Klarna

POSITION PAPER
Your reference: EBA/CP/2016/16

European Banking Authority

Stockholm 26 January 2017

Draft Guidelines on internal governance

Klarna AB (publ), (Klarna), appreciated the possibility to attend the public hearing on 5 January 2017 and welcomes the opportunity to comment upon the draft guidelines on internal governance, (draft Guidelines).

About Klarna

Klarna was founded in Stockholm in 2005 with the idea to simplify buying. Today, we're one of Europe's fastest growing companies. In 2014 we joined forces with SOFORT and formed Klarna Group, the leading European payment provider.

Klarna Group has more than 1,400 employees and is active on 18 markets. We serve 45 million consumers and work with 65,000 merchants.

Turnover 2015 for the Klarna Group was 297 MEUR

Klarna AB (publ) is a Swedish credit market company with a license to conduct financing business under the supervision of the Swedish Financial Supervisory Authority, (SFSA).

In general

The Capital requirements regulation and directive (Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms (CRR) and Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV) and has entered into force after the current guidelines, GL44, entered into force. Member States should have implemented the CRV IV into their national laws and regulations. In Sweden this has been done through legislation (Swedish Banking and Financing Business Act) and through SFSAs Regulation and General Guidelines regarding governance, risk management and control at credit institutions (FFFS 2014:1). Klarna thinks, like EBA, that it is important to have harmonized base for effective arrangements, processes and mechanism of internal governance in financial institutions. However, even if there is an analysis of the potential costs accompanied to the draft GL Klarna can see no survey or analysis of the actual need for revising GL 44. Does EBA have signs of deficiencies in GL 44 that have had consequences that merit a complete revision of the guidelines? Klarna is not aware of any such deficiencies and the consultation document does not shed light on whether any such deficiencies have been identified.

The understanding of the Guidelines and a proper implementation requires a well-defined rationale and a description of the material changes and the purpose for these.

Klarna AB (publ)
Org nr: 556737-0431
Sveavägen 46
SE-111 34 Stockholm

Tel: +46 (0)8 - 120 120 00
Web: www.klarna.com
E-mail: info@klarna.com

Because of the change of structure between the two versions, it is also difficult to see or discover where changes have been made. Klarna would much welcome a comparison table. In some cases just one word has been changed compared to GL44, and it is unclear if the new wording is meant to change the whole meaning of the requirement or if the scope should be the same, see for example rule 92 d where "significant" is changed to "material" and rule 106 where "management body shall" is changed to "management body should".

Furthermore, Klarna finds that the draft Guidelines in some parts are too detailed and therefore too restrictive and not really adapted to small and medium sized institutions.

Corporate governance structures

It is stated in the rationale and objective, rule 19 of the draft Guidelines that the draft Guidelines does not advocate any particular structure and are intended to embrace all existing governance structures. This was also stressed by the EBA at the public hearing, and it was said that they have chosen to be vague, e.g. such as by not defining the word "management body", with the intention to allow for national competent authorities to incorporate the requirements in accordance with national law. For clarity reasons, Klarna would recommend this to be expressed in the draft Guideline.

Despite the intention, the draft Guidelines appears to miss the aim to create a guidance that easily can be applied to all sorts of governance structures. The Swedish corporate governance structure lies somewhere in between the Anglo-American and the continental models in several respects. The Swedish Companies Act stipulates that companies must have three decision-making bodies in a hierarchical relationship to one another: the Shareholders´ Meeting, the Board of Directors and the Chief Executive Officer. In practice the CEO usually carries out his duties together with a management team. There must also be a controlling body, the statutory auditor, which is appointed by the shareholders´ meeting. According to the Swedish Corporate Governance Code the shareholders´ meeting´s decisions on election and remuneration of the Board of Directors are to be prepared in a structured, clearly stated process governed by the shareholders (through the Nomination Committee) that provides conditions for well-informed decision-making. The task of the Nomination Committee is among others to specify the duties and profile of Board members, including the chairman, appropriate to the company's operations and in line with the articles of association of the company and the interest of all shareholders. If the shareholders decide to appoint a Nomination Committee, the committee constitutes a body under the Shareholder´s Meeting and is thus not a committee under the Board of Directors.

