Riunione del 18 novembre 2024

Alberto Balestreri

Materiale riservato ai membri della Commissione Banche, Intermediari Finanziari ed Assicurazione dell'ODCEC di Milano

Commissione Banche, Intermediari finanziari e Assicurazioni

Ordine del giorno

1. Esame ed approvazione dei verbali delle precedenti riunioni;
2. Digital resilience in the Italian Financial Sector: evidences from the supervisory incident reporting framework –Banca d'Italia.
3. Evolving IT and cybersecurity risks – SSM Supervision Newsletter
4. Eventi formativi;
5. Varie ed eventuali.

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB – "The art of bending without breaking – banking on operational resilience"

"Now, you might primarily associate a bank's resilience with its financial strength – particularly given the significant increases in capital and liquidity buffers following the post-crisis reforms. But I'll highlight why financial resilience alone is far from sufficient to weather the storms brewing over today's risk landscape.

Consider the example of **Amsterdam Trade Bank (ATB)**, which filed for bankruptcy although it had ample capital and liquidity. What went wrong? **Imagine the bank's credit officers turning up at the office one Friday morning in April 2022, trying to access their documents – and all they see on the screen is that access is denied.** Why?

Owing to sanctions ATB had lost access to its IT systems, which were run by third-party providers. As a result, the bank couldn't provide banking services anymore. **There weren't adequate contingency arrangements in place – because a scenario in which IT systems weren't operable had seemed too unrealistic – and so the bank had to close shop.**

https://amsterdamtradebank.com/

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB – "The art of bending without breaking – banking on operational resilience"

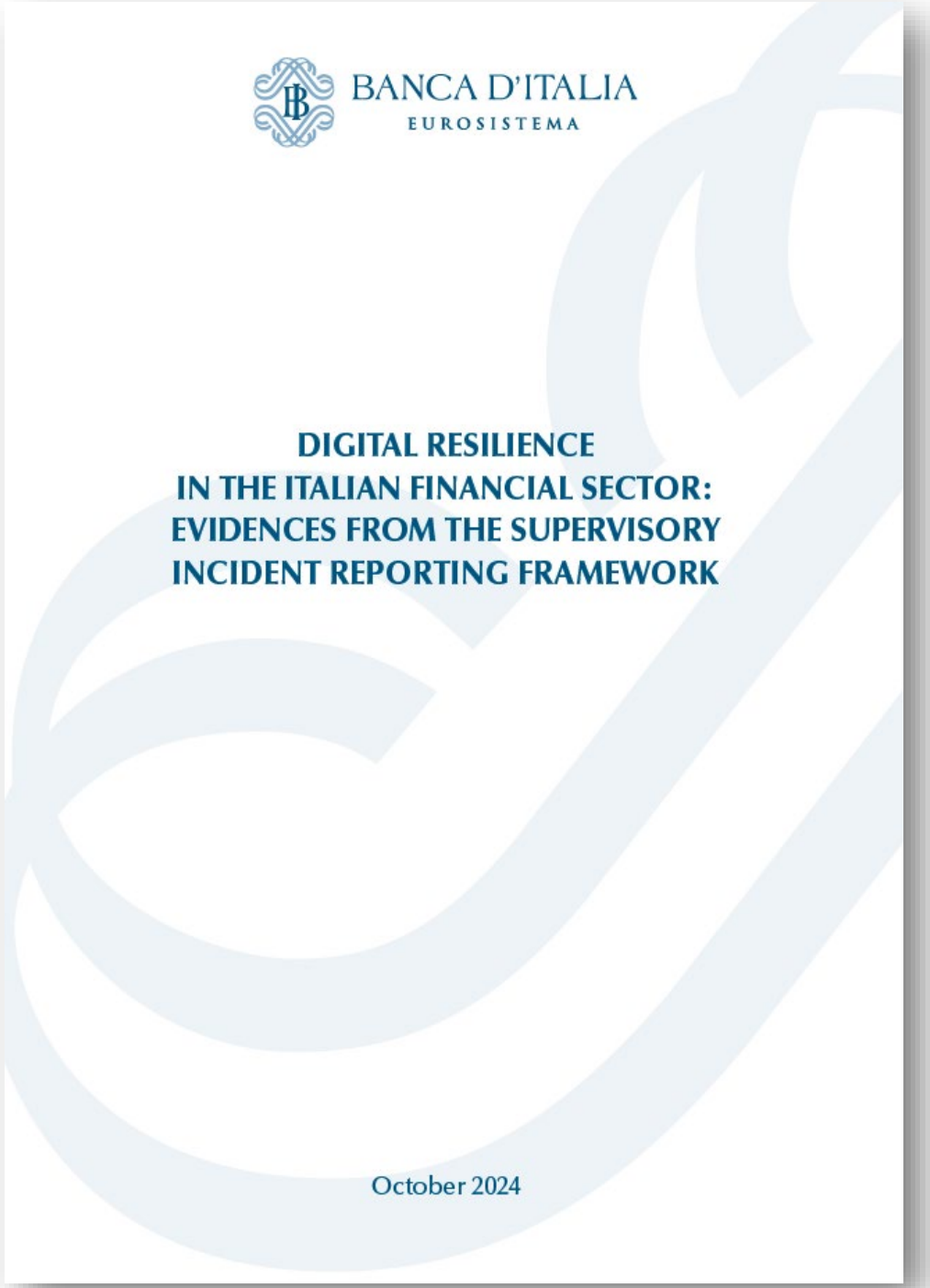
"In 2023 when the New York arm of an investment bank was hit by a ransomware attack, it literally sent a runner with a USB stick across downtown Manhattan to help settle trades in the $25 trillion US treasury market.

