Il termometro dei mercati finanziari (7 dicembre 2018)

a cura di Emilio Barucci e Daniele Marazzina

08/12/2018 08:34

L'iniziativa di Finriskalert.it "Il termometro dei mercati finanziari" vuole presentare un indicatore settimanale sul grado di turbolenza/tensione dei mercati finanziari, con particolare attenzione all'Italia.

07-dic-18	Legenda					
Valutazione complessiva		Calma		↑	in miglioramento	
		Turbolenza		↔	stabile	
		Tensione		↓	in peggioramento	
Mercati italiani	07-dic	30-nov	23-nov	16-nov	09-nov	Tendenza
Rendimento borsa italiana	-2.33	2.53	-0.87	-1.97	-0.68	↓
Volatilità implicita borsa italiana	22.12	21.13	21.00	21.31	20.26	↓
Future borsa italiana	18615	19200	18695	18810	19205	↓
CDS principali banche 10Ysub	615.97	631.14	632.12	628.91	602.17	↑
Tasso di interesse ITA 2Y	0.74	0.85	0.97	1.34	1.20	↑
Spread ITA 10Y/2Y	2.39	2.36	2.44	2.15	2.20	↔
Mercati europei	07-dic	30-nov	23-nov	16-nov	09-nov	Tendenza
Rendimento borsa europea	-3.61	1.15	-1.37	-1.51	0.47	↓
Volatilità implicita borsa europea	18.01	15.44	15.79	15.16	14.03	↓
Rendimento borsa ITA/Europa	1.28	1.39	0.50	-0.46	-1.15	↔
Spread ITA/GER	2.88	2.90	3.08	3.12	2.99	↑
Spread EU/GER	1.03	1.01	1.08	1.07	1.03	↔
Politica monetaria, cambi e altro	07-dic	30-nov	23-nov	16-nov	09-nov	Tendenza
Euro/Dollaro	1.139	1.132	1.134	1.139	1.135	↑
Spread US/GER 10Y	2.60	2.70	2.72	2.70	2.78	↑
Euribor 6M	-0.246	-0.253	-0.257	-0.257	-0.257	↓
Prezzo Oro	1246	1219	1223	1221	1211	↓
Spread 10Y/2Y Euro Swap Curve	0.99	1.03	1.04	1.06	1.08	↑

Significato degli indicatori

- Rendimento borsa italiana: rendimento settimanale dell'indice della borsa italiana FTSEMIB;
- Volatilità implicita borsa italiana: volatilità implicita calcolata considerando le opzioni at-the-money sul FTSEMIB a 3 mesi;
- Future borsa italiana: valore del future sul FTSEMIB;
- CDS principali banche 10Ysub: CDS medio delle obbligazioni subordinate a 10 anni delle principali banche italiane (Unicredit, Intesa San Paolo, MPS, Banco BPM);
- Tasso di interesse ITA 2Y: tasso di interesse costruito sulla curva dei BTP con scadenza a due anni;
- Spread ITA 10Y/2Y : differenza del tasso di interesse dei BTP a 10 anni e a 2 anni;
- Rendimento borsa europea: rendimento settimanale dell'indice delle borse europee Eurostoxx;
- Volatilità implicita borsa europea: volatilità implicita calcolata sulle opzioni at-the-money sull'indice Eurostoxx a scadenza 3 mesi;
- Rendimento borsa ITA/Europa: differenza tra il rendimento settimanale della borsa italiana e quello delle borse europee, calcolato sugli indici FTSEMIB e Eurostoxx;
- Spread ITA/GER: differenza tra i tassi di interesse italiani e tedeschi a 10 anni;
- Spread EU/GER: differenza media tra i tassi di interesse dei principali paesi europei (Francia, Belgio, Spagna, Italia, Olanda) e quelli tedeschi a 10 anni;
- Euro/dollaro: tasso di cambio euro/dollaro;
- Spread US/GER 10Y: spread tra i tassi di interesse degli Stati Uniti e quelli tedeschi con scadenza 10 anni;
- Prezzo Oro: quotazione dell'oro (in USD)
- Spread 10Y/2Y Euro Swap Curve: differenza del tasso della curva EURO ZONE IRS 3M a 10Y e 2Y;
- Euribor 6M: tasso euribor a 6 mesi.

