|  |  |  |
| --- | --- | --- |
| GLs Section - Article - Paragraph | Proposal for amendment | Justification |
| Subject Matter, Scope and Definition |  |  |
| 6.  | The “CYBER RESILIENCE OVERSIGHT EXPECTATIONS (CROE) FOR FINANCIAL MARKET INFRASTRUCTURE” issued by ECB shall also be taken into consideration for alignment of controls.  |  |
| 10 | Remove the word “operational” from the Operational and Security Incident | The description really refers to a security Incident. After all security incidents are part of the Operational Incidents. For the sake of avoidance of confusion, if operational incidents need to be included, they need to be clearly defined.Since continuity of ICT systems and services is included in terminology Availability specified above, why is the term continuity included in this definition. Are you referring to something else?  |
|  | It is not clear what Management Body is: is it the Board of Directors or the Executive Management of the Bank?  | Need to clarify to avoid confusion  |
| Guidelines |  |  |
| 2 | The Management body should have at least one expert on Information Security / ICT risks field in order to be able to properly execute governance.  |  |
| 7 | These guidelines to apply in all subsidiaries of financial institutions (whether FIs or not – e.g. Insurance Companies).  | In case the FI’s IT serves multiple subsidiaries, it is complex to have different security controls on different subsidiaries. For consistency purposes, security controls shall be aligned.  |
| 8.a  | The wording “security objectives” is not clear.  | We suggest that the wording “measures” is sufficient |
| 9 | Specific assurance is better to be specified. For the security measures a SOC2 type II security attestation by an independent assessor shall be provided.  | Without explicitly stating compliance assurance, service providers can never move to the right direction.  |
| 11 | The Internal Control Function (2LD) which manages ICT Risks shall be Information Security and Operational Risk Management depts. | In a typical FI environment the management of ICT risks as a 2LD is taking place thru 2 different departments: ORM and InfoSec. It is not clear how a single dept. can manage ICT risks alone.  |
| 15 | It is not clear whether the ICT Risk Management Framework is a single framework.  | There are separated InfoSec and ORM frameworks. Consolidating the two in a single framework will create operational inconsistencies. Do we need to keep both live, or shall we merge them.  |
| 19 | Include also that the regulatory requirements should be considered before defining the criticality functions/processes/information assets | There are cases where the criticality is imposed by regulations: PCI, Swift, and GDPR.  |
| 22 | It is not clear how it is expected to monitor threats.  | Please clarify.  |
| 25 | The timely manner shall be set to a specific threshold. Also the provision to CAs shall be specified to be “on an annual basis”. | Timely manner leads to very subjective implementation. The regulator shall define the threshold, quarterly/semi-annually are good candidates.  |
| 28 | Follow-up process for the verification of critical security related findings shall be extended to all critical ICT findings (independently whether these are security or non-related).  |  |
| 30 | The Information Security Policy shall NEVER be communicated to third parties.  | ISP is a confidential document and its distribution shall be protected. For third parties a legal document reflecting the needed parts of the policy can be used instead.  |
| 34 .g | Provision for password complexity and/or strong customer authentication is vague.  | This leads to multiple interpretations (may, and/or). Banks may understand it differently than regulators. It is recommended that this becomes more solid.  |
| 39 | Critical patches shall be deployed no later than 1 month.  | For alignment with PCI DSS requirements.  |
| 39.e | It is not clear in the context what integrity for information means. Can you please make this clearer?  |  |
| 40 | The item is very generic. Does the control refer to manual processes, or does it focus on automated processes (i.e. Static and Dynamic Code Analysis before going live).  |  |
| 42 | Clarify how you expect/understand FIs to actively monitor technological developments to ensure that they are aware of security risks.  |  |
| 43 | It is not clear how the security monitoring process will help an FI identify an operational incident which will be a security incident.  |  |
| 55 | Processes and procedures are usually not approved by the Management Body, but from executive/senior management structures.  |  |
| 75 | It is not clear what these measures shall be.  | The word development creates confusion. Are you referring to the processes of a librarian or to something else? |
| 78 | An addition could be made that copying of production data to other environments shall not be taking place. Only scrambled data can reside on non-production environments.  | There is a wide practice across the industry that prod data are copied to testing systems.  |
| 81 | The term “asset owner” is used in point (e). It is not clarified in the definitions section who is this person (the business owner or the IT person responsible for the application?) |  |
| 84 |  | It is not clear what does external data refer to.  |
| 86 | Approval of BCPs shall be approved by Executive Management. | Management Body (BOD) shall approve the strategy but not the specific BCPs of all functions.  |
| 100 | It is not clear the wording: “what product functionality permits”.  | This wording creates an ambiguity whether this is optional or not.  |