And most recently, the CrowdStrike incident caused the operating system of a major provider to crash, displaying the so-called blue screen of death, leading to significant disruptions across sectors – including at a few banks."

https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240904~629e00231e.en.html

2. Digital resilience in the Italian Financial Sector: evidences from the supervisory incident reporting framework –Banca d’Italia.

1. Aumento degli incidenti segnalati e riduzione del sotto-reporting;
2. Aumento del ruolo dei fornitori terzi;
3. Implementazione di DORA come fattore di ampliamento degli strumenti a disposizione della Vigilanza;
4. Sviluppo delle metodologie di governance dei rischi ICT e dei rischi Cyber;
5. Nuovo ruolo dei consiglieri indipendenti e dei membri del Collegio Sindacale.



Framework per il reporting

1. Banca d'Italia, *Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza*
2. European Banking Authority, *Revised Guidelines on major incident reporting under PSD2 of 7 March 2017* and subsequent updates.
3. European Central Bank, *IT risk – ECB to roll out cyber incident reporting framework* 2017.
4. *RTS connessi al Regolamento DORA*

Table 1

FINANCIAL ENTITIES SUBJECT TO THE INCIDENT REPORTING FRAMEWORK DURING 2023

FINANCIAL ENTITY	NUMBER
Italian significant banks or banking groups	12
Branches of non-EU banks or banking groups	8
Subsidiaries of EU banks or banking groups	8
Italian less significant banks or banking groups	76
Payment institutions	43
Electronic money institutions	10

