Guidelines on information and communication technology security and governance

Guidelines on information security and governance – Service Provider 1/2

- *Guideline 6 – Information security policy and measures* Where applicable and relevant, the information security policy or parts of it should also be communicated and applied to service providers.
- *Guideline 7 - Information security function*:
  - d) ensure that the information security requirements are adhered to when using service providers;
  - e) ensure that all employees and service providers accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions;
- *Guideline 11 – Security monitoring* : Undertakings should establish and implement procedures and processes to continuously monitor activities that impact the undertakings' information security. The monitoring should cover, at least:
  - a) internal and external factors, including business and ICT administrative functions;
  - b) transactions by service providers, other entities and internal users; and
  - c) potential internal and external threats.

Guidelines on information security and governance – Service Provider 2/2

- *Guideline 25 – Outsourcing of ICT services and ICT systems:* In case of outsourcing of critical or important functions undertakings should ensure that contractual obligations of the service provider (e.g. contract, service level agreements, termination provisions in the relevant contracts) include, at least, the following:
  - a) appropriate and proportionate information security objectives and measures including requirements such as minimum information security requirements, specifications of undertakings' data life cycle, audit and access rights and any requirements regarding location of data centres and data encryption requirements, network security and security monitoring processes;
  - b) service level agreements, to ensure continuity of ICT services and ICT systems and performance targets under normal circumstances as well as those provided by contingency plans in the event of service interruption; and
  - c) operational and security incident handling procedures including escalation and reporting.

Guidelines on information security and governance - BCM

- *Guideline 19 – Business continuity management* As part of the undertakings overall business continuity policy, the AMSB has the responsibility for setting and approving the undertakings' **ICT continuity policy.** The ICT continuity policy should be communicated appropriately within undertakings and should apply to all relevant staff and, where relevant, to service providers.
- *Guideline 22* As part of the response and recovery plans, undertakings should consider and implement continuity measures to mitigate failure of service providers, which are of key importance for undertakings' ICT service continuity
- *Guideline 23 – Testing of plans* Test results should be documented and any identified deficiencies resulting from the tests should be analyzed, addressed and reported to the AMSB.