I colori sono assegnati in un'ottica VaR: se il valore riportato è superiore (inferiore) al quantile al 15%, il colore utilizzato è l'arancione. Se il valore riportato è superiore (inferiore) al quantile al 5% il colore utilizzato è il rosso. La banda (verso l'alto o verso il basso) viene selezionata, a seconda dell'indicatore, nella direzione dell'instabilità del mercato. I quantili vengono ricostruiti prendendo la serie storica di un anno di osservazioni: ad esempio, un valore in una casella rossa significa che appartiene al 5% dei valori meno positivi riscontrati nell'ultimo anno. Per le prime tre voci della sezione "Politica Monetaria", le bande per definire il colore sono simmetriche (valori in positivo e in negativo). I dati riportati provengono dal database Thomson Reuters. Infine, la tendenza mostra la dinamica in atto e viene rappresentata dalle frecce: ↑, ↓, ↔ indicano rispettivamente miglioramento, peggioramento, stabilità.

Chatbot: il miglior modo di

trovare la risposta prima ancora di cercarla

a cura di Deloitte Italia

07/12/2018 11:17

"Può una macchina pensare come un essere umano? Molti dicono di no. Il problema è che è una domanda stupida. È ovvio che le macchine non possono pensare come le persone. Una macchina è diversa da una persona e pensa in modo diverso. La domanda interessante è poiché qualcosa pensa diversamente da noi vuol forse dire che non sta pensando? "

Nel 1950 Alan Turing cercava di spiegare come un computer potesse comportarsi come un essere umano. La sua teoria "il gioco dell'imitazione" apriva la pista a quello che circa mezzo secolo più tardi avrebbe caratterizzato il processo di trasformazione dell'economia in industria 4.0 basata, cioè, su una produzione industriale del tutto automatizzata e interconnessa.

Proprio nella teoria di Alan Turing, risiede il principio di funzionamento dei Chatbot che ad oggi costituisce un fenomeno in ampia crescita e che, secondo un'analisi condotta da Gartner, tenderà ad aumentare ancora entro il 2020[1].

Cosa sono i Chatbot

I Chatbot sono software progettati per avere una conversazione con un utente attraverso messaggi di testo o vocali (c.d. NLP-Natural Language Process).

Alla base del funzionamento dei Chatbot ci sono algoritmi di Intelligenza Artificiale, una disciplina che comprende teorie e tecniche rivolte allo sviluppo di macchine in grado di svolgere compiti e azioni tipici della intelligenza umana.

Ciò che distingue i diversi prodotti di Intelligenza Artificiale sono i modelli di apprendimento[1] che possono essere principalmente distinti tra *Machine Learning* e *Deep Learning*.

Il *Machine Learning* comprende i metodi con cui le macchine riescono ad apprendere come compiere delle attività, ad esempio, attraverso l'analisi dei risultati e la correzione degli errori del proprio comportamento precedente.

Il *Deep Learning*, invece, tende proprio a emulare la mente umana attraverso la programmazione di reti neurali, ispirandosi al funzionamento dei neuroni biologici nelle fasi di apprendimento e riconoscimento.