Figure 1

NUMBER OF REPORTED INCIDENTS IN ITALY

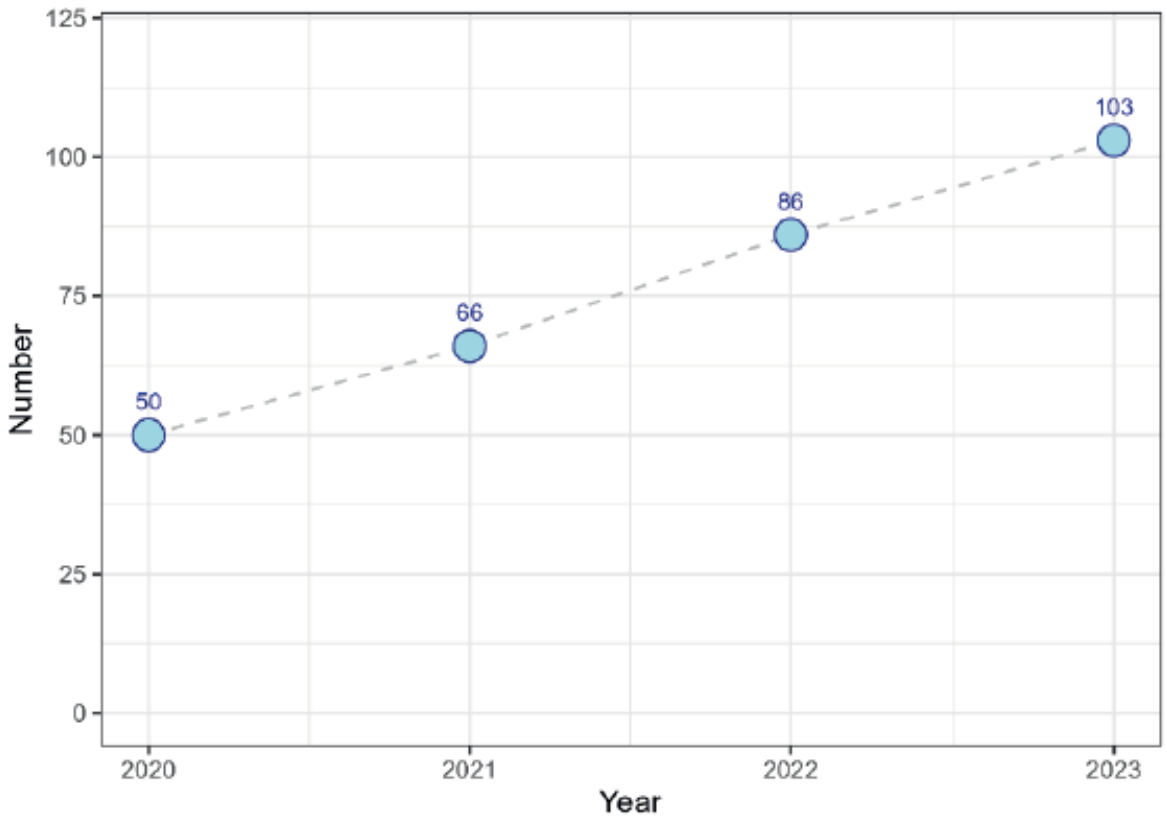
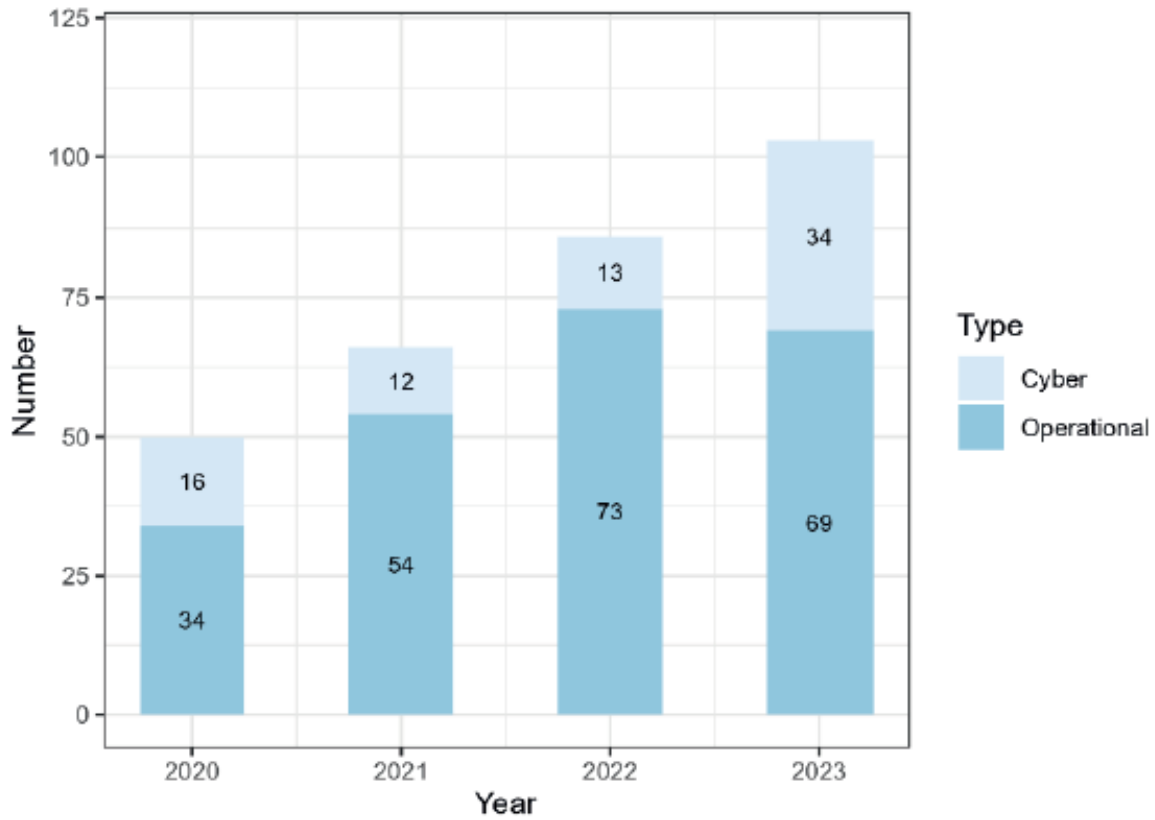


