T. FLEMMING RUUD
KATHARINA SCHRAMM
ADRIAN KYBURZ

AKTUELLER STAND DER INTERNEN STEUERUNG UND KONTROLLE IN DER SCHWEIZ

Einblicke in die Praxis und Implikationen für das interne Audit*

Das Institut für Accounting, Controlling & Auditing (ACA-HSG) der Universität St. Gallen veröffentlichte kürzlich eine Studie zum aktuellen Stand des internen Kontrollsystems (IKS) in Schweizer Unternehmen ausserhalb des Finanzsektors. Der vorliegende Beitrag basiert auf den Studienergebnissen.

1. EINLEITUNG

Ein zentrales Aufgabengebiet des internen Audits ist nach wie vor die Prüfung und Verbesserung der internen Steuerung und Kontrolle, welche häufig als Teilbereich des Risikomanagements und der Governance erachtet wird und vor allem mit dem Risikomanagement viele Schnittmengen aufweist [1]. In Zeiten von komplexen Risiken ergeben sich rund zwei Jahrzehnte nach der grossen internationalen Regulierungswelle im Bereich der Governance Möglichkeiten und Herausforderungen für das IKS in Schweizer Unternehmen. Obwohl das IKS als wertschaffendes Instrument zur Unterstützung der Zielerreichung eingesetzt werden kann, können Schwachstellen potenziell langwierige Folgen in den operativen Geschäftsprozessen, in der finanziellen Berichterstattung oder im Bereich der Compliance nach sich ziehen. Zudem führen Doppelspurigkeiten möglicherweise zu Ineffizienzen oder zu einer Abwehrhaltung der Mitarbeitenden. Wird das IKS aber insbesondere von Unternehmen, die gemäss Art. 728 a des Obligationenrechts (OR) im Rahmen der ordentlichen Revision zum Nachweis der Existenz eines IKS verpflichtet sind, nicht bloss als Selbstzweck zur Erfüllung der regulatorischen Anforderungen erachtet, kann es effektiv zum Unternehmenserfolg beitragen [2].

Aktuell wurde am Institut für Accounting, Controlling & Auditing der Universität St. Gallen (ACA-HSG) eine umfassende Studie zum IKS in Schweizer Unternehmen ausserhalb des Finanzsektors durchgeführt [3]. Insgesamt nahmen 64 Personen teil, mehrheitlich Finanzleiter, Leiter des IKS und der Controlling-Abteilung. Mit Hinblick auf die Branchenzugehörigkeit der Teilnehmer waren zu 38% die Industrie, zu 18% der Gesundheitssektor und zu 10% die Konsumgüterbranche vertreten. Weitere in den Ergebnissen repräsentierte Sektoren sind Technologie, Grundstoffe, Energie, Telekommunikation und Verbraucherservice. In Bezug auf die Unternehmensgrösse sind drei fast gleichmässig grosse Teilgruppen zu identifizieren: Kleine Unternehmen mit bis zu 250 Mitarbeitenden (35%), mittelgrosse Unternehmen mit 251 bis 999 Mitarbeitenden (29%) und grosse Unternehmen mit 1000 oder mehr Mitarbeitenden (36%). Ausgangslage und Intention der Studie war es zu untersuchen, welche Ziele mit dem IKS verfolgt werden, welche Rahmenwerke zum Einsatz kommen, mit welcher Maturität die einzelnen Komponenten ausgestaltet sind und wo die befragten Nichtfinanzunternehmen weitere Verbesserungspotenziale für die Zukunft identifizieren. Da Mehrfachnennungen bei verschiedenen Fragen möglich waren, können die kumulierten Prozentzahlen nachfolgend mehr als einhundert Prozent betragen.