Three-lines of defense model

In the rationale, rule 20, it says that the draft Guidelines takes into account the "three lines of defense" model. Klarna thinks it is important that the draft Guidelines in this respect are in line with the BCBS Corporate governance principles for banks in order to avoid contradicting requirements. Klarna thinks this has been the intention of the EBA (rule 18). However, in order to achieve this Klarna believes that it is important that certain changes as outlined below are made since there is a risk that the concept that the

Klarna

first line of defense is overall responsible for risk management, including internal control[1] could easily be misunderstood given the terminology used in the draft Guidelines.

The BCBS Guidelines defines internal control system as
"A set of rules and controls governing the bank's organizational and operational structure, including reporting processes, and functions for risk management, compliance and internal audit".

Rule 114 of the draft Guidelines describes this model well. However, other parts of the guidelines are less clear on this. Therefore and to underline more clearly that the first line is responsible for risk management and must also establish internal control systems, Klarna suggests that the second and third line of defense (that is the Risk Control Function, the Compliance Function and the Internal Audit Function), when referred to collectively is referred to as "Independent Control Functions" (instead of Internal Control Functions) to better underline that these functions are part of (and not the entire) internal control system of the institution. Consequently, the defined term "Heads of Internal Control Functions" should be changed to "Heads of Independent Control Functions". Also, the "Risk Management Function" should be renamed "Risk Control Function" as it was in GL 44. The reason for this, being that "Risk Management" shall be performed also in the first line (in accordance with what is stated in rule 20) and not only in the second line functions. It should be clarified to what extent this is reflected in the guideline since the wording can be interpreted as if the guideline only regulates the responsibilities for the control functions in second and third line and not first line. Risk Control is the terminology that should be used for the independent risk control performed in the second line.

In order to make it clearer that the concept of internal control that the draft Guidelines commends is the same as outlined in the BCBS Guidelines, Klarna strongly recommends EBA to apply the principles in rule 114 in all relevant parts of the draft Guidelines.

It should be clarified to what extent this is reflected in the guideline since the wording can be interpreted as if the guideline only regulates the responsibilities for the control functions in second and third line and not first line.

Answers to the EBA questions

Q1 Are the guidelines regarding the subject matter scope, definitions and implementation appropriate and sufficiently clear?
The definitions are not clear enough.

- The meaning of "staff " could be better defined. Should e.g. contractors or consultants be included in the concept?
- For reasons stated above, the term ***Independent*** Control Functions" (rather than ***Internal*** Control Functions) should be used. Consequently the defined term "Heads of Internal Control Functions" should be changed to "Heads of Independent Control Functions".
- The definition of "Conflict of interest" does not correspond to the use of the concept in the text, section 9.3.

[1] The concept that "internal control" is a responsibility for the management and the first line (and something wider than only the work performed in the second and third lines of defense) is also described in e.g. item 93 of the Guidelines on Corporate Governance principles for banks issued by the Basel Committee in July 2015.

Klarna

- The concept of conduct risk should be defined in accordance with EBA/GL/2014/13 – "Conduct risk means the current or prospective risk of losses to an institution arising from inappropriate supply of financial services including cases of wilful or negligent misconduct".
- The definition of Compliance risk in GL44 is not included in the draft Guidelines and there is no explanation for this. It could be useful with a definition but the one provided for in GL44 is too wide since it includes violations and non-compliance with agreements.
- To increase the understanding it is better to write out the meaning of key concepts rather than refer to directives and other documents.

Even though the guidelines do not advocate any particular structure and are intended to embrace all existing governance structures it appears to miss the aim to create guidance that easily can be applied to all sorts of governance structures as described above. A conversion clause is not enough to give a clear and sufficient guidance for Member States which do not have a dual board structure as for example Sweden with a kind of unitary board structure (rule 9). Further, the statement that the reference to the members of the management body in its management function should be understood as applying also to the Chief Executive Officer, CEO, worsens the situation further (rule 10).

Q2 Are there any conflicts between the responsibilities assigned by national company law to a specific function of the management body and the responsibilities assigned by the Guidelines, in particular within paragraph 23, to either the management or supervisory function?