Figure 2

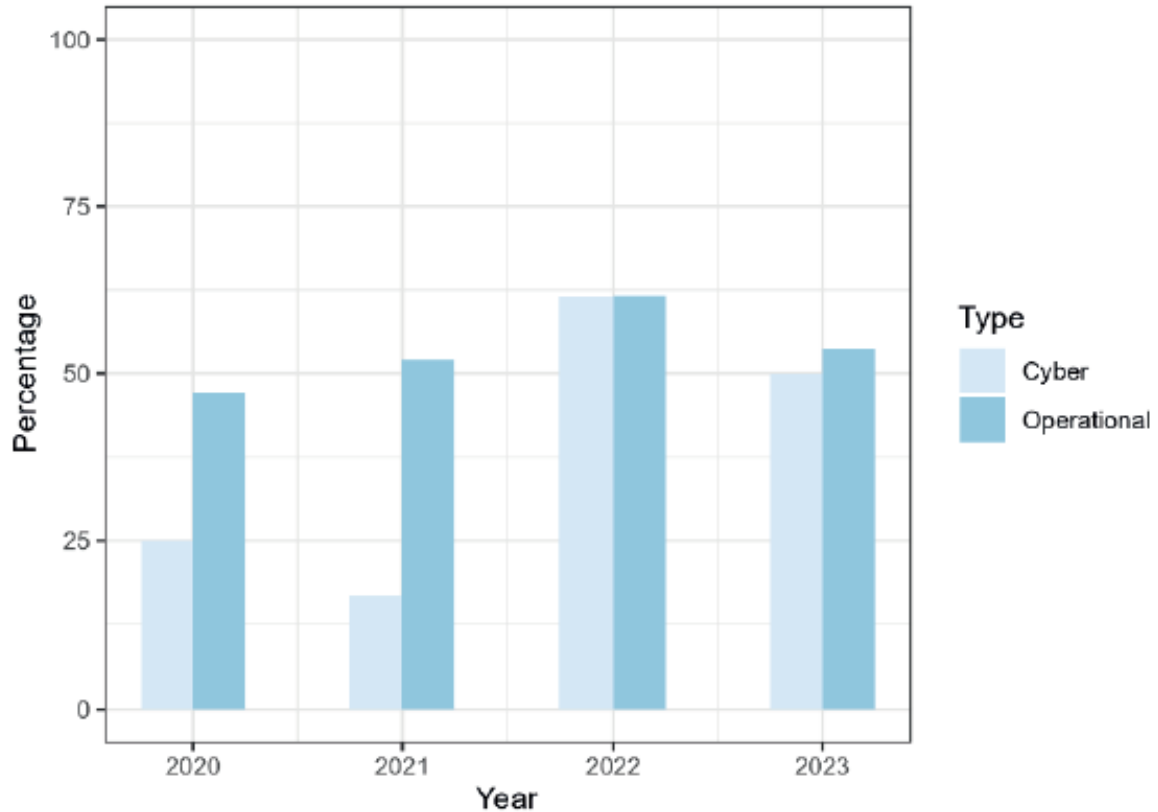
TYPE OF INCIDENTS REPORTED (1)



