FÜNF FRAGEN AN FÜNF HEADS INTERNAL AUDIT

Technologische Entwicklungen in der Internen Revision

Sandra Würmli und Thomas Flüeler (Co-Geschäftsführung IIA Switzerland) sowie Patrizia Pabst (Fachleiterin Wirtschaftsprüfung Expertsuisse) sprachen mit den folgenden Heads Internal Audit: Daniel Dal Santo, Gabriela Federer Wenger, Holger Kremmling, Mirko Lanzi und Pascal Stirnimann.

Daniel Dal Santo

DR. OEC. HSG, DIPL. WIRTSCHAFTSPRÜFER, LEITER INTERNE REVISION, RAIFFEISEN SCHWEIZ GENOSSENSCHAFT

Gabriela Federer Wenger

EMBA IMD, DIPL. WIRTSCHAFTSPRÜFERIN, EX-UNTERNEHMENSLEITERIN MITREVA, LEITERIN INTERNE REVISION MIGROS-GRUPPE

Holger Kremmling

DIPL. BETRIEBSWIRT (BA), HEAD OF INTERNAL AUDIT, CLARIANT

Mirko Lanzi

EXECUTIVE MBA, B. A. USI, SWISS CERTIFIED PUBLIC ACCOUNTANT, CERTIFIED FRAUD EXAMINER, CHIEF AUDIT EXECUTIVE, ENTE OSPEDALIERO CANTONALE

Pascal Stirnimann

BETRIEBSÖKONOM FH, DIPL. WIRTSCHAFTSPRÜFER, CERTIFIED INTERNAL AUDITOR UND ZUGELASSENER REVISIONSEXPERTE, DIREKTOR EIDGENÖSSISCHE FINANZKONTROLLE

Was macht für Sie eine gute Unternehmensaufsicht/ Corporate Governance aus?

Grundvoraussetzung ist, dass der «tone at the top» stimmt: ein offener, transparenter und fairer Meinungsaustausch in den Gremien, welcher unterschiedliche Ansichten und Fähigkeiten reflektiert und durch langfristig orientierte Entscheidungen Vertrauen bei Kundinnen und weiteren Stakeholdern schafft. Die Interne Revision ist Teil einer guten Corporate Governance und ist gleichzeitig Kontrollorgan, Assurance-Geber, Sparring Partner und verlängerter Arm sowie Informationslieferant und Ideengeber für das oberste Aufsichtsorgan.

Erstens: Sie umfasst die nachhaltige Unternehmensführung, ethische Grundsätze, Integrität, Transparenz, die Zusammensetzung des Verwaltungsrats (VR) sowie die unabhängige Prüfung und Einhaltung von Vorschriften. Zweitens: Verschiedene Assurance-Provider, u. a. Interne Revision, Risikomanagement, inkl. Externer Revision, haben ihre Tätigkeiten in der Organisation aufeinander abgestimmt und in einer Assurance Map transparent dargestellt. Damit erhält der VR nicht nur Auskunft über Risiken und deren Mitigation, sondern auch ein Instrument zur Überwachung zusammen mit den Berichterstattungen der Assurance-Provider.

Gute Corporate Governance zeichnet sich durch Transparenz, einen ethischen Verhaltenskodex, der gelebt wird, und Integrität des Verwaltungsrats und des Managements aus. Dieses fördert nicht nur Vertrauen bei Mitarbeitenden und Investoren/-innen, sondern ist die Basis für den Unternehmenserfolg. Die langfristige Entwicklung und Nachhaltigkeit im Blick zu haben, trägt neben der Etablierung eines wirksamen Risikomanagements zur Stabilität in Unternehmen bei.

Eine gute Governance basiert auf klaren und einfachen Regeln, Praktiken und Prozessen. Eine Unternehmens-Governance muss sicherstellen, dass angemessene Entscheidungsprozesse und Kontrollen vorhanden sind, um die Interessen aller Stakeholder zu balancieren. Das Modell der drei Linien, entwickelt vom The Institute of Internal Auditors, ermöglicht eine Gesamtübersicht und zeigt, wie interne und externe Akteure interagieren. Koordination und Zusammenarbeit zwischen den Beteiligten sind wesentlich, um Doppelarbeit und unabgedeckte Bereiche zu vermeiden.

Knackpunkt sind nicht die Regelungen. Sie sind schnell erstellt und nicht kompliziert. Viele geizen zudem nicht mit tollen Grundsätzen zur Aufsicht der Verwaltungs- und Unternehmensführung. Warum kommt es dennoch regelmässig zu Versäumnissen? Der kritische Faktor ist die Führung: Die Vorgaben müssen konsequent vorgelebt und eingehalten werden, sonst sind sie «toter Buchstabe». Dies kann vielerorts noch verbessert werden. Genau deswegen führen wir regelmässig Prüfungen durch.