Rule 17 and 19 conflict with national law. According to the Swedish law the Board is the only management body that has the responsibility which the draft Guidelines distribute between the management body in its management function (in Sweden the CEO) and in its supervisory function (in Sweden the Board). It should also be noted that the management body (the CEO), pursuant to Swedish law, has only a limited executive role which makes it even more difficult to reconcile the dual structure presupposed in the draft Guidelines with how Swedish institutions function in accordance with Swedish legislative requirements. The responsibilities for the management body (the CEO) according to Swedish legislation may however be documented and duly approved. It is a too far-reaching requirement in rule 19 h to require committees to include notes of the discussion in the minutes of the meeting. Klarna is afraid that such a requirement would prevent and hamper the possibility for discussion between the committee members. It should be sufficient to document the decision taken or the proposal for decision to be taken by the Board in its whole. In order to encourage the ambition that the discussion in the management body shall be open and critical (as outlined e.g. in rule 26), Klarna proposes that the wording in rule 19 h which suggesting that also discussions should be recorded is taken out in the final version of the Guidelines.

In rule 23 it says that the management body should ensure the integrity of the financial information. It is unclear what integrity means, if the meaning is propriety the wording should be changed.

Klarna think it is too far-reaching to require that no members of the management body in its supervisory function may perform an executive function. The Swedish Corporate Governance Code contains a rule stating that no more than one member of the Board may be a member of the executive management of

Klarna

the company. Klarna strongly recommends this part of rule 24 to be revised and either let this be a matter regulated in national law/regulations or to accept that at least one member of the management body in its supervisory function also holds an executive function. This would enable the CEO or chairman of the management body in its management function to participate also in the management body in its supervisory function.

Klarna believes that it is too far-reaching to include the Risk Committee in rule 24 i), it should be enough that the Audit Committee is involved.

Rule 32 is an example where the conversion clause does not work. The "management body in its management function" and the "management body" in some cases must be interpreted as the CEO according to Swedish law. The CEO shall as such make decisions as provided for by law as well as in accordance with the delegation from the Board. The CEOs decision-making thus is performed by one single person and due to this the last sentence in the rule should be deleted.

Q3 Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear?

As stated above a conversion clause is neither appropriate nor sufficiently clear to cover all management structures among the Member States.

The requirement to create different specialized committees with independent members requires very large Boards which may counteract efficiency and rather create a diffuse and ineffective work within the management body. The requirements in the Guidelines on suitability may also counteract the possibility to keep a very large and suitable management at all times for both large and small institutions. This covers also rule 42. Overall the requirements on the different committees are too detailed; it must be possible to structure the business in different ways depending on the national law and the business in each institution.

According to Swedish regulations a unitary board, which has collective responsibility, shall/may establish various committees consisting of Board members. The committees produce data and suggestions that are discussed and decided by the Board collectively. In the light of that it is difficult to see the rationale behind the requirement where Board members, with the right qualifications, simultaneously cannot participate in various committees.

It is not possible according to Swedish law to create a Nomination Committee with members from the management board. When the CRD IV was implemented the Swedish Government stated in the preparatory work that the requirements on a Nomination Committee are not applicable in Sweden.

Rule 40 is too restrictive and it is difficult to see how this requirement could be fully supervised. The paragraph should be deleted, see also above.

Klarna

It is of outmost importance to keep a clear line between the role of the Risk Committee and the Risk Control Function. The overall responsibility for the Risk Committee is normally to create policies and control the compliance with those. The Risk Control Function normally has the responsibility to control the compliance further down in the organization. It is important to keep the boundary between different functions within the institution. Rule 47 g. can be given as a clear example of this where the draft Guidelines states that the Risk Committee, which consists of Board members, shall examine the alignment between all financial products and services offered to clients (...). This task should rationally be placed at the Risk Control Function. Further, the last sentence of the same rule should be amended as follows:

Klarna thinks that the word "quality" should be deleted from rule 50 a. as it is superfluous.

