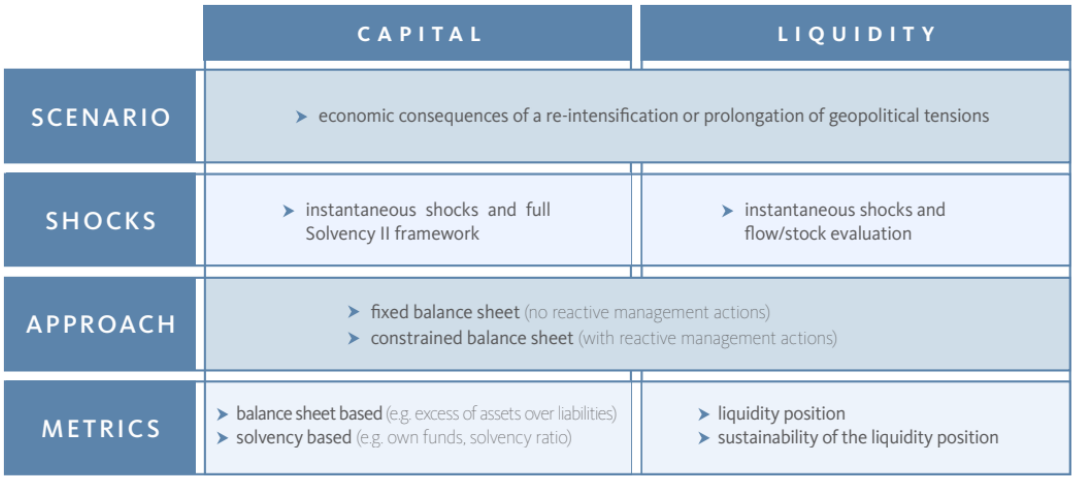
Comparing the liquidity needs against liquid assets, for all the participants liquid assets were adequate to steadily sustain the liquidity needs caused by the stressed scenario.

The importance of the liquid assets as a necessary liquidity source as well as the fact that the main liquidity needs are generated by the surrenders are shared insights comparing to the 2021 exercise.

Moving to the macroprudential aspect of the exercise, sales of assets was identified as one of the reactive management actions mostly used, applied by the participants both in the capital and in the liquidity component.

The structure of the liquidity component allowed for a more comprehensive identification of such effects considering both the impact stemming from the “embedded” and “reactive” management actions. Specifically for the liquidity, the net

sales amounted overall to EUR 305.6 bn, which accounts to approximately 4.0% of the average quarterly bond trading volumes at EEA level. EIOPA will assess the need for issuing recommendations on relevant aspects where risks were identified.



The outcome of the exercise will inform supervisory processes at European and National level. Insights gathered on the behaviour of the industry under stressed conditions should also inform the discussion on the capital relief at political level in the context of the Solvency II review.

To read more: https://www.eiopa.europa.eu/document/download/f8a234b0-a84a-49ff-975e-c47f8849bfc0_en?filename=Report%20-%20Insurance%20Stress%20Test%202024.pdf

2024 Report on the State of the Cybersecurity in the Union

This document marks the first report on the state of cybersecurity in the Union, adopted by ENISA in cooperation with the NIS Cooperation Group and the European Commission, in accordance with Article 18 of the Directive (EU) 2022/2555 (NIS2).

The report aims at providing policy makers at EU level with an evidence-based overview of the state of play of the cybersecurity landscape and capabilities at the EU, national and societal levels, as well as with policy recommendations to address identified shortcomings and increase the level of cybersecurity across the Union.

The drafting of this report precedes the transposition date of NIS2. As a result, some of the data presented here may not fully reflect cybersecurity capabilities following the transposition deadline of 17 October 2024.

Still, this report includes several data points unlikely to change in the short- and mid-term and serves as a snapshot of the state of cybersecurity in the Union just before NIS2 is fully implemented by EU Member States (MSs).

The recent past has been characterised by horizontal policy initiatives including but not limited to NIS2, CRA, CSOA and EUDIF that improve the EU cybersecurity policy framework and establish all necessary structures and processes to allow for targeted improvements at the Union level of cybersecurity moving forward.

Sectorial policy initiatives (e.g. DORA, NCCS, Aviation) were adopted in parallel to address specific sectorial challenges.

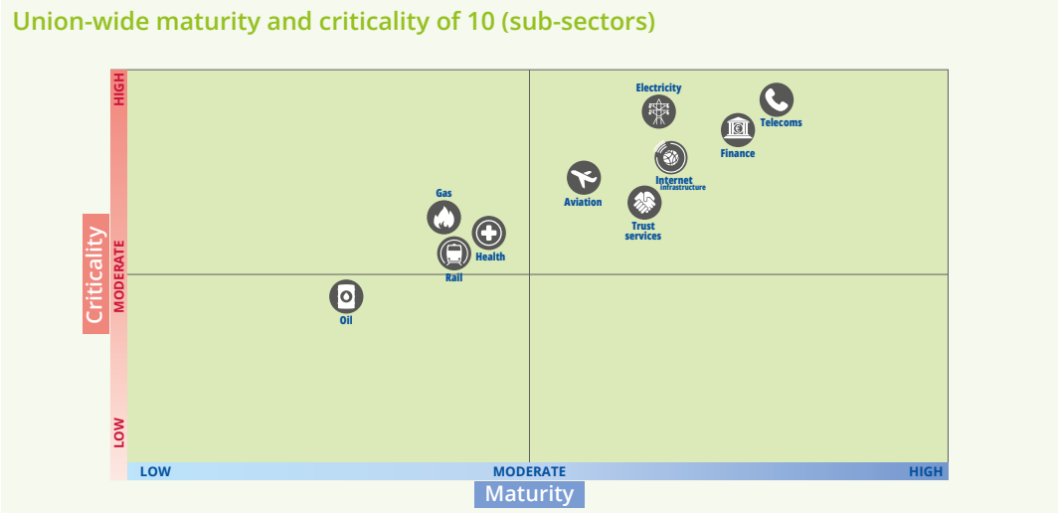
At the same time the volatile geopolitical landscape has influenced the goals and tactics employed by state and non-state threat actors, while an assessment of the threat landscape reveals an increase in cybersecurity incidents in the EU with ransomware and DDoS attacks getting the lion's share among the various types of attack observed.

