orell füssli
gruppe

Reglement

Betrifft	**Risikomanagement und Internes Kontrollsystem (IKS) der Orell Füssli Gruppe**
Dokumenten-ID	REK-0005
Geltungsbereich	OF Gruppe
Gültig ab	01.05.2021
Freigabe durch	VR
Verantwortlich	CEO
Autor	BMU

1 Zweck des Reglements

Die Notwendigkeit zum Aufbau und zur Dokumentation des Risikomanagements und des IKS basiert auf folgenden für börsenkotierte Gesellschaften verbindliche Bestimmungen bzw. Leitlinien:

- Schweizer Aktienrecht
- SIX Corporate Governance-Richtlinie (RLCG) vom 1. Januar 2016
- Swiss Code of Best Practice for Corporate Governance (Economiesuisse) vom 28.08.2014

Das Gesellschaftsrecht[1] geht noch einen Schritt weiter, indem es verlangt, dass der Verwaltungsrat ein funktionierendes Internes Kontrollsystem (IKS) sicherstellen muss und die Existenz des IKS, soweit es für die finanzielle Berichterstattung relevant ist, durch die externe Revision im Revisionsbericht zu bestätigen hat.
Um den Vorschriften zur formalen Ausgestaltung eines IKS Rechnung zu tragen, aber auch mit dem Ziel ein effektives und effizientes Arbeitsinstrument für die Führung bereitzustellen, werden hier die verbindlichen Grundlagen für ein IKS der OF Gruppe festgelegt. Für die organisatorische Umsetzung werden, soweit notwendig, zusätzliche Weisungen erlassen.

2 Inhalt des Reglements

2.1 Internes Kontrollsystem IKS

Das IKS in der OF Gruppe zielt auf eine systematische Kontrolle der Risiken ab. Das interne Kontrollsystem ist umfassend und deckt auch jene Bereiche ab, die durch die externe Revision nicht erfasst werden. Die externe Revision prüft es im Rahmen der gesetzlichen Anforderungen. Die Basis des IKS ist das Risikomanagement, welches Risiken identifiziert, Massnahmen evaluiert und empfiehlt, um allfällige Risiken zu vermindern oder zu verhindern.
Die Beschreibung des IKS stellt deshalb im Wesentlichen auf die Erfassung der Risiken ab und baut auf dem divisionalen Risikomanagement auf.
Grundsätzlich liegt die Verantwortung für die gruppenweite Umsetzung des Risiko- und IKS-Managements beim Verwaltungsrat und der Gruppenleitung des Orell Füssli Gruppe (OFG). Zu diesem Zweck wurde in Anlehnung an das international gebräuchliche Risiko- und Kontroll-Framework COSO das IKS für Orell Füssli strukturiert.
Mit der internen Kontrolle werden die folgenden Ziele angestrebt:

- Die Effizienz und Effektivität der Tätigkeiten / Prozesse werden beurteilt und ggf. verbessert.
- Die Zuverlässigkeit und Integrität der finanziellen Berichterstattung und der Risikoberichterstattung werden sichergestellt.

[1] Schweizerisches Obligationenrecht Art. 728a, b OR

- Die Einhaltung (Compliance) der anwendbaren Normen, d.h. öffentliche Gesetze und Verordnungen sowie interne Anordnungen, Weisungen und Leitbilder des Unternehmens werden geprüft.
- Die Transparenz über die Risikosituation durch regelmässige Berichterstattung und allfällige Abweichungen davon wird geschaffen.

2.2 Risiko und Risikomanagement

Das Risiko wird einerseits bestimmt durch die Eintretenswahrscheinlichkeit und andererseits durch das Ausmass des möglichen Schadens. Dementsprechend heisst Risikoverminderung Beeinflussung der Eintretenswahrscheinlichkeit und oder Massnahmen zur Reduktion des möglichen Schadens. Die Risikoverminderung ist Aufgabe des Risikomanagements, das Bestandteil der Führungsaufgabe ist und durch das IKS überwacht wird.

Das Ergebnis des Risikomanagements wird in den Divisionen in einem **Risikokataster** festgehalten. Dieser wird nach den oben erwähnten Risikokategorien gegliedert und umfasst wichtige Einzelrisiken und die zugehörigen Massnahmen. Auf der Gruppenebene wird anhand der divisionalen Risikokataster eine Synthese erarbeitet, die durch spezifische Gruppenrisiken ergänzt wird.

2.3 Compliance

Schäden können auch entstehen, wenn geltende Gesetze und interne Weisungen nicht eingehalten werden. Compliance ist in der Verantwortung des CEO's und der Divisionsleiter, die zu ihrer Unterstützung Aufgaben (aber nicht die Verantwortung) an die Risk Officers delegieren können.