Come, Dove e Quando si applicano i Chatbot

Come - I Chatbot si applicano ogniqualvolta viene ricercata una informazione sia questa un codice, un dato una procedura etc.. Tanto più la richiesta è chiara e dettagliata quanto più sarà rapido e preciso il Chatbot a fornire la risposta. La comprensione della domanda e dell'intento sottostante riveste quindi un ruolo cruciale. Originariamente i Chatbot nascono con le risposte organizzate in percorsi logici e associate tramite *Machine Learning* a una o più parole chiave, se nella domanda è presente la parola chiave il Chatbot identifica il percorso da seguire per arrivare puntualmente all'informazione richiesta. Spesso un percorso ha più diramazioni ed è allora che il Chatbot pone una domanda utile a raccogliere ulteriori elementi e prendere la "strada giusta". È importante tenere a mente che tutti gli input che un utente da in pasto ad un Chatbot concorrono ad aumentare la capacità degli stessi di riconoscere l'intento sottostante ogni domanda grazie al *Deep Learning* sui dati storici. La crescente mole di dati ha accelerato il processo di evoluzione dei Chatbot che riescono oggi a comprendere il significato della domanda senza passare dalle parole chiave.

Dove — Sempre più spesso sui siti internet compare l'icona per chiedere informazioni via chat in aggiunta ai contatti telefonici e mail. A presidio di questi canali di comunicazione vengono solitamente utilizzati i Chatbot per vantaggi di economicità, efficienza e qualità rispetto ad un approccio tradizionale:

- la diffusione di internet implica che utenti sparsi per il mondo possano accedere ad un sito in qualunque momento e deve quindi essere garantita copertura 24/7 per eventuali richieste di supporto;
- nella maggioranza dei casi le richieste di informazioni riguardano tematiche ricorrenti la cui risoluzione può essere gestita in automatico in modo che gli operatori in carne ed ossa possano dedicarsi alle casistiche più particolari/complicate;
- l'acquisizione e aggiornamento delle conoscenze necessarie a garantire risposte affidabili e tempestive avviene mediante un processo iterativo di *continuous improvement* diversamente dai Customer Care tradizionali dove gli operatori devono essere formati, costantemente aggiornati e sostituiti in caso di assenza o dimissioni.

Quando — Nell'era di Google siamo tutti abituati a ricercare/ottenere risposta in pochi secondi e nessuno è più disposto ad attendere, o peggio ancora, ad essere messo in attesa per avere un'informazione. Si è di fatto creato un benchmark con cui misurare i tempi di risposta di qualsiasi richiesta di supporto sia su canali telefonici che digitali. I Chatbot permettono di gestire le comunicazioni in modalità "botta e risposta" tenendo alto il livello di ingaggio dell'utente che spesso non si rende neanche conto di interagire con un bot. Ma fino a che punto è lecito utilizzare i Chatbot all'insaputa dell'utente? Noi siamo dell'avviso che un utente in cerca di un'informazione sia interessato ad avere una risposta precisa e puntuale piuttosto che curarsi del metodo utilizzato per fornirla. In fin dei conti se il risultato di una moltiplicazione è giusto, a chi importa sapere com'è stato calcolato?

I Chatbot nel settore finanziario

Il ricorso ai Chatbot rappresenta un trend in crescita giustificato, oltre che dalla profonda trasformazione digitale che sta travolgendo tutte le Industry, dalla necessità di trovare nuove modalità di comunicare con *Millennial e Digital Native*.

A livello mondiale sono molte le Industry che stanno intervenendo soprattutto sull'ambito Customer Care dove ogni anno vengono spesi circa €1.300 miliardi per gestire oltre 265 miliardi di richieste[2]. Da uno studio sul mercato US[3], si stima che i Chatbot permetteranno di ridurre il costo del Customer Care del 30% generando benefici per il cliente finale e per l'organizzazione grazie alla velocizzazione dei tempi di risposta e

alla riduzione del backlog. Nell'ambito dei Financial Services, il potenziale dei Chatbot non si limita ad evolvere i canali di comunicazione esistenti ma permette alle istituzioni di creare nuove modalità di interazione con la clientela facilitando il percorso di trasformazione dall'erogazione di servizi finanziari a piattaforma accessibile 24/7 a supporto di molteplici esigenze non più solo finanziare.