Wo wird KI bei Ihnen bereits eingesetzt und welche Herausforderungen ergeben sich daraus?

Der Einsatz von KI steht bei uns am Anfang und erfolgt erst punktuell. KI setzen wir dort ein, wo die neue Technologie nicht zu erhöhten Risiken führt, jedoch zu einem nachhaltig hohen Nutzen, wie z. B. zur Effizienzsteigerung von Prozessen, beiträgt. Geschäftsentscheide von grosser Tragweite werden immer durch einen Menschen getroffen. Neben den rechtlichen Herausforderungen sind insbesondere die Daten-Governance (akkurate, vollständige und relevante Daten), das Modellrisikomanagement (Freigabe und laufende Überwachung) sowie der nachhaltige Kompetenzaufbau von grosser Bedeutung.

KI setzen wir punktuell unterstützend für die Berichterstattung inkl. der Generierung von Grafiken, welche Problemstellungen visualisieren, und das Wissensmanagement ein. Dafür wurden die intern bereits zur Verfügung stehenden Lösungen verwendet, um den Anforderungen des IT-Nutzungsreglements zu entsprechen. Die komplexe Systemumgebung hat eine Automatisierung von Routineaufgaben nicht erlaubt. Ebenso sind wir angesichts mannigfacher vertraulicher Unternehmensdaten sowie Personendaten aktuell zurückhaltend in der Verwendung von KI-Tools, welche ausserhalb der Unternehmensgruppe betrieben werden.

Die künstliche Intelligenz steht am Anfang ihres Potenzials. Wir erleben die ersten Annäherungsversuche an die neue Technologie, welche uns neue Möglichkeiten eröffnet. Die Technologie kommt in verschiedenen Unternehmensbereichen zur Anwendung und auch bei uns in der Internen Revision machen wir erste Erfahrungen. Neben der technologischen Komponente ergeben sich Herausforderungen sowohl im Datenschutz als auch bei ethischen Fragen. Global tätige Unternehmen müssen die existierenden und noch zu erwartenden regulatorischen Vorgaben verschiedener Länder erfüllen, was zusätzliche Komplexität schafft.

Als Krankenhaus befinden wir uns in einer explorativen Phase mit Pilotprojekten in Forschung, Klinik und Verwaltung. Wir beginnen mit kleinen Innovationen und weiten diese später aus. Die Herausforderung besteht darin, zu verstehen, wo investiert werden soll, um den besten Nutzen zu erzielen (Pflege, Prozesseffizienz, wirtschaftlicher Nutzen). Zudem ist es wichtig, die Governance für künstliche Intelligenz und ethische Regeln festzulegen. Die Interne Revision spielt eine begleitende Rolle bei der Einführung neuer Technologien.

Wir arbeiten an der Entwicklung von Tools, welche uns bei der Risikoanalyse entlasten sollen. Auch für Datenanalysen bei Prüfungen experimentieren wir mit KI. Zudem prüfen wir KI-Applikationen, welche in der Verwaltung eingesetzt werden. Ich will nicht verhehlen: Es sind noch zahlreiche Herausforderungen zu meistern. Zum Beispiel sind fehlende strukturierte Daten eine Herausforderung.
Auch müssen unsere Mitarbeitenden neue Kompetenzen entwickeln. Dies berücksichtigen wir bei der Weiterbildung und Rekrutierung.