2. RAHMENWERKE, VERANTWORTLICHKEITEN UND ZIELSETZUNGEN

Die bekanntesten Rahmenwerke zum IKS oder zum Risikomanagement, welches ersteres miteinschliesst, sind bei den repräsentierten Schweizer Nichtfinanzunternehmen die

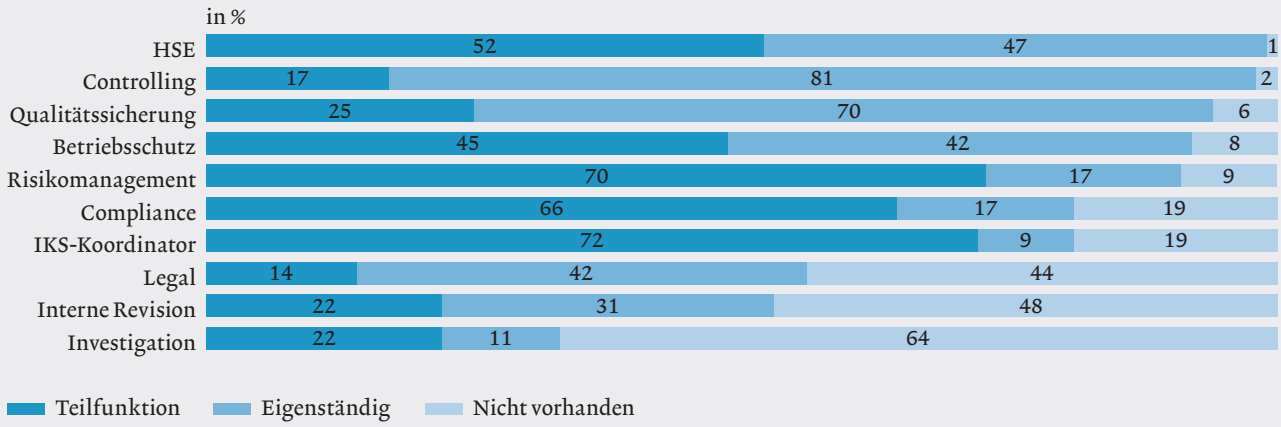


T. FLEMMING RUUD, PROF., PHD, WP (N), PROFESSOR FÜR BETRIEBSWIRTSCHAFTSLEHRE (INTERNAL CONTROL/INTERNAL AUDIT), UNIVERSITÄT ST. GALLEN, ST. GALLEN



KATHARINA SCHRAMM, MASTER OF ARTS HSG/INTERNATIONAL MANAGEMENT (CEMS), DOKTORANDIN, WISSENSCHAFTLICHE MITARBEITERIN VON PROF. T. FLEMMING RUUD, UNIVERSITÄT ST. GALLEN, ST. GALLEN

Abbildung 1: **RISIKO- UND KONTROLLFUNKTIONEN IN SCHWEIZER NICHTFINANZUNTERNEHMEN**



beiden *Frameworks des Committee of the Sponsoring Organizations of the Treadway Commission (COSO)* aus den Jahren 2013 [4] (48%), respektive 1992 [5] (47%). Verbreitet sind zudem die ISO Norm 31000:2009 zum Risikomanagement [6] (ein Update der Norm im Jahr 2018 wurde nach der Durchführung der Studie publiziert) (42%) und das COBIT 5-Rahmenwerk [7] (23%) der *Informations Systems and Control Association (ISACA)* für Informationssysteme. Hinsichtlich der in den Unternehmen eingerichteten Risiko- und Kontrollfunktionen ist erkennbar, dass die Controlling-Abteilung bei 81%, die Qualitätssicherung bei 70% sowie die *Health, Safety & Environment (HSE)*-Division bei 47% als eigenständige Funktionen vorhanden sind. Weitere Aktivitäten wie Betriebsschutz, Risikomanagement, Compliance oder die IKS-Koordinationsstelle sind seltener eigenständige Funktionen, dafür jedoch relativ häufig einer anderen Stelle als Teilfunktion angegliedert. Das interne Audit ist – zum Beispiel aufgrund der Unternehmensgrösse, infolge des wirksamen Zusammenspiels anderer Aktivitäten oder wegen Outsourcings an externe Dienstleister – bei 31% als Funktion sowie bei 22% als Teilfunktion etabliert (vgl. *Abbildung 1*). In diesem Zusammenhang ist erläuternd anzumerken, dass das interne Audit anders als bei den über das Rundschreiben 2017/1 Corporate Governance – Banken [8] der *Finanzmarktaufsicht (Finma)* adressierten Banken, Finanzgruppen und Effektenhändlern in Schweizer Nichtfinanzunternehmen nicht regulatorisch vorgeschrieben ist.

