Combining Internal Audit and Second Line of Defense Functions?
Task Force of Professional Practices Committee of the Institute of Internal Auditors Netherlands.

**Task force members**
drs. S.C.J. Huibers, EMIA RO CRMA | Author of white paper
drs. P.A. Hartog, CIA
G.M. Wolswijk, RA

**Foreword, input and review**
M.N.J. Kee RA | President of IIA Netherlands

This white paper is based on the outcome of the study of a task force of the Professional Practices Committee of the Institute of Internal Auditors in the Netherlands (IIA Netherlands) that was approved by its Board. It is a synthesis of existing guidance and includes the perspective of stakeholders. It does not intend to set new standards or provide new guidance.

©2014, Institute of Internal Auditors Netherlands.
# Contents

Foreword – President of IIA Netherlands ................................................................. 4

Executive Summary ................................................................................................. 5

1 Introduction and context .................................................................................. 8

2 Perspectives ....................................................................................................... 12
  2.1 Stakeholder perspective .............................................................................. 12
  2.2 Professional standards perspective ......................................................... 13

3 Basic conditions and safeguards .................................................................... 15
  3.1 Basic conditions and safeguards when combining functions ................. 15
  3.2 Assurance roles and roles with safeguards and basic conditions .......... 18

References ........................................................................................................... 21

Annex Professional guidance ............................................................................. 23

Glossary – abbreviations .................................................................................... 26
Many different organizational design models are in place to assist the Management Board in its accountability for effective risk management, compliance and audit activities across the organization. Of course the primary responsibility for maintaining sound controls and compliance lies with line management, but increasingly dedicated functions are established to support and oversee these ‘in control’ activities. The different design models range from separate support functions (i.e. Risk Management, Compliance and Internal Control in addition to Internal Audit) to a fully combined Risk, Compliance and Audit function.

There are many different views across companies and industries on the benefits, feasibility and acceptability of combining risk, compliance and assurance functions. Management Boards, Supervisory Boards (in particular the Audit Committee) and other governing bodies want to know if such combinations are possible, under which circumstances, based on which basic conditions and facilitated by which safeguards. The key question is if the internal audit function can work independently and objectively if support is provided on areas relating to risk management, compliance and internal controls.

In order to answer these questions and provide clear direction to the stakeholders involved, a task force of IIA Netherlands conducted research and held roundtable sessions.

This paper provides an overview of existing global standards and good practices and considers the different stakeholder perspectives.

Stakeholders and Governance, Risk Management and Compliance (GRC) professionals are invited to engage in further dialogue about this subject.

Finally, I would like to thank those who have participated in the research and roundtables and, in particular, Sam Huibers for his key role in the task force and for writing this paper.

Michel Kee,
President of IIA Netherlands
Executive Summary

The Three Lines of Defense Model, in which Internal Audit is positioned as an independent separate function in the third line of defense, is considered to be a good practice from the perspective of independent assurance. Management acts as the first line of defense (owning the processes, risks and controls), various support functions including Risk Management, Internal Control and Compliance oversight functions are the second line of defense (monitoring the process, its risks and controls), and internal audit represents the third line of defense (providing assurance and advice). However, in practice the responsibilities and, hence, job titles of Chief Audit Executives (CAEs) vary. Often combinations exist of Internal Audit and second line of defense functions such as Risk Management, Compliance and Internal Control. At both smaller and larger organizations, various names are used for the audit function, including “Audit”, “Internal Audit & Internal Control”, “Risk Management & Internal Audit”, or simply “Compliance”.

This triggered the question of to what extent and how these second line of defense functions can be combined with the Internal Audit function (IAF) without jeopardizing the auditor’s independence and objectivity.

In this paper, we will refer to the total portfolio of assurance and consulting activities as the Governance, Risk Management and Compliance (GRC) activities in which both the IAF and second line of defense functions, such as Risk Management, Internal Control and Compliance, have a role.

Conclusion

The outcome of our research and roundtable sessions is that combining the IAF and second line of defense functions is not the preferred solution from the perspective of the three lines of defense model and the auditor’s independence and objectivity.

(... combining the IAF and second line of defense functions is not the preferred solution from the perspective of the three lines of defense model and the auditor’s independence and objectivity.)

