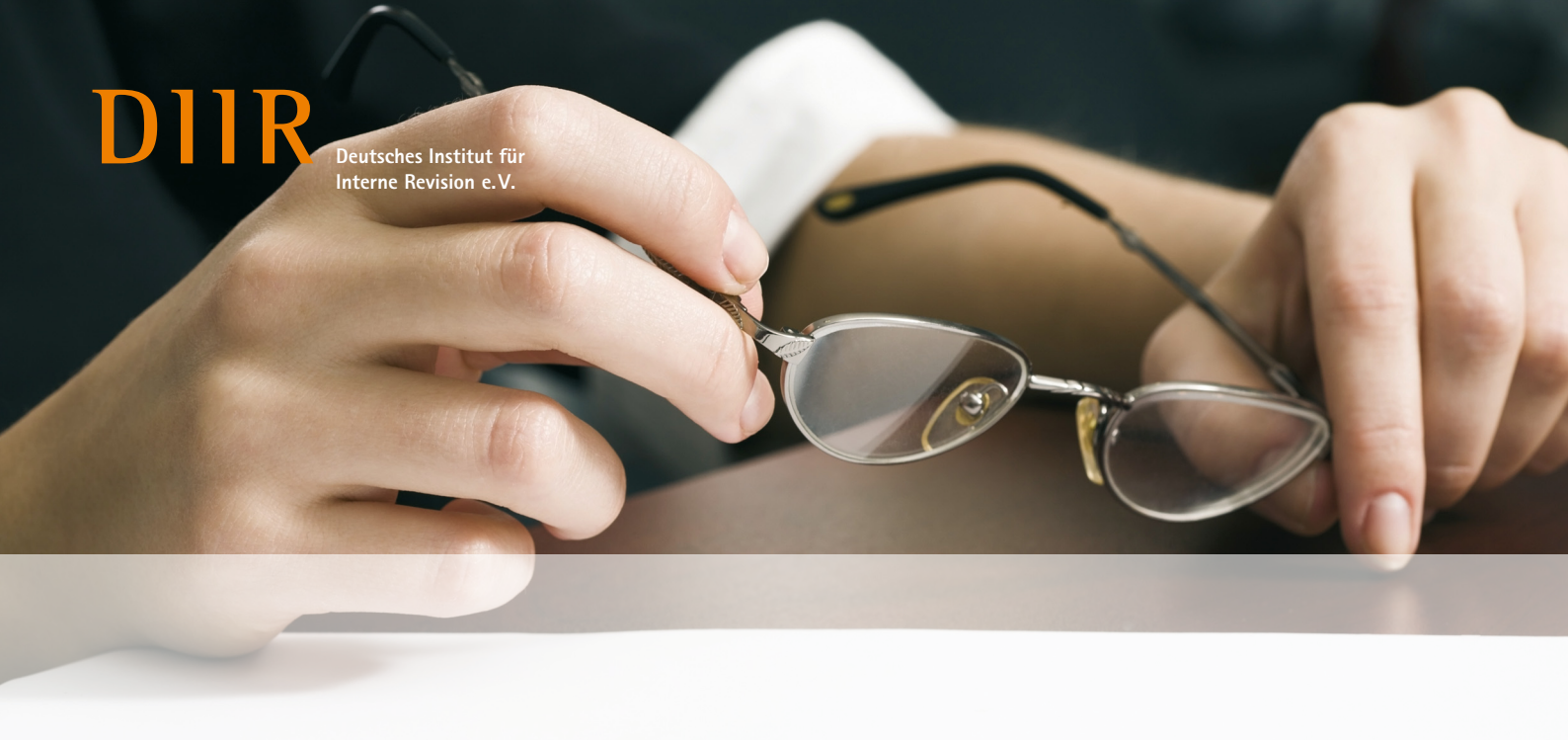


DIIR Deutsches Institut für Interne Revision e.V.