2.4 Schulung

Ein wesentliches Element für die erfolgreiche Bewirtschaftung des Risiko- und IKS-Systems ist eine regelmässige Schulung in IKS-Fragen sowohl für den Risk Officer der OFG, die Risk Officers der Divisionen und die Mitarbeiterinnen und Mitarbeiter. Der Risk Officer OFG stellt die Ausbildung und regelmässige Weiterbildung der Zielgruppen sicher, nachdem er den konkreten Bedarf erhoben hat. Er genehmigt ein adäquates, stufen- und bedarfsgerechtes Schulungskonzept. Dabei lässt er sich durch die HR Funktion oder durch externe Anbieter unterstützen.

2.5 Compliance Meldestellen OFG

Alle Mitarbeitende sind dazu verpflichtet, Nichteinhaltung von Weisungen bzw. bereits den Verdacht einer Nichteinhaltung ihren Vorgesetzten zu melden. In Fällen, in denen Mitarbeitende sich dabei unwohl fühlen würde, können sie sich bei einer der folgenden Meldestellen OFG melden:

- Intern: Risk Officer OFG
- Extern: Herr Guido Seitz, Rechtsanwalt, Zürich, www.riversidelaw.ch

2.6 Berichterstattung

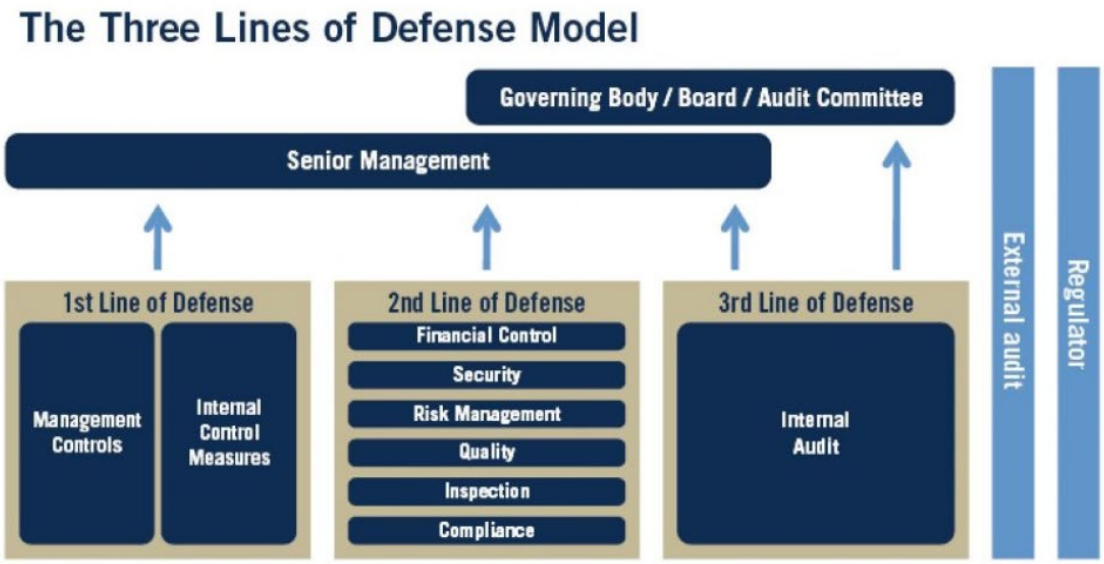
Die Berichterstattung erfolgt stufengerecht mittels:
- Risikobericht (2-mal jährlich aktualisiert)
- Risiko- und IKS-Bericht (Planung, Umsetzung, Ergebnisse, Massnahmen)
- durch:
- Risk Officer OFG
- zuhanden:
- Gruppenleitung OFG
- Verwaltungsrat Audit Committee
- Verwaltungsrat (mindestens 1 mal jährlich)

2.7 Führungsinstrumente zur Unterstützung vom IKS

Zur Bewirtschaftung der beschriebenen Risiken stehen verschiedene Führungsinstrumente zur Verfügung, welche bei Orell Füssli eingesetzt werden. Es sind dies das strategische und das finanzielle Controlling, Qualitätsmanagement-Systeme, Prozessaudits sowie andere Kontrollinstrumente, vom 4-Augen-Prinzip über Unterschriftsregelungen bis zur Internen und Externen Revision.

2.8 Organisation und Einbindung im OF-Assurance Konzept

Risikomanagement und IKS werden in erster Linie durch die Divisionen getragen. Die Gruppe sorgt für die systematischen Grundlagen, Ausbildung, Koordination und Überwachung im Sinne der Corporate Governance Auflagen. Die Organisation ist in das „OF-Assurance Konzept“ eingebunden. In diesem Konzept wird vom bekannten „Three Lines of Defense“-Modell ausgegangen, um die unterschiedlichen Rollen zur internen Unternehmenssteuerung und deren Zusammenspiel innerhalb der OF-Gruppe transparent darzustellen.



