GUIDELINES FOR THE **COMPLIANCE FUNCTION**

IIA Norge

Guidelines for the Compliance function

PREFACE

A working group whose members work with compliance in several different industries has developed the document «Guidelines for the Compliance function». The working group heads Network Compliance, a sub-faculty of the Association of Internal Auditors Norway (IIA Norge).

IIA Norge would like to thank the following people for their help with the development of this guidance and incorporation of responses following the consultation round:

Izabella Salicath, the Norwegian Export Credit Agency
Janne Britt Saltkjel, Multiconsult ASA
Mette Knutsen, Assuranceforeningen Skuld
Gunnar Holm Ringen, PwC
Ann Christin Flatland, Nets
Lars Kolbjørnsen, Norsk Hydro
Christina Strømodden, DNB
Kathrine Stang Ottesen, Norges Bank (the Norwgian Central Bank)

The goal of the working group has been to describe the purpose, responsibilities and duties of a compliance functions, as well as the relevant assumptions and success factors, regardless of industry. The principles in this guidance may also be useful for organizations without a discrete compliance function, but which have a similar function with comparable duties.

The target group for these guidelines is organizations that would like to either establish a compliance function, or develop their existing compliance function further.

Translated from the Norwegian original
by Katie Huchler, BDO AS

September 2015
ISBN 978-82-92750-13-1

CONTENTS

1. INTRODUCTION

The emergence of compliance functions is relatively new, and it began in the USA shortly after the turn of the millennium. The establishment of compliance functions was a direct consequence of several scandals, the Enron scandal in 2001 being the most significant. These scandals led to improvements in the legal framework, as well as the recognition of weaknesses in regulatory risk management and internal control. Non-American organizations soon followed suit, and several Norwegian organizations have since established a compliance function. The word «compliance» can be loosely translated into Norwegian using the words «samsvar» or «etterlevelse», which both imply conformity or compliance with laws, rules and guidelines. There is however no Norwegian term for the compliance function, and for many the role and duties of the compliance function are still unclear. There is therefore a need to clarify both of these elements, as well as the criteria that need to be met to allow the compliance function to fulfil its duties in a satisfactory manner.

1.1. The purpose of this guidance

The need to establish a compliance function will depend on, amongst other things, the industry and the organization, although typically the drivers are regulatory requirements and/or exposure to the risk of violating laws and regulations. Examples of this can be corruption risk or reputational risk. For some industries/organizations, it is a legal requirement to have a compliance function.

In this guidance we have tried to describe «best practice» for compliance functions regardless of industry, regulation and size. It does not cover the legal requirements to which compliance functions may be subject, rather it introduces the basic principles of the function. Individual adaptations will naturally depend on each organization's nature, size and risk profile.

Several industry specific guidelines have been developed internationally to describe the elements of an effective compliance function, depending on the specific regulatory requirements. Common components from these guidelines, in combination with practice in Norwegian industry, form the basis of this guidance.

This document uses the term «compliance function». This does not mean that there is necessarily one person who holds this position. Rather, compliance work represents a specialized approach to identifying risk, as well as designing and implementing internal controls, which together reduce the risk of failure to comply with relevant laws and regulations.

Throughout this document, we have sought to provide some clarification regarding the organization of a compliance function, as well as the distribution of roles and responsibilities between the different functions of an organization, such as the legal department, internal audit, risk management and compliance.

1.2. General information about the compliance function

«Compliance» refers to conformity with both external[1] and internal[2] laws and regulations. Compliance is a line management responsibility reporting ultimately to executive management (see Section 2.1 on the three lines of defence). The compliance function should, nevertheless, contribute to helping line management develop and implement an effective system of internal control in order to manage the risk of violating external and internal laws and regulations (compliance risk).

The compliance function should have a preventive, advisory and supervisory role, with particular emphasis on:

- Facilitating the effective identification of risk of violation of relevant external requirements, such as compliance with laws and regulations, as well as providing advice on risk reduction measures.
- Developing and facilitating the implementation of internal controls that will provide the organization with protection from compliance risk.
- Monitoring and reporting on the effectiveness of control measures.
- Providing the business with advice about acceptable behaviour and practices in relation to the interpretation of external and internal rules.
- Monitoring relevant regulatory developments within the compliance function's areas of responsibility.
- Ensuring awareness and training.

When performing the tasks above, the compliance function should cooperate with other subject matter experts/departments, such as legal, risk, human resources, quality management, internal control and internal audit.

