FINANSTILSYNET

Se vedlagte høringsliste

9. oktober 2014

Ref. hem/pdn

J.nr. 10121-0019

Ny revisionsbekendtgørelse i høring

FINANSTILSYNET
Århusgade 110
2100 København Ø

Tlf. 33 55 82 82
Fax 33 55 82 00
CVR-nr. 10 59 81 84
finanstilsynet@ftnet.dk
www.finanstilsynet.dk

ERHVERVS- OG VÆKSTMINISTERIET

Finanstilsynet sender hermed vedhæftede udkast til bekendtgørelse om revisionens gennemførelse i finansielle virksomheder m.v. samt finansielle koncerner (revisionsbekendtgørelsen) i høring. Udkastet er blevet til efter dialog med Finanstilsynets Rådgivende Revisionsudvalg, med deltagelse af Finanstilsynet, Foreningen af Interne Revisorer (IIA) og FSR – Danske Revisorer.

Neden for gennemgås de væsentligste ændringsforslag kort. Der henvises i øvrigt til vedlagte udkast til revisionsbekendtgørelse.

1. Omfanget af intern revisions arbejde

Finanstilsynet foreslår, med den nye revisionsbekendtgørelse, at indføre et eksplicit krav om, at den af intern revision udførte revision skal omfatte virksomhedens administrative og regnskabsmæssige praksis på alle væsentlige og risikofyldte områder i virksomheden, herunder forretningsgange og interne kontrolprocedurer. Ved forslaget til ændring indføres således et krav til omfanget af den interne revisionsfunktions operationelle revision. De omfattede virksomheder vil være dem, der allerede i dag er underlagt kravet om intern revision, dvs. virksomheder der i gennemsnit har 125 fuldtidsansatte i virksomheden eller koncernen, eller som på grund af størrelse og kompleksitet har valgt at oprette en intern revision. Der henvises til § 22, stk. 1, § 28, stk. 4, § 49, stk. 2 og bilag 4, afsnit 2.2, i udkastet.

I henhold til den nuværende revisionsbekendtgørelse skal intern revision deltage i revisionen af de væsentlige og risikofyldte poster i regnskabet, såfremt intern revision påtegner årsregnskabet. Derudover er der i revisionsbekendtgørelsen reelt kun få krav til, hvilke opgaver intern revision skal udføre, da der er lagt op til stor aftalefrihed i aftalen om arbejdsopgaver (intern revisions funktionsbeskrivelse), der indgås mellem bestyrelsen og den interne revision.

Baggrunden for forslaget er, at Den Internationale Monetære Fond (IMF) ved sin undersøgelse af Finanstilsynet i 2014 konstaterede, at Finanstilsynet ikke stiller et eksplicit krav om, at intern revision skal udføre operationel

revision af alle risikofyldte og væsentlige områder i virksomhederne under tilsyn. IMF har dog oplyst, at de har fået det indtryk, at de største institutter i Danmark i praksis har intern revision, som udfører operationel revision af alle væsentlige og risikofyldte områder.

En række internationale organisationer har opstillet lignende krav henholdsvis anbefalinger til, at intern revision skal/bør udføre operationel revision af alle væsentlige og risikofyldte områder og funktioner, jf. de europæiske Solvens II regler for forsikring, den europæiske banktilsynsmyndigheds retningslinjer vedrørende intern ledelse (GL 44), Basel Komiteens principper for intern revision i pengeinstitutter (BCP) og den internationale sammenslutning af forsikringstilsyn (IAIS) princip om risikostyring og interne kontroller. Der henvises til appendiks til dette brev, hvor de relevante dele af ovennævnte principper er gengivet.

2. Øvrige ændringsforslag

Der er foretaget opdatering af henvisninger, ændringer af terminologi m.v. som følge af den nye lov om investeringsforeninger (lov nr. 597 af 12. juni 2013).

Der er ligeledes foretaget opdatering af henvisninger, ændringer af terminologi m.v. vedrørende engagementer, som følge af Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber.

Det foreslås præciseret, at intern revision skal alene må påtage sig opgaver, som den har tilstrækkelige ressourcer til at udføre, jf. § 24, stk. 2, i udkastet.

Øvrige ændringsforslag i selve bekendtgørelsen er tekniske rettelser.