Die bereits 1992 im COSO-Rahmenwerk vorgesehenen Bereiche operative Geschäftstätigkeit, finanzielle Berichterstattung und Compliance sind typischerweise bis heute noch die am häufigsten verfolgten IKS-Ziele bei den befragten Unternehmen. Es zeigt sich konkret, dass Compliance-Ziele – intern sowie gegenüber externen Anspruchsgruppen – und die Ziele der finanziellen Berichterstattung durchschnittlich als am relevantesten beurteilt werden. Während rund 80 bis 90% der Studienteilnehmer diesen Zielen eine starke Priorität einräumen, sind operative Ziele (40%) und Ziele der nichtfinanziellen Berichterstattung (18%) deutlich seltener im Fokus.

3. AUSGESTALTUNG UND REIFEGRAD DER IKS-KOMPONENTEN

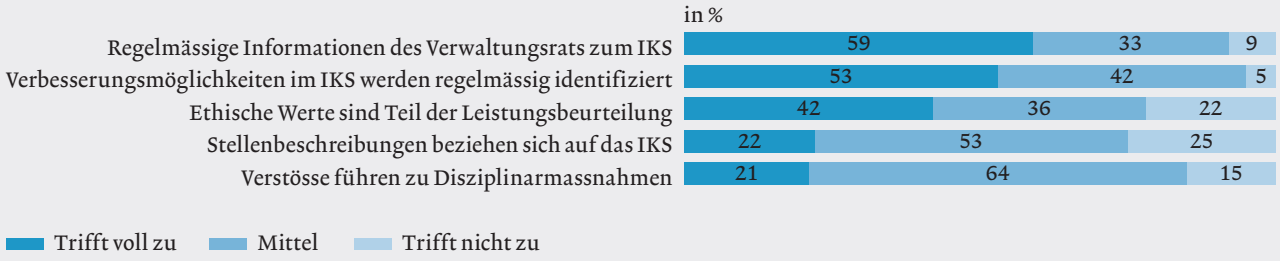
In Anlehnung an das bekannteste IKS-Rahmenwerk in Schweizer Nichtfinanzunternehmen, das COSO (2013) [4], wurden dessen Komponenten Steuerungs- und Kontrollumfeld, Risikobeurteilung, Steuerungs- und Kontrollaktivitäten, Information und Kommunikation sowie Monitoring mit Blick auf ihre Ausgestaltung und den jeweiligen Reifegrad hin untersucht. Für die Bestimmung des Reifegrads wurde das Reifegradmodell der Carnegie-Mellon-Universität [9] herangezogen, welches sich in der Reihenfolge zunehmender Maturität in die fünf Stufen anfänglich (ad hoc, keine Standardisierung), strukturiert (anfängliche Strukturen, Mindestdokumentation), etabliert (Standardisierung, einheitliche Anwendung), geführt (Anforderungen der Anspruchsgruppen sind erfüllt, Mehrwert ist anerkannt) und optimiert (kontinuierliche Entwicklung und Verbesserung des IKS) unterteilt.

Das Steuerungs- und Kontrollumfeld des IKS umfasst verschiedene Aspekte, darunter Werte und Prinzipien (einschliesslich des *Tone at the Top*), die Philosophie und Arbeitsweise von Verwaltungsrat und Geschäftsleitung, Strukturen, Kompetenzen, Verantwortlichkeiten und das Personalwesen. In den befragten Unternehmen kommen bei der Ausgestaltung vor allem die regelmässige Information des Verwaltungsrats zu Themen des IKS und die Identifikation von Verbesserungsmöglichkeiten zum Tragen (vgl. *Abbildung 2*). Zweiundvierzig Prozent geben ausserdem an, dass ethische Werte voll in die Leistungsbeurteilung einbezogen werden. Insgesamt schätzt die Mehrheit der Befragten unabhängig



ADRIAN KYBURZ,
DR. OEC. HSG,
INTERNAL AUDITOR,
BASEL

Abbildung 2: **AUSGESTALTUNG DES STEUERUNGS- UND KONTROLLUMFELDS**



von der Unternehmensgrösse das Steuerungs- und Kontrollumfeld entweder als geführt oder als etabliert ein. Nur wenige Unternehmen, dies sind 4% der mittelgrossen und 5% der kleinen, betrachten den Reifegrad noch als anfänglich.