INTERNAL AUDIT

	Daniel Dal Santo	Gabriela Federer Wenger	Holger Kremmling	Mirko Lanzi	Pascal Stirnimann
Welche Rolle spielt das Internal Audit bei (der Identifizierung, Bewertung und dem Monitoring von) Cyber-Sicherheitsrisiken im Unternehmen?	Das Management von Cyber-Risiken basiert auf einem klar definierten internen Kontrollsystem, weshalb für die Interne Revision die klassische Prüftätigkeit der IKS-Beurteilung (Angemessenheit und Wirksamkeit) im Vordergrund steht. Zusätzlich identifizieren wir im Rahmen der Prüfplanung besondere Risikokonstellationen und stimmen die Prüfungen intern ab (CISO, Cyber Intelligence, Red / Blue Team etc.). Bei spezifischen Themen holen wir uns Unterstützung von externen Securityfachpersonen. Die Interne Revision ist damit Teil des Gesamtdispositivs zur Abwehr von Cyber-Gefahren.	Es bringt die Aussensicht ein: Als unabhängige Instanz überprüft das Internal Audit, ob die bestehenden Sicherheitsmassnahmen effektiv sind und den aktuellen Bedrohungen standhalten können. Es steht in engem Austausch mit dem CISO und dem Risikomanagement, bezieht diese in die Planung (Identifizierung) ein, analysiert IT-Infrastruktur, Prozesse und Richtlinien. Mit der Bewertung der Feststellungen bzw. Risiken hilft es der Organisation, Prioritäten zu setzen. Das permanente Monitoring wird durch den CISO als Second Line gewährleistet und steht auf der Besprechungsagenda mit dem Internal Audit.	Der Internen Revision eines Unternehmens obliegt die unabhängige Überprüfung des Risikomanagements. Hierzu gehört auch, die dabei identifizierten Risiken und Schwachstellen der Cyber-Technologie aufzuzeigen. Bei produzierenden Unternehmen sieht man häufig im Bereich Produktion (Operations) die grössten Sicherheitslücken bezüglich Angriffen von aussen. Cyber-Risiken kommen allerdings nicht nur von aussen, sondern werden auch durch eigene Mitarbeitende verursacht. Hier sollte die Interne Revision sicherstellen, dass das interne Kontrollsystem des Unternehmens genügend Schutz bietet.	Das Internal Audit überprüft durch kontinuierliches Monitoring und spezifische Audits ständig die Angemessenheit und Konformität des Informationssicherheits-Managementsystems (ISMS) und der Massnahmen. Es trägt zur Identifizierung technischer, organisatorischer und rechtlicher Lücken bei und erleichtert die Risikobehandlung. So unterstützt es die kontinuierliche Verbesserung der Informationssicherheit und stellt sicher, dass die Systeme und ihre Sicherheit den geltenden Vorschriften, besten Praktiken und geschäftlichen Anforderungen entsprechen.	Eine zentrale Rolle! Es handelt sich um eine Kernaufgabe. Cyber-Sicherheit ist ein Schlüsselelement in der Verwaltung. Versäumnisse bei der Sicherheit führen daher zu bedeutenden Kosten, einem Reputationsschaden und Vertrauensverlust der Nutzenden. Darum führen wir jährlich zahlreiche Cyber-Sicherheitsprüfungen durch und leisten einen Beitrag zur Verbesserung. Die Verwaltung verfügt zudem über zahlreiche kritische Infrastrukturen, wo eine gute Cyber-Resilienz unverhandelbar ist. Die zentralen Handlungsfelder haben wir Anfang Juli in einem Synthesebericht zusammengefasst, welcher auf unserer Website verfügbar ist.
Was sind aus Ihrer Sicht die wichtigsten Änderungen in den Global Internal Audit Standards? Wie ist der aktuelle Stand der Umsetzung in Ihrem Unternehmen?	Die überarbeiteten Standards geben uns, neben vielen inhaltlichen und formellen Änderungen zur Verbesserung der Revisionstätigkeit, vor allem die Gelegenheit, unser Fundament – sprich die Strategie und unsere strategischen Stossrichtungen – zu überdenken und im Führungsteam und mit dem Prüfausschuss weiterzuentwickeln. Gerade aufgrund der vielen technologischen Entwicklungen wird sich unser Berufsstand in den nächsten Jahren stark verändern: Dies müssen wir aktiv angehen. Derzeit sind wir mitten in diesen strategischen Diskussionen und werden bis Jahresende die Umsetzung abschliessen.	Akzentuierung: 1) Enge Zusammenarbeit mit den Stakeholdern. 2) Ethik und Integrität zur Förderung einer Kultur der Transparenz und Verantwortung. 3) Integrieren technologischer Ressourcen in Prüfungsprozesse, um die Effizienz der Prüfungen zu steigern und fundierte Empfehlungen geben zu können. 4) Proaktives Risikomanagement, um zukünftige Risiken zu antizipieren und strategische Empfehlungen zu geben. 5) IR muss agil und anpassungsfähig sein, um auf sich schnell ändernde Prozesse und Risiken reagieren zu können. 6) Standardabweichungen müssen durch Comply-Or-Explain-Massnahmen erläutert werden.	