(1) Cyber incidents include both cyber attacks and other incidents classified as cyber in the incident reporting framework, such as accidental data leakages.

Figure 3

THIRD-PARTY PROVIDER INVOLVEMENT IN REPORTED INCIDENTS



A. Operational incidents

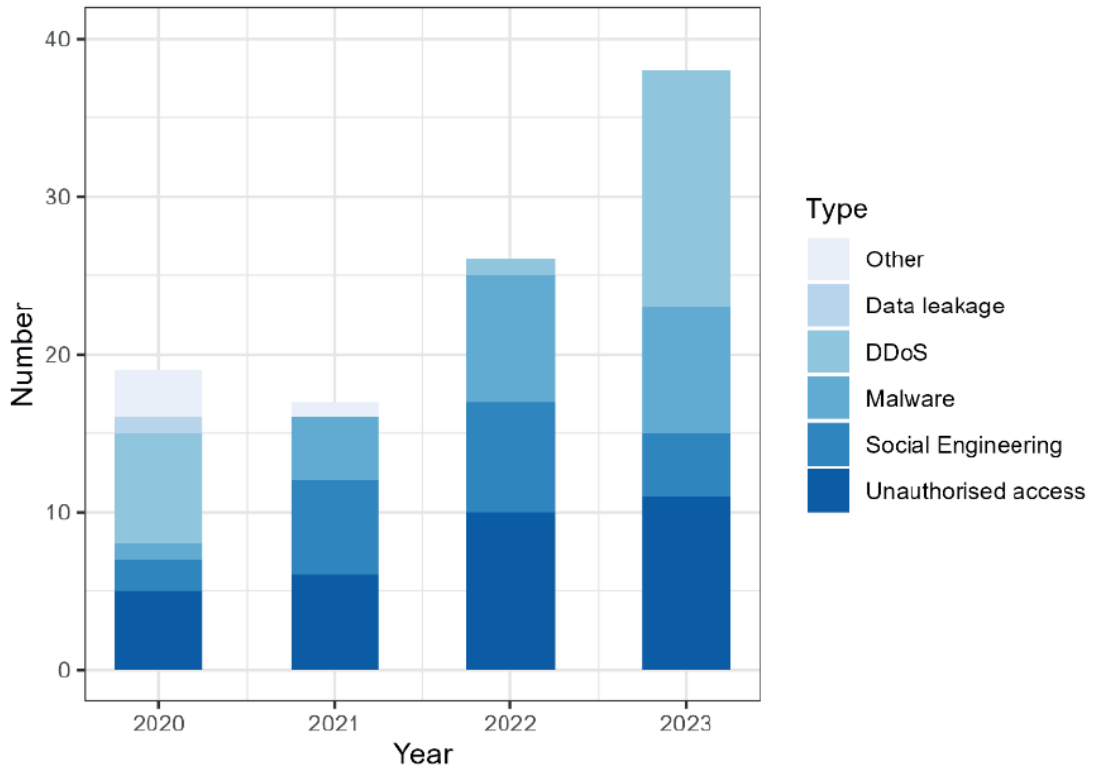
1. Software failures (malfunctions/bugs, incorrect update operations, application modifications);
2. Hardware failures (connectivity and/or network equipment problems);
3. Poor ability of the systems to adequately manage operational peaks (for example in the event of an increase in traffic generated by users);
4. Incidents related to human errors and internal processes;
5. change management processes (so-called ICT change risk) > human errors and incorrect system configurations.