Klarna is of the opinion that it in subparagraph 50 h is clarified that the duty to review audit reports is limited to such audit reports which are submitted to the Audit Committee.

Q4 Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear?

No, the criteria in Annex I are very unclear. What a policy should contain has been mixed with actions taken or shortcomings noted by independent control functions. Klarna does not think it is reasonable to require a policy to include e.g. weaknesses identified by each control function (6 c) or recommendations made by the internal audit function (6 d). Of course recommendations by the independent control functions should be considered, but these should definitely not be included in a policy document. Annex I should therefore be revised and rewritten.

Moreover, Klarna notes that some of the items mentioned in Annex 1 to the draft Guidelines concerns matters that according to Swedish company law fall within the responsibilities of the CEO. If a policy adopted by the Board addresses issues that are normally the responsibility of the CEO pursuant to applicable company law, this will not be helpful to clarifying governance arrangements in the institution.

Rule74 should be coordinated with the Guidelines on competent authority review process. The competent authority has the possibility to require any information from the entity when the authority so wishes. Therefore there is no need to specifically require institutions to communicate the policy with the competent authority and this should as a consequence be deleted.

Rule 76, it should not be the competent authority´s task to ensure that a group-wide written internal governance policy is compliant with the requirement but rather only the consolidating institution. The authority should review the compliance and take actions if necessary. The first sentence should therefore be rewritten.

Klarna

Klarna thinks it would be helpful if the Guidelines with regards to risk culture would give some guidance on what a following-up procedure or monitoring procedure should include.

What is meant with "outside the institution" in rule 84 a? If this is to be kept in the final version it needs to be explained.

It is neither possible nor recommendable to list unacceptable behaviors in a policy as stipulated in rule 87 c. It may result in a black or white behaviour, if an unacceptable behaviour is not on the list it can be interpreted as an accepted behaviour. Normally the law and regulations specifies what is unacceptable behaviour and it should be enough to give some examples, if any, of unacceptable behaviors. Further, it would be very difficult to review the compliance of the code of conduct relative a black and white list.

Maybe Klarna has not understood things correctly, but to us it seems like rule 88 and 89 govern the same thing? What is the intention? This must be clarified. Furthermore, when it comes to periodically Klarna thinks it should be sufficient to send reports annually.

Klarna finds that the wording in rule 91 is unclear. However, conflicts of interest are well described in GL 44 rule 16.2 and this wording should therefore be kept. Further, GL 44 also includes customers.

The requirement in rule 92 f. leads to a requirement to review all legal and natural persons who may have a relation to persons under (a) to (e) which seems very far-reaching. The requirement in rule 92 f. should be deleted.

The requirement in rule to issue a statement – if any conflict of interest is identified – may violate the bank secrecy or privacy regulations and should therefore be removed. It is also unclear what is meant by "issue a statement". If there really is a need for such publication it should be anonymized or information on a generally basis.

Klarna thinks it is unclear if it is a whistleblowing system which is intended with the internal alert procedure in section 9.4 or something different. If something else is intended it is important to clarify the purpose with an internal alert procedure and the requirement to report an incident. The overall aim must be that incidents actually are reported. Furthermore, it is important that the requirement in rule 97 does not prevent staff from reporting to his/her manager/head.

What is meant with "... in the context of further investigations or subsequent judicial proceedings ..." in rule 102 b? This should be deleted. Furthermore, the requirement in rule 102 d. is not compatible with the possibility to be anonymous.

Klarna

In the context of Section 11 on Outsourcing policy Klarna would strongly recommend EBA to revise and update the present CEBS Guidelines on outsourcing and preferable include guidance on e.g. outsourcing to cloud companies.

Q5 Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear?

The part on proportionality should be placed at the beginning of the draft Guidelines since it covers the all of the rules in it.

Q6 Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear?

What is meant with "strong" in rule 113? It needs to be clarified.

Rule 119 is another example where it is not specified which function is responsible and can be interpreted as together. It could be clarified by adding "in their respective area of responsibility".

The requirements in rule 121 are not compatible with Swedish law since a Board member never could have an executive responsibility, except for the CEO when he/she is part of the Board. Further, if the CEO should be responsible for an internal control function, it is impossible for that person to be independent (see also rule 125 b.).