La clientela deve essere "educata" a relazionarsi con una Banca a portata di click attraverso un linguaggio diverso dalla classica terminologia bancaria in modo da stimolare la propensione all'utilizzo delle funzionalità digitali. I Chatbot rivestono un ruolo chiave nell'accelerare il processo di sviluppo della cultura finanziaria dei clienti, possono infatti agire anche in modalità proattiva ad esempio segnalando eventi che intervengono sul conto corrente (es. accredito di una fattura attiva) per "catturare" l'attenzione e proporre poi ulteriori azioni (es. trasferimento su deposito vincolato) volte ad ottimizzare la posizione.

In definitiva i Chatbot assolvono l'arduo compito di supportare il cliente per semplificare un'operatività bancaria mediamente complessa stimolando una gestione attiva della propria situazione finanziaria.

Conclusione

I Chatbot rappresentano un punto di non ritorno nel rapporto uomo-macchina, fino ad oggi l'accesso alla tecnologia presupponeva la presenza di competenze sempre più elementari (es. bambini di 4 anni abilissimi utilizzatori di Ipad) ma comunque necessarie (es. per vedere i cartoni animati bisogna saper accedere all'applicazione). D'ora in avanti l'interazione uomo-macchina evolverà con dinamiche molto più simili a quelle sociali, cosi' come l'essere umano impara dagli errori (commessi direttamente o tramandati dalla storia) cosi' anche le macchine impareranno dagli errori dell'uomo. È bene ricordare che i Chatbot accumulano enormi moli di dati dalle interazioni con gli utenti e che una quota parte significativa è fisiologicamente errata ma grazie al *Deep Learning* le anomalie con il tempo vengono identificate e isolate permettendo alla macchina di imparare come irrobustire il proprio modello di conoscenze. Non è un futuro troppo lontano quello in cui i Chatbot sapranno prima di noi cosa stiamo per chiedergli e ci forniranno la risposta ancor prima della domanda.

Giacomo Mazzanti — Director Deloitte Consulting

Nicole Vismara — Manager Deloitte Consulting

Sonia Salotto — Consultant Deloitte Consulting

Note

[1] "Cos'è l'Intelligenza Artificiale, perché tutti né parlano e quali sono gli ambiti applicativi", AI for Business, Agosto 2018

[2] "How chatbots can help reduce customer service costs by 30%", IBM, October 2017

[3] "The chatbots explainer", BI Intelligence, 2016

BIS: Clouds — emerging prudential approaches for insurance companies

08/12/2018 10:23

Insurers have made increasing use of cloud computing in recent years. Cloud services were initially applied to business support functions, such as customer management or collaboration applications. Currently, cloud computing is being used in core business functions, such as product development, distribution, underwriting or claims administration.

Cloud computing brings a number of benefits to the insurance industry. It lets insurers share available-on-demand networks, servers, storage, application and services that can be rapidly scaled up or down, and accessed anytime and anywhere. In this way, cloud computing allows insurers to quickly launch new products and services, make business processes more efficient and reduce information technology (IT) costs.

The use of third-party cloud computing services may pose risks that are different from traditional outsourcing arrangements. Besides the operational risks of any outsourcing activity, cloud computing may pose additional risks to the insurance sector, given (i) shared computing resources in some cloud deployment models; (ii) the type of information that is stored and processed; (iii) the different geographical location of computing resources and providers; as well as (iv) the small number of global cloud providers, resulting in market concentration that could have systemic implications. The cross-border nature of cloud services complicates the effective oversight of all these risks.

The Financial Stability Institute (FSI) of the bank for International Settlement (BIS) outlines the emerging regulatory and supervisory approaches in selected jurisdictions to cloud computing activities in the insurance sector. Using publicly available information and interviews with relevant officials, we analyse the regulatory and supervisory approaches of 14 authorities worldwide and present key insights on the emerging prudential treatment of cloud computing in the insurance industry.

Authorities apply their frameworks for general outsourcing and for governance, risk management and information security to cloud computing. Some authorities include cloud-specific sections in these frameworks. Other authorities have issued cloud-specific recommendations or supervisory expectations. Regardless of the approach taken, cloud computing arrangements are subject to regulatory requirements only if they are deemed as material. However, the criteria for deciding whether such arrangements are material vary across jurisdictions.