Die Risikobeurteilung bezieht sich auf die Identifikation und Bewertung von Risiken anhand vordefinierter Kriterien. In den teilnehmenden Unternehmen findet die Risikobeurteilung in den meisten Fällen (55%) einmal jährlich statt, bei jeweils 17% auch halbjährlich, quartalsweise oder kontinuierlich. Ad hoc-Risikobeurteilungen werden bei 22% durchgeführt. Als wichtige Aspekte, die in die Risikobeurteilung miteinfliessen, werden hauptsächlich Eintrittswahrscheinlichkeit (94%), interne und externe Faktoren (94%), Auswirkung (88%) sowie deliktische Handlungen (72%) identifiziert. Zu bemerken ist, dass bei 30% der Befragten auch Chancen berücksichtigt werden (vgl. *Abbildung 3*). Die Ausgestaltung der Risikobeurteilung ist in der Praxis vor allem abhängig vom Risiko- und Kontrollbewusstsein der Mitarbeitenden sowie von der Art, Relevanz und Anzahl der Risiken im Unternehmensumfeld. Der Reifegrad der Risikobeurteilung ist für grosse und mittelgrosse Unternehmen sogar besser als der des Steuerungs- und Kontrollumfelds, wohingegen neun Prozent der kleinen Unternehmen sie noch als anfänglich einstufen.

Steuerungs- und Kontrollaktivitäten umfassen alle Massnahmen, die der Handhabung der identifizierten Risiken entsprechend des vom Verwaltungsrat festgelegten Risikoappetits dienen. Dabei kommen besonders stark direktive (steuernde) Massnahmen wie Anweisungen oder Prozessbeschreibungen (79%), präventive (vorbeugende) Massnahmen wie eine positive Unternehmenskultur (60%) und korrektive (verbessernde) Massnahmen (61%) zum Einsatz. Detektive Massnahmen, die auf die zeitnahe Aufdeckung von Fehlern und Schwachstellen ausgerichtet sind, werden bei 38% stark und bei 43% zumindest zu einem gewissen Mass angewendet. Besonders häufige Massnahmen stellen zum Beispiel das Vier-Augen-Prinzip, Genehmigungsverfahren, Budgetvergleiche und Analysen sowie Funktionentrennungen dar (vgl. *Abbildung 4*). Mit Bezug auf den Reifegrad beurteilen mittelgrosse Unternehmen diesen etwas zurückhaltender als grosse und kleine Unternehmen. Dies mag damit zusammenhängen, dass die Prozesse trotz geringerer Ressourcen bei kleineren Unternehmen überschaubar sind, während diese bei grossen Unternehmen zwar komplexer sind, aber auch mehr IKS-Ressourcen zur Verfügung stehen. Mittelgrosse Unternehmen können vor allem in Wachstumsphasen jedoch häufig von zunehmend komplexen Prozessrisiken gekennzeichnet und gleichzeitig noch mit verhältnismässig geringeren Ressourcen ausgestattet sein.

«Zur Information und Kommunikation zählt insbesondere die zeitnahe Kommunikation aller relevanten Risiko- und Kontrollinformationen an die zuständigen Stellen.»