1.3. Internal control

The term «internal control» encompasses the processes and measures that are intended to reduce the risk of events that could threaten the organization's achievement of its objectives. This is, among other things, to ensure effective and efficient operations, reliable reporting and compliance with external and internal regulations, cf. The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Internal control therefore implies more than the pure «hard» control measures, such as authorizations, reconciliation procedures, quality assurance, but also the «soft» controls related to attitudes, values, culture and expertise.

1 By external laws and regulations is meant first and foremost laws, statutory instruments, and decisions made by public authorities based on statutory powers. Some people include in this definition also industry norms and standards as well as contractual commitments in sales or supplier contracts.

2 By internal laws and regulations is often meant policy guidelines and instructions from the Board and executive management.

1.4. Operational risk and compliance risk

«Operational risk» is the risk of failure of processes related to business operations. «Compliance risk» is the risk that the company's operations lead to violation(s) of regulatory requirements (including statutory regulations). Compliance risk is therefore considered to be an operational risk. For example, the possibility of failure in IT systems poses an operational risk, but if this also means that the business cannot fulfil a legal requirement that is supported by the IT system, the system's failure can as also be considered to be a compliance risk.

The individual organization must be aware of establishing the structure which is best suited to the achievement of effective risk management. This assessment must be documented. Some organizations have divided the structure of the second-line's monitoring of operational risk and compliance risk while other businesses have placed the functions together in the same department. Regardless of their position, there should be a close dialogue and coordination of the work between the various functions. The organizational position and segregation of duties from other control functions are essential prerequisites for providing the compliance function with authority and the ability to exercise its role. Chapter 2 describes in further detail the most important aspects related to organization and duties which must be taken into account when establishing a compliance function.

2. ORGANIZATION AND DUTIES

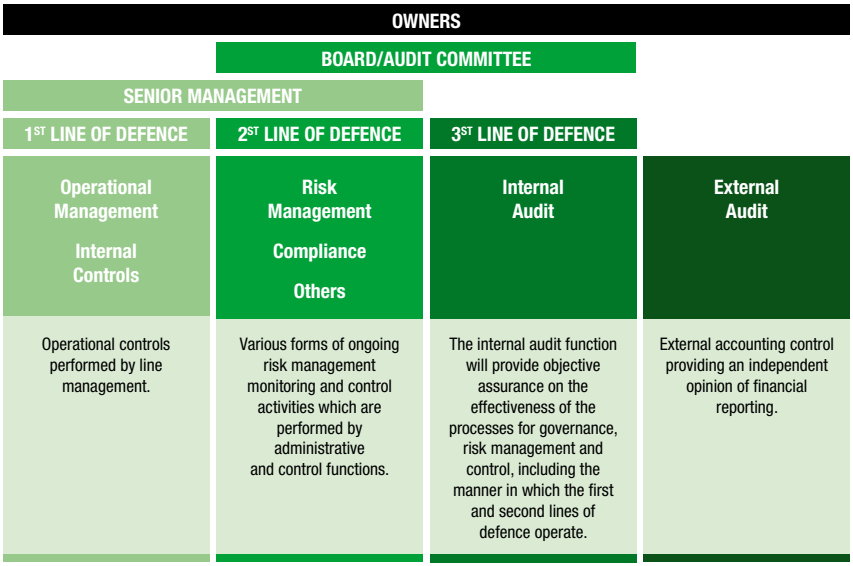
2.1. The Three Lines of Defence and segregation of duties

As a basis for the effective use of resources, as well as to avoid the risk of unsatisfactory monitoring of controls or of duplication of risk management functions and activities, it is important to define clearly the roles and responsibilities of the various organizational functions. This also involves clarifying the interfaces between the functions and their positioning in the organization's overall risk management and internal control structure.

The «Three Lines of Defence» model (see illustration on next page) provides a high level overview of the roles and responsibilities for internal control and risk management in a simple and effective manner. Even in organizations where a formal risk management framework or system does not exist, the model can help improve efficiency and understanding of the organization's enterprise risk management and internal control.

The model provides a description of the control structure in an organization, and distinguishes between three groups (or lines) that are involved in effective internal control and risk management:

- Functions that own and manage risk (first line)
- Functions that exercise oversight over risk (second line)
- Functions that provide independent assurance (third line)



The first line of defence owns and manages operational risk, and must therefore ensure the adequacy of internal control performed by employees in this line, e.g. sales people, clerical staff and other such functions. This entails, amongst other things, implementing measures in order to ensure that their activities comply with external and internal requirements. This includes activities to identify, assess, monitor and follow up the risk of compliance violations, as well as implementing corrective measures where it is deemed necessary in order to manage deficiencies in both the process and the control. The daily operational control activities are typically performed by staff in this line within limits established by operational management.