This report concludes that the maturity of the EU cybersecurity policy framework has reached a considerable level and that the following period could place emphasis on supporting private and public sector entities with the implementation of the legislation by EU MSs, with the support of the European Commission and ENISA.

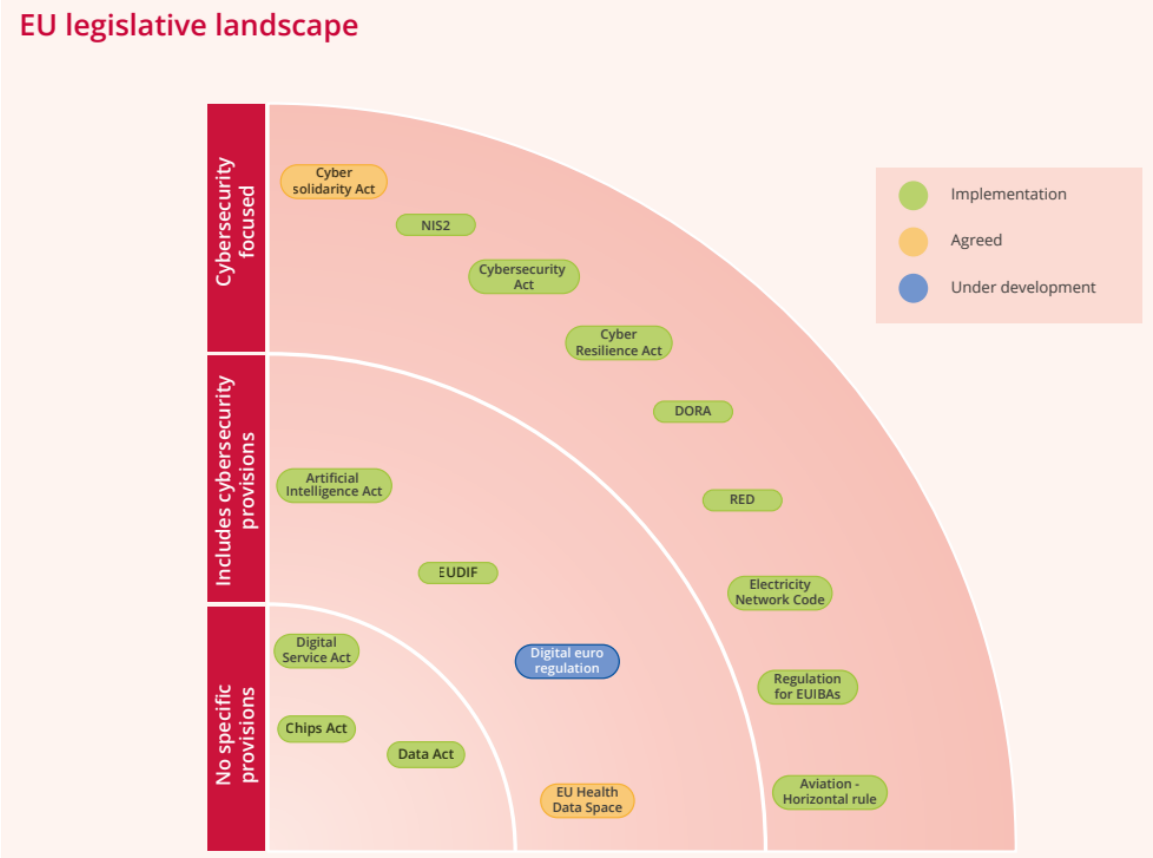
The plethora of mechanisms, processes and platforms for collaboration established within this framework, such as the NIS Cooperation Group, EU-CyCLONe and the CSIRTs Network to name but a few, provide a solid basis and a comprehensive toolbox to address the shortcomings identified in key policy areas, namely Policy Implementation, Cyber Crisis Management Skills and Supply Chains.


Cybersecurity Threats for 2030
1
Supply Chain Compromise of Software Dependencies
2
Skill Shortage
3
Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems
4
Exploitation of Unpatched and Out-of-date Systems
5
Rise of Digital Surveillance Authoritarianism / Loss of Privacy
6
Cross-border ICT Service Providers as a Single Point of Failure
7
Advanced Disinformation / Influence Operations (IO) Campaigns
8
Rise of Advanced Hybrid Threats
9
Abuse of AI
10
Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure
THREATS 2030


Hacktivist activity is increasing and becoming more unpredictable


Union-wide maturity and criticality of 10 (sub-sectors)
Criticality
HIGH
MODERATE
LOW
Electricity
Telecoms
Finance
Internet Infrastructure
Aviation
Trust services
Gas
Health
Rail
Oil
LOW
MODERATE
HIGH
Maturity

LEGISLATIVE CONTEXT



In the recent past, several legislative developments have taken place. After the entry into force of the Directive (EU) 2016/1148 (NIS Directive) in 2016 and the Cybersecurity Act in 2019, a major policy milestone at EU level was the EU Cybersecurity Strategy (published on 16 December 2020).

Several regulatory measures have been taken since then, with important new legislation being put in place to complement the EU cybersecurity framework. More specifically, mention shall be made of the following legislative files.

• Five years after the date of transposition of the NIS Directive, the new NIS2 Directive entered into force on 16 January 2023 setting the date for transposition by the Member States on 17 October 2024.

The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU by imposing legal obligations on entities across 18 sectors of the economy, including in terms of security requirements and the notification of incidents.