I bilag 1 ”Konklusioner og oplysninger i revisionsprotokollatet vedrørende årsrapporten” foreslås der tilføjet afsnit for finansielle holdingvirksomheder, forsikringsholdingvirksomheder og for ikke finansielle dattervirksomheder, samt ændret lidt på strukturen af bilaget efter ønske fra revisorerne.

I bilag 2 ”Beskrivelse af revisors arbejdshandlinger” er henvisningerne til de nye ledelsesbekendtgørelser (bekendtgørelse om ledelse og styring af pengeinstitutter m.fl., bekendtgørelse om ledelses og styring af forsikringsselskaber og tværgående pensionskasser og bekendtgørelse om ledelses, styring og administration af danske UCITS) opdateret. De øvrige ændringsforslag er hovedsagligt konsekvensrettelser, som følge af opdatering af henvisninger og tekniske ændringer til selve bekendtgørelsen.

Bilag 3 ”Opsummering af bemærkninger i revisionsprotokollatet vedrørende årsregnskabet” er uændret.

Bilag 4 ”Intern revisions opgaver og ansvar” indeholder forslag til konsekvensrettelser primært som følge af forslaget om regulering af omfanget af intern revisions arbejde.

3. Høringsfrist

Finanstilsynet skal anmode om eventuelle bemærkninger til udkastet senest den 6. november 2014 kl. 12.

Bemærkninger kan sendes pr. mail til hem@ftnet.dk eller pr. post til Finanstilsynet, Århusgade 110, 2100 København Ø, Att.: Helene Miris Møller.

Eventuelle spørgsmål kan rettes til fuldmægtig Helene Miris Møller på tlf. 33 55 84 38 eller specialkonsulent Pernille Dalby Nielsen på tlf. 33 55 82 89.

Med venlig hilsen

Helene Miris Møller
fuldmægtig

Appendiks:

Baggrund for forslag om regulering af omfanget af intern revisions arbejde (operationel revision)

1. Solvens II

De europæiske Solvens II regler for forsikring vil medføre krav om operationel revision for forsikringsselskaberne.

Følgende fremgår af Kommissionens udkast til forordning, artikel 271, stk. 2, litra a, om den interne audit funktions arbejdsopgaver:

> *"establish, implement and maintain an audit plan setting out the audit work to be undertaken in the upcoming years, taking into account all activities and the complete system of governance of the insurance or reinsurance undertaking;"*

2. EBA-retningslinjer vedrørende intern ledelse (GL44)

Den Europæiske Banktilsynsmyndighed (EBA) udgav i september 2011 "EBA Guidelines on Internal Governance (GL44)". Af retningslinjernes afsnit 29 om intern revision fremgår følgende om arbejdsopgavernes omfang:

> *"1. The Internal Audit function („IAF") shall assess whether the quality of an institution"s internal control framework is both effective and efficient.*
>
> *2. The IAF should have unfettered access to relevant documents and information in all operational and control units.*
>
> *3. The IAF should evaluate the compliance of all activities and units of an institution (including the RCF and Compliance function) with its policies and procedures. Therefore, the IAF should not be combined with any other function. The IAF should also assess whether existing policies and procedures remain adequate and comply with legal and regulatory requirements.*
>
> *4. The IAF should verify, in particular, the integrity of the processes ensuring the reliability of the institution's methods and techniques, assumptions and sources of information used in its internal models (for instance, risk modelling and accounting measurement). It should also evaluate the quality and use of qualitative risk identification and assessment tools. However, in order to strengthen its independence, the IAF should not be directly involved in the design or selection of models or other risk management tools.*

> *5. The management body should encourage the internal auditors to adhere to national and international professional standards. Internal audit work should be performed in accordance with an audit plan and detailed audit programs following a „risk based" approach. The audit plan should be approved by the audit committee and/or the management body.*
>
> *…*
>
> *6. The IAF should report directly to the management body and/or its audit committee (where applicable) its findings and suggestions for material improvements to internal controls. All audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their resolution."*

RCF er risikostyringsfunktionen (Risk Control Function).

3. Basel Komiteen's principper (BCP)

Basel Komiteen offentliggjorde i juni 2012 en række principper for intern revision i pengeinstitutter "The internal audit function in banks".