Zur Information und Kommunikation zählt insbesondere die zeitnahe Kommunikation aller relevanten Risiko- und Kontrollinformationen an die zuständigen Stellen. In der Praxis wird sie am häufigsten durch Regelungen und Weisungen (84%), Ad hoc-Mitteilungen (55%), Veranstaltungen auf Abteilungsebene (39%) oder durch Präsenzschulungen

Abbildung 3: **AUSGESTALTUNG DER RISIKOBEURTEILUNG**

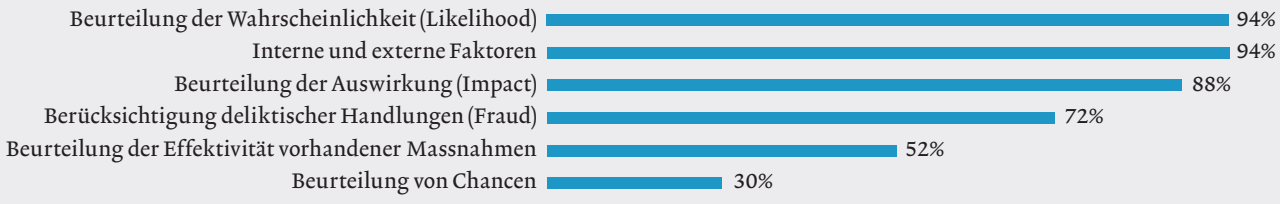
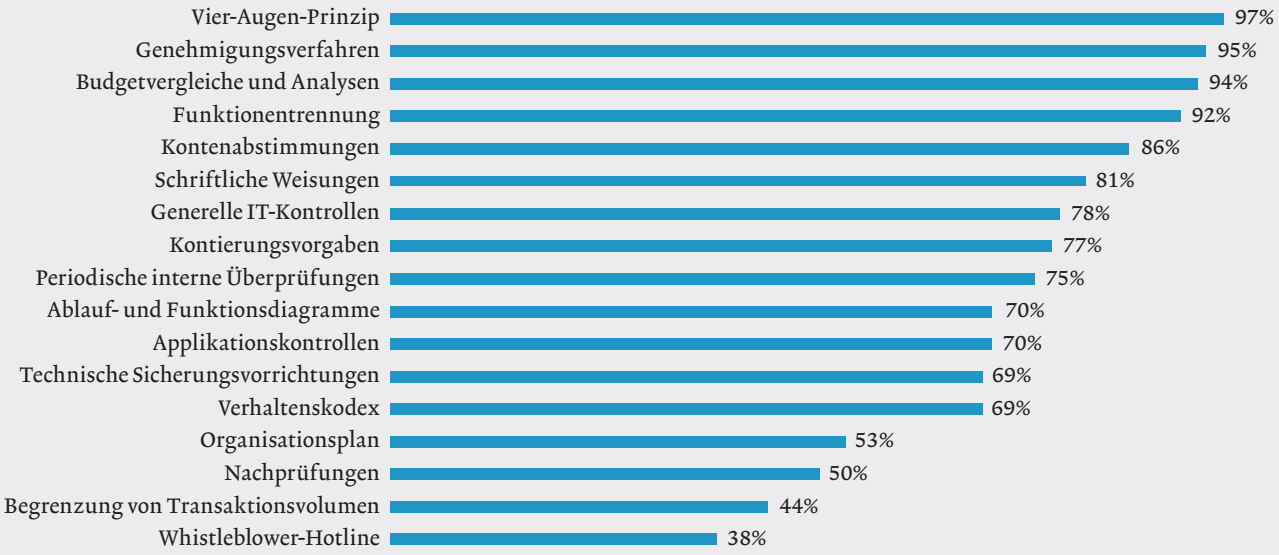