The second line of defence monitors, guides and helps to improve and report on the first line controls when performing of its own control activities. The second line has internal control at its core. It is management's responsibility to establish various control functions in order to help design and / or monitor the controls that are carried out by the first line. The control activities in the second line are, for example, performed by finance, compliance, risk management and Health and Safety. The specific functions will vary by organization and sector.

The third line of defence is performed by internal audit, and provides governing bodies and senior management with a greater degree of independent and objective assurance than the second line of defence regarding the design and operation of internal controls. Internal audit can, among other things, evaluate whether the organization's processes for governance and control are appropriate and whether internal control functions as intended, including whether the first and second lines of defence are working efficiently and effectively, and are contributing to the organization's achievement of its goals.

It is important to be aware that the functions of the second and third line of defence should act independently of the units they monitor and control. In other words, they should not perform tasks that are the responsibility of the first line, rather they should verify and monitor that the tasks are performed in accordance with external and internal rules and regulations.

Clear mandates and job descriptions are important for being able to distinguish the different functions one from another as well as their areas of responsibility. Management should assess and consider the positioning of the various functions within the organization.

2.2. Management's commitment

The board of directors is responsible for ensuring that the organization operates in accordance with laws and regulations. The CEO is responsible for establishing appropriate risk management and internal controls based upon the guidelines and risk appetite determined by the board. The board's guidelines can require the establishment of a compliance function for the achievement of well- functioning and documented compliance with external and internal regulations.

The structure, responsibilities, functions and authority of the compliance function should be based upon a functional description which has been approved by the organization's management. It should include a description of:

- Organizational positioning, interaction and interface with other control functions and line managment.
- Mandate and budget which balances responsibilities, duties and authority.
- Access to information.
- Reporting responsibilities.

2.3. Reporting and independence

The compliance function must report to a level of seniority in the organization that allows it to discharge its responsibilities whilst at the same time safeguarding its independence from line management. Even though the position in the organization may vary, the compliance function should have the possibility to report directly to senior management, ideally to the CEO. The compliance function should report to the board at least annually, and on other occasions, as required.

People working in and with responsibility for the organization's compliance function should, wherever possible, be organized independently from the operational part of the organization (line management). This means for example that the function should not perform or be responsible for operation activities, or that staff in the compliance function should be precluded from working in the units they are assigned to monitor.

Some small businesses will not have the resources available to create a discrete position to work with compliance. In such cases it is important that the job description identifies and addresses this issue since a mix of roles can negatively impact upon the compliance function's independence. The starting point should be that the business will provide sufficient resources to have a well-functioning and independent compliance function. The function can involve line management in providing assistance in solving problems so long as this does not violate independence requirements.

2.4. Organizational position and organization

The compliance function's organizational positioning will vary by organization and industry. Determination of the most appropriate positioning will depend on the compliance function's focus areas and the other areas and functions with which compliance cooperates and to which it reports internally. The organization's general structure and the maturity of its work in the areas of risk management and internal controls (often industry-dependent), can also be decisive when choosing where in the organization the compliance function should be positioned.

In some organizations, the compliance function is organized into its own separate unit reporting to the CEO on a par with other administrative functions. Some businesses have positioned the compliance function together with risk management, and in that way gathered financial, operational and compliance risk management into one area. Other organizations have positioned the compliance function in the unit for quality assurance which has responsibility for the organization's management systems and governing documents. The compliance function can also be placed together with other risk and control functions in the finance department reporting to the CFO.

Many organizations with their own legal department will choose to place the compliance function there, with reporting to General Counsel. This may be appropriate, given that the legal department is responsible for the interpretation of statutes, regulations and decisions produced by public authorities which fall within the compliance function's mandate. A legal department that exclusively supports business operations, including the execution and management of contracts, will have limited professional interaction with the compliance function and will often be seen as participating in decisions made by line management; in such instances, alternative options for the positioning of the compliance function should be explored.

In some cases, the compliance function is positioned within HR, a decision rooted in the function's cooperation with HR when it comes to the implementation of and compliance with ethical guidelines as well as the management of processes for background checks, training, whistleblowing and disciplinary procedures.