Principperne 1, 6, 7 og 13 omhandler den interne revisions arbejdsopgaver og omfanget heraf. Principperne er citeret nedenfor sammen med de tilhørende relevante vejledende tekster fra Basel Komiteen's dokument med principperne. Det ses tydeligt af principperne, at intern revision i pengeinstitutter ifølge Basel Komiteen skal udføre operationel revision af alle væsentlige og risikofyldte områder og funktioner i pengeinstitutter:

> *"**Principle 1: An effective internal audit function provides independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.**"*
>
> *"**Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.***
>
> *29. The scope of internal audit activities should include the examination and evaluation of the effectiveness of the internal control, risk management and governance systems and processes of the entire bank, including the organisation's outsourced activities and its subsidiaries and branches.*
>
> *30. The internal audit function should independently evaluate the:*

• Effectiveness and efficiency of internal control, risk management and governance systems in the context of both current and potential future risks;

• Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data);

• Monitoring of compliance with laws and regulations, including any requirements from supervisors (see the following subsection for more details); and

• Safeguarding of assets.
…"

*"**Principle 7: The scope of the internal audit function's activities should ensure adequate coverage of matters of regulatory interest within the audit plan**.*

32. Internal audit should have the appropriate capability regarding matters of regulatory interest and undertake regular reviews of such areas based on the results of its robust risk assessment. These include policies, processes and governance measures established in response to various regulatory principles, rules and guidance established by the relevant authorities. In particular, the internal audit function of a bank should have the capacity to review key risk management functions, regulatory capital adequacy and liquidity control functions, regulatory and internal reporting functions, the regulatory compliance function and the finance function.

(a) Risk management
33. A bank's risk management processes support and reflect its adherence to regulatory provisions and safe and sound banking practices. Therefore, internal audit should include in its scope the following aspects of risk management:
• the organisation and mandates of the risk management function including market, credit, liquidity, interest rate, operational, and legal risks;

• evaluation of risk appetite, escalation and reporting of issues and decisions taken by the risk management function;

• the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting on all the risks resulting from the bank's activities;

• the integrity of the risk management information systems, including the accuracy, reliability and completeness of the data used; and

• the approval and maintenance of risk models including verification of the consistency, timeliness, independence and reliability of data sources used in such models.
When the risk management function has not informed the board of directors about the existence of a significant divergence of views between senior management and the risk management function regarding the level of risk faced by the bank, the head of internal audit should inform the board about this divergence.

(b) Capital adequacy and liquidity
34. Banks are subject to the global regulatory framework for capital and liquidity as approved by the Committee and implemented in national regulation. This framework contains measures to strengthen regulatory capital and global liquidity. The scope of internal audit should include all provisions of this regulatory framework and in particular the bank's system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the bank's risk exposures and established minimum ratios.

35. Internal audit should review management's process for stress testing its capital levels, taking into account the frequency of such exercises, their purpose (e.g., internal monitoring vs. regulator imposed), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used.

36. Additionally, the bank's systems and processes for measuring and monitoring its liquidity positions in relation to its risk profile, external environment, and minimum regulatory requirements, should fall within the audit universe.

(c) Regulatory and internal reporting
37. In addition to the matters identified above, internal auditors should regularly evaluate the effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for both internal management and the supervisor.

38. This includes standardised reports which record the bank's calculation of its capital resources, requirements and ratios. It may also include public disclosures intended to facilitate transparency and market discipline such as the Pillar 3 disclosures and the reporting of regulatory matters in the bank's public reports.

(d) Compliance[1]

[1] To be read in conjunction with the Committee's Compliance and the compliance function in banks, April 2005.

39. The scope of the activities of the compliance function should be subject to periodic review by the internal audit function.

40. Compliance laws, rules and standards include primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank.

41. The audit of the compliance function should include an assessment of how effectively it fulfils its responsibilities.

(e) Finance

42. A bank's finance function[2] is responsible for the integrity and accuracy of financial data and reporting. Key aspects of Finance's activities (e.g. calculations, profit and loss valuations and reserves) have an impact on the level of a bank's capital resources and therefore associated controls should be robust and consistently applied across similar risks and businesses. As such, it is important that these controls are subject to periodic internal audit review, using resources and expertise to provide an effective evaluation of bank practices.

43. Internal audit should devote sufficient resources to evaluate the valuation control environment, availability and reliability of information or evidence used in the valuation process and the reliability of estimated fair values. This is achieved through reviewing the independent price verification processes and testing valuations of significant transactions.