It also requires Member States to increase preparedness with, for instance, extended prerogatives and missions for Computer Security Incident Response Teams (CSIRTs) and competent authorities.

The NIS2 Directive also promotes cooperation among all Member States by continuing and strengthening the Cooperation Group set up originally under the NIS Directive to support and facilitate strategic cooperation and the exchange of information among Member States.

It also institutionalises the EU-CyCLONe network, aimed at improving preparedness for and the coordinated management of large- scale cybersecurity incidents and crises at the operational level and to ensure the regular exchange of relevant information among Member States and EUIBAs.

• The Cyber Resilience Act (CRA) was adopted on 23 October 2024. The CRA introduces common cybersecurity requirements for products with digital elements, hardware and software, with the aim of minimising product vulnerabilities and ensuring that cybersecurity is taken seriously both at the design and production phases and that vulnerability management is guaranteed across the support period for such products.

Manufacturers will have to apply the rules 36 months after their entry into force. Reporting obligations regarding actively exploited vulnerabilities and severe cybersecurity incidents are also introduced, applicable 21 months after the entry into force of the Act.

• The Cyber Solidarity Act (CSOA) is expected to enter into force in early 2025. The CSOA lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

It introduces three main pillars to strengthen solidarity at Union level to better detect, prepare for and respond to significant or large-scale cybersecurity incidents, comprising the European Cybersecurity Alert System (pan-European Network of Cyber Hubs), the Cybersecurity Emergency Mechanism and the European Cybersecurity Incident Review Mechanism.

• The amendment to the Cybersecurity Act (CSA amendment) is expected to enter into force by the end of 2024. The proposed targeted amendment aims to enable, by means of implementing acts by the Commission, the adoption of European cybersecurity certification schemes for 'managed security services', in addition to information and communications technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act.

• The Regulation regarding measures for a high common level of cybersecurity at EU Institutions, Bodies and Agencies of the Union (EUIBAs) was adopted in 2023 and entered into force on 7 January 2024.

• Commission Implementing Regulation (EU) 2024/482 which lays down rules for the application of the Cybersecurity Act as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) entered into force in February 2024 and will be applicable as of 27 February 2025.

A number of sector-specific cybersecurity initiatives, such as:

• Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) entered into force on 16 January 2023;

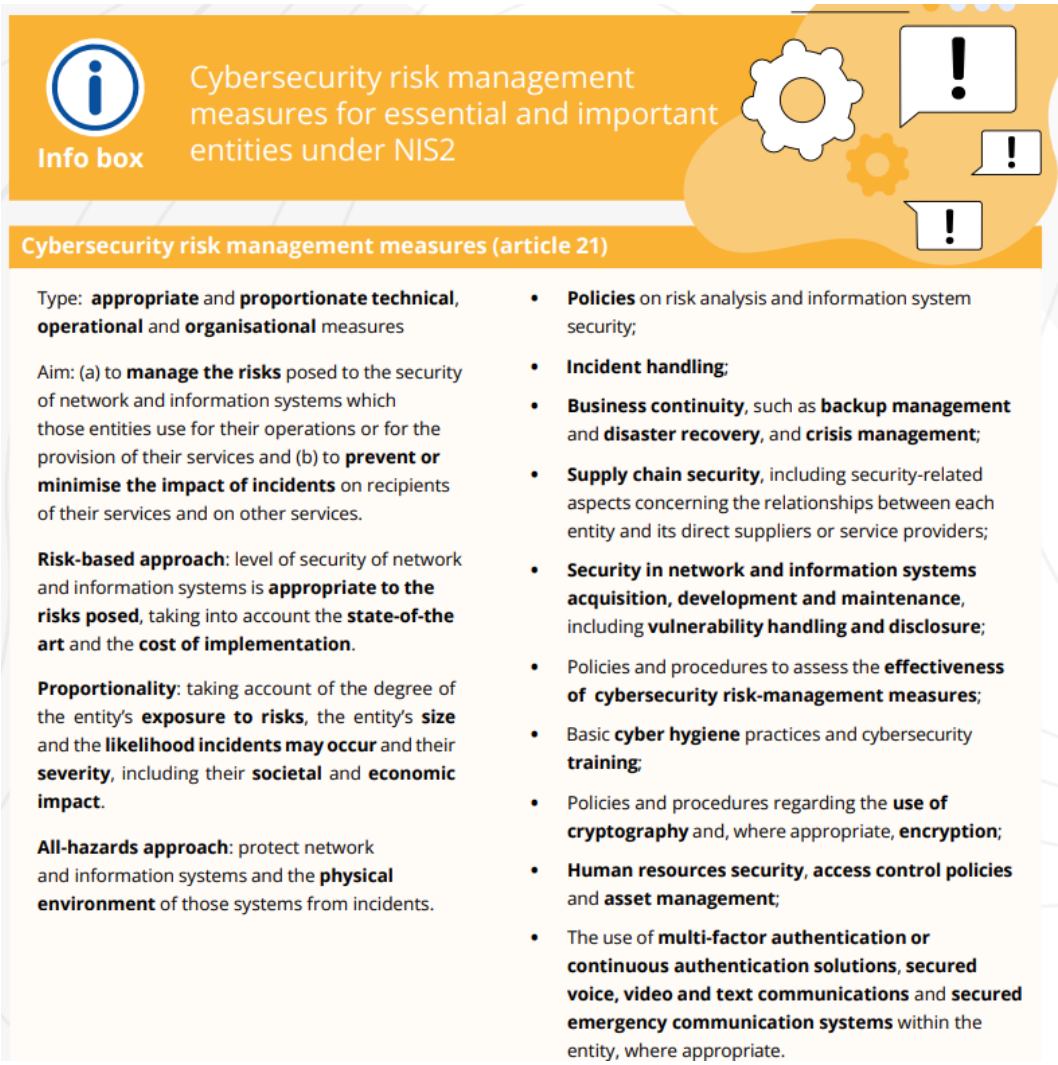
• Commission Delegated Regulation (EU) 2022/164512 and Commission Implementing Regulation (EU) 2023/20313 were adopted in 2022 in the aviation sector;

• The Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS) was adopted on 11 March 2024;

• The new European Digital Identity Framework amending Regulation (EU) No 910/2014 entered into force in May 2024;

• The European Health Data Space (EHDS) Regulation is in the final stages of the adoption process.

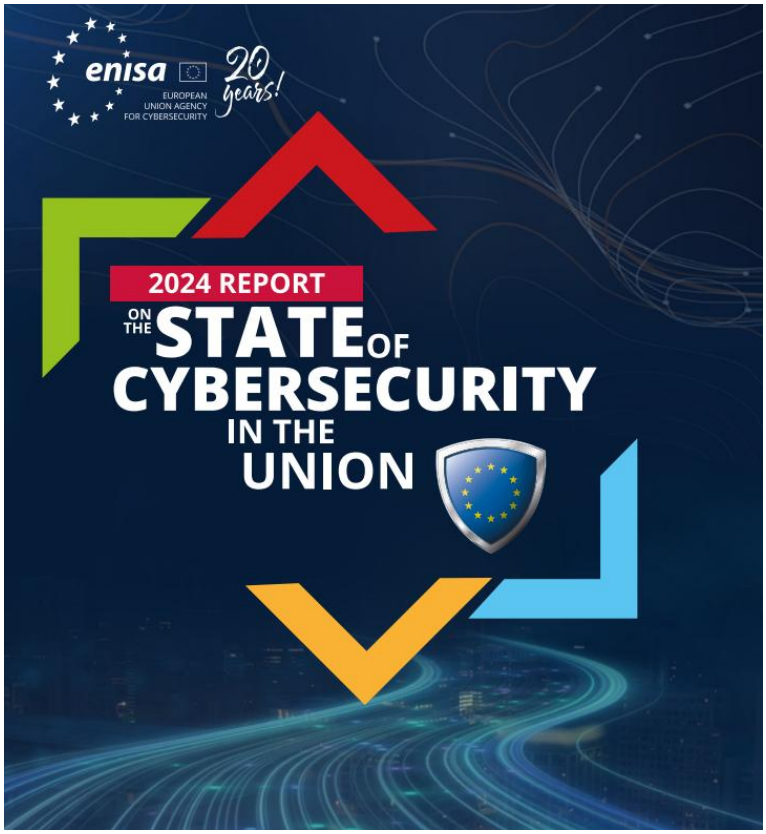
• Other recent Union legislation relevant to the cybersecurity realm include among others the Artificial Intelligence Act (AIA), Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act - DMA), Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act - DSA), Regulation (EU) 2023/178 (Chips Act) and Regulation (EU) 2023/2854 (Data Act).



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

To read more: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union



Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure

Issued by the Office of the National Cyber Director, following consultation with the Cybersecurity and Infrastructure Security Agency

Purpose

The purpose of this Playbook is to provide an easy-to-use resource for Federal agencies and grant recipients to strengthen cybersecurity in critical infrastructure projects.

The Playbook provides guidance for projects that include technologies that, if impacted by a cyber incident, could affect the safety, reliability, or operability of critical infrastructure.

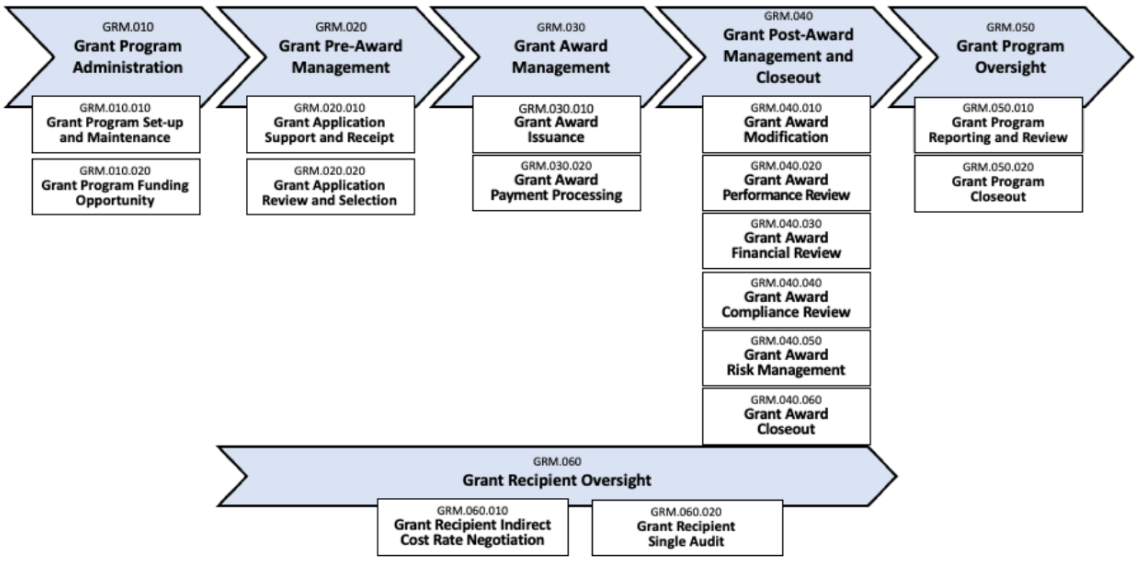


Figure 1: Federal Grants Management Business Lifecycle

Critical infrastructure owners and operators must be vigilant against growing risks posed by inadequately secured systems and should take measures to strengthen and secure systems to maintain safe, functional, and resilient critical infrastructure.

Our nation's critical infrastructure is at risk, in part, because legacy systems, built without the forethought of cybersecurity, are largely still in use.

The Infrastructure Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA), and Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act provide historic investments in the nation's critical infrastructure and provide an opportunity to ensure we build and maintain infrastructure that is resilient to cyber threats and aligned with the secure and resilient-by-design principles set forth in the National Cybersecurity Strategy and NSM-22.

Table of Contents

The Office of the National Cyber Director (ONCD) issues this Playbook resource in furtherance of the strategic objectives in the National Cybersecurity Strategy. The Cybersecurity and Infrastructure Security Agency (CISA) and other departments and agencies provided technical expertise in the development of this Playbook.

This Playbook is intended to provide Federal agencies and grant recipients with tools to build cyber resilience into their projects.

Adding cybersecurity requirements into Federal funding programs and upholding them throughout the projects' lifecycle allows grant program managers, recipients, and subrecipients to identify, prioritize, and address key cyber risks more easily.

Safeguarding the future of American infrastructure requires collaboration between the Federal Government; SLTT governments; and critical infrastructure owners and operators.

Federal agencies should include provisions such as cybersecurity principles, best practices, and controls in their awards and subawards, consistent with applicable law and guidance.

The recommended cybersecurity requirements in this Playbook help recipients develop long-term strategies to continuously address cyber risk on asset performance. Where appropriate, agencies should encourage recipients and subrecipients to set cybersecurity goals above the baseline requirements.

A Project Cyber Risk Assessment and Project Cybersecurity Plan, as outlined in Section 3, should be required for every critical infrastructure grant project that has a technology nexus. In instances where a recipient has multiple projects within a system, it may be appropriate to develop an overall plan for the system.

These systems and assets may include elements, components, and full systems of information technology (IT), operational technology (OT), industrial control systems (ICS), supervisory control and data acquisition (SCADA), and other systems.

To read more: https://www.cisa.gov/sites/default/files/2024-12/Playbook%20for%20Strengthening%20Cybersecurity%20in%20Federal%20Grant%20Programs%20508.pdf

Governing Council statement on macroprudential policies – the ECB's framework for assessing capital buffers of other systemically important institutions

EUROPEAN CENTRAL BANK
EUROSYSTEM

The ECB will enhance the floor methodology used to assess capital buffers for other systemically important institutions (O-SIIs) so that it also takes into account the systemic importance of O-SIIs for the banking union as a whole. In December 2022 the Governing Council announced that the ECB will continue to promote the development of a common EU methodology for O-SII buffers. This will counter unwarranted heterogeneity in the way buffers are set and ensure more consistency in the required loss-absorption capacity of O-SIIs.

The existing ECB floor methodology, which has been in place since 2016, only takes a national perspective. The enhanced floor methodology will also include a banking union perspective for assessing the systemic importance of all O-SIIs for the banking union as a whole.

The enhanced floor methodology will lead to a more consistent treatment of OSIIs across Member States participating in the banking union. The enhanced ECB O-SII floor methodology will contribute to financial stability within the banking union, in line with the ECB's mandate under Article 1 of the SSM Regulation, by assessing the systemic importance of all O-SIIs for the banking union as a whole.

The reduction of the unwarranted heterogeneity in buffer levels for the most systemically important banks in the banking union will make the banking system of the banking union more resilient to shocks and will increase the level playing field.

Moreover, the enhanced ECB methodology will contribute to deepening financial integration by reducing the current disparity between capital requirements for domestic and cross-border activities within the banking union. This reflects the significant progress made in the banking union. Since the inception of the ECB's O-SII floor methodology in 2016, there has been further harmonisation of regulation, supervision and resolution (although some elements of the banking union are not yet complete).

This harmonisation mitigates the systemic risk arising from cross-border exposures within the banking union. Accordingly, the Basel Committee for Banking Supervision recognised in 2022 that this progress in the banking union could be embedded in the assessment framework for global systemically important banks (G-SIBs). Recognition of this progress is therefore also warranted in the framework used to assess the importance of all O-SIIs for the banking union as a whole. This is done by considering cross-border exposures within the banking union to be partly equivalent to domestic exposures.

The ECB will ensure that, for each O-SII at the highest level of consolidation within the banking union, the O-SII buffer should be no less than the higher of the minimum buffer rates implied by the banking union perspective and the national perspective. In line with the EU legal framework, the ECB's O-SII floor implied by the national perspective is retained without changes. The enhancements to the floor methodology focus on those institutions that are most systemically important from a banking union perspective. For most O-SIIs the buffer floor implied by the national perspective is higher than that implied by the banking union perspective. The enhanced ECB O-SII methodology will be applied in line with the ECB's responsibilities under Article 5 of the SSM Regulation to

assess O-SII buffer levels. The ECB will use the enhanced floor methodology to assess O-SII buffers notified by the national authorities, starting from 1 January 2025.

The framework will be capital neutral in 2025 and 2026. After that, the banking union floor will be increased in two increments and, as a result, the enhanced methodology will be fully phased in as of 1 January 2028. The ECB will monitor the application of the enhanced floor methodology, taking into consideration developments in the banking union and in European financial regulation.

To read more:
https://www.ecb.europa.eu/press/govcstatement/pdf/ecb.govcstatement202412~b1f786e5f1.en.pdf?360ec51a85fd451326c879c9d4c4fe54

Monetary policy and sentiment-driven fluctuations

Staff Working Paper No. 1,106, By Jenny Chan

Bank of England

Sentiments, or beliefs about aggregate demand, can be self-fulfilling in models departing slightly from the complete information benchmark in the New Keynesian framework.

Through its effect on aggregate variables, the policy stance determines the degree of complementarity in firms' production (pricing) decisions and consequently, the precision of endogenous signals that firms receive.

As a result, aggregate fluctuations can be driven by both fundamental and non-fundamental shocks.

The distribution of non-fundamental shocks is endogenous to policy, introducing a novel trade-off between stabilising output and inflation.