The role of the compliance function is in some cases performed by internal audit, given that internal audit may provide interpretation and give advice on how to ensure compliance with specific legal requirements. Such a solution impairs internal audit's independence with regard to compliance work, and does not represent a compliance function as an independent second line feature as defined in this guidance.

Local compliance employees in selected units in the organization can contribute to efficient and proper performance of compliance work. They can serve as independent compliance managers and / or represent an «extended arm» of the central compliance function by taking responsibility for providing advice, training, monitoring and reporting. In many businesses, such roles are taken on by staff, who also have other roles and responsibilities. For them to be able to exercise their duties in a satisfactory manner, their responsibilities, duties and reporting lines, including the relationship to the central compliance function, must be clearly defined.

These examples show that there is no one right answer as to where the compliance function «belongs» in an organization. Before deciding where the compliance function should be positioned, management should, inter alia, determine the function's focus areas, the areas with which the function will interface and have a professional collaboration, the organization's need for a centre of excellence within risk management and internal control, and the positioning that will best allow the compliance function to exercise its responsibilities in a satisfactory manner.

If management chooses to outsource all or part of the compliance function, it must ensure that the fundamental requirements of a compliance function are safeguarded. It should be noted that specific legislation may limit the possibility of outsourcing of the compliance function.

2.5. Authority, information, resources and expertise

In addition to organizational positioning, it is equally important to determine the organizational level at which the compliance function should be placed. To ensure that the compliance program is managed in an efficient manner, the central as well as local compliance function should be placed at the «senior management» level, and have sufficient experience and subject matter expertise, as well as personal and professional authority. In addition, the function should have adequate resources.

The organization should appoint a person with overall responsibility for the compliance function. The responsible individual, and the compliance function generally, should have access to the required information regarding the company's operations and its decisions through, e.g. access to computer systems, governing documents, physical property, personnel and documents from governing bodies. In addition, the compliance function should have the right to participate in internal meetings, as and when necessary, in order to perform monitoring of activities and discharge its responsibilities in a satisfactory manner.

The compliance function should be tailored to the nature, scope and complexity of the entity's operations. This means that management should define the professional skills and industry knowledge that the compliance function is required to possess in order to be able to fulfil its responsibilities. The function must be assigned a budget, framework conditions and a mandate in order to keep its staff up to date ensuring the necessary access to knowledge and skills development, and to address issues when necessary by carrying out an examination of the facts of a case. For the compliance function to operate effectively, it should be allocated the necessary resources for training and continuing professional development, as well as additional capacity and expertise when needed. The resourcing situation should be assessed regularly, at least once a year.

2.6. Remuneration

The organization should establish a remuneration model that ensures the independence of the compliance function. The remuneration and incentive system for the compliance function should not contain significant performance-based components that could lead to conflicts of interest and influence the objectivity of the staff working in the function. Furthermore, remuneration should be at a level that makes it possible to employ individuals possessing the necessary competence and seniority.

3. METHODOLOGY: COMPLIANCE FUNCTION'S KEY ACTIVITIES

This chapter addresses the most important elements of a compliance program and describes the role that the compliance function would normally have in the various activities.

3.1. Risk methodology

For the effective and appropriate execution of the compliance role, including the prioritization of tasks and use of resources, the compliance function should assume a risk-based approach. Risk assessments are a prerequisite for a compliance program that is tailored to the organization. Risk assessments reveal those activities and areas that require policies and procedures. In certain areas, such a risk assessment process is mandatory.

The board should define the organization's risk appetite, in other words it should decide the level of risk that is acceptable in the different areas. Risk reduction measures may be needed to prevent the risk appetite being exceeded. Work must be adapted to the organization's specific risk profile. Mapping of compliance risk may be part of the organization's overall risk assessment.

An assessment of compliance risk is based on the external and internal regulations applicable to the organization, where violations can have significant consequences, for example in the form of government sanctions, financial loss, damages and loss of reputation. An assessment should be made of the areas of the business (product areas, professional disciplines, geographies) that are the most exposed to the identified compliance risks. In addition, it would be natural to consider risk drivers, such as industry culture, corporate culture (i.e. beliefs, values, and management communications), incentive systems, and internal control measures. The risk assessment process should be conducted regularly, at least annually.

A periodic compliance plan / action plan should be created, based on the outcome of the risk assessment. A risk-based plan is a necessary tool for the effective management of compliance risk. The plan should provide an overview of all activities and tasks to be undertaken during the period related to the prevention / reduction of compliance risk. The plan must be approved by management and coordinated with other management processes and relevant organizational units.