Abbildung 4: **AUSGESTALTUNG DER STEUERUNGS- UND KONTROLLAKTIVITÄTEN**



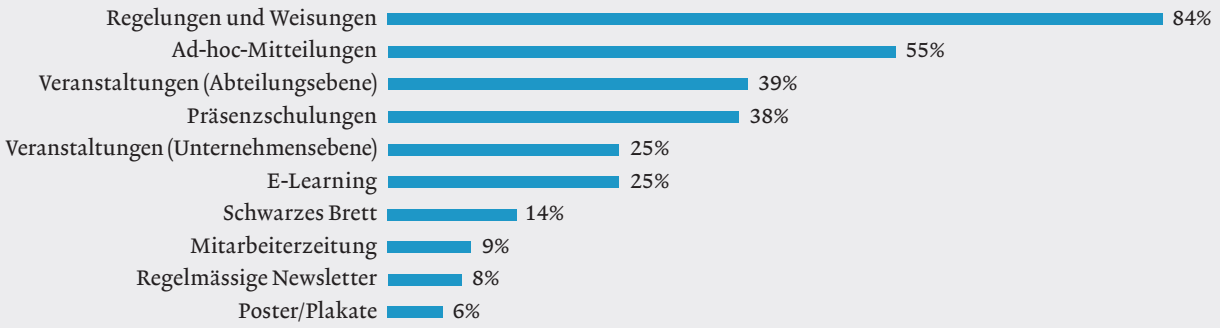
(38%) umgesetzt. Hinsichtlich des Reifegrads sind die Ergebnisse durchwachsen, insgesamt schätzt die Mehrheit über alle Unternehmensgrössen hinweg diese Komponente aber entweder als etabliert oder als strukturiert ein. Bei grossen Unternehmen beurteilen 47% die Information und Kommunikation zum IKS als geführt, 9% der kleinen erachten sie sogar als optimiert.

Das Monitoring des IKS wird bei den Befragten generell am häufigsten durch eine separate Beurteilung durchgeführt. Eine Ausnahme bilden dabei mittelgrosse Unternehmen, die vermehrt auch auf Ad-hoc-Prüfungen oder auf ein kontinuierliches Monitoring setzen (vgl. *Abbildung 6*). Besonders hervorzuheben ist, dass mehr oder gleich ein Fünftel der grossen (24%) und mittelgrossen Unternehmen (20%) angeben noch über kein systematisches Monitoring zu verfügen. Obwohl der Reifegrad des Monitorings von 41% der grossen, 36% der mittelgrossen und 54% der kleinen Unternehmen zusammengenommen entweder als optimiert oder als geführt beurteilt wird, schätzen ihn in diesen Grössenkategorien 6%, 4% und 5% der Befragten gleichzeitig noch als anfänglich ein.

4. VERBESSERUNGSPOTENZIALE UND BEREICHE MIT ZUNEHMENDER BEDEUTUNG

Abschliessend wurden von den teilnehmenden Unternehmen Verbesserungsmöglichkeiten für die künftige Ausgestaltung identifiziert. So sehen beispielsweise 56% im Bewusstsein

Abbildung 5: **AUSGESTALTUNG VON INFORMATION UND KOMMUNIKATION**



der Mitarbeitenden, 45% in der Anpassung an Veränderungen und 38% im Monitoring bzw. in der kontinuierlichen Verbesserung ein grosses Optimierungspotenzial. Gemäss den Erwartungen werden personelle Ressourcen insbesondere von kleinen Unternehmen besonders hervorgehoben. Dahingegen werden die strukturellen Voraussetzungen, die Koordination zwischen den Kontrollfunktionen, die vorhandenen Fachkenntnisse, das Kosten-Nutzen-Verhältnis sowie die Verständlichkeit von IKS-Richtlinien bereits mehrheitlich positiv und zufriedenstellend beurteilt. Bei diesen Aspekten erkennen jeweils weniger als 20% weitere Verbesserungsmöglichkeiten. Mit zunehmender Bedeutung für die Zukunft schätzen die Unternehmen darüber hinaus folgende Bereiche ein: Anpassung an organisatorische Veränderungen (74%), Prozessintegration (63%), Automatisierung (62%), Dokumentationsbedarf (60%) sowie den Finanz- und IT-Fokus des IKS (jeweils 58%) (vgl. *Abbildung 7*). Somit könnten aktuelle Entwicklungen wie Digitalisierung oder der Einsatz von Data Analytics in der internen Steuerung und Kontrolle künftig stärker berücksichtigt werden.