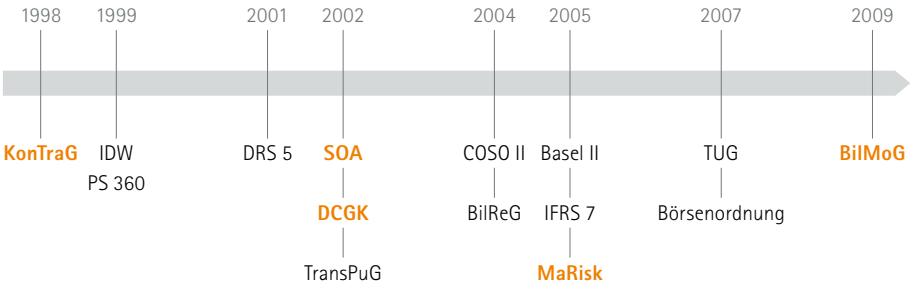
Wie erhöhte Überwachungsanforderungen für Vorstände und Aufsichtsräte durch das BilMoG mit vorhandenen Mitteln erfüllt werden können

Eine starke Interne Revision hilft Vorständen und Aufsichtsräten, Haftungsrisiken zu minimieren

Über eine Vielzahl gesetzlicher Initiativen sind die Anforderungen an Unternehmenssteuerung und -überwachung und damit die Haftungsrisiken für Vorstände und Aufsichtsräte verschärft worden. Die Gründe dafür liegen auf der Hand. Sorgfaltspflichtverletzungen wurden bereits in jüngerer Vergangenheit in immer stärkerem Maße sanktioniert. Dies bedeutet für Vorstände und Aufsichtsräte unter anderem, Unternehmenssteuerung und -überwachung weiter zu optimieren.

- **Machen die gestiegenen Anforderungen ein Aufsichtsratsmandat zu einem unkalkulierbaren persönlichen Risiko?**
- **Wie können Vorstände sicherstellen, dass sie die verschärften Kontrollanforderungen erfüllen?**
- **Welchen Beitrag kann die Interne Revision hier für Vorstände und Aufsichtsräte leisten?**

Gesetze und Regelungsinitiativen



Die Interne Revision unterstützt bei der Abdeckung der BilMoG-Anforderungen

Mit der Neufassung des § 107 AktG Abs. 3 betont das BilMoG erstmals außerhalb des Finanzdienstleistungssektors die Rolle der Internen Revision als ein anerkanntes, wesentliches Element der Unternehmenssteuerung und -kontrolle. Zudem fordert das Aktiengesetz ausdrücklich Sorgfaltspflichten und Kontrollinstanzen, die durch die Unternehmensleitung einzurichten (§§ 90, 91 AktG) und deren Einrichtung durch die Unternehmensleitung vom Aufsichtsorgan zu überwachen sind (§ 111 AktG Abs. 1): das Interne Kontrollsystem, das Risikomanagementsystem und das Interne Revisionssystem.

Vorstand und Aufsichtsrat müssen sich mit dem gesamten Internen Kontrollsystem und Risikomanagementsystem auseinandersetzen (§ 107 AktG Abs. 3). Um hier zu profunden Aussagen zu kommen, sind reine stichtagsbezogene und auf einzelne ausgewählte Prozesse konzentrierte Prüfungen (ex post) nicht mehr ausreichend. Vorstände und Aufsichtsräte haben vielmehr dafür Sorge zu tragen, die Überwachungs- und Kontrollinstanzen so auszurichten, dass Sorgfaltsverletzungen möglichst frühzeitig erkannt und verhindert werden, bevor sie sich in der Zukunft zu haftungsrelevanten Tatbeständen ausweiten können (ex ante).

Zu diesem Zweck prüft eine starke Interne Revision als unabhängige Instanz alle Prozesse des Unternehmens und damit das gesamte Interne Kontrollsystem. Der Abschlussprüfer bezieht sich schwerpunktmäßig auf die Rechnungslegung zum Stichtag und berichtet über die wesentlichen Schwächen des rechnungslegungsbezogenen Internen Kontroll- und Risikomanagementsystems.

Die Interne Revision ist auch deshalb der geeignete Partner der Unternehmensleitungen und der Kontrollorgane, weil sie über in vielen Jahrzehnten entwickelte Methoden und globale Standards zur Bewältigung der angesprochenen Problemfelder verfügt.

Aus der Begründung zum Regierungsentwurf (§ 107 AktG Abs. 3):

„Die Überwachung des internen Kontrollsystems, des ... internen Revisionssystems und des Risikomanagementsystems ist umfassend angelegt ...

... das interne Risikomanagementsystem [ist] somit als allgemeines Risikomanagementsystem zu verstehen, das nicht auf die Rechnungslegung beschränkt ist ...