3.2. Governance framework

Each organization should have a framework of governing documents incorporating the policies, procedures, processes and checklists that are rooted in the organization's vision and strategy (from top down). The framework should encompass documents which describe the organizational structure (i.e. organization, roles and responsibilities), and the management system (i.e. process framework, overall strategy, risk management, planning and monitoring). The formulation of policies and procedures should be based on the risk assessment, so that it is relative to the risks facing the organization. The compliance function should be a driving force in ensuring that the business establishes and maintains governing documents for high risk areas.

Governing documents and frameworks must be accessible to all employees, and the documents must be subject to regular reviews and updates.

In order to ensure the required coverage and to minimize duplication, the compliance function should share information and coordinate activities with other internal and external providers of control, monitoring and verification services. This will typically be the legal department, risk management units, HR manager, finance department, internal audit, as well as other individuals in the line management.

It is good practice for employees to be given the opportunity to provide suggestions for improvements to internal governing documents.

3.3. Tone at the top, communication and training

By including topics related to risk management, internal control and compliance on the agenda in management meetings and by their monitoring of their respective responsibilities generally, management, both top and middle management, set the standard for the organization's compliance work («tone at the top»). In addition, it is necessary that managers engage in training and information about ethical guidelines, policies and procedures and how these affect the daily working life of employees (building a compliance culture).

The compliance function should develop and maintain material and plans for training of employees, and contractors in the relevant external and internal regulations. Training in areas with high inherent compliance risks should be mandatory, and line managers have responsibility for ensuring that their employees participate in relevant training. The training may be in the form of case discussions, demonstration of tools and dilemma training, and can be implemented in workshops, classroom training or e-learning. It may also be necessary to adapt the training's scope, content and frequency to different groups of employees and their particular risk exposure.

Training of employees must be continually and regularly monitored and evaluated. A log of completed training should be maintained. A training status review should be part of the compliance function's annual plan. Special consideration should be given to the training that should be mandatory for new employees, other employees and contractors, as well as customers and suppliers.

3.4. Background checks (Integrity Due diligence)

An area the compliance function is often responsible for is the risk-based system for background checks of business partners, also called «Integrity Due Diligence» (IDD). IDD is the examination and assessment of business partners, including ownership and key personnel (such as directors and officers), in order to obtain reasonable assurance of their integrity and business ethics. Collaboration with business partners, such as agents, partners and suppliers, may put the organization at risk of being involved in corruption or other forms of financial crime. Examples are tax evasion, money laundering or social dumping, which could lead to accusations of complicity and / or loss of reputation.

Organizations should conduct a risk-based IDD before establishing relationships with new business partners. The activities the IDD should be risk-based. Guidelines should be issued with criteria for when an IDD is to be performed and how to prioritize resources. These criteria should, as a minimum, determine whether an IDD should be performed and if so, how thorough the investigations should be

in each case. An IDD should be undertaken on potential partner companies if they are new to the organization. It may also be relevant to perform IDDs on existing business partners if any new or suspicious information makes this necessary.

3.5. Registering deviations / reporting loss events

The compliance function should help to facilitate the reporting of loss events and deviations from regulatory requirements. A system should be created that provides an overview of any violations or suspected violations of laws, regulations and internal policies. The objective will be, amongst others things, to identify whether individual incidents / deviations have been caused by a random error or whether they are more systematic in nature, and whether the errors are the result of conscious or unconscious decisions. An overview of individual violations, each of which may individually have only minor impact can help to identify systematic weaknesses which cumulatively can have significant consequences.

The purpose of such a list would be to ensure that the compliance function can identify risks and propose corrective and preventive measures, as well as consider whether policies, routines and procedures are sufficiently effective. The documentation should also help identify whether there are some departments, sections or areas that stand out, and where it is necessary to take action to remedy the failure to comply with regulations.

3.6. Whistleblowing

All organizations should have a proper whistleblowing channel in line with the requirements of the Norwegian Working Environment Act. The compliance function should, as a minimum, ensure that the organization has established a satisfactory whistleblowing channel. In practice, the compliance function often has responsibility for the establishment and monitoring of the whistleblowing channel.
The whistleblowing channel will typically be part of organizations' anti-corruption efforts, and it may be natural that the compliance function is responsible internally. The compliance function may in many organizations also act as a channel for receiving whistleblowing reports and be responsible for receiving and ensure that reports are investigated, examined, and dealt with in a proper manner. This role can also be undertaken by an external whistleblowing function, who will often act in consultation with the compliance function and the legal department.