> *«Aktuelle Entwicklungen wie Digitalisierung oder der Einsatz von Data Analytics könnten in der internen Steuerung und Kontrolle künftig stärker berücksichtigt werden.»*

5. FAZIT UND AUSWIRKUNGEN AUF DAS INTERNE AUDIT

Gemäss Standard 2130 der beruflichen Grundlagen des *Institutes of Internal Auditors (IIA)* [10] soll das interne Audit «die Organisation bei der Aufrechterhaltung wirksamer Kontrollen unterstützen, indem es deren Effektivität und Effizienz bewertet sowie kontinuierliche Verbesserungen fördert». Dabei sollen unter anderem Schwerpunkte gelegt werden auf die Angemessenheit und Wirksamkeit des IKS für die Erreichung der strategischen Ziele der Organisation, die Zuverlässigkeit und Integrität von Daten des Rechnungswesens und von operativen Informationen, die Effektivität von Geschäftsprozessen und Programmen, die Sicherung des Betriebsvermögens sowie auf die Einhaltung von Gesetzen, Verordnungen, Richtlinien, Verfahren und Verträgen. Somit ist das interne Audit durch seine organisatorische Stellung sowie sein auf das Schaffen von Mehrwerten ausgelegtes Mandat insgesamt in einer sehr guten Ausgangslage, den Verwaltungsrat, welcher nach Art. 716 a OR für das Festlegen

Abbildung 6: **AUSGESTALTUNG DES MONITORINGS**

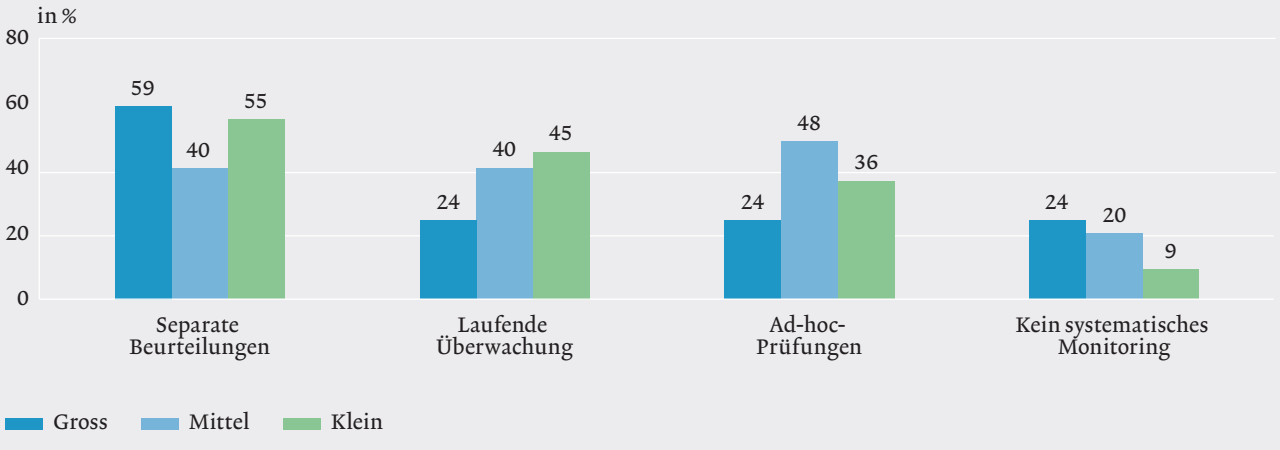
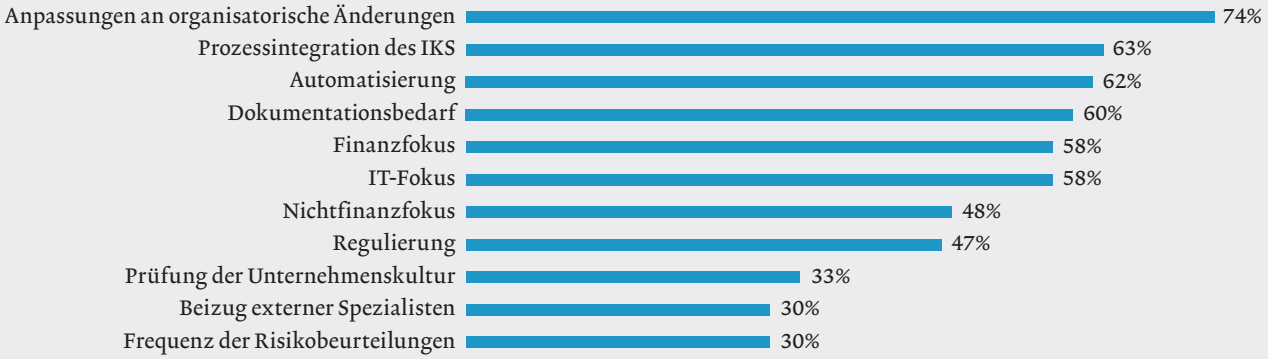