Both strong inflation targeting and nominal flexibilities increase the variance of non-fundamental shocks, which are shown to be suboptimal. Moreover, the Taylor principle is no longer sufficient to rule out indeterminacy.

Instead, an interest rate rule that places sufficiently low weight on inflation eliminates non-fundamental volatility and thereby the output-inflation trade-off.

Introduction

Economic forecasts often feature significant uncertainty, suggesting that a range of outcomes may be possible. In part, this uncertainty reflects the interconnectedness of decisions among agents.

For instance, investment may be contingent on expected demand. Meanwhile, demand depends on labor market conditions, which in turn rely on supply.

These interdependencies imply that uncertainty about how others will behave, and what they believe, may be a source of friction. However, workhorse models for policy analysis typically abstract from such uncertainty.

Instead, by assuming that agents have common knowledge about the state of the economy and its evolution, they limit the potential for fluctuations as a result of dispersed, yet correlated information.

Such correlation is plausible, since information is often endogenous, simultaneously reflecting and coordinating agents' actions.

How agents use their signals is reflected in their actions, which consequently affects the composition and equilibrium informativeness of such signals.

These information frictions leave room for sentiment, or beliefs about aggregate demand, to be a source of fluctuations, orthogonal to those induced by changes in fundamentals such as technology or preferences.

Monetary policy, through its effect on the strategic interactions of firms and households, can potentially engender or inhibit such fluctuations. This paper addresses the role of monetary policy in a model in which sentiment-driven fluctuations can arise.

Specifically, I embed decision-making under uncertainty about endogenous outcomes into a New Keynesian model, building upon the framework proposed by Benhabib et al. (2015). A continuum of firms is linked through factor prices and aggregate demand externalities, as in the canonical model.

While such linkages provide a motive for coordination, firms lack common knowledge about the current economic state due to dispersed information. They commit to production (pricing) before outcomes are known, basing their decision on a signal that confounds aggregate and idiosyncratic demand. Aggregate demand is both an endogenous outcome and a source of correlation.

Dispersed information impedes coordination among firms, while endogenous signals correlate their actions. These features give rise to an equilibrium where sentiments, or beliefs about aggregate demand, can drive fluctuations.

To read more: https://www.bankofengland.co.uk/working-paper/2024/monetary-policy-and-sentiment-driven-fluctuations

https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2024/monetary-policy-and-sentiment-driven-fluctuations.pdf

Due to evolving legal landscape & changes in the framework of administrative law, Federal Reserve Board will soon seek public comment on significant changes to improve transparency of bank stress tests & reduce volatility of resulting capital requirements

In view of the evolving legal landscape, the Federal Reserve Board will soon seek public comment on significant changes to improve the transparency of its bank stress tests and to reduce the volatility of resulting capital buffer requirements.

The Board's stress test evaluates the resilience of large banks by estimating their losses, revenue, and capital levels under a hypothetical recession scenario that changes each year. Capital acts as a cushion to absorb losses and allows banks to continue lending to households and businesses even during a recession.

Since its inception over 15 years ago, large banks in the stress test have more than doubled their capital levels, an increase of more than $1 trillion.

The Board intends to propose changes that include, but are not limited to:

- disclosing and seeking public comment on all of the models that determine the hypothetical losses and revenue of banks under stress;

- averaging results over two years to reduce the year-over-year changes in the capital requirements that result from the stress test; and

- ensuring that the public can comment on the hypothetical scenarios used annually for the test, before the scenarios are finalized.

These proposed changes are not designed to materially affect overall capital requirements.

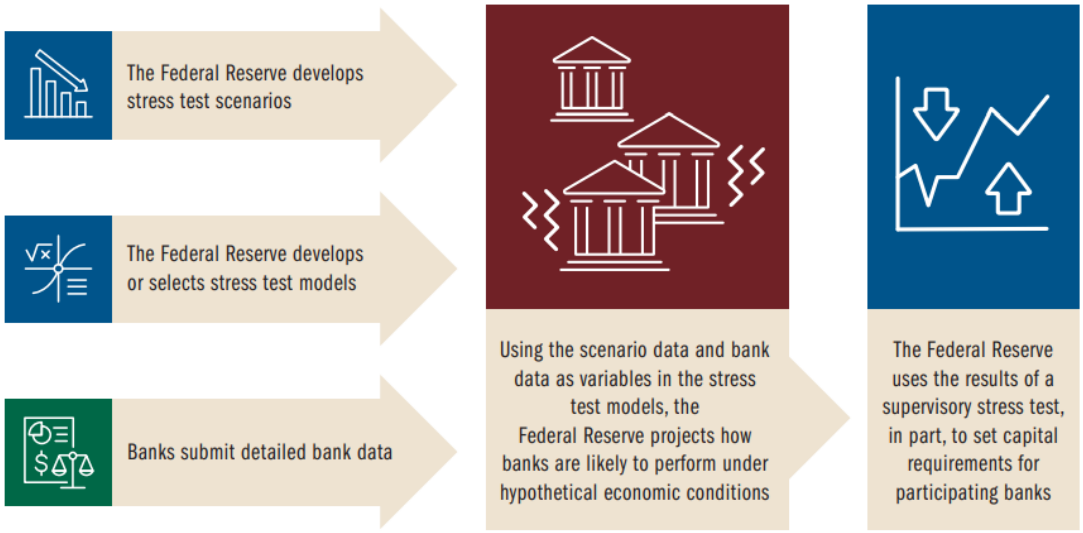
The framework of administrative law has changed significantly in recent years. The Board analyzed the current stress test in view of the evolving legal landscape and determined to modify the test in important respects to improve its resiliency.

The Board will continue its exploratory analysis, which assesses additional risks to the banking system in ways that are separate from the stress test. The analysis would be used to inform bank supervision and financial stability assessments. It will continue to be disclosed in aggregate and not affect bank capital requirements.