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Die im Rahmen des Risk- und IKS-Managements aktiven Verantwortungsträger und Instanzen werden nachfolgend beschrieben.
Verwaltungsrat (VR): Der Verwaltungsrat ist gegenüber den Aktionären und dem Gesetz verantwortlich für die Wirksamkeit des gruppeweiten Risiko-, IKS- und Compliance-Managements und hat im Rahmen des Jahresberichtes über die Funktionsfähigkeit des IKS zu rapportieren. Die Überwachung der Risiko- und IKS-Aktivitäten, nicht aber die Verantwortung für dieselben, hat der VR an das Audit Committee delegiert. Der VR beurteilt die Risikosituation und lässt sich über den Stand des IKS informieren.
Das VR Audit Committee

- beurteilt zweimal jährlich die aktuelle Risikosituation, sowie den Stand der festgelegten IKS Prüfungsvorhaben,
- beurteilt die Vorschläge der Divisionen zu IKS Prüfungsvorhaben für das kommende Jahr und legt diese fest,
- identifiziert in Zusammenarbeit mit dem CEO, dem CFO und dem Risk Officer OFG allfällige Prüfpunkte für die interne/externe Revision und legt diese fest.

CEO und DivL: Die Risikoüberwachung und -handhabung im Rahmen der üblichen Geschäftstätigkeit fällt in die Verantwortung des CEOs und der Divisionsleiter. Diese Verantwortlichen haben dabei vor allem das Controlling (inkl. Strategisches Controlling) derart auszugestalten, dass den Anforderungen an eine gute Chancen- und Risikokontrolle Genüge getan wird. Sie können einen Teil der Kontrollaufgaben, nicht aber ihre Verantwortung innerhalb der Unternehmen an Mitarbeitende delegieren.
Risk Officer OFG: Der Risk Officer OFG koordiniert die Umsetzung und Funktionsfähigkeit des Risiko-, IKS- und Compliance-Managements auf Stufe Gruppe (Siehe Abschnitt 11).
Risk Officer Division (ROD): Der ROD betreut die Belange des Risiko-, IKS- und Compliance-Managements innerhalb einer Division.
Abstimmung mit dem Sicherheitsbeauftragten (SIBE): Der Sicherheitsbeauftragte informiert den CEO, den Risk Officer OFG, die Divisionsleiter und die ROD über relevante Sicherheitsfragen, die für das Risiko- und Compliance Management von Bedeutung sind. Er wird vom Risk Officer OFG über die Risikosituation im Rahmen der Berichterstattung orientiert.
Abstimmung mit dem Versicherungskoordinator: Auf Gruppenstufe nimmt der CFO OFG die Funktion eines Versicherungskoordinators wahr. Er bündelt und koordiniert die Versicherungsbedürfnisse der Divisionen und stellt den optimalen Risikotransfer des Konmzerns an Versicherungsunternehmen sicher. Werden auf Divisionsstufe Risikotransfer-Wünsche erkannt, so ist der Versicherungskoordinator beizuziehen.
Externe Revision: Die externe Revision erfüllt die vom Gesetzgeber angeordnete Organfunktion. Im Weiteren muss die externe Revision die Existenz der Internen Kontrolle, soweit sie für die finanzielle Berichterstattung relevant ist, im Revisionsbericht bestätigen.
Interne Revision: Die Interne Revision (IR) unterstützt den Verwaltungsrat bei der Ausübung seiner Aufsichtsfunktion. Die IR nimmt seine Aufgaben unabhängig und selbständig wahr. Sie beurteilt die Wirksamkeit und Effizienz des Risikomanagements, der internen Steuerungs- und Kontrollsysteme sowie der Führungsprozesse (Governance) und trägt zu deren Verbesserung bei. Die Interne Revision überprüft ferner die Einhaltung von Normen (Compliance) und erbringt unabhängige und objektive Assurance- und Beratungsdienstleistungen.

2.9 Aufgaben des Risk Officers OFG

Der Risk Officer OFG stellt auf Stufe Gruppe die Umsetzung und Funktionsfähigkeit des Risiko- und IKS-Managements sicher. Er hat dabei vor allem Koordinations- und Kontrollaufgaben wahrzunehmen, die durch ihn selbst ausgeführt oder an Spezialisten delegiert werden. Zudem erarbeitet der Risk Officer OFG Vorgaben für die Qualität spezifischer Prozesse und macht Verbesserungsvorschläge bei erkannten Schwachstellen. Er führt die ROD der Divisionen fachlich. Der Risk Officer OFG rapportiert dem CEO und dem Audit Committee des VR. Er ist verantwortlich für die Führung der ROD und für die Berichterstattung an VR AC, GL, CEO und an den Sