Consultation on EBA GLs on ICT and security risk management

GLs Section - Article - Paragraph	Proposal for amendment	Justification
GL 4.2.1 Governance article 3	Remove 'occupying key roles'.	This should apply to all staff.
GL 4.2.3 article 7 until 9	Remove article 8 and 9 or only prescribe additional outsourcing arrangements in reference to EBA GL 2019 on outsourcing.	Article 8 and 9 refer to guidelines which are already prescribed in the GL 2019/XX on outsourcing.
General remark on the use of terminology	Consistently use the term 'Financial Institutions' throughout these guidelines, instead of mentioning the appropriate department or level (including the three lines of defence) where the responsibility for a specific requirement lies.	We understand and endorse the three levels of defence approach and description, but believe it should be up to the Financial Institution on how to manage this.
General remark on three lines of defence (see articles 11, 13, 27, 32 and 33)	Adjust the wording for the three lines of defence.	The three lines of defence are not described clearly and consistently.
GL 4.3.1 Article 15	Divide this article into two separate articles. The second article should cover 'Financial institutions should ensure…incident."	This second article should be part of change management under GL 4.6.3.
GL 4.3.3 Article 21	Clarification of or confirmation that this article covers a risk based approach referring to 'annually or at shorter intervals, if required'.	
GL 4.3.5 article 25	Remove second sentence of this article.	Not reporting twice separately as the PSD2 already requires these risk assessments. PSPs have to comply with the law as laid down in the PSD2.
GL 4.3.6 article 27	Substitute 'approve the audit plan' by 'be informed on the audit plan'.	The audit committee is an independent body within the organisation.
GL 4.4.1 article 29	Remove this article.	This article is already covered by Article 5 of Directive 2015/2366 which prescribes the conditions to obtain a license. One of which is the development of an information and security policy. Please note that the responsibility for fraud scenarios lies with fraud operations.
GL 4.4.2 article 32	All text between brackets should be removed.	In our opinion the segregation of the ICT security function and the ICT operations function is already covered in the second sentence of this article.
GL 4.4.2 article 33	The first line (operational) and second line (Information security function) of defence are not described separately and are unclear. For example 33d belongs to first line/	

	operational management and is not the responsibility of the information security function. Sub d: to ensure that a third party adheres to security requirements is in our opinion difficult/unfeasible to enforce	Adjust wording
GL 4.4.3 article 34e	'Removed' should be substituted by 'deactivated' or 'withdrawn'.	
GL 4.4.5 article 39	This article should encompass a risk based approach or something more generic. Furthermore we would like to recommend prescribing the goals instead of activities in this article. Add 'detection and response' to 'data leakage prevention systems'.	
General remark on the lack of definitions, for instance: • **article 32 (information security function is this the CISO?)** • **article 44 (information security standards)** • **80 (business managed applications)** • **81^{e} (urgent or emergency ICT changes)**	Add some definitions.	We advise to add some definitions to clarify what is meant. Furthermore we advise to use standard definitions (e.g. COBIT, ISO etc.) where possible.
GL 4.4.7 article 45	Substitute 'new threats' by identified threats. In our opinion this article introduces a separate framework. Can you clarify on this matter?	
GL 4.4.7 article 49	We suggest not to use a specific term for non-critical systems ('at least every 3 years').	We are of the opinion that every PSP is capable to manage without any prescription, referring to 'at least every 3 years'.
GL 4.4.7 article 50	This article should be rephrased.	We suggest to prescribe that only certified payment terminals have access to the network.
GL 4.4.8 article 53	Remove 'occupying key roles'.	This should apply to all staff.
GL 4.5 article 58	Substitute 'document the configuration' by 'contain the configuration'.	

GL 4.5 article 62	Substitute ‘restoration’ by ‘recovery’.	
GL 4.5 article 63	Replace ‘in one or more locations out of the primary site, which are secure and sufficiently remote…’ by ‘in one or more different locations, which are secure and not exposed to the same environmental risks’.	
GL 4.5.1 article 64	In the first sentence the word (financial) ‘institutions’ lacks.	
GL 4.6	We do not see how this GL can be applied to an agile working environment, as this is quite common for Dutch PSP’s.	
GL 4.6.1	We are of the opinion that procurement management should be out of scope of these guidelines.	These guidelines contain ICT and security risk management provisions.
GL 4.6.2 article 75	Substitute ‘prevent’ by mitigate the risk of.	
GL 4.6.2 article 78	Substitute ‘unverified’ by ‘unauthorised’ or ‘unaccepted’.	
GL 4.6.3 article 81	Clarification of or confirmation that this article covers a risk based approach.	We do agree that an ICT change management process should be in place, but not all ICT systems are equally qualified/ sensitive.
GL 4.7.1 article 84	This article covers a business impact analysis. In our opinion this article resembles article 17. Can you clarify or elaborate on this?	
GL 4.7.2 article 86	Substitute ‘management body’ by ‘responsible management’. Add ‘besides other risks’ in the sentence ‘… the plans should specifically consider…’.	In our opinion the term “management body” refers to board level. BCP’s are usually described at a much more technical level than the board is used to. BCP’s cover all risks, not only ICT risks.
GL 4.7.2 article 87	The RTO is an objective. If a maximum time is required we suggest to use the term MTO (Maximum Tolerable Outage).	
GL 4.7.2 article 88	This article implies that ICT is responsible for certain fraud scenarios, f.e. phishing. Clarify or rephrase this article.	As mentioned previously the responsibility for fraud scenarios lies with fraud operations.
General remark	These guidelines refer to EBA Guidelines on outsourcing arrangements (article 7 and 92) which are not yet finalised.	
GL 4.8	In our opinion this article covers responsibilities which are out of	This lies outside the mandate of the CIO.

	scope for ICT, these are covered by Operations.	
General remark	Please explain the relationship between the EBA ICT risk assessment guideline within SREP, and these draft guidelines (preferably with a mapping between the requirements if possible).	
General remark	Most of the guidelines with regard to business continuity are acceptable. In some cases however the complexity of a financial institution is taken into account and requirements for content of plans (BCP and Recovery plans) are much too detailed. This will lead to plans that are unmanageable, unmaintainable and practically not usable.	