Die neuen Standards gelten ab 2025 und wir sind gerade in den Vorbereitungen, unsere Prozesse – wo notwendig – anzupassen und werden diese ab nächstem Jahr anwenden. Die Vereinfachung und Klarheit der neuen Standards helfen bei der Adaptierung und Diskussion mit den jeweiligen Stakeholdern/-innen. Der stärkere Fokus auf die Rolle im Bereich Risikomanagement, Governance und Ethik verhilft der Internen Revision zu einer klaren Positionierung im Unternehmen. Damit einher geht aber auch eine grössere Verantwortung, nicht nur gegenüber den internen, sondern neu auch den externen Stakeholdern/-innen.	Die wichtigste Änderung ist meiner Meinung nach die Festlegung einer Strategie für die Interne Revision im Einklang mit der Unternehmensstrategie. Diese Strategie ermöglicht es, langfristig eine exzellente Servicequalität zu gewährleisten und zukünftigen Bedürfnissen gerecht zu werden. Die Interne Revision sollte ein Geschäftspartner sein, der mit den Veränderungen im Geschäft und der technologischen Entwicklung Schritt hält. Wir haben eine Gap-Analyse in Bezug auf die neuen Standards durchgeführt und einen Aktionsplan erstellt, um bis Januar 2025 konform zu sein.	Wir führen unsere Prüfungen nach unterschiedlichen Standards durch und sind Anpassungen gewohnt. Darum sind wir bei der Umsetzung der neuen Vorgaben gut unterwegs. Wir begrüssen zudem die strukturellen und inhaltlichen Anpassungen. Sie stärken das Vertrauen in die Arbeit der Internen Revisionen. Bei vielen Prüfungen müssen wir überdies bereits heute umfangreichere Vorgaben einhalten, zum Beispiel bei den Abschlussprüfungen (ISA oder SA-CH) oder bei unseren Prüfungen als oberste Rechnungskontrollbehörde im öffentlichen Sektor (ISSAI). Wir sind also entspannt, was die neuen und strengeren Vorgaben betrifft.
Wie stellen Sie sich den Arbeitsalltag von Internal Auditors in zehn Jahren vor?	In einer schnelleren, automatisierteren und informierteren Umwelt werden die traditionellen Tugenden von Internal Auditors weiterhin gefragt sein. Sie kennen das Geschäft ausgezeichnet (unterstützt durch neue Technologien), stehen für eine unabhängige Perspektive auf die Prüfobjekte (mit höherer Prüfsicherheit aufgrund von automatisierten Prüfungen und Vollstichproben), kommunizieren proaktiv mit den Anspruchsgruppen (mittels neuer Präsentationsformen und Medien) und haben auch in zehn Jahren unverändert Spass und Freude an der Arbeit.	Technologie, sich wandelnde Geschäftsmodelle und neue regulatorische Anforderungen werden den Arbeitsalltag von Internal Auditors dynamischer, technologiegetriebener und strategischer gestalten, mit stärkerem Fokus auf eine interdisziplinäre Zusammenarbeit mit den verschiedenen Assurance-Providern und Kommunikation. Die Zunahme der Volatilität und Unsicherheit in allen Volkswirtschaften wird zu weiterem Stress in globalen Lieferketten führen und damit für grundsätzlich jede Unternehmensgruppe die Bedeutung einer unternehmerischen Sichtweise auch in der Internen Revision weiter schärfen.	Die Positionierung bleibt der Schlüssel zum Erfolg. Nur wenige Funktionen haben einen so breiten Einblick wie die Interne Revision. Mit der Unterstützung achtsamer Verwaltungsräte, die in der Internen Revision einen echten Mehrwert sehen über die regulatorische Notwendigkeit hinaus, wird die Interne Revision effizient ihre Assurance-Rolle wahrnehmen. Technologien wie Datenanalysen und KI werden ein integrierter Teil von automatisierten Revisionsprozessen sein. Gleichzeitig werden Internal Auditors Sparringspartner/-innen sein, die noch mehr vorausschauend und weniger rückblickend agieren.	Die tägliche Arbeit wird hoch technologisch und kollaborativ sein. Automatisierungswerkzeuge und künstliche Intelligenz werden genutzt, um grosse Datenmengen in Echtzeit zu analysieren und Anomalien sowie Risiken frühzeitig zu erkennen. Die Kommunikation mit Management und Stakeholdern wird kontinuierlich sein, mit strategischen Analysen und Empfehlungen. Fortlaufende Weiterbildung wird ein integraler Bestandteil der Routine sein, um über neue Vorschriften und Technologien auf dem Laufenden zu bleiben. So sehe ich eine Transformation der Rolle vom Assurance-Anbieter zum strategischen Partner.	Das Spannende an der Arbeit von Internal Auditors und EFK-Prüfenden ist gleichzeitig auch das Herausfordernde: sich ständig neuen Herausforderungen zu stellen und neues Wissen anzueignen. Dies ist einzigartig und wird in der Zukunft nicht anders sein, als es heute bereits ist. Das Wichtigste für mich und meine Mitarbeitenden ist aber, dass unsere Arbeit in Zukunft weiterhin notwendig, wichtig und spannend sein wird. Sie bietet gute Perspektiven. Eine Anstellung als Prüferin resp. Prüfer zu suchen, ist weiterhin ein ausgezeichneter Entscheid, den ich nur empfehlen kann!

Vielen Dank für das Gespräch.