Regulatory frameworks have a number of common requirements and expectations for cloud computing. Authorities generally focus on (i) the adequacy of information security and data confidentiality; (ii) the strength of IT and cyber-security capabilities at cloud service providers; (iii) the effectiveness of recovery and resumption capabilities; and (iv) the adequacy of audit rights (ie the supervisory authority's access to documentation and information, and ability to conduct on-site

inspections at the provider). Also, authorities are generally using non-binding guidance through principles and recommendations and adopting a proportionate approach (ie tailored to reflect the size, complexity or risk profile of financial institutions or outsourced service).

Cloud computing outsourcing arrangements are generally supervised as part of the oversight of operational risks. Authorities usually assess cloud computing practices as part of insurance companies' off-site and on-site reviews of operational risk, following a risk-based approach. Before an insurer enters into a cloud servicing agreement, some authorities require notification, while others prescribe a consultation or approval process: the approaches to this communication vary widely. At the very least, most authorities expect informal communication from insurers on their material cloud computing plans.

Authorities are increasingly using thematic reviews and informal contacts with cloud providers to complement their oversight of the cloud computing business. Targeted reviews on the use of cloud services in the financial/insurance industry or on closely related areas such as information security risks are helping authorities to gain an industry-wide perspective on cloud computing. In addition, some authorities have established a dialogue with cloud service providers with the aim of better understanding the cloud services business and, in particular, its evolution over time. This helps supervisors to evaluate how insurers are managing cloud-related risks.

The study yields some useful insights on the emerging regulatory and supervisory approaches for cloud computing in the insurance sector. Some key specific considerations for insurance authorities include:

- There is value in clarifying regulatory/supervisory expectations on insurers' use of cloud computing services. The usefulness of this approach is to address the unique risks posed by cloud computing and to provide a reasonable level of regulatory certainty with respect to the use of cloud services by the financial industry.
- Developing a supervisory framework to assess concentration risk in cloud computing is work in progress. While authorities generally acknowledge that reliance on a relatively small number of providers may result in systemic risk for insurers, very few perform industry reviews of the concentration risks arising from cloud service providers.
- Enhancing cross-border cooperation, particularly in terms of information-sharing, is essential for the effective supervision of the cloud computing business. Users and providers of cloud services may be located in different jurisdictions. Even if they are physically in the same place, data storage could be elsewhere. Therefore, international cooperation between different national authorities, in particular by sharing relevant information on cloud service providers, is especially important when it comes to ensuring effective oversight of cloud activities.

Regulating and supervising the clouds: emerging prudential approaches for insurance companies (PDF)

FSB: 2018 list of global systemically important banks

08/12/2018 10:13

1. The Financial Stability Board (FSB), in consultation with Basel Committee on Banking Supervision (BCBS) and national authorities, has identified the 2018 list of global systemically important banks (G-SIBs), using end-2017 data and the updated assessment methodology published by the BCBS in July 2013. One bank has been added to and two banks have been removed from the list of G-SIBs that were identified in 2017, and therefore the overall number of G-SIBs decreases from 30 to 29 (see Annex).
2. The changes in the allocation of the institutions to buckets (see below for details) reflects the effects of changes in underlying activity of banks.
3. In November 2011 the FSB published an integrated set of policy measures to address the systemic and moral hazard risks associated with systemically important financial institutions (SIFIs). In that publication, the FSB identified as global systemically important financial institutions (G-SIFIs) an initial group of G-SIBs, using a methodology developed by the BCBS. The November 2011 report noted that the group of G-SIBs would be updated annually based on new data and published by the FSB each November.
4. FSB member authorities apply the following requirements to G-SIBs:

   Higher capital buffer: Since the November 2012 update, the G-SIBs have been allocated to buckets corresponding to higher capital buffers that they are required to hold by national authorities in accordance with international standards. Higher capital buffer requirements began to be phased in from 1 January 2016 for G-SIBs (based on the November 2014 assessment) with full implementation by 1 January 2019. The capital buffer requirements for the G-SIBs identified in the annual update each November will apply to them as from January fourteen months later. The assignment of G-SIBs to the buckets, in the list published today, determines the higher capital buffer requirements that will apply to each G-SIB from 1 January 2020.