For the 2025 stress test, the Board plans to take immediate steps to reduce the volatility of the results and begin to improve model transparency. The Board intends to begin the public comment process on its comprehensive changes to the stress test during the early part of 2025.

Figure 1. How stress testing works for large banks

The Federal Reserve conducts stress tests to ensure that large banks are sufficiently capitalized and able to lend to households and businesses even in a severe recession. The stress tests evaluate the financial resilience of banks by estimating losses, revenues, expenses, and resulting capital levels under hypothetical economic conditions.



To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20241223a.htm

Public responses to consultation on Format for Incident Reporting Exchange (FIRE)

On 17 October 2024, the FSB published Format for Incident Reporting Exchange (FIRE): Consultation report. Interested parties were invited to provide written comments by 19 December 2024. The public comments received are available below.

▼ Responses received

- Bank Policy Institute (BPI)
- Deutsche Börse Group
- Financial Service Sector Coordinating Council (FSSCC)
- German Banking Industry Committee (GBIC)
- Global Federation of Insurance Associations (GFIA)
- Global Financial Markets Association
- Global Legal Entity Identifier Foundation
- Investment Company Institute (ICI)
- Institute of International Finance (IIF)

The FSB has developed FIRE to reduce fragmentation in the reporting of operational incidents, including cyber incidents, and enhance cross-border cooperation.

This consultation report sets out a common format that financial firms can use for the reporting of operational incidents, including cyber incidents. The proposed Format for Incident Reporting Exchange (FIRE) provides a set of common information items and is designed in a way to maximise flexibility and interoperability.
FIRE's features support flexibility for authorities that adopt the format in full or in part. For instance, of the 99 information items defined, 51 are optional, allowing authorities to decide which to implement based on their needs.

Incident reporting is a key mechanism for supervisors to monitor disruptions within financial firms. However, differences in reporting approaches across jurisdictions result in fragmented requirements and coordination challenges.

FIRE aims to promote convergence, address operational challenges arising from reporting to multiple authorities and foster better communication within and across jurisdictions.

The consultation package consists of:

(i) a 'human-readable' format,

(ii) a structured data model of FIRE using the reporting-language-agnostic Data Point Model method, and

(iii) a taxonomy in eXtensible Business Reporting Language (XBRL) as a sample machine-readable version of FIRE.

The taxonomy package is linked in the right-hand column of this page.

FIRE has been developed by the FSB in consultation with private sector participants.

The FSB invites comments on this consultation report and welcomes replies to the consultation questions by 19 December 2024.

Responses will be published on the FSB's website unless respondents expressly request otherwise.

Scope of FIRE

The design of FIRE covers reporting of operational incidents (inclusive of cyber incidents), primarily from financial institutions to financial authorities.[6] Previous FSB stocktakes identified that many authorities do not have a different approach or reporting mechanism for cyber incidents specifically. Rather, many frameworks treat cyber incident reporting as part of broader operational incident reporting. For that reason, the scope of FIRE extends beyond the FSB's previous work on cyber resilience.

To establish the boundary for incident types and underlying causes within the scope of FIRE, three additional terms and associated definitions are provided to complement equivalent cyber terminology found in the FSB Cyber Lexicon.[7]

Figure 1: 'Operational' terminology

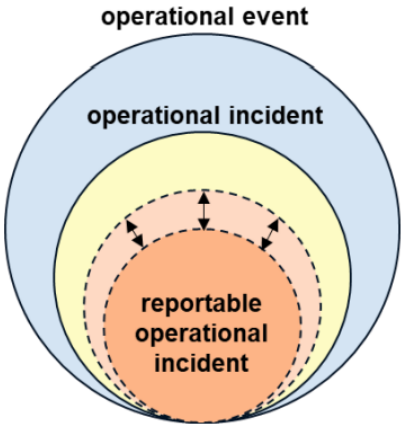
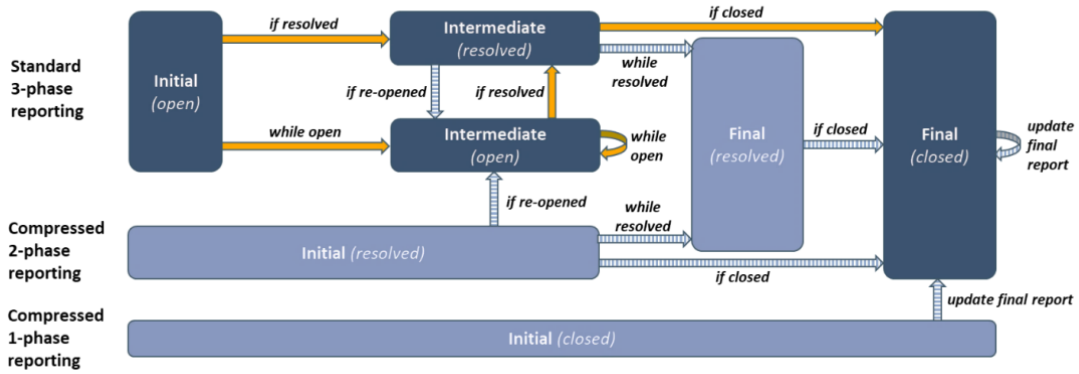
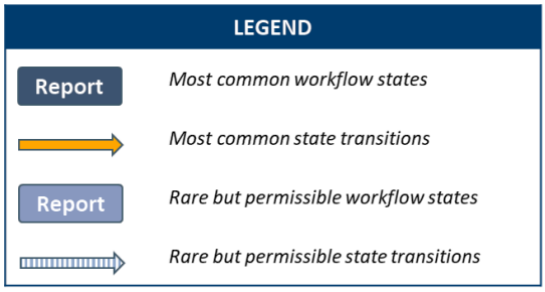


