POSITION PAPER

Our reference: 2019/01/004
Your reference: EBA/CP/2018/15

2019-03-13 European Banking Authority

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

The Swedish Bankers´ Association (SBA) appreciates the opportunity to comment upon the EBA draft Guidelines on ICT and security risk management. Feedback has been collected from various stakeholders at our member banks, covering the three lines of defense. We have divided the comments into two parts: first, general remarks, and second, specific comments.

1. General remarks

1. Many requirements in the guideline are reasonable and constitutes expected ICT and information security related internal control areas in financial institutions. However, the way the requirements have been drafted in the guideline are too prescriptive and too detailed and are thereby limiting the risk management options available to financial institutions (such as governance structures, internal controls and other security related measures). In addition, the prescriptive design of the guideline will not be able to withstand the rapid nature of changes in the ICT and information security risk landscape in the years to come. It might ultimately limit financial institutions ability to innovate in the information and cyber security domain.

   <u>The SBA's suggestion:</u>
   A guideline that is more to the point, principle based and outcome-focused is preferred.

2. As it relates to information security governance, the way section "4.4.2. Information security function" has been formulated is a particular concern for Swedish financial institutions. Paragraph 32 and 33 in its current wording might contradict the related rules and regulations from the Swedish FSA on the responsibilities of control functions (FFFS 2014:1) and the requirements on a dedicated person to lead and coordinate the information security work in the first line of defense (FFFS 2014:5). According to the Swedish FSA, an information security function that lead and coordinate the information security

work cannot be placed in the second line of defense. For reference, please see page 22 in the Swedish FSA supervisory report from 2017: https://www.fi.se/contentassets/7c8169d883f643f290632afe70989af7/bank-tillsynsrapport2017ny.pdf

The SBA's suggestion:
The wording can contradict the related rules and regulations from the Swedish FSA on the responsibilities of control functions (FFFS 2014:1). We are puzzled on how the Swedish FSA (and EBA) will proceed on this matter and are concerned as this can create additional confusion. There must be appropriate supervision that creates the conditions for increased information and cyber security in society.

3. On this matter, we agree with the response from the European Banking Federation (EBF) on this consultation and we believe that (most of) the tasks listed in paragraph 33 should be performed by the first line of defense and that the second line should independently control and report on the effective implementation of those tasks. For instance, awareness and training, risk monitoring controls and reporting are first line tasks. The second line can complement these through independent monitoring, control and assurance reviews, but it should not diffuse the responsibility of the first line in these areas. Another way to put this is that the second line of defense should perform its required activities also in the risk area of ICT and security risk.

   The SBA's suggestion:
   There is no need to regulate these duties in detail as it relates to the ICT and security risk area. The guideline would benefit from having a clear description on what duties and responsibilities resides with the respective lines of defense, on an overall level. This description should be in line with EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU.

4. Another area of specific concern is "4.6. ICT Project and Change management". These requirements could be perceived to dictate that project management and system development methodologies should follow the waterfall model, i.e. a linear sequential design approach for software development. Most financial institutions have already or are in the process to adopt agile software development. This is another example of this guideline limiting the options available for financial institutions, in this case not only related to risk management but also to business development.

The SBA's suggestion:
Section "4.6. ICT Project and Change management" would benefit if it is redesigned. The chapter is not aligned with modern project management practices for system / application development (e.g. Agile, Tribes). EBA needs to focus on what is to be achieved (control principles) and less on how this should be achieved.

2. Specific comments

Definitions
10.
Current wording of "ICT projects":
"Any project, or part thereof, where ICT systems and services are changed, replaced or implemented. ICT projects can be part of wider ICT or business transformation programmes."

The SBA's suggestion: The definition is too wide. We suggest that the wording …, or part thereof,… is deleted in the first sentence resulting in the following definition: "Any project where ICT systems and services are changed, replaced or implemented. ICT projects can be part of wider ICT or business transformation programmes."

4.2.1 Governance
2. In this paragraph under "ICT governance", the management body is also required to set roles and responsibilities for information security risk and business continuity, not only for ICT risks. The question is rather what chapter 4.2.1 covers. Is it only ICT risk or also information security risk and business continuity? The chapter headline should reflect this.

3. The concept of "key roles" as it relates to training is vague. Staff in general should receive information security training.