... Im Hinblick auf die sorgfältige Wahrnehmung der Überwachungsaufgabe liegt es im Interesse des Aufsichtsrats, den Vorstand zu veranlassen, stringente Kontrollsysteme und Informationsabläufe zu installieren, ... und somit eigene Sorgfaltspflichtverletzungen auszuschließen."

Aus der Begründung zum Regierungsentwurf (§§ 289 HGB Abs. 5, 315 Abs. 2 Nr. 5):

„... die unzureichende Einrichtung [eines internen Kontroll- und Risikomanagementsystems kann] die Möglichkeit einer Sorgfaltspflichtverletzung durch die Geschäftsführungsorgane bergen ..."

Effiziente Unternehmensüberwachung durch risikoorientierte Prüfung

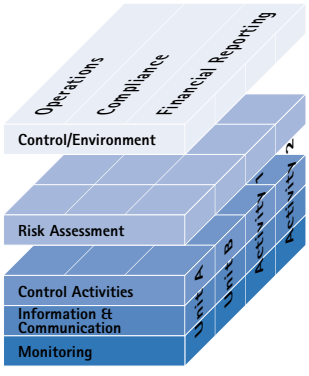
Die Planung der Revisionsprüfungen erfolgt anhand risiko- und prozessorientierter Modelle. So muss der Rahmenprüfungsplan, das „Audit Universe", risikoorientiert aufgebaut sein und alle Prozesse im Unternehmen umfassen (siehe diesbezüglich auch die DIIR-Publikation „Risikoorientierte Prüfungsplanung nach MaRisk", ZIR 2/2008 S. 60 ff.). Ferner legen die anzuwendenden Standards des IIA (Institute of Internal Auditors) fest, dass die Prüfungsplanung der Internen Revision auf Basis einer dokumentierten Risikobeurteilung erfolgt (siehe IIA Standards „Internationale Standards für die berufliche Praxis der Internen Revision", Praktischer Ratschlag 2010.A1) und alle Organisationseinheiten bzw. Geschäftsprozesse anhand strukturierter Elemente abdeckt:

- Risikomanagementmeldungen
- Abweichungen Ist-Plan bei Finanzkennzahlen, z. B. Umsatz und Ergebnis
- Hinweise zum Internen Kontrollsystem
- Hinweise zur Betriebs- und Prozessstruktur der Organisationseinheit

Das Audit Universe stellt für das Unternehmen und die Unternehmensleitung nachweisbar dokumentiert die geforderte systematische Planung der Unternehmensüberwachung sicher.

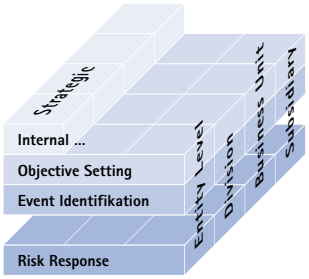
Übersicht über die Bestandteile des COSO ERM-Modells

COSO I:
Internal Control (IC)



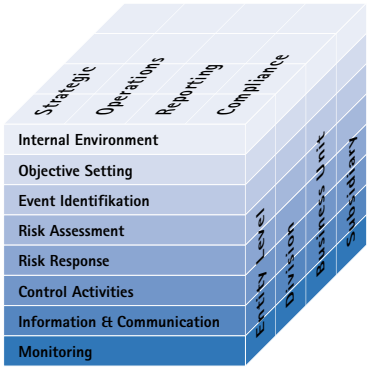
1992

Änderungen/
Ergänzungen



+

COSO II:
Enterprise Risk Management



2004

Mit dem COSO ERM Framework steht der Internen Revision ein erprobtes und anerkanntes Rahmenmodell zur Verfügung. Dieses ist weltweit umfassend im Einsatz

und wird auch von maßgeblichen Organisationen wie der US-amerikanischen Börsenaufsicht SEC anerkannt. Für IT-spezifische Fragestellungen hat sich zudem das daraus abgeleitete CoBiT-Modell als Maßstab etabliert.

Mit der Fokussierung auf die Schlüsselkontrollen (key controls) des Internen Kontrollsystems im Unternehmen verfügt die Interne Revision über eine effiziente Methode, die Angemessenheit und Wirksamkeit der wesentlichen Kontrollen zu überprüfen und zu dokumentieren.