   Total Loss-Absorbing Capacity (TLAC): G-SIBs are required to meet the TLAC standard, alongside the regulatory capital requirements set out in the Basel III framework. The TLAC standard will be phased-in from 1 January 2019 for G-SIBs identified in the 2015 list (provided that they continue to be designated as G-SIBs thereafter).

   Resolvability: These include group-wide resolution planning and regular resolvability assessments. The resolvability of each G-SIB is also reviewed in a high-level FSB Resolvability Assessment Process (RAP) by senior regulators within the firms' Crisis Management Groups.Higher supervisory expectations: These include supervisory expectations for risk management functions, risk data aggregation capabilities, risk governance and internal controls.

1. In November 2014 the BCBS published a technical summary

of the methodology. The BCBS publishes the annually updated denominators used to calculate banks' scores and the thresholds used to allocate the banks to buckets and provides the links to the public disclosures of the full sample of banks assessed, as determined by the sample criteria set out in the BCBS G-SIB framework. From this year, the BCBS also publishes the twelve high-level indicators of the banks in the main sample used in the G-SIB scoring exercise.

2. The BCBS published in July 2018 a revised version of its assessment methodology, replacing the July 2013 version.10 The revised assessment methodology will take effect in 2021 (based on end-2020 data), and the resulting higher capital buffer requirement would be applied in January 2023.
3. A new list of G-SIBs will next be published in November 2019.

Table 1: G-SIBs as of November 201811 allocated to buckets corresponding to required levels of additional capital buffers

Bucket[12]	G-SIBs in alphabetical order within each bucket
5 (3.5%)	(Empty)
4 (2.5%)	JP Morgan Chase
3 (2.0%)	Citigroup Deutsche Bank HSBC
2 (1.5%)	Bank of America Bank of China Barclays BNP Paribas Goldman Sachs Industrial and Commercial Bank of China Limited Mitsubishi UFJ FG Wells Fargo
1 (1.0%)	Agricultural Bank of China Bank of New York Mellon China Construction Bank Credit Suisse Groupe BPCE Groupe Crédit Agricole ING Bank Mizuho FG Morgan Stanley Royal Bank of Canada Santander Société Générale Standard Chartered State Street Sumitomo Mitsui FG UBS Unicredit Group

Source: Financial Stability Board FSB G-SIB18

ECB: Euro Cyber Resilience Board for pan-European Financial Infrastructures

07/12/2018 11:38

Benoît Cœuré, Member of the Executive Board of the ECB, informed the audience of the second meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures on the latest development in cyber finance across European markets.

The cyber threat facing the financial sector continues to be a challenge. From banking trojans affecting individual customers to systemic threats posed by ransomware and targeted attacks from advanced persistent threat (APT) groups, the landscape is evolving on a daily basis.

The Eurosystem cyber strategy for financial market infrastructures rests on three pillars: individual FMI resilience, sector resilience and strategic regulator-industry collaboration. I am pleased that in the last few months, the ECB and the Eurosystem have made significant progress in putting in place the building blocks for enhancing the cyber resilience of the European financial ecosystem and operationalising the strategy.

The ECB developed two key tools to improve FMI resilience: the cyber resilience oversight expectations (CROE and the TIBER-EU Framework.

The CROE serves three key purposes: (i) it provides FMIs with detailed steps on how to operationalise the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, ensuring they are able to make improvements and enhance their cyber resilience over a sustained period of time; (ii) it provides overseers with clear expectations against which to assess FMIs under their responsibility; and (iii) it provides the basis for a meaningful discussion between the FMIs and their respective overseers. The central banks of the Eurosystem will work closely with the various financial infrastructures to enhance their cyber resilience, with the CROE serving as a good basis for this work.