Figure 4: Report phase workflow and valid states

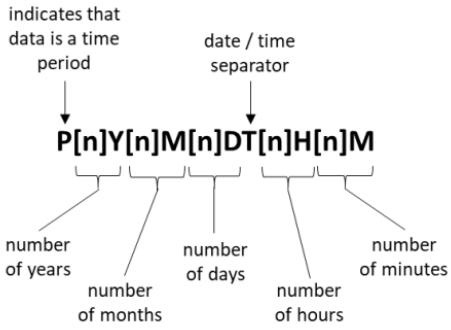




	Initial	Intermediate	Final
Open	✓	✓	✗
Resolved	✓	✓	✓
Closed	✓	✗	✓

Estimated resolution timeframe

An information item for providing an **estimated timeframe for incident resolution** is included within the format such that the reporting entity can provide an indicative view to receiving entities of when they might expect the incident to be brought under control. The ISO 8601 standard[19] is used to record time periods in a consistent fashion. Each time element can be optionally expressed, allowing reporting entities to provide estimates in minutes, hours, days, months or even years.



To read more: https://www.fsb.org/2025/01/public-responses-to-consultation-on-format-for-incident-reporting-exchange-fire/

FSB FINANCIAL STABILITY BOARD

Format for Incident Reporting Exchange (FIRE)

Consultation report

Disclaimer

The International Association of Hedge Funds Professionals (IAHFP)(hereinafter "Association") enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice;

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the courts might place on the matters at issue.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

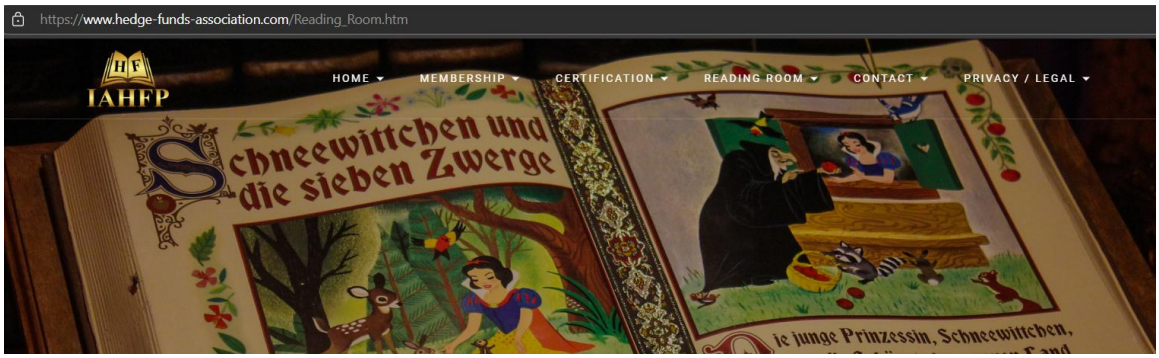
Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems. The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

International Association of Hedge Funds Professionals (IAHFP)

The Association is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Our reading room:
https://www.hedge-funds-association.com/Reading_Room.htm



"Mirror, mirror on the wall, who in this land is fairest of all?"

Children's fiction can open up new perspectives for adults. Black swan events, exercising (or failing to exercise) the zero trust principle, risks and opportunities are all there.

Investigating the facts is the next pleasure. In 1994, Eckhard Sander claimed that the character of Snow White was based on the life of Margaretha von Waldeck, a German countess born in 1533. At the age of 16, Margaretha was forced by her stepmother, Katharina of Hatzfeld, to move away to Brussels. There, Margaretha fell in love with a prince who would later become Philip II of Spain.

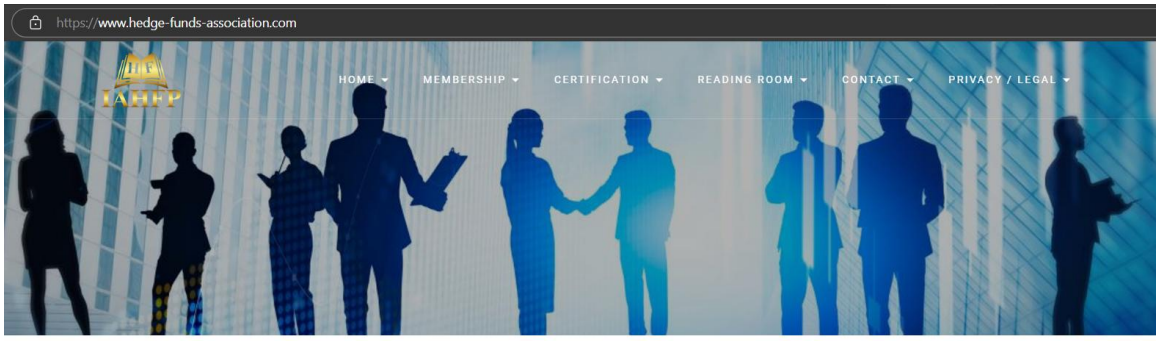
Graham Anderson compares the story of Snow White to the Roman legend of Chione, recorded in Ovid's Metamorphoses. The name Chione means "snow" in Greek and, in the story, she is described as the most beautiful woman in the land, so beautiful that the gods Apollo and Hermes both fell in love with her.

For Snow White, the death of her real mother and the arrival of a stepmother is a disaster. Snow White is forced to leave home, but she discovers who she is, and moves along the path to self-discovery and resilience. This is a story about development set in motion by the arrival of evil. Does it look familiar?

Contact Us

Lyn Spooner
Email: lyn@hedge-funds-association.com

George Lekatis
President of the IAHFP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@hedge-funds-association.com
Web: www.hedge-funds-association.com



WELCOME

You are a risk and compliance officer working for hedge funds, or perhaps a consultant or analyst. You are part of a team that offers investors a unique range of strategies tailored to meet their specific investment objectives.

Your fund has the ability to generate positive returns in both rising and falling markets, and gives investors opportunities for absolute returns, skill-based strategies and diversification.