Bankia

EBA draft Guidelines on ICT and security risk management

—

Comments on the proposals

Marzo 2019

1. Comments on the proposals (1/5)

SECTION	PART	COMMENTS
Definitions	---	• Page 14: The definition of risk tolerance in the draft follows what we are used to call as risk appetite, instead of tolerance. We understand risk tolerance as the variability regarding the established risk appetite that the organization can accept under some circumstances. These are, in fact, the most common definitions we usually listen to in the market. Could you clarify the definitions of both appetite and tolerance? We also understand that risk appetite can consider the aggregate level of risk as a medium value of the addition of risks in the organization, and not only their addition.
ICT governance and strategy	Governance	• Page 15 – Point 3: We would like to receive more detail about what is considered as staff members occupying key roles. Also we would like to know if the information security training, that these key roles should receive on an anual basis, can be fulfilled using a general information security training for all the staff, or it is expected to be a different and specific training.
	Use of third party providers	• Page 16 – Point 7: Does it mean that the measures set out in these Guidelines should be included in the outsourcing risk assessments whenever the outsourced service is related to payment services?

1. Comments on the proposals (2/5)

SECTION	PART	COMMENTS
ICT risk management framework	Organisation and objectives	• Page 16 - Point 11: Where it is mentioned that the second line of defence should take responsibility for the management of ICT risks, isn't it more correct to say they should take accountability, since the responsibility to manage ICT risks during the daily tasks is the first line? The second line would have an internal control function, but not the responsibility for the daily risk management. • Page 17 – Point 13a: Could you give more details about the expected content for the process to determine the risk tolerance for ICT risks? Point 13c: Could you specify the definition of controls in comparison to mitigation measures, and as part of them? That is, inside the mitigation measures, which ones do you consider as controls? Point 14: The lessons learned, should be gathered explicitly in a specific document for that purpose, or it is enough to add them to the different appropriate documents, in an implicit way? Point 15: Where it is said "financial institutins should ensure that before any major change of ICT system or ICT services, processses or procedure....", what do you mean by major change? Point 16: Where it is said "... mapping of their business functions, roles and supporting processes", instead of roles, do you mean information assets? Can you explain in more detail this mapping?

1. Comments on the proposals (2/5)

SECTION	PART	COMMENTS
ICT risk management framework	Classification and risk assessment	• Page 18 – Point 20: We don't think that a review of the classification of the information assets and relevant documentation should be done every time a risk assessment is performed. We understand this task should be included in other activities. When a risk assessment takes place, we think the classification already assigned by the owner of the asset or documentation should be considered directly to determine the posible impact that a risk event could produce. Point 21: We think this point should be less restrictive, so that different risk management methodologies can be implemented depending on the characteristics of the organization. For a very complex and big organization, to associate the ICT risks to every business function, or information asset could be difficult to maintain and not practical. Could you also define business function?

1. Comments on the proposals (3/5)

SECTION	PART	COMMENTS

Information security	Information security function	• Page 19 – Point 32:
		  • Where it is said "… this function should be the second line of defense function", we understand that the information security function, in the best case, could be part of the second line of defence, but not the only component of the second line of defence. Also, the operational day by day activities related to information security would be part of the first line of defence. Can you clarify and explain in more detail this point?
		  • On the other hand, when it is said "… with the responsibilities assigned to a designated person", which kind of person do you refer to? The CISO?

	ICT operations security	• Page 21 – Points 39c and 39f: Is the encryption referred to sensitive data? Otherwise, do you mean to encrypt all the data? This should be a bit more specified in the draft.
	Information security reviews, assessment and testing	• Page 23 – Points 45 and 46: Do you mean to have a specific security testing environment? Point 49: We think that testing all the critical security measures on an annual basis can be too much for complex organizations. We think the same about testing all non-critical systems every 3 years. These requirements should be adapted to the kind of organization we are talking about.
	Information security training and awareness	• Page 23 – Point 53: A security awareness program can be considered as a targeted information security training for the staff members occupying key roles?

1. Comments on the proposals (4/5)

SECTION	PART	COMMENTS
ICT Operations management	---	• Page 24 – Point 63: Is it acceptable that the remote location/s are in the same city as the primary site but far away in distance?
	ICT Incident and problem management	• Page 25 – Point 64: Could you specify which incidents are considered security incidents and which ones are considered another kind of ICT incidents.? Could you give examples?

1. Comments on the proposals (5/5)

SECTION	PART	COMMENTS
ICT Project and Change management	ICT systems acquisition and development	• Page 27 – Point 77: Could you specify the definition of errant coding practices?
Business continuity management	Business continuity planning	• Page 29 – Point 87: We would like to receive more explanation and details about this point, specially when it is said "… should prioritise business continuity actions using a risk-based approach". Can you give more examples? If several business continuity plans exist depending on the scenario, in case a business disruption occurs that implies several of them, a previous risk assessment is needed to decide wich one to choose?
	Testing of plans	• Page 30 – Point 95a: Where it is said"… an adequate set of severe but plausible testing scenarios…", if the critical functions are tested independently, that is, first a critical function is recovered and then another, and so on, can it be considered a severe testing scenario?

Bankia

SIGAMOS TRABAJANDO