Dear all,

Overall we think that the guidance document contains sufficient reasonable advice. However there are a few remarks we have and would like you to take into consideration.

- Though presented as supplemental guidance to the CPMI-IOSCO PFMI we foresee it shall be used as a standard. As such a “level playing field” should be reached.
1.3.3 for example is aimed at the value chain as a whole, whilst the principles and supplemental guidance are not applicable to all stakeholders. 1.3.6 tries to achieve this but basically as stated this depends on the eventual adoption in legal frameworks of relevant jurisdictions. Both those statements and their applicability have a negative impact on this “ level playing field”.
- Cyber resilience overlaps in principle with existing standards and best practices. Room of integration is given in 2.2.6 though a lot of principles demand specifics that intervene/shift focus with those existing standards. An example is 2.2.7 where clear roles, responsibilities should be defined for managing cyber risk. Responsibilities for managing risk must be defined regardless of its domain being continuity, operational, financial it or cyber.
- We suggest to combine 3.2.1 and 3.2.2 such that assets supporting business functions and processes inherit the criticality given to those functions and processes. Independent classification of assets and functions may lead to discrepancy as ownership/responsibility may be different. This impacts the prioritisation of the FMI its efforts.
- For 4.2.1 we would like to state that currently leading cyber resilience standards are not available. Leading (information/cyber) security standards are available.
- 4.4.1 we would like to see a general statement that requirements should be met within applicable legal frameworks and may not contradict as this might also apply to other requirements missing such specific clause.
- 6.2.2 We would like to see the term time-critical systems used. Resumption within 2 hours is not applicable to all critical systems as they are not all time-critical.
In general the guidance doesn’t pay a lot of attention to the sourcing of services, this whilst sourcing of a service could have a big impact on the cyber resilience of an FMI.

Kind regards,
Equens SE

Eric Luijks
General Manager
Risk Management
www.equens.com