SIA S.p.A.

via Francesco Gonin, 36 - 20147 Milano
t. +39 02 6084.1 - f. +39 02 6084 3920

www.sia.eu - info@sia.eu

capitale sociale euro 22.091.286,62 i.v.
r.i., c.f. e p. iva n. 10596540152
r.e.a. n. 1385874 di Milano

Filiali estere:
Belgicastraat 1 - 8-1930 Zaventem - Belgio
Winthontlaan 200 - 3526 KV Utrecht - Paesi Bassi

SIA-RGO-0000808-2016

To Committee on Payments and
Market Infrastructures - CPMI
cpmi@bis.org

International Organization of
Securities Commissions -IOSCO
consultation-2015-09@iosco.org

Milan, 22 February 2016

Re: **Consultative report – Guidance on cyber resilience for financial market infrastructures – November 2015**

Dear Sirs,

with reference to the abovementioned document, we hereby forward to you our considerations and suggestions concerning the same.

Kind regards,

Massimo Arrighetti
Chief Executive Officer

CPMI-IOSCO – SIA COMMENTS ON THE CONSULTATIVE REPORT "GUIDANCE ON CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURE" (NOVEMBER 2015)

Issue	Comment / reasoning
Overall	The guidelines aim to raise the quality of the whole ecosystem. The investments requested will imply significant efforts. We would like to highlight that the **impacts** will be not only on the FMIs but - **mainly - on the critical service providers**. Additional requirements and systems are required to the solutions now in place. In addition, since the entry points of the ecosystem that could be compromised may be many and various - we suggest paying attention to the **guideline also to the vendors and to vendor products**. Besides, we suggest paying attention to other **players that are not of "systematic importance"** and that therefore will not be directly subject to the cyber requirements (and to the consequent investments). If not impacted by the same rules and conditions, the non-critical service provider could introduce risks to the whole competitive ecosystem – having the possibility to work with a reduced value infrastructure and to offer low-cost services (however interconnected).
1 Introduction 1.1.5 Settlement finality and recovery time objective	The guide sets out a unique framework for all operators and lays down the foundations for the harmonious raising of defenses. We believe that the inclusion of cyber scenarios is an additional element that makes **it very challenging to achieve the three basic assumptions[1], in particular the 2hr recovery time objective**. As for the management of physical disaster scenarios it took time to achieve full business continuity - even for cyber scenarios operators need to work progressively through contingency plans with improvement programs where milestones are ruled by the Regulator and shared among all involved subjects..
4.3 Interconnections 4.3.1 Risks from interconnections	Regarding the risks from interconnections, a criterion to increase the global defenses could be the **asymmetry in the technologies** adopted. The trade-off between asymmetry (on the technologies) and interoperability (on the functionalities) can be considered. Furthermore, the paragraph extends the validity of the requirements to all service providers and not only to those critical ones. It might be useful to have **an accreditation scheme and certification of service providers** in order to facilitate the choice and control.
5 Detection 5.2.1 Continuous monitoring	In our opinion, for an effective detection of attacks affecting data integrity, full usage of **digital signature technology** should be applied. This solution could be considered when application messages and files are exchanged, processed and stored as well as for application and system configuration of static files. In this way, authenticity conflicts and unexpected changes can be detected immediately. Full usage of digital signature could be needed to significantly change business applications. In the meantime adoption of **file-integrity monitoring or change-detection systems checks** could be a starting point. These technologies could be tuned to detect changes to critical static files, and report when such changes are noted. Changes affecting files that do not regularly change (e.g. configuration modules), indicate a possible compromise.

[1] The three basic assumptions are the following: 1. PFMIs as starting point; 2. Settlement Finality; 3- End-of-day settlement and 2h RTO.

Issue	Comment / reasoning
6 Response and recovery 6.2.2 Resumption within two hours	We would like to highlight that **in case of APT- Advanced Persistent Threats** the disruption and disenablement of data may not be massive or not be on a high scale and not with high volumes of data. Therefore the two hours criteria could be a difficult parameter to define. The two hours criteria can also be difficult to set in case of APTs that exploit a group of FMIs or Critical Service Providers or vendors solutions interconnected among themselves.
6 Response and recovery 6.3.2 Data integrity	Making data integrity criteria work effectively **may lead to a serious re-design** of applications and of the approach to the business continuity and to the solutions of recovery. In our opinion the maintenance of a **"golden copy" of critical data** needs to be highlighted as a leading criterion. To assure the full integrity of data, additional criteria could be **the reconciliations of the business critical data** (done systematically with a frequency in line with the operating cycles) and - in case of batch processes - the protection of the **periodical critical cut-off** (hourly or daily or weekly or monthly according to the business needs).
7 Testing 7.2.2.d Red team tests	We suggest introducing criteria to guarantee **the screening of the red team companies** in order to assure the utmost integrity of the code of conduct of the company of external experts engaged (very likely due to the complexity of the matter). Trust and assurance of this kind of subject is a sensitive point that could also cause controversy among countries. On this matter an **alignment with the national cyber security agencies** would be advisable.
9 Learning and evolving 9.3.1 Metrics	Due to the evolution of the technologies and of the interconnections and due to the relatively immature state of the art, we suggest to introduce **a criterion of "regular review"** of the metrics defined **and** criterion **of "continuous improvements of the metrics** chosen.