Conclusion

The outcome of our research and roundtable sessions is that combining the IAF and second line of defense functions is not the preferred solution considering the Three Lines of Defense Model as well as safeguarding the auditor’s independence and objectivity as advocated by the Institute of Internal Auditors (The IIA). However, situations may arise where combining functions is perceived to be beneficial to the organization and where it is possible to do so. If so, the basic conditions are to be met and adequate safeguards should be in place to ensure the independence and objectivity of the auditor.
From a management perspective, combining functions can even be preferable and can provide the basis for the design of the organization’s GRC structure. If the organization’s GRC processes are not yet very mature, there may be a temporary role in which Internal Audit supports the setup and design of the methodology. In other situations it may be a deliberate choice to have some functions combined as part of the organization’s assurance model. The drivers for combining functions can be reducing the span of control; expected efficiency and synergies from having all expertise related to assurance, governance, risk, internal control and/or compliance under one umbrella; or simply the fact that the structure grew historically without making explicit rational decisions on how to optimize the organization’s GRC structure.

While the Supervisory Board may have similar considerations, it may put forward other or additional, perhaps even contradictory views. The Supervisory Board/Audit Committee (SB/AC) may play a balancing act to ensure that both internal and external stakeholders are satisfied and adequate safeguards are in place to achieve the company objectives. Considerations with respect to structuring governance in a way that optimizes the safeguarding of assets and compliance with laws and regulations may prevail over more internally oriented considerations. In addition, the SB/AC should monitor that the IAF can and will operate in an effective and objective manner.

Note that in some sectors, such as the financial services industry, regulations apply that require separate Risk Management and Compliance functions. The decisive factor will be the sector-specific regulations the organization has to comply with, and guidance set by relevant governing bodies is to be adhered to.

**Basic conditions and safeguards**

The basic conditions and safeguards to ensure the auditors’ independence and objectivity when combining the IAF and other functions are summarized below and will be described in more detail in this paper. References to the relevant parts of The IIA’s International Professional Practices Framework (IPPF), comprising the Standards and further guidance, are included in the document as well.

**However, situations may arise where combining functions is perceived to be beneficial to the organization and where it is possible to do so. If so, the basic conditions are to be met and adequate safeguards should be in place to ensure the independence and objectivity of the auditor.**

**Basic conditions and safeguards**

The basic conditions and safeguards to ensure the auditors’ independence and objectivity when combining the IAF and other functions are summarized below and will be described in more detail in this paper. References to the relevant parts of The IIA’s International Professional Practices Framework (IPPF), comprising the Standards and further guidance, are included in the document as well.
### Basic conditions and safeguards

**Overarching basic conditions and safeguards**

<table>
<thead>
<tr>
<th>[The IIA Position Paper, 2013]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effectiveness not to be compromised:</strong> lines of defense should not be combined or coordinated in a manner that compromises their effectiveness with respect to providing independent and objective assurance.</td>
</tr>
<tr>
<td><strong>Make consequences explicit:</strong> Internal Audit should clearly communicate the impact of the combination to senior management and the governing bodies (and obtain their approval).</td>
</tr>
</tbody>
</table>

**Subsequent basic conditions and safeguards**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No management responsibility:</strong> Internal Audit should not assume any managerial responsibilities with respect to the audit object. The IAF can facilitate and support, but should never assume ownership.</td>
</tr>
<tr>
<td><strong>Formalize:</strong> roles and responsibilities are to be described in the audit charter in order to avoid ambiguity and provide clarity in the organization.</td>
</tr>
<tr>
<td><strong>Maturity:</strong> in case of a temporary role in which Internal Audit supports the setup of second line of defense functions or design of methodology, the approach is to be approved by the AC.</td>
</tr>
<tr>
<td><strong>Outsourcing:</strong> if Internal Audit is involved in second line of defense activities, the task of providing objective assurance regarding these specific activities will have to be outsourced, either externally or internally to other departments.</td>
</tr>
<tr>
<td><strong>Segregation of duties:</strong> potentially conflicting roles are to be allocated to different individuals and/or (sub-)departments.</td>
</tr>
</tbody>
</table>

Finally, when combining internal audit and second line of defense functions and addressing the question of the auditor’s independence, one has to go beyond focusing on the function’s label only. Therefore, in this paper we also describe the different types of roles that can be fulfilled by the auditor, always taking into consideration any basic conditions and safeguards that may apply.

The common principles to take into consideration when combining internal audit and other functions are full transparency regarding the considerations involved and formalizing the organization’s assurance model. This is important not only to ensure compliance with the international Standards for the professional practice of internal auditing, but also to ensure the full support and commitment of senior management and the SB in order to be perceived as a true value-adding business partner in the organization.

Table 1. Basic conditions and safeguards when combining Internal Audit and second line of defense functions
1 Introduction and context

The Three Lines of Defense Model (see Figure 1, p. 8) is promoted as a good governance practice and advocated by professional bodies, such as The IIA. In early 2013, The IIA issued an international position paper on the three lines of defense model as part of an effective control environment. This paper presents the implementation of the model as a way to enhance clarity on roles and responsibilities regarding ownership and monitoring of risks and controls and on how the effectiveness of risk management systems can be improved.

Three lines of defense model

“In the Three Lines of Defense Model, management control is the first line of defense in risk management, the various risk, control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third. Each of these three ‘lines’ plays a distinct role within the organization’s wider governance framework” [The IIA, 2013]. The different lines of defense within an organization can be described as follows:

- First line of defense – management: business management has the primary responsibility for monitoring and controlling the operations. They own the processes, risks and controls.
- Second line of defense – support functions: management is supported in its monitoring responsibility by separate functions. Examples of these second line of defense functions are Internal Control, Risk Management and Compliance. They monitor the risks and controls.
- Third line of defense – Internal Audit: provides additional independent assurance on the activities of the first and second line of defense. This may include operational audits to assess the controls in various business processes and review the effectiveness of the second line of defense.
functions, such as Risk Management.

- Fourth line of defense – external auditor, regulators and external bodies: additional independent assurance by the external auditor, e.g. typically the company’s financial auditor, limited to the area of financial reporting.

**Second line of defense functions**

As explained above, management often establishes various support functions to help build and/or monitor the first line of defense tasked with risk management, control and compliance monitoring. The nature and activities of these functions will vary per organization and industry. Typical functions in the second line of defense charged with GRC activities include:

- "A Risk Management function that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization" [The IIA, 2013].

- "A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring" [The IIA, 2013].

- An internal control function supports management in identifying key process risks and defining and implementing preventive and detective controls to mitigate these risks.

- Business ethics and special investigations: functions with professionals that focus on communicating and providing training on the company’s code of conduct, overseeing the whistleblowing process and promoting fraud awareness. A team of specialists may be dedicated to follow up on suspicions and allegations of fraud.

**Figure 2. Example of combination of Internal Audit and second line of defense functions**
Management establishes these functions to ensure that processes and controls are properly designed, in place and operating effectively and that identified risks are mitigated.

Particularly in the non-financial sector, when there are no specific regulator requirements regarding the establishment of separate Risk Management and Compliance functions, the activities are often combined (see Figure 2, p.9).

In practice, the boundaries between the activities relating to internal auditing, risk management and compliance are not always that well defined. This triggered the question of to what extent these second line of defense functions can be combined with the IAF, and, if so, how and under which circumstances and conditions this would be acceptable.
Quote of CAE during one of the roundtable meetings: “I have been the CAE in four different organizations. And, although one might expect that I would use these experiences to change the structure and activities of my internal audit departments so they would look similar, I can tell you one thing: that is not the case.”

The objective of the task force of IIA Netherlands was to address dilemmas with respect to combining internal audit with second line of defense functions in the organization’s assurance model. The key dilemma was if and how to combine certain activities while remaining objective and independent in the Internal Audit role. The main research question was:

To what extent and, if so, under what conditions is combining the IAF with Risk Management, Compliance and Internal Control and/or other second line of defense functions acceptable?

First, the aim of the project was not to issue new guidance, but to provide a synthesis of existing guidance in order to be consistent with The IIA’s global Standards as a starting point. Second, the aim was to gain insight into current audit practices. To this end, we held roundtable sessions with Dutch CAEs of multinational organizations and other leading audit professionals. In the next section we will further address this dilemma and the perspectives of the different stakeholders.
2 Perspectives

2.1 Stakeholder perspective

The initial research by the task force and the subsequent roundtable meetings clearly highlighted that the design of the GRC structure and the IAF varies per organization and is usually driven by what senior management and the SB (supported by the AC) consider desirable.

The management considerations regarding combining functions discussed at the roundtable meeting can be summarized as follows:

- **Optimizing the span of control**: limiting the number of people reporting to the Board on assurance activities.
- **Efficiency**: cost control and providing more efficient assurance when organizing assurance activities are under one umbrella. Combining functions may make it easier to prevent the duplication of activities, and oversight as a whole may require fewer resources than in a situation where activities are dispersed across separate functions. If there is separation, coordination can still happen, but may depend on the willingness of managers to cooperate instead of having clear accountability under one combined leadership role.
- **Historical**: the organization of activities could be the product of historical developments; activities may have been gradually expanded and allocated to a single department.
- **Synergy**: creating synergies by bringing together professionals under one umbrella. This may result in a more holistic approach on GRC activities driven by one shared vision. In addition, the vision and strategy will be executed by a group of professionals with a similar mindset as well as complementary competencies. This may be perceived by management as more effective than separating functions. In addition, a larger function might facilitate career planning since in a larger pool more positions and development opportunities can be offered. Furthermore, combining various duties into one leadership role could potentially attract better qualified and more experienced professionals.

...the design of GRC and the IAF varies per organization and is usually driven by what senior management and the SB (supported by the AC) consider desirable.
• **Maturity**: the role of Internal Audit may also depend on the maturity of the processes and controls of the organization. Internal Audit may have a (temporary) role to support the design of the methodology and GRC activities in the company.

While the SB may have similar considerations, it may put forward other, additional, or perhaps even contradictory views. The SB/AC may play a balancing act between ensuring that both internal and external stakeholders are satisfied and that adequate safeguards are in place to achieve company objectives. Considerations with respect to structuring governance in a way that optimizes the safeguarding of assets and compliance with laws and regulations may prevail over more internally oriented considerations such as efficiency. In a recent trend analysis titled *Enhancing Value Through Collaboration* [The IIA, The Pulse of the Profession, Global Report, 2014], ACs have ‘risk management effectiveness’ in their top five attention areas. The associated investment could clash with cost reduction, which is highlighted as a main priority for executive management. In addition, the SB/AC should monitor that the IAF can and will operate in an effective and objective manner.

Finally, the design of governance and other considerations are often very situational and may involve a combination of the factors mentioned above. It may also be affected by the personal preference and experience in other companies of CAEs, management and the SB/AC.

### 2.2 Professional standards perspective

During one of the roundtable sessions, the following dilemmas were raised with respect to combining internal audit with other assurance-related activities:

- How to provide an independent opinion on the effectiveness of the second line of defense;
- How to provide assurance on GRC activities that are provided by professionals in the same department;
- How to deal with the potential perception that the objectivity of activities of the second line of defense in which the audit function is involved has been compromised.

The International Professional Practices Framework of the Institute of Internal Auditors (IPPF), comprising of the Standards and other guidance, does not explicitly address the combination of functions in one department. In most cases the focus is at the activity, rather than the organization, level.
IPPF Performance Standard 2050 – *Coordination* states that the CAE should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

The IIA Practice Guide for this standard, *Coordinating Risk Management and Assurance* [The IIA, 2012], states that if the IAF facilitates risk management activities, basic conditions apply. These basic conditions are described in the next section.

The IIA’s recent Position Paper *The Three Lines of Defense in Effective Risk Management and Control* states that “risk management is normally strongest when there are three separate and clearly identified lines of defense” [The IIA, 2013]. Based on this model, combining functions is not the preferred solution, but it may occur nonetheless. In certain situations it is possible to combine the IAF with functions of the second line of defense, such as Risk Management and Compliance, provided that the necessary basic conditions are met.

In the Annex, we will give a more detailed overview of the main guidance that is currently available from professional bodies, such as The IIA and the Risk & Insurance Management Society (RIMS). In the table in this Annex, we include references on the conditions and safeguards in relation to the guidance described in the next section.

From the guidance it can be concluded that the combination of Internal Audit with other second line of defense functions, such as Risk Management and/or Compliance functions, is possible in certain situations, provided that the required basic conditions and safeguards are in place. In order to provide further practical guidance, we will discuss these situations and basic conditions in more detail in the next section.

**Closing remark: Sector-specific regulations**

Another important factor for GRC processes, such as risk management, is the nature of the entity where they occur. Combining functions is certainly not justifiable for organizations where these processes, e.g. risk management, are a part of the primary process. It will depend on the sector-specific regulations and laws the organization has to comply with. Also, in heavily regulated sectors a combination of supporting functions and Internal Audit may not be desirable.
3 Basic conditions and safeguards

In the previous section we described the current professional guidance regarding the auditor’s role with respect to other assurance providers. In this section we will discuss in more detail the possible safeguards and conditions when combining Internal Audit with second line of defense functions.

