|  |  |
| --- | --- |
|  |  **Division Bank and Insurance**Austrian Federal Economic ChamberWiedner Hauptstraße 63 | P.O. Box 3201045 ViennaT +43 (0)5 90 900-DW | F +43 (0)5 90 900-272E bsbv@wko.atW http://wko.at/bsbv |

Your ref., Your message of Our ref., person in charge Extension Date

 BSBV 145/Horvath 3141 4th March 2019

**EBA Consultation Paper – EBA draft Guidelines on ICT and security risk management**

The Division Bank and Insurance of the Austrian Federal Economic Chamber, as legal representative of the entire Austrian banking industry, appreciates the possibility to comment on the above cited consultation paper and would like to submit the following position:

|  |  |
| --- | --- |
| **GLs Section - Article - Paragraph** | **Proposal for amendment** |
| Subsection 4.6.1 (ICT projectmanagement) paragraph 66 – “Financial institutions should implement a governance process with an adequate project implementation leadership to effectively support the implementation of the ICT strategy through ICT projects.” | EBA should prodive a clear definition of “project implementation leadership” |
| Subsection 4.6.1 (ICT projectmanagement) paragraph 70 – “Financial institutions should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has an adequate knowledge required to ensure secure and successful project implementation.” | EBA should provide a clear definition of “adequate knowledge”. |
| Subsection 4.6.2 (ICT systems acquisition and development)  | Referring to the section on “ICT Project and Change Management”, in particular section 4.6.2. on “ICT systems acquisition and development”, we suggest adding a reference to ISO 27001 A.14 on system/software development life cycle (SDLC) as ISO 27001 can be considered as an appropriate software solution.  |

Yours sincerely,

Dr. Franz Rudorfer

Managing Director

Division Bank and Insurance