|  |
| --- |
| Consultation Paper - EBA draft Guidelines on ICT and security risk management - Bits AS, Norway |

1. Specific comments

Chapter 4.2.1 Governance

3. The guidelines specify that ‘members occupying key roles’ must receive appropriate training. We believe that this must apply to all members of staff, not only to an undefined set of key roles. This is also in contrast to the principle in section 30 of chapter 4.4.1 where it is clearly stated that the information security policy should apply to all employees, and section 52 chapter 4.4.8 where training applies to all employees.

Chapter 4.3.5 Reporting

25. For many financial institutions the results of the individual risk assessments may constitute information at a too detailed level to be reported to the management body. We propose that the management body only shall receive aggregated information about the total risk ICT risk picture for the financial institution.

Chapter 4.4.2 Information security function

The guidelines specify that the financial institutions should assign the responsibilities to a designated person at the second line of defence, i.e. in the control function. We believe that the control function should monitor and control the information security function and hence that this person must be located independently of the control function.

Chapter 4.4.5 ICT operations security

The chapter starts with an ambition to “identify potential vulnerabilities”, but then continues to describe a set of best practices for ICT security. There must be a clearer connection between the identification of the potential vulnerabilities and the actions that must be taken as a consequence of the identification of the potential vulnerabilities.

Chapter 4.6.1 ICT project management
Chapter 4.6.2 ICT systems acquisition and development

Although we agree with the guidelines in this chapter, we believe that they relate primarily to large development projects using the waterfall method. Most financial institutions are using an agile project method, and hence these guidelines will increase the burden on project management effectively reducing the speed of development. The guidelines could benefit from a more outcome-oriented focus enabling the project management to deploy these principles without setting up a specific organisation and following principles of waterfall project management.