3.1 Basic conditions and safeguards when combining functions

If the IAF and second line of defense functions are combined, the key overarching basic conditions and safeguards that need to be in place, as described in the IIA’s Position Paper [The IIA, 2013], are the following:

- **Effectiveness not compromised**
  ‘There are instances where internal audit has been requested to establish and/or manage the organization’s risk management, compliance and internal control activities.’ If this is the case, the different functions should never be combined or coordinated in a manner that compromises the effectiveness of the IAF and the expectation of senior management and the governing bodies that independent, objective assurance will be provided regarding being ‘in control’ of the business.

- **Make consequences explicit**
  ‘Internal audit should clearly communicate to senior management and the governing bodies the nature and impact of the combination.’

Besides this guidance in The IIA Position Paper, we would like to emphasize that in addition to the IAF communicating the consequences to senior management and the AC, there should also be a clear common understanding of the considerations involved, the mitigating measures taken and explicit approval of the combination. In this way the expectation of senior management and the governing bodies that independent, objective assurance will be provided by the IAF is addressed in a transparent way.

The Position Paper is not very specific on what kind of compensating measures may be considered. We will therefore provide some more insight into the conditions and safeguards
based on professional Standards, Position Papers and Practice Guides.

‘There are instances where Internal Audit has been requested to establish and/or manage the organization’s risk management, compliance and internal control activities.’

Subsequent basic conditions and safeguards:

- **No management responsibility**
  The IAF should not make managerial decisions and remains accountable for the process [The IIA, 2004, 2009]. The IAF can facilitate, but should never assume ownership: line management should always be closely involved with the process and they should decide on the risk appetite and the mitigating controls. If, for example, the Internal Audit facilitates the documentation of an internal control framework, then management, in its capacity as process owner, has to sign off on the overall process design, including the control design.

- **Formalization by documenting roles and responsibilities in the audit charter**
  It is important to avoid any ambiguity regarding the potential roles of Internal Audit and second line of defense functions in the organization by explicitly defining these roles. The aim, mandate and nature of the IAF’s activities should be documented in the organization’s audit charter and be approved by the Management Board and the AC. If the IAF is also responsible for one or more second line of defense functions, this should be explicitly stated in the charter, along with the role and responsibilities of the IAF in this respect and the impact on the IAF’s mandate.
• **Maturity**

Internal audit professionals may have the knowledge and expertise to support management in setting up, designing and strengthening risk management controls and compliance programs. In fact, they may be considered the GRC experts in a particular organization that are best equipped to help management with this matter. In case of a temporary role in which internal audit supports the setup and design of methodology, the approach is to be aligned with the Audit Committee [Practice Guide – Performance Standard 2050, The IIA, 2012].

• ** Outsourcing**

Some organizations allocate risk management activities to the IAF, which then acts as a provider of consulting services. In that capacity, the IAF can play a facilitating role in identifying, assessing and introducing risk management methods. If an IAF coordinates a second line of defense function such as Risk Management, another (external) party will have to provide objective assurance on these activities so that Internal Audit does not give an opinion on its own activities [IPPF Performance Standard 2010/2050, The IIA, 2013]. The level of assurance required, if any, may vary per function and organization and is to be determined as part of the annual risk assessment. The scope and frequency of the second line of defense activities is part of the risk-based audit plan that will be approved by senior management and the AC.

• **Applying segregation of duties within the IAF**

Auditors should avoid any potential conflicts of interest by maintaining an independent position. The perception of independence is also an important aspect of this. One of the alternative measures available to help achieve this is to put into place segregation of duties within the IAF. One of the key principles here is ensuring segregation by grouping together activities whose aims are non-identical or at least not potentially conflicting. For example, within the IAF, assurance-related activities could be segregated from consulting-related GRC activities. If the size of the department permits it, an additional safeguard (i.e. ‘second best’ option) would be to segregate the assurance-related activities into a separate sub department.

Based on the principle of independence, the Standards require that internal auditors who were previously responsible for a particular item in another capacity should refrain from auditing that object during the same year [Performance Standard 1130 A.1, The IIA, 2013]. This rule should
also be applied to consulting and participating roles as described in the section below. An auditor who played a role with respect to an audit object should be precluded from conducting assurance activities regarding that object for a period of at least one year.

A key point here is that the organizational structure is not the only factor in deciding what is permissible; the actual roles and activities also need to be considered, as well as the basic conditions mentioned before. Therefore, in the next section we will look in more detail at the roles and responsibilities at activity level.

### 3.2 Assurance roles and roles with safeguards and basic conditions

The roundtable meetings explicitly concluded that what matters is not so much the name given to a function; what really matters is how its activities are carried out and what actual activities are being performed or not.