Abbildung 7: **BEREICHE MIT ZUNEHMENDER BEDEUTUNG**



der Organisation und folglich auch für die interne Steuerung und Kontrolle verantwortlich ist, auf möglicherweise sinnvolle Anpassungen aufmerksam zu machen. Dieser kann anschliessend die erforderlichen Weisungen erteilen und geeignete Verantwortlichkeiten zur Umsetzung der Empfehlungen festlegen. Daher stellt das interne Audit ein wichtiges Verbindungsglied zur Prüfung und Verbesserung des IKS zwischen den operativen Prozessen und den strategischen Entscheidungsträgern dar und trägt zur Verankerung des IKS in der Unternehmenskultur sowie im Bewusstsein der auditierten Einheiten bei. Unternehmen, welche über ein internes Audit verfügen, können das IKS im Auditplan priorisieren und die für die Prüfung und Verbesserung des IKS notwendigen Ressourcen zur Verfügung stellen. Somit können sie selbst die Wahrscheinlichkeit erhöhen, dass das IKS nicht nur als notwendige Bürokratie, sondern als wertschaffendes Instrument für die Zielerreichung auch tatsächlich akzeptiert und gelebt wird. ■

Anmerkungen: *Die Durchführung der Studie wurde durch PricewaterhouseCoopers AG, Zürich, Hilti Lab for Integrated Performance Management, St. Gallen sowie ABB Asea Brown Boveri Ltd., Zürich, unterstützt und ist für interessierte Personen auf der Website des ACA-HSG online (aca.unisg.ch/de/arbeitsgebiete/ruud) abrufbar.

1) Schweizerischer Verband für Interne Revision (IIA Switzerland) (2017). Internationale Standards für die berufliche Praxis der Internen Revision. Standard 2100 Art der Arbeiten. Englisches Original: vgl. IIA. **2)** Pfaff, D., Ruud, T.F., Bänziger, M., Glanz, S., Kessler, F.J., Kyburz, A., & Stopper, M.H. (2016). Schweizer Leitfaden zum Internen Kontrollsystem (IKS) (7. ed.). (D. Pfaff, & F.T. Ruud, Eds.) Zürich: Orell Füssli Verlag AG. **3)** Ruud, F., Kyburz, A. & Schramm, K. (2018). Das Interne Kontrollsystem in Schweizer Unternehmen ausserhalb des Finanzsektors. **4)** Committee of the Sponsoring Organizations of the Treadway Commission [COSO] (2013). Internal Control – Integrated Framework. Jersey City. **5)** Committee of the Sponsoring Organizations of the Treadway Commission [COSO] (1992). Internal Control – Integrated Framework. Jersey City. **6)** ISO – International Organization for Standardization. (2009). ISO 31000:2009, Risk Management – Principles and Guidelines. **7)** ISACA (2012). COBIT 5: A business framework for the governance and management of enterprise IT. **8)** Finma (2017). Rundschreiben 2017/1 Corporate Governance – Banken. **9)** Chrissis, M., Konrad, M., & Shrum, S. (2009). CMMI® Richtlinien für Prozess-Integration. München: Addison-Wesley. **10)** Schweizerischer Verband für Interne Revision (IIA Switzerland) (2017). Internationale Standards für die berufliche Praxis der Internen Revision. Standard 2130 Kontrollen. Englisches Original: IIA.