B. Cyber incidents

Figure 4

TYPE OF CYBER ATTACK PERFORMED

(multiple classification possible)



Principali fattori di debolezza

i. Limited level of security awareness among employees with specific reference to risks emerging from social engineering attacks;

ii. Management of remote access applications and/or procedures for remote access to workstations not always adequate (e.g., presence of unplanned remote access tools, identification of operators before granting remote access, single factor authentication procedure);

iii. Application configurations not always adequate (e.g., storage of credentials in the browser); Inadequate risk assessment processes (e.g., branch computer applications operational even while they are closed, inadequate physical security on the entities' premises);

iv. Lack or imperfect application of the anti-DDoS systems, including the lack of coverage towards some internet facing applications and the lack of appropriate stress-testing of the defence measures in place;

v. Delays in the patching processes.

vi. Strengthen and improve the security of the Supplier's systems from a technical and organizational perspective

3. Evolving IT and cybersecurity risks – SSM Supervision Newsletter. 13 november 2024

ECB Banking Supervision continuously evaluates banks' management of IT risk, with supervisors' findings from on-site inspections and banks' IT risk reporting providing two major sources of information.

As has been emphasised in recent years, **banks still have work to do across a range of measures.** They **must ensure** that their defences and their risk management framework are fit for purpose.

IT risks and cyber threats are constantly evolving as bad actors innovate and try to find new ways of penetrating a bank's defences.

It is therefore critical that banks invest in their resilience and that they can quickly respond and recover if necessary.

1. Rising cybersecurity threats: ransomware and ICT third-party service providers

The banking sector has witnessed a surge in significant cyber incidents over the last year.

There has been no major impact to date, but **banks should not become complacent** – instead, they should stay alert to threats and well prepared to deal with them.

Ransomware attacks have emerged as a particularly concerning threat with the potential to disrupt banking operations and compromise sensitive information.

Attacks on information and communication technology (ICT) **third-party service providers** have highlighted the risk of spillover effects: weaknesses in one provider can cascade and affect not just one but many interconnected banks.

Some banks are still facing challenges in implementing basic cybersecurity controls and many key areas remain insufficiently developed in certain banks.

These areas include security testing, vulnerability management, network segmentation, security detection, response and recovery capabilities and identity and access management.

Moreover, IT security risk assessment frameworks require significant improvement.

2. IT outsourcing risk: navigating dependencies and concentration

The already-substantial reliance on third-party service providers is continuing to grow.

Cloud expenses are increasing, although at a slower pace than last year.

Banks **need to understand the potential for concentration risk** and keep a watchful eye out for sectoral developments.

The Digital Operational Resilience Act, which will enter into force in January 2025, emphasises that the ultimate responsibility for managing such risks lies with banks' boards. This means that banks need to ensure they have appropriate management and oversight of outsourcing arrangements in place.

This should encompass pre-outsourcing analysis, continuous monitoring of service levels and contract adherence, adequate exit strategies (regularly tested) and the involvement of relevant third-party service providers in crisis response plans.

Supervisory reviews carried out in 2023 identified weaknesses in these areas, underscoring the need for enhanced governance and oversight.

3. IT change risk: managing change and innovation

As banks' IT infrastructure evolves, the number of IT projects (and related spending) is on the rise.

Many of these projects are part of **broader digital transformation initiatives.**

Improving IT infrastructure is essential but **IT changes, whether large or small, must be managed thoroughly.**

This is especially important because incidents related to IT changes remain the most prevalent root cause of unplanned downtime in critical IT systems.

4. IT availability risk: preparing for the inevitable

IT incidents can affect any organisation, including banks.

Adequate preparation and regular testing are crucial to achieve a higher level of operational resilience.

Banks must establish **mature frameworks** in which business and technology functions are fully aligned to optimise incident management, business continuity management and crisis communication.