Often these roles are linked to the maturity of the organization’s process and controls. The IAF has a key role in the design and embedding of GRC-related activities in terms of supporting or participating in projects or even coordinating these activities.

In line with The IIA Position Paper on ERM [The IIA, 2004/2009] and based on publications on the role of the internal auditor in project auditing [Huibers, 2008-2013], the roles regarding GRC activities can be broken down into four categories:

- **The assurance role**: the traditional roles of the internal auditor
- **The consulting role**: consulting roles are roles that can be undertaken, provided that the basic conditions are met and safeguards are in place;
- **The participating role**: participating roles that can be undertaken, again provided that the basic conditions are met and safeguards are in place;
- Roles that auditors should certainly not undertake.

Table 2 (on the next page) provides examples of the potential internal auditor roles, including those subject to basis conditions and safeguards that are similar to the ones described in the previous section (for safeguards, see also the professional standards and guidance in the references, in particular [The IIA, 2004/2009]). The table is not a comprehensive list; it merely illustrates the different type of roles involved.

**Roles that can be undertaken by the internal auditor**

Table 2 describes the roles that can be undertaken by the internal auditor with respect to GRC activities, with safeguards where appropriate.
<table>
<thead>
<tr>
<th>Type of role</th>
<th>GRC roles</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurance</td>
<td>Assurance on second line of defense</td>
<td>Provide assurance on the effectiveness of the second line of defense organization and its activities.</td>
<td>Review the effectiveness of the Risk Management function.</td>
</tr>
<tr>
<td></td>
<td>Compliance and process audits</td>
<td>Provide assurance by performing operational audits.</td>
<td>Perform operational audits, such as HR, supply chain and IT audits.</td>
</tr>
<tr>
<td></td>
<td>Consolidated risk reports</td>
<td>Consolidate reporting on risks to senior management</td>
<td>Identify risks during internal audits and, for example, safety review by Compliance are combined in one report to senior management.</td>
</tr>
<tr>
<td></td>
<td>Evaluate risks and controls</td>
<td>Evaluate control frameworks and assess related risks and controls.</td>
<td>Design review on control framework of a business process redesign project.</td>
</tr>
<tr>
<td>Consulting roles – legitimate roles with safeguards</td>
<td>Advise second line on methodology</td>
<td>Advise the second line on methodology such as risk assessment methodology.</td>
<td>Advise on the design of a risk assessment program and the relevant awareness creation.</td>
</tr>
<tr>
<td></td>
<td>Advise on internal control design</td>
<td>Advise on documentation of standard control frameworks.</td>
<td>Advise on the format and the way controls are documented in the ORCA format (i.e. Objective-Risks-Control Alignment).</td>
</tr>
<tr>
<td></td>
<td>Sounding board – objective observer</td>
<td>Raise questions to reflect on.</td>
<td>Act as a business sparring partner and challenge management based on best practices.</td>
</tr>
<tr>
<td></td>
<td>Coach/trainer</td>
<td>Advise on designing learning experiences or act as coach.</td>
<td>Train the organization in describing procedures and controls.</td>
</tr>
<tr>
<td>Participating roles – legitimate roles with safeguards</td>
<td>Facilitate risk assessments</td>
<td>Facilitate business risk assessments.</td>
<td>Assist management with risk awareness and risk identification sessions.</td>
</tr>
<tr>
<td></td>
<td>Initiate GRC initiatives</td>
<td>Initiate GRC initiatives to improve governance and assessment of risks and controls.</td>
<td>Initiate projects to improve the governance and monitoring of risks and controls, supported by issue and task management tools to monitor the status of follow-up actions.</td>
</tr>
<tr>
<td></td>
<td>Project/process coordinator</td>
<td>Coordinate project activities regarding risk methodology and Control Self Assessments (CSAs).</td>
<td>Coordinate a project to implement CSAs so management can assess the level of compliance with company rules themselves.</td>
</tr>
<tr>
<td></td>
<td>Documentation of controls</td>
<td>Support in the documentation of controls.</td>
<td>Support management in documenting controls using a predefined format as part of a business process redesign project.</td>
</tr>
<tr>
<td></td>
<td>Proactive Quality Assurance (QA) partner – facilitating role</td>
<td>QA partner that not only identifies risks but also translates them into real business issues and makes recommendations.</td>
<td>Support management by proactively providing recommendations on how to mitigate identified risks.</td>
</tr>
</tbody>
</table>

Table 2. Examples of roles of the internal auditor in GRC (adapted from [The IIA, 2004 & 2009] and [Huibers, 2008 -2013])
Roles that should not be undertaken by the internal auditor

Roles that should not be undertaken by the internal auditor with respect to GRC activities.