Durch die berufsständischen Standards ist sichergestellt, dass die Arbeit der Internen Revision nach verbindlichen Grundprinzipien erfolgt. Die Standards regeln zum Beispiel die Durchführung von Verfahrens- und Systemprüfungen durch die Interne Revision. Durch diesen systematischen und zielgerichteten Prüfungsansatz wird die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und optimiert sowie das Unternehmen bei der Erreichung seiner Unternehmensziele unterstützt.

Gleichzeitig liefern die DIIR-Standards mit dem Standard Nr. 3 „Qualitätsmanagement in der Internen Revision" dem Aufsichtsrat Beurteilungskriterien, welche für die nach § 107 AktG Abs. 3 geforderte Überwachung der Wirksamkeit der Internen Revision notwendig sind. Anhand dieses Standards kann die Interne Revision auch durch einen Dritten außerhalb des Unternehmens überprüft und bestätigt werden.

Mit ihrem ex ante-Prüfungsansatz, mit dem die präventive Risikovermeidung immer stärker in den Vordergrund gerückt ist, hat die Interne Revision die Herausforderung der geänderten Anforderungen bereits angenommen und sich entsprechend ausgerichtet.

Financial Audit		Operational/Strategic Audit
▪ Fokus auf die Informationsprozesse, die in den Jahresabschluss münden (statisch-stichtagsbezogen)	**Gegenstand**	▪ Fokus auf die Geschäftsprozesse und das Geschäftsumfeld im Sinne des „Understanding the Business" (dynamisch-prozessorientiert)
▪ Primär vergangenheitsorientiert (ex post)	**Betrachtung**	▪ Stärker zukunftsorientiert (ex ante)
▪ Ordnungsmäßigkeit des Jahresabschlusses	**Ausrichtung**	▪ Geschäft des Unternehmens
▪ Prüfungsrisiko (interne Kontrollen)	**Orientierung**	▪ Geschäftsrisiko (Geschäftsprozesse)
▪ Kennziffern und Krisensymptome	**Risikoanalyse**	▪ Key Performance-Indikatoren
▪ Prüfersicht	**Risikobeurteilung**	▪ Unternehmenssicht bzw. Sicht der Unternehmensleitung
▪ Bestätigungsvermerk, Prüfungsbericht (mit Erläuterungen zu Einzelpositionen)	**Prüfungsergebnis**	▪ Bestätigungsvermerk, Prüfungsbericht (mit Maßnahmen/Hinweisen zu Benchmark- und Best-Practice-Prozessen)

Kern ist dabei die präventive Risikobegrenzung anhand der Prüfung von Geschäftsprozessen. Präventives Risikomanagement ist dann erfolgreich, wenn Prozesse möglichst vollständig analysiert, Schwachstellen innerhalb der Prozesse erkannt und als potenzielle Risikoquellen eliminiert werden. Dieser Ansatz führte zum Operational Audit, welches mittlerweile in der Revision „best practice" geworden ist und zum Wechsel in der Ausrichtung hin zur zukunftsorientierten „ex ante" Denk- und Handlungsweise in der Revision dient.

Präventive Risikobegrenzung durch Prüfung von Geschäftsprozessen

Die Orientierung am Geschäftsrisiko und eine profunde Risikoanalyse auf der Basis von Key Performance-Indikatoren in Verbindung mit einer kompetenten Risikobeurteilung aus Sicht der Unternehmensleitung forcierte die weitere Entwicklung hin zum Management- oder Strategic Audit einer erfolgreichen modernen Revision heutiger Prägung.

Orientierung am Geschäftsrisiko

Konsequente Schwachstellenbeseitigung und Prozessverbesserungen

Im Regelfall resultiert aus Prüfungen die Identifikation von Schwachstellen. Die Interne Revision gibt entsprechende Empfehlungen zur Beseitigung der Schwachstellen und zur konsequenten Prozessverbesserung.

Systematische Methoden und Verfahren identifizieren Schwachstellen und ermöglichen eine präventive Risikoerkennung.

Hierbei kommen moderne Revisionstools zum Einsatz. Dazu zählen Tools für die Massendatenanalyse, wie beispielsweise in Einkauf oder Vertrieb, ebenso wie für Systemprüfungen in IT-Systemen. Sie unterstützen die Revision bei der Identifikation von Schwachstellen ebenso wie bei der präventiven Risikoerkennung und Aufdeckung von Fraud-Vorfällen im Unternehmen. Neben der Fokussierung auf Schlüsselkontrollen ist die Interne Revision häufig unter Wahrung ihrer Unabhängigkeit und unter Vermeidung von Interessenkonflikten bei wesentlichen Projekten begleitend tätig. Dies versetzt sie in die Lage, frühzeitig auf potenzielle Schwachstellen hinzuweisen und somit Mängel im Internen Kontrollsystem ex ante vermeiden zu helfen.

