

Risk Committee Resource
Guide for Boards

Illustrative planning tool:
Risk committee calendar of activities



Illustrative planning tool: Risk committee calendar of activities

Risk committees can use this tool to help plan their annual activities and meeting agendas. This tool is current, based on our understanding of the NPR, as of December 2011. It considers the requirements for risk committees as set forth by the U.S. Securities and Exchange Commission (SEC) as well as the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") as further clarified through the Federal Reserve's notice of proposed rule making (NPR) on enhanced prudential supervision, in addition to our understanding of common practices in the marketplace and is subject to change if additional guidance is issued. The "Results From:" section indicates if the action or responsibility results from a leading practice grounded in the NPR or our understanding of a common or emerging practice. The action or responsibility, as described, may not be an explicit legislative or regulatory requirement or proposal, but may be an action that may result from other legislative or regulatory requirements or proposals. The "Suggested Frequency" section offers a suggestion for how often the activity could be performed, while the "Meeting Month" section provides an area where the risk committee can mark the months in which an activity could be performed. The risk committee might use this tool in conjunction with the "sample risk committee charter," and it should be tailored to reflect the responsibilities in the company's risk committee charter.

This document is not an all-inclusive list of activities that a risk committee should or must execute. The planning tool contains general information only and does not constitute, and should not be regarded as, legal or similar professional advice or service. Deloitte does not accept any responsibility for any errors this publication may contain, whether caused by negligence or otherwise, or for any losses, however caused, sustained by any person that relies on it. The information presented can and will change; we are under no obligation to update such information. Deloitte makes no representations as to the sufficiency of these tools for your purposes, and, by providing them, we are not rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. These tools should not be viewed as a substitute for such professional advice or services, nor should they be used as a basis for any decision that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte does not assume any obligations as a result of your access to or use of these tools.

This planning tool is designed for use by U.S. public companies; exceptions to the requirements noted below may apply for certain issuers. Many of the items presented here are not applicable to voluntary filers. All companies should consult with legal counsel regarding the applicability and implementation of the various activities identified.

Action/Responsibility	Results from		Suggested frequency	Meeting month												Comments
	Leading practice grounded in the NPR	Common practice		January	February	March	April	May	June	July	August	September	October	November	December	
Enterprise responsibilities																
Help to set the tone and develop a culture of the enterprise vis-à-vis risk, and promote open discussion regarding risk, integrate risk management into the organization's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them	●	●	Continuously													
Provide input to management regarding the enterprise's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business	●	●	Annually													
Monitor the organization's risk profile — its ongoing and potential exposure to risks of various types		●	Continuously													

Action/Responsibility	Results from		Suggested frequency	Meeting month												Comments
	Leading practice grounded in the NPR	Common practice		January	February	March	April	May	June	July	August	September	October	November	December	
Enterprise responsibilities																
Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products), and transactions and exposures (e.g., by amount) and prioritize them prior to being sent to the board's attention		●	Annually and as needed													
Review and confirm that all the responsibilities outlined in the charter have been carried out		●	Continuously													
Monitor all enterprise risks; in doing so, the committee recognizes the responsibilities delegated to other committees by the board and understands that the other committees may emphasize specific risk monitoring through their respective activities	●	●	Annually and as needed													
Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities; consider a mix of self- and peer evaluation, supplemented by evaluations facilitated by external experts		●	Annually													
Oversee the risk program/interactions with management																
Review and approve the risk management infrastructure and the critical risk management policies adopted by the organization	●	●	Annually													
Periodically review and evaluate the company's policies and practices with respect to risk assessment and risk management and annually present to the full board a report summarizing the committee's review of the company's methods for identifying and managing risks and reporting risks and risk management deficiencies	●	●	Annually and as needed													
Continually, as well as at specific intervals, monitor risks and risk management capabilities within the organization, including communications about escalating risk and crisis preparedness and recovery plans	●	●	Continuously													
Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed		●	Continuously													
Communicate formally and informally with the executive team and risk management regarding risk governance and oversight		●	Continuously													
Discuss with management and the CRO the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies		●	Continuously													

Action/Responsibility	Results from		Suggested frequency	Meeting month												Comments
	Leading practice grounded in the NPR	Common practice		January	February	March	April	May	June	July	August	September	October	November	December	
Oversee the risk program/interactions with management																
Review and assess the effectiveness of the company's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address as appropriate management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs	●	●	Annually and as needed													
Monitor governance rating agencies and their assessments of the company's risk and proxy advisory services policies, and make recommendations as appropriate to the board		●	Annually and as needed													
In coordination with the audit committee, understand how the internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs		●	Annually													
Chief risk officer																
Ensure that the company's CRO (if applicable) has sufficient stature, authority, and seniority within the organization and is independent from individual business units within the organization	●	●	Annually and as needed													
If the CRO reports to the risk committee, review the appointment, performance, and replacement of the CRO of the company in consultation of the nomination and governance committee and the full board		●	Each board meeting													
Reporting																
Understand and approve management's definition of the risk-related reports that the committee should receive regarding the full range of risks the organization faces, as well as their form and frequency of such reports		●	Annually and as needed													
Respond to reports from management so that management understands the importance placed on such reports by the committee and how the committee views their content		●	Annually and as needed													
Read and provide input to the board and audit committee regarding risk disclosures in financial statements, proxy statements, and other public statements regarding risk		●	Annually													
Keep risk on both the full board's and management's agenda on a regular basis		●	Continuously													
Coordinate (via meetings or overlap of membership), along with the full board, relations and communications with regard to risk among the various committees, particularly between the audit and risk committees		●	Continuously													

Action/Responsibility	Results from		Suggested frequency	Meeting month												Comments
	Leading practice grounded in the NPR	Common practice		January	February	March	April	May	June	July	August	September	October	November	December	
Charter review																
Review the charter at least annually and update it as needed to respond to new risk-oversight needs and any changes in regulatory or other requirements		●	Annually and as needed													
Review and approve the management-level risk committee charter, if applicable		●	Annually													
Perform any other activities consistent with the charter, the company's bylaws, and governing laws that the board or risk committee determines are necessary or appropriate		●	Continuously													
Submit the charter to the full board for approval	●	●	Annually													

Contacts

Henry Ristuccia

U.S. Co-Leader
Governance & Risk Management
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Donna Epps

U.S. Co-Leader
Governance and Risk Management
Deloitte Financial Advisory Services LLP
+1 214 840 7363
depps@deloitte.com

Maureen Errity

Director
Center for Corporate Governance
Deloitte LLP
+1 212 492 3997
merrity@deloitte.com

Scott Baret

Partner
Global Leader, Enterprise Risk Services – Financial Services Industry
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Edward Hida

Partner
Global Leader – Risk & Capital Management
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
+1 212 436 4854
ehida@deloitte.com

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.