<table>
<thead>
<tr>
<th>Type of role</th>
<th>Description of roles not to be undertaken by the internal auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>No role Internal audit</td>
<td>Setting the risk appetite.</td>
</tr>
<tr>
<td></td>
<td>Imposing the GRC process.</td>
</tr>
<tr>
<td></td>
<td>Managing risks identified in quality assurance.</td>
</tr>
<tr>
<td></td>
<td>Taking managerial decisions regarding the proposed solutions.</td>
</tr>
<tr>
<td></td>
<td>Implementing solutions on behalf of management.</td>
</tr>
<tr>
<td></td>
<td>Being accountable for project deliverables.</td>
</tr>
<tr>
<td></td>
<td>Being accountable for embedding project deliverables in the organization.</td>
</tr>
</tbody>
</table>

Table 3. Example of roles not to be undertaken by internal audit with respect to GRC (adapted from [The IIA, 2004 & 2009] and [Huibers, 2008 -2013])

The IAF can assist business management but should not assume managerial responsibility. In Table 3 above, we give clear examples of roles the IAF should not undertake. If it assumes these roles, it has crossed the line and, therefore, cannot provide sufficient safeguards to ensure independence and objectivity.

The main conclusion of this final section is that when combining risk, compliance and assurance functions and addressing the question of auditor’s independence, one should not only look at the name of the function. The focus should be on what Internal Audit is actually doing and how this is aligned with the expectations of management and other stakeholders. This should be clearly defined in the audit charter and communicated to the stakeholders.
References

The literature listed below is a selection of recent publications by professional organizations discussing the role of internal auditing in relation to second line functions. While these sources reflect the current trends and views, they are not intended, if that were even possible, as a comprehensive list of the available literature.


References for the overview of internal audit roles in relation to GRC. The tables are based on and have been supplemented from:

Dissertation and various related articles based on ongoing research of S.C.J. Huibers published by IIA Netherlands and the professional bodies in the Netherlands for registered IT auditors (NOREA) and chartered accountants (NBA). Original dissertation of drs. S.C.J. Huibers EMIA RO CRMA, Executive Master of Internal Auditing: *The role(s) of the internal auditor in projects*, Amsterdam Business School, University of Amsterdam, 2008. Published by Kluwer (http://financebase.kluwerfinancieelmanagement.nl/) and can be downloaded from the website of the IIA Netherlands (www.iia.nl/iia-academy/universiteiten/scripties). His international publications are available in the Knowledge-leader® database of Protiviti (http://tinyurl.com/mlo4bua) and the site of Taylor and Francis in the United States (http://tinyurl.com/pnvacz3).
Annex Professional guidance

IIA - International Professional Practices Framework (IPPF)
The International Standards and Guidance of the Institute of Internal Auditors, the International Professional Practices Framework (IPPF), do not explicitly address the combination of functions in one department.

IPPF Performance Standard 2050 – Coordination states that the CAE should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

The IIA Practice Guide for this standard, Coordinating Risk Management and Assurance [The IIA, 2012], states that if internal audit facilitates risk management activities, the following basic conditions apply:
- It should be clear that management remains responsible for risk management and “whenever Internal Audit acts to help the management team to set up or to improve risk management processes, the AC should approve its plan of work” [The IIA, 2012].
- “The nature of Internal Audit’s responsibilities should be documented in the internal audit charter and approved by the board. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed” [The IIA, 2012].
- This is in line with IPPF Attribute Standard 1000 [The IIA, 2013] that states that the purpose of and authority and responsibility for the internal audit activity should be formally defined in an internal audit charter.
- “Internal Audit cannot give objective assurance on any part of the risk management framework for which it is responsible. Other suitably qualified parties should provide such assurance” [The IIA, 2012].

Position Paper on Three Lines of Defense
The IIA’s recent Position Paper The Three Lines of Defense in Effective Risk Management and Control states that “risk management is normally strongest when there are three separate and clearly identified lines of defense” [The IIA, 2013]. Based on this model, combining functions is not the preferred solution, but it may occur nonetheless. In certain situations it is possible to combine the IAF with functions of
the second line of defense, such as Risk Management and Compliance, provided that the necessary basic conditions are met.