Hinzu kommt, dass die meisten modernen Revisionsbereiche neben Generalisten über hervorragend ausgebildete Spezialisten verfügen, um die in der heutigen Geschäftswelt oft sehr komplex gewordenen Themen ordnungsgemäß und in einer adäquaten Detailtiefe prüfen zu können. Auch die Berufsstandards verpflichten die Revision, über das Wissen, die Fähigkeiten und sonstige Qualifikationen zu verfügen, die erforderlich sind, um ihrer Verantwortung gerecht zu werden (siehe IIA Standards „Internationale Standards für die berufliche Praxis der Internen Revision", Praktischer Ratschlag 1210) und diese durch regelmäßige fachliche Weiterbildung zu erweitern (siehe IIA Standards

Berufsstandards, gezielte Weiterbildung und die Nähe zum Unternehmensgeschehen der Revision bilden die Grundlage für strukturierte Verfahren.

„Internationale Standards für die berufliche Praxis der Internen Revision", Praktischer Ratschlag 1230). Nicht zu unterschätzen ist auch die ganzjährige „Nähe zum Unternehmensgeschehen", welche die Interne Revision beispielsweise im Gegensatz zu externen Beratern hat. Diese versetzt die Revision durch ihre unternehmensspezifische Erfahrung in die Lage, Vorstände und Aufsichtsräte als „unternehmensinterner Berater" sehr effektiv in deren Überwachungsaufgaben zu unterstützen.

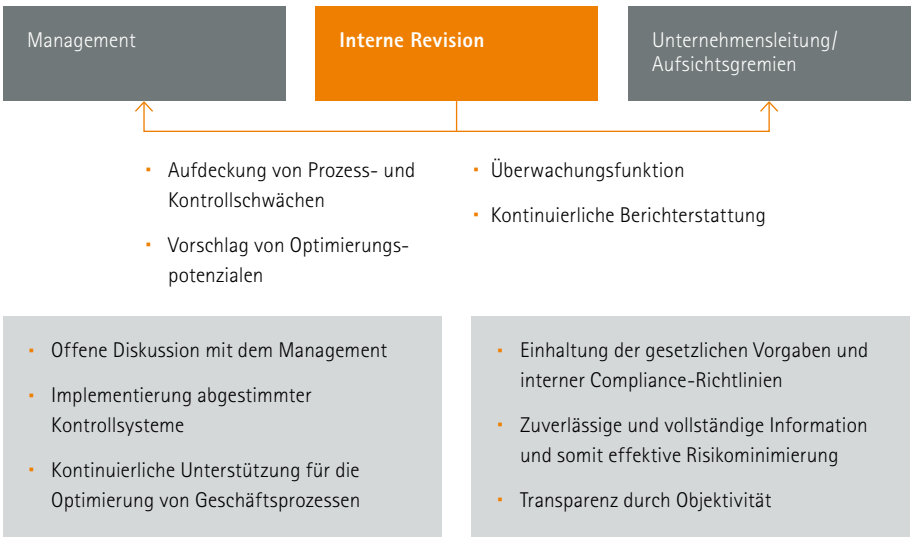
Etablierte und effiziente Kommunikationssysteme ermöglichen einen wirksamen Eskalationsprozess.

Mit dem erprobten Revisionsansatz des Follow Up, das zur Umsetzungskontrolle der für die Beseitigung der festgestellten Schwachstellen vereinbarten Maßnahmen eingesetzt wird, verfügt die Revision über ein etabliertes und effizientes Kommunikationssystem an die Unternehmensleitung. Neben der Statusmeldung über den Status der Risikominimierung im Unternehmen steht damit gleichzeitig im Falle von Verzögerungen bei der Umsetzung ein wirksamer Eskalationsprozess zur Verfügung.

Revision erkennt und dokumentiert Optimierungspotenziale – das schafft Mehrwert.