44. Internal audit should also include in its scope (the list is not intended to be exhaustive):

- *The organisation and mandate of the finance function;*
- *The adequacy and integrity of underlying financial data and finance systems and processes for completely identifying, capturing, measuring and reporting key data such as profit or loss, valuations of financial instruments and impairment allowances;*
- *The approval and maintenance of pricing models including verification of the consistency, timeliness, independence and reliability of data sources used in such models;*
- *Controls in place to prevent and detect trading irregularities;*
- *Balance sheet controls including key reconciliations performed and actions taken (e.g. adjustments).*

…"

[2] Finance includes valuation, modelling, product control and financial control.

*"**Principle 13: The internal audit function should independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes**."*

4. IAIS's principper (ICP)

International Association og Insurance Supervisors (IAIS) har offentliggjort en række principper for forsikringsselskaber – "Insurance Core Principles, Standards, Guidance and Assessment Methodology" fra 1. oktober 2011. Heraf fremgår der i princip 8 om risikostyring og interne kontroller tillige en række principper for intern revision i forsikringsselskaber.

"8.2.6 The control functions (other than internal audit) should be subject to periodic internal or external review by the insurer's internal auditor or an objective external reviewer. The internal audit function should be subject to periodic review by an objective external reviewer."

"Internal audit function

8.6 The supervisor requires the insurer to have an effective internal audit function capable of providing the Board with independent assurance in respect of the insurer's governance, including its risk management and internal controls.

8.6.1 Part of the oversight role of the Board is to ensure there are means for it to receive independent assurance from an internal audit function that is not operationally involved in the business and is not subject to any conflicts of interest.

8.6.2 The internal audit function should provide independent assurance to the Board through general and specific audits, reviews, testing and other techniques in respect of matters such as:
- the overall means by which the insurer preserves its assets and those of policyholders, and seeks to prevent fraud, misappropriation or misapplication of such assets;
- the reliability, integrity and completeness of the accounting, financial reporting and management information and IT systems;
- the design and operational effectiveness of the insurer's individual controls in respect of the above matters, as well as of the totality of such controls (the internal controls system);
- other matters as may be requested by the Board, Senior Management or the supervisor; and
- other matters which the internal audit function determines should be reviewed to fulfil its mission, in ac-

cordance with its charter, terms of reference or other documents setting out its authority and responsibilities.

…

Main activities of the internal audit function

8.6.7 The audit function should carry out such activities as are needed to fulfil its responsibilities. These activities include among others:
- establishing, implementing and maintaining a risk-based audit plan to examine and evaluate general or specific areas, including on a preventive basis;
- reviewing and evaluating the adequacy and effectiveness of the insurer's policies and processes and the documentation and controls in respect of these, on a legal entity and group-wide basis and on an individual subsidiary, business unit, business area, department or other organisational unit basis;
- reviewing levels of compliance by employees and organisational units with established policies, processes and controls, including those involving reporting;
- evaluating the reliability and integrity of information and the means used to identify, measure, classify and report such information;
- ensuring that the identified risks and the agreed actions to address them are accurate and current;
- evaluating the means of safeguarding insurer and policyholder assets and, as appropriate, verifying the existence of such assets and the required level of segregation in respect of insurer and policyholder assets;
- monitoring and evaluating governance processes;
- monitoring and evaluating the effectiveness of the organisation's control functions;
- coordinating with the external auditors and, to the extent requested by the Board and consistent with applicable law, evaluating the quality of performance of the external auditors; and
- conducting regular assessments of the internal audit function and audit systems and incorporating needed improvements.

8.6.8 In carrying out the above tasks, the internal audit function should ensure all material areas of risk and obligation of the insurer are subject to appropriate audit or review over a reasonable period of time. Among these areas are those dealing with:
- market, underwriting, credit, liquidity, operational and reputational risk;
- accounting and financial policies and whether the associated records are complete and accurate;
- extent of compliance by the insurer with applicable laws, regulations, rules and directives from all relevant jurisdictions;

- intra-group transactions, including intra-group risk transfer and internal pricing;
- adherence by the insurer to the insurer's remuneration policy;
- the reliability and timeliness of escalation processes and reporting systems, including whether there are confidential means for employees to report concerns or violations and whether these are properly communicated, offer the reporting employee adequate protection from retaliation, and result in appropriate follow up; and
- the extent to which any non-compliance with internal policies or external legal or regulatory obligations is documented and appropriate corrective or disciplinary measures are taken including in respect of individual employees involved."