Several clear weaknesses were identified in these areas. **Weaknesses included outdated or incomplete business continuity plans, a lack of formal incident management procedures, insufficient recovery tests, poorly defined and tested recovery objectives and inadequate recovery priorities which are not based on proper risk assessment.**

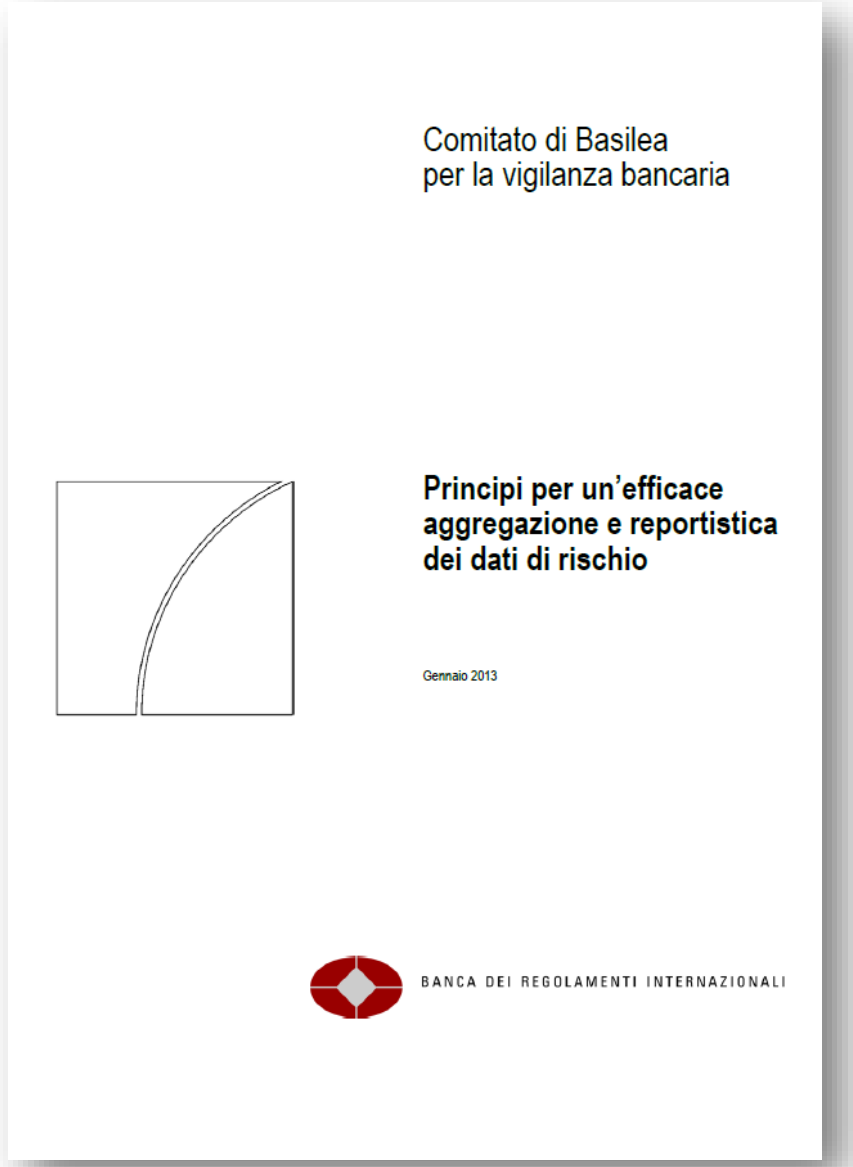
In addition, **the absence of documented crisis communication strategies** could lower the effectiveness of responses during major IT-related incidents.

5. Data quality management: addressing the weakest link

Data quality management remains the weakest risk control domain in the banking sector, having shown insufficient year-on-year improvement.

Supervisory assessments have identified some **deficiencies in respect of key controls for data quality management, the management of data architecture models and the implementation of "golden sources".**

In line with the Basel Committee on Banking Supervision's principles for effective risk data aggregation and risk reporting, it is crucial **to prioritise risk data aggregation and risk reporting projects to enhance data quality, ensure accurate risk assessment and support informed decision-making.**



6. IT governance, risk management and IT audits: strengthening oversight

Effective IT governance, risk management and IT audits are essential for robust cybersecurity and IT risk management.

In some banks there are gaps in fundamental, as is the case for IT asset management and the key risk indicators reported to the management body. **Effective IT asset management is a prerequisite for effective IT risk management and IT change management.**

It is crucial to address gaps to enhance overall resilience.