Rule 128 states that the head of the internal control function etc. are still responsible for these activities and for maintaining an internal control function within the institution. If the guidelines open up for the possibility to outsource the operational task of the internal control function, the remaining functions within the institution cannot maintain this function within the institution but rather to maintain the ability to verify and control that the outsourced activities are properly managed. Further, the principle of proportionality has to be taken into account.

Rule 129 should be rewritten since the concept of internal control functions and institutions are mixed.

Rules 130 and 132 seem to regulate the same matter and should preferable be gathered into one rule to increase the understanding and readability.

In rules 144 and 145 the responsibility for ensuring internal compliance with the new product approval policy has been shared between the Compliance Function and the Risk Management Function. A shared responsibility risk creating either overlap or that issues fall in-between. Klarna firmly believes that an institution should be able to assign the main responsibility to either one of the functions, Risk Control or Compliance, see also rule 148. Many institutions have already assigned this to either one of the two, and it would be very unfortunate if these institutions have to reorganize well-functioning NPA-processes due to the draft Guidelines. Furthermore, it would be desirable if all requirements regarding the new product process could be listed in the same section; see for example rules 158-160 regarding risk and 181 regarding compliance.

Klarna

Further, the wording in rule 145 seems to give the Compliance Function a veto right "... and approval by the compliance function". This is unfortunate, the Compliance Function should assess compliance with the new product and significant changes to products but should not make the business decision.

In rule 149 the risk management function (RMF) is discussed. The text is difficult to understand or apply since it does not take into consideration the different lines of defense nor the responsibility which lies with the business, the first line of defense. The content becomes more understandable if the reference to the RMF instead refers to the Risk Control Function as in GL 44.

Regarding rule 158 the text could be more flexible and therefore changed as follows.

In line with section 14, before decisions on material changes or exceptional transactions are taken, the RCF ~~RMF~~ should be involved, when relevant, in the evaluation of the impact of such changes and exceptional transactions on the institution´s and group´s overall risk and should report its finding directly to the appropriate management ~~body~~ level before a decision on the change is taken.

In rule 160 different kinds of situations seem to have been mixed without any real logic. It has the feel of a "catch-all" rule. The rule should be changed to an explanatory note.

In the first sentence in rule 175, "to manage its compliance risk", should be changed to, "to monitor its compliance risk".

Rule 178 refers to "system". To clarify that the term system does not necessarily mean an IT-system Klarna suggests that the term "process" is used instead.

Rules 180 and 181 state, again, that cooperation should take place, see above rules 144 and 145. Cooperation within an institute is fundamental to fulfil the requirement for an authorization in accordance with the legal requirements. If the draft Guidelines addresses this requirement it means that the competent authority must be able to verify that such cooperation actually takes place, which in turn creates demand that the institutions can show a process for the cooperation. In total, the requirement becomes vague and too far-reaching and should therefore be removed.

With regard to the section 15.3 on Internal Audit Function it would be desirable if all items related to the Internal Audit Function could be gather under the same section, for example rule 69 (structures and activities should be reviewed by the Internal Audit Function).

Klarna also believes that limitations to the risk based approach that are to be applied by the Internal Audit Function shall be limited to the greatest extent possible. Therefore, it is suggested that the review described in rule 69 should be based on a risk-based approach and that this should be reflected in the wording of the rule. A new wording of rule 69 could then be "All these structures and activities [...] should, *subject to a risk based approach* be subject to review by the Internal Audit Function"

In rule 183 "monitoring" in the third sentence should be changed to "audit".

Klarna

Regarding rule 189 the Internal Audit Function should also have unfettered access to persons within the institution. Persons should therefore be added to the first sentence

The requirement in rule 192 is not compatible with GL44 rule 29 5. which states that the audit plan should be approved by the audit committee and/or the management body. This should also be stated in the draft Guidelines.

The last sentence in rule 193 should be removed.

Rule 196 is incomplete, something must be missing. Further, it is unclear if the text refers to the first line or the second line of defense.

Sincerely yours,

Camilla Wahlstedt
Senior Compliance Officer