Enhancing cyber resilience is of crucial importance. Equally important, however, is to test whether the enhancements that have been introduced by individual entities are effective. To that end, the ECB published the TIBER-EU Framework in May and the TIBER-EU Services Procurement Guidelines in August. The hope is that over time, this sophisticated level of testing will help strengthen our financial infrastructures and raise standards among threat intelligence and red team testing providers.

In terms of sector resilience, exercises are a key component of building market-wide preparedness for a cyber incident. In March, we told you about our forthcoming market-wide exercise, which we held in June. The exercise, UNITAS, took the form of a facilitated discussion among market participants – many of whom are here today – on a cyber scenario. The scenario involved a cyberattack on a number of financial infrastructures, resulting in a loss of data integrity and a knock-on effect on other financial infrastructures.

With regard to strategic regulator-industry collaboration, our third pillar, the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures was formally established in March 2018, as a forum for strategic discussions between financial infrastructures and authorities. As you know, our objectives are to raise awareness of the topic of cyber resilience; to act as a catalyst for joint initiatives to develop effective solutions for the market; and to provide a place to share best practices and foster trust and collaboration.

Of course, cyber risk is borderless and it is an international issue. So the Eurosystem's initiatives are part of a growing international effort to combat cyber threats. In October this year, G7 ministers and central bank governors published the "Fundamental Elements for Threat-Led Penetration Testing", which complements the TIBER-EU Framework, and the "Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector". In 2019, the G7 Cyber Expert Group will move ahead with conducting the first global cross-border cyber

crisis simulation exercise.

In November, the Financial Stability Board (FSB) published a Cyber Lexicon. Having a common set of definitions in non-technical language will support the work of the FSB, standard-setting bodies, authorities and financial institutions to address cyber security and cyber resilience in the financial sector. The ECB continues to participate in these international fora, ensuring that global initiatives are aligned with our work in Europe.

From an operational perspective, the Market Infrastructure Board, which is in charge of the Eurosystem-operated financial infrastructures, continues to scale up its activities to ensure the continued cyber resilience of its systems and platforms.

In March, four key areas for further focus were identified: 1) crisis management and incident response; 2) information sharing; 3) awareness and training; and 4) third-party risk. There was general agreement that these key areas warranted further thought and focus. The UNITAS exercise further confirmed that these areas require attention.

FSB issues its 5th annual report

07/12/2018 11:26

The Financial Stability Board (FSB) issues its fifth annual report, that provides an update on the key activities of the FSB and its audited annual financial statements for the 12-month period ended 31 March 2018.

The report provides an update on the FSB's work as it pivoted from a primary focus on new policy development towards evaluating policies that have been implemented and addressing any unintended consequences. It provides an update on the activities, publications and decisions by the FSB during the course of the year, and sets out details on the FSB's governance.

The FSB's current priorities are designed to build on that strong foundation to reinforce the G20's objective of strong, sustainable and balanced growth.

Vigilant monitoring to identify, assess and address new and emerging risks remains at the heart of the FSB's work. Through structured analysis and candid discussion among its diverse and expert members, the FSB assesses risks arising from a broad range of developments and trends in the financial system – including those relating to technological change which can cut across traditional boundaries.

The FSB's focus has pivoted from a primary focus on new policy development towards evaluating policies that have been implemented and addressing any unintended consequences. The FSB's approach to dynamic and effective implementation will help ensure that the new regulatory framework keeps pace with a changing financial system in as efficient a manner as possible, while continuing to meet the objectives that were set by the G20 Leaders.

FSB: 5th Annual Report (PDF)

Direttore: Emilio Barucci.
Capo redattore: Tommaso Colozza.
Redattori: Roberto Baviera, Marco Bianchetti, Michele Bonollo, Stefano Caselli, Andrea Consiglio, Silvia Dell'Acqua, Giancarlo Giudici, Gaetano La Bua, Daniele Marazzina, Carlo Milani, Aldo Nassigh, Nino Savelli.