4.2.2 Strategy
5c. There should be room for a separate information security strategy as long as there is a clear connection to the ICT strategy.

6. The concept of "action plans" as it relates to supporting the ICT strategy seems vague. What is meant by "action plans" and what are the expectations on those? Could they be initiatives/projects/programmes etc?

4.2.3 Use of third party providers

8. a) Vague terms are introduced: "minimum cybersecurity requirements" and "data life cycle". Do these terms point to some specific concepts or are they only being used as general terms? We suggest that these terms are removed and that the first part of this section is enough: "appropriate and proportionate information security objectives and measures...".

4.3.1 Organisation and objectives

11. According to this paragraph, an internal control function in 2nd line of defence should "take responsibility for the management of ICT risks". What does this mean exactly? Is it the same requirements defined in EBA/GL/2017/11 Guidelines on internal governance under Directive 2013/36/EU, paragraphs 174 – 180 on risk management function's role in identifying, measuring, assessing, managing, mitigating, monitoring and reporting on risks?

The SBA's suggestion: Change the wording to "Internal control function should take responsibility of the control of ICT risks".

15. The second sentence in this paragraph is oddly placed. It should belong to the list of activities in the ICT risk management framework in paragraph 13.

4.3.3 Classification and risk assessment

19. This is a broad ranging requirement that seems to consider both structured and unstructured information. The classification of both structured and unstructured information according to confidentiality, integrity and availability would demand unproportional resources in relation to the additional security level it could possibly add, i.e. not using a risk-based approach.

The SBA's suggestion: This paragraph should focus on structured data with the proposed wording "...consider the confidentiality, integrity and availability requirements on structured data". A suggested definition of "structured data" to include in the guideline would therefore be:
"Structured data is information that is structured systematically, which typically includes information within IT applications and database records structured according to a data model, as for example a relational or hierarchical schema".

4.3.5. Reporting

25. Reporting should be adapted to the relevant audience. Requiring individual risk assessments to be reported to the management body is in many cases not relevant. This would demand unproportional resources compared to the outcome.

The SBA's suggestion: Clearly state that reporting should be done on an aggregated level to the management body.

4.4.1 Information security policy
29. It is unclear on what level in the organisation this policy should be ratified. This should be clarified in the requirement.

4.4.2. Information security function
32. We agree with the conclusions from the EBF that in our view it would be too restrictive and less effective to impose a specific operational or organisational model given that these may vary significantly across financial institutions. It would be more efficient to only list the requirements regarding the security and risk management control objectives. On local Swedish level, this requirement is also in direct conflict with the Swedish FSA interpretation from 2017 of its own regulations FFFS 2014:1 and FFFS 2014:5: page 22:
https://www.fi.se/contentassets/7c8169d883f643f290632afe70989af7/bank-tillsynsrapport2017ny.pdf

"In its supervision, FI has noted that some banks have placed the person responsible for managing and coordinating information security work in one of the control functions. FI finds this to be an inappropriate placement of this position of responsibility, because information security is part of the bank's risk management and shall hence be monitored and controlled by the control functions. Placing this position of responsibility in a control function risks limiting the independence of the function."

33. We agree with the conclusions from the EBF that (most of) the tasks listed in the guidelines (33) should be performed by the first line of defence and that the second line should independently control and report on the effective implementation of those tasks and have the possibility to complement them (e.g. by issuing norms and executing independent controls).

4.4.5 ICT operations security
39.
a) The desired outcome to "identify potential vulnerabilities" that starts this section is not addressed in the text that follows. Instead it addresses the remediation of known vulnerabilities.

The SBA's suggestion: To make this paragraph clearer, we suggest splitting what should be achieved (the outcome) and how it should be achieved (the measures). Suggested wording: "a) evaluate and remediate vulnerabilities by ensuring software and firmware are up to date, including the software provided by financial institutions to its internal and external users, by deploying critical security patches or by implementing compensating controls;"

b) From a network security perspective, it might be counterproductive to only require security baselines for certain “critical network components”.

The SBA’s suggestion: Instead, there should be a framework in place that defines the level or type of security baseline for any given network device, in a risk-based manner. Suggested wording: “b) secure configuration baselines of all network components such as core routers or switches should be implemented in a risk-based manner;”

c) This statement contains a mixture of completely different security measures with different purposes. To make this paragraph clearer, we suggest an outcome-based approach should be used. E.g. what is it that should be achieved with network segmentation, DLP and encryption respectively?

f) How does this relate to the encryption requirements in item c above? Consider combining these requirements into one.