Conclusion

The evolving IT landscape and cybersecurity risks present significant challenges for the banking sector.

The increasing frequency and sophistication of cyber incidents, in particular ransomware attacks and breaches involving ICT third-party service providers, underscore the **critical need for robust cybersecurity measures and effective IT and cyber risk management.**

This is crucial both within banks and across third-party service providers.

Conclusion

By **addressing the identified weaknesses and enhancing their risk management frameworks**, banks can improve their resilience.

Banks should focus on:

- continuously improving cybersecurity controls;
- managing IT outsourcing;
- managing IT change risks;
- robust incident management;
- business continuity plans;
- strong IT governance.

These are essential bulwarks for safeguarding the integrity and stability of the banking sector in 2024 and beyond.

Conclusion

Over the past five years, ECB Banking Supervision has consistently identified operational resilience and in particular IT outsourcing and IT security/cyber risks as a supervisory priority, and it will continue assessing those risks via on-site inspections and targeted reviews of outsourcing arrangements and cyber resilience.

From 2025 onwards, ECB banking supervision will further increase its efforts to ensure compliance with DORA regulation.

4. Eventi formativi

SAVE THE DATE

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

2024

MARTEDI

19

NOVEMBRE

14:30 | 17:30

MACRO-MICRO: QUALI LE ATTESE PER IL PROSSIMO 2025?

WEBINAR **ZOOM** > ISCRIZIONE > **CLICCA QUI**

SALUTI DI BENVENUTO:

MARCELLA CARADONNA
PRESIDENTE ODCEC MILANO

NANCY SATURNINO
CONSIGLIERE DELEGATO ODCEC MILANO

INTRODUZIONE DEI LAVORI:

UBERTO BARIGOZZI | VICE PRESIDENTE COMMISSIONE BANCHE, INTERMEDIARI FINANZIARI E ASSICURAZIONI ODCEC MILANO

IL QUADRO MACROECONOMICO

ALBERTO BALESTRERI
PRESIDENTE COMMISSIONE BANCHE, INTERMEDIARI FINANZIARI E ASSICURAZIONI ODCEC MILANO

I MERCATI FINANZIARI SOSPESI TRA POLITICA MONETARIA E POLITICA INTERNAZIONALE

GIAN PAOLO RIVANO
AMARANTO SIM S.P.A.

LE ATTESE PER IL MERCATO AZIONARIO 2025

ALESSANDRO STANZINI
BANCA ALETTI GRUPPO BANCO BPM

IL MERCATO OBBLIGAZIONARIO DEL PROSSIMO 2025

PAOLO MOIA
ZURICH BANK

IL PRIVATE MARKET COME STRUMENTO ALTERNATIVO DI INVESTIMENTO

MANUELA BERNARDELLI
UBS EUROPE

COMMISSIONE BANCHE, INTERMEDIARI FINANZIARI E ASSICURAZIONI

3 CFP

Ai sensi del Regolamento UE n. 2016/679 nonché del D.lgs. n. 196/2003 e successive modifiche e integrazioni, **l'evento potrebbe essere oggetto di videoregistrazione**. In caso di adesione alla iniziativa, la partecipazione sarà resa visibile a tutti gli uditori.

Riunioni programmate per il 2024

1. ~~Martedì 16 gennaio, ore 18,00 – MS Teams~~
2. ~~Martedì 13 febbraio, ore 18,00 – MS Teams~~
3. ~~Martedì 19 marzo, ore 18,00 – MS Teams~~
4. ~~Martedì 16 aprile, ore 18,00 – MS Teams~~
5. ~~Martedì 14 maggio, ore 18,00 – MS Teams~~
6. ~~Martedì 11 giugno, ore 18,00 – MS Teams~~
7. ~~Martedì 17 settembre, ore 18,00 – MS Teams~~
8. ~~Lunedì 18 novembre, ore 18,00 – MS Teams~~
9. **Martedì 10 dicembre, ore 18,00 – MS Teams**

5. Varie ed eventuali