**Practice Guide on Coordinating Risk Management and Assurance**

The Practice Guide *Coordinating Risk Management and Assurance* states that management activities may be delegated to a separate Risk Management function [The IIA, 2012]. In addition, some organizations allocate risk management activities to the IAF, which then acts as a provider of consulting services. In that capacity, the IAF can play a role in identifying, assessing and facilitating risk management methods.

**Publication by RIMS and IIA**

The Risk & Insurance Management Society (RIMS) and the IIA have issued a joint publication focusing on optimal collaboration between the Risk Management function and the IAF [The IIA / RIMS, 2012]. It calls for more collaboration, and in some cases even sharing of resources, in order to meet stakeholder expectations as effectively and efficiently as possible.

**Position Paper on Role of Internal Auditing in ERM**

The Position Paper *The Role of Internal Auditing in Enterprise-wide Risk Management* by the IIA [The IIA, 2004/2990] provides further guidelines on the roles of the IAF in risk management. These roles should not necessarily be allocated to a single department. The paper includes a diagram that distinguishes between assurance roles and consulting roles, both of which can be undertaken by internal auditors, provided the basic conditions are met. For example, the IAF can coordinate the activities to put into place risk management and develop and maintain the ERM framework. However, as mentioned before, this requires that certain basic conditions are met; the key condition is that internal auditors do not assume any management responsibility, so as to ensure their independence.

In the table on the next page we summarize the basic conditions and include references to the standards and guidance.
### Basic conditions and safeguards

| Overarching basic conditions and safeguards in the IIA Position Paper [2013] |
|-------------------------------------------------|-----------------------------------------------------------------|
| **Effectiveness not to be compromised:** lines of defense should not be combined or coordinated in a manner that compromises their effectiveness with respect to providing independent and objective assurance. | The IIA Position Paper Three Lines of Defense [2013] |
| **Make consequences explicit:** Internal Audit should clearly communicate the impact of the combination to senior management and the governing bodies (and obtain their approval). | The IIA Position Paper Three Lines of Defense [2013] |

<table>
<thead>
<tr>
<th>Subsequent basic conditions and safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No management responsibility:</strong> Internal Audit should not assume any managerial responsibilities with respect to the audit object. The IAF can facilitate, but should never assume ownership.</td>
</tr>
<tr>
<td><strong>Formalize:</strong> roles and responsibilities are to be described in the audit charter in order to avoid ambiguity and provide clarity in the organization.</td>
</tr>
<tr>
<td><strong>Maturity:</strong> in case of a temporary role in which Internal Audit supports the setup of second line of defense functions or design of methodology, the approach is to be approved by the AC.</td>
</tr>
<tr>
<td><strong>Outsourcing:</strong> if Internal Audit is involved in second line of defense activities, potential assurance regarding these specific activities will have to be outsourced externally or internally to other departments.</td>
</tr>
<tr>
<td><strong>Segregation of duties:</strong> potentially conflicting roles are to be allocated to different individuals and/or (sub-)departments.</td>
</tr>
</tbody>
</table>

Table 4. References and guidance from the IIA regarding basic conditions and safeguards when combining Internal Audit and second line of defense functions
The IIA glossary — abbreviations

AC — Audit Committee
CAE — Chief Audit Executive
IIA — Institute of Internal Auditors
IAF — Internal Audit Function
GRC — Governance, Risk Management and Compliance
IPPF — International Professional Practices Framework of the IIA
ORCA — Objective-Risks-Control Alignment; framework to ensure alignment of objectives, risks and controls across the enterprise.
RIMS — The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the practice of risk management.
SB/AC — Supervisory Board / Audit Committee
QA — Quality Assurance

About the Institute

Established in 1941, the Institute of Internal Auditors (the IIA) is an international professional association.
IIA Netherlands is an independent association, based in Naarden, the Netherlands. IIA Netherlands is recognized by IIA as a national institute. This paper is based on the outcome of a study of the Professional Practices Committee of IIA Netherlands. The author can be contacted via IIA Netherlands at iia@iia.nl.
Disclaimer

IIA Netherlands publishes this document for informational and educational purposes. This publication does not aim to provide definitive answers to specific individual circumstances and as such is only intended to be used as a reference. IIA Netherlands recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this document.

Copyright

Copyright ©2014 Institute of Internal Auditors the Netherlands.

For permission to reproduce, please contact IIA Netherlands at iia@iia.nl. The sources of any quotes or references, including the author, should always be cited.