4.4.6 ICT Security monitoring
47.
Current wording: “Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet facing critical applications. “

The SBA’s suggestion: “Financial institutions should ensure that tests of security measures are conducted in the event of changes to *critical* infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet facing critical applications.”

Comment and rationale: By adding “critical” to the control statement the statement better reflects the proportionality principle. E.g. Minor or low risk changes to non-critical or low risk processes, infrastructure or systems might not need security testing depending on the type of risks associated with the change (risk-based approach).

4.5. ICT Operations management
56. How will the requirement, “as far as possible”, be measured by NCA:s for compliance? The requirement should be clarified.

4.6.1. ICT project management
68, 69, 71, 72. The requirements are too prescriptive as they do not allow for strategy implementation through non-project activities, e.g. agile/lean methods.

The SBA's suggestion: The following changes (mainly by deleting existing wording) are therefore suggested:

68. Financial institutions should establish and implement an ICT project management policy which defines the phases of each project. ~~and includes at a minimum:~~

~~a) project objectives;~~
~~b) roles and responsibilities;~~
~~c) project risk assessment;~~
~~d) project plan, timeframe and steps;~~
~~e) procurement management;~~
~~f) key milestones;~~
~~g) and change management requirements.~~

69. The policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function. ~~through all phases of an ICT project~~.

71. The responsibilities of the project team members should be defined and documented in the project plan. ~~and approved by the project implementation leader.~~

72. Establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or aggregated, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. ~~Financial institutions should include project risk in their risk management framework.~~

4.6.2. ICT systems acquisition and development

73. – 76. These requirements could be perceived to dictate that project management and system development methodologies should follow the waterfall model, i.e. a linear sequential design approach for software development. However, most financial institutions have already or are in the process to adopt agile software development. This is another example of this guideline limiting the options available for financial institutions, in this case not only related to risk management but also to business development.

The SBA's suggestion: The following changes (mainly by deleting existing wording) are therefore suggested:

73. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. ~~This process should include:~~

~~a) setting objectives during the development phase;~~

~~b) technical implementation (including secure coding/programming guidelines);~~
~~c) quality assurance standards; and~~
~~d) testing, approval and release, irrespective of whether the development is done in house or externally by a third party.~~

74. Financial institutions should ensure that before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined. ~~In addition, this should include provisions for technical specifications and test plans which are approved by the relevant business management as well as ICT management.~~

76. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. ~~When applicable, regression testing should be performed to ensure that new ICT systems perform in the same way as previously developed and tested systems. They should also use test environments that adequately reflect the production environment so that the behaviour of the ICT systems in the production environment can be predicted and sufficiently tested.~~

4.6.3 ICT change management
The requirements in this chapter are too prescriptive.

The SBA's suggestion: The following changes (mainly by deleting existing wording) are therefore suggested:

81. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are assessed, tested, approved and implemented in a controlled manner. ~~The ICT change management process should contain at least the following elements:~~
~~a) a process for recording all change requests to ICT systems;~~
~~b) an evaluation, testing, and approval process for all change requests to ICT systems - specifically financial institutions should evaluate the impact of the proposed changes and the potential implementation risks. Following approval, and based on the outcome of the evaluation, the process should include a formal acceptance of any new residual risks;~~
~~c) testing and independent validation processes of ICT systems' changes for possible compatibility and security implications prior to deployment to production environment;~~
~~d) an authorisation process, only after which ICT changes move to production. This authorisation process should be undertaken by responsible personnel in such a way so that a rollback can be performed in case of a malfunction;~~
~~e) a process for urgent or emergency ICT changes. Financial institutions should handle changes in case of emergency (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards. Such~~

~~changes should be traceable and notified ex-post to the relevant asset owner for ex-post analysis; and~~
~~f) a process to update ICT systems' documentation to reflect the changes carried out, where necessary.~~

82. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate the risk involved. These changes should be in accordance with the financial institutions formal change management process. ~~part of financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented and authorised.~~

SWEDISH BANKERS' ASSOCIATION

Åsa Arffman Peter Göransson