Mit ihren Prüfungsberichten, die explizit Maßnahmen und Hinweise zu Benchmark- und Best Practice-Prozessen enthalten, liefert die Revision einen Mehrwert für das Unternehmen und gibt der Unternehmensleitung Sicherheit hinsichtlich der Angemessenheit und Wirksamkeit der eingerichteten Überwachungs- und Kontrolleinrichtungen. Damit haben die Unternehmensleitungen und die Aufsichtsorgane einen wesentlichen Teil der an sie gerichteten Überwachungsanforderungen nachweisbar dokumentiert und abgedeckt.

Mandat der Internen Revision



Strukturierte Information und Berichterstattung

Die unterjährige und jährliche Berichterstattung an die Unternehmensleitung sowie an das Aufsichtsorgan unterstützt grundsätzlich die zur Erfüllung der Sorgfaltspflichten von Unternehmensleitung und Kontrollorgan erforderlichen Kommunikations- und Informationsprozesse. Mit der Berichterstattung werden insbesondere die festgestellten Mängel im Bereich der Internen Kontrollen und des Risikomanagements aufgezeigt und dokumentiert. Die Dokumentation dient als Grundlage für die Beseitigung der Mängel.

Erfüllung von Sorgfaltspflichten bedeutet auch: etablierte Kommunikations- und Informationsprozesse

In diesem Zusammenhang ist darauf hinzuweisen, dass die Interne Revision durch das BilMoG auch stärker in den Fokus der Jahresabschlussprüfung gerückt ist, da der Abschlussprüfer in der Bilanzsitzung des Aufsichtsrats bzw. Prüfungsausschusses über die wesentlichen Schwächen des Internen Kontrollsystems und des Internen Risikomanagementsystems bezogen auf den Rechnungslegungsprozess berichten muss. Die Existenz einer funktionsfähigen Revision wird somit auch von externer Seite überwacht, was sich zusätzlich positiv auf die Qualität der Revisionsarbeit auswirken wird.

BilMoG fordert eine angemessene und wirksame Interne Revision.

Was bleibt zu tun?

Damit die Interne Revision ihre Wirkung entfalten kann, sind einige Grundvoraussetzungen unabdingbar. Ziele und Befugnisse müssen vereinbart und verbindlich z. B. durch eine Geschäftsordnung/Charta vom Vorstand in Kraft gesetzt und unternehmensweit kommuniziert werden. Die Interne Revision muss der Unternehmensleitung direkt unterstellt sein und regelmäßig an Vorstand und Prüfungsausschuss berichten. Die Ressourcen- und Personalausstattung der Internen Revision muss der Größe und Komplexität des Unternehmens angemessen sein. Insbesondere müssen die Mitarbeiter entsprechend ausgebildet sein – zum Beispiel als Certified Internal Auditor (CIA) – und regelmäßig weiterentwickelt werden. Die Qualität der Facharbeit der Internen Revision sollte ihrerseits ferner regelmäßig intern oder extern geprüft werden.

Auch hierzu bietet der Berufsstand der Internen Revision eine Fülle von praktischen Hinweisen und Gestaltungshilfen.

Die Aufgaben und Ziele des DIIR

Als gemeinnützige Organisation vertritt das DIIR – Deutsches Institut für Interne Revision e.V. mit Sitz in Frankfurt am Main die Interessen der Revisoren. Hauptanliegen ist der ständige nationale und internationale Erfahrungsaustausch und die Weiterentwicklung in allen Bereichen der Internen Revision. Heute zählt das Institut über 2.300 Firmen- und Einzelmitglieder aus Wirtschaft, Wissenschaft und Verwaltung. Es unterstützt die in der Internen Revision tätigen Fach- bzw. Führungskräfte mit der Bereitstellung von Fachinformationen. Weitere Ziele und Aufgaben sind die wissenschaftliche Forschung sowie vor allem die Entwicklung von Grundsätzen und Methoden der Revision.

Nähere Informationen:
DIIR e.V.
Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 713769-0
Fax (069) 713769-69
www.diir.de
info@diir.de

Das DIIR in Zahlen

- Gegründet 1958
- Über 2.300 Mitglieder
- 26 Arbeitskreise und mehr als ein Dutzend (branchenspezifische) Erfahrungsaustauschtage pro Jahr
- Mehr als 160 Seminare, Tagungen und sonstige Weiterbildungsveranstaltungen über die DIIR-Akademie

DIIR Deutsches Institut für Interne Revision e.V.