3.7. Monitoring and evaluation

The organization should evaluate and test internal controls to see whether they work in practice, and be aware of potential weaknesses and areas of risk.

The compliance function should monitor and evaluate the effectiveness of the line management's internal controls ensuring compliance with relevant laws, regulations and internal rules. It may be relevant to monitor all or part of M&A transaction processes, procurement and sales processes, to name just a few areas. This will help to determine whether policies and procedures are designed effectively, whether they are in compliance with applicable regulatory requirements and whether they are carried out in practice. In addition to ongoing monitoring, relevant methods for monitoring and evaluation may include audits, random tests, questionnaires, interviews or inclusion in employee surveys.

Those tests that have been performed must be documented, e.g. by means of a compliance log. This will create verifiability, so that the organization has documentation of its testing for later review by other control and supervisory bodies (such as internal audit and government agencies).

3.8. Documentation

Documentation is an important part of an organization's compliance work. Anything that is not documented will often be considered as having not been performed. Missing documentation may be regarded as failure to comply and could have consequences in observing the reporting requirements from public authorities, investigators or in legal proceedings. Documentation of control activities and measures, including risk assessments, incidents, routine deviations, training etc., should ensure traceability and verifiability as well as evidence of the action taken, and, by implication, of the action not taken to prevent or manage compliance risk.

3.9. Reporting

The organization should establish an appropriate format for reporting by the compliance function. Reporting should provide management and the board with relevant and accurate information about matters that are defined as within the compliance function's areas of responsibility. The reports form the basis for the Board's and management's assessment of internal control and assessment of the need for any measures. Reporting will also serve as documentation to ensure verifiability internally and externally to supervisory bodies.

Typical topics for reporting will be:

- Significant regulatory changes.
- Assessment of the risk of violation of laws and regulations/ compliance risk.
- Measures taken to reduce the risk of violation of laws and regulations.
- Whistleblowing reports and ongoing investigations.
- The status of compliance in priority areas - the results of monitoring and evaluation activities.
- Violations of rules and regulations / loss incidents.
- Reports from supervisory bodies.
- Measures for responding to internal audit reports or investigations.

The compliance function should report to management and the board at least once a year, but more frequent reporting will often be appropriate. The function should also be able to provide ad hoc reports without delay when the results of control evaluations, the severity of violations of laws regulations etc. dictate this.

ABOUT NETWORK COMPLIANCE

Network Compliance was established in 2014 in response to a growing need for a meeting place for those who work with compliance, to act as a forum for discussion of both theoretical and practical issues. Some examples of topics the network discusses are the interface with other business functions such as controllers, internal audit and risk managers, as well as a definition and clarification of the term compliance, in addition to the sharing of best practices, experiences and templates.

In addition to providing unique networking opportunities, the Network seeks to develop guidelines and templates to assist the compliance function. The Network arranges membership meetings, seminars and develops relevant courses.

The Network is industry independent and open to anyone who works with or has an interest in compliance. The network is part of the Norwegian Institute of Internal Auditors Association , but is managed by a separate committee with representatives from the compliance functions of various industries.

THE NORWEGIAN INSTITUTE OF INTERNAL AUDITORS ASSOCIATION (IIA NORGE)

The Norwegian Institute of Internal Auditors Association (IIA Norge) is the association for all those who work with or have an interest in the fields of internal audit, governance (corporate governance), risk management, compliance and control.

Our motto is *«Progress through sharing of knowledge.»*

- We facilitate the sharing of knowledge and experience through training, courses, conferences and networking meetings.
- We offer international certification schemes, with Certified Internal Auditor (CIA) being the most widely recognized, and we have a partnership with the Norwegian business school, BI, to attain the title Diploma of Internal Auditors.
- We provide professional input through a trade publication.
- We translate and make available standards, guidelines and templates for the practice of internal auditing and for guidance to risk management and compliance functions.
- We have our own networking groups for:

| COMPLIANCE | RISK | FRAUD | IT AUDIT
| FINANCE | PUBLIC SERVICE | LEADERSHIP NETWORK

For more information, contact:
IIA Norway
Postboks 1417 Vika, 0115 OSLO, post@iia.no or call (+47) 932 37 912
Further information can be found online: www.iia.no

IIA Norge
Postboks 1417 Vika, 0115 Oslo
Visiting address: Munkedamsveien 3B, 3. etg.
E-post: post@iia.no
www.iia.no

IIA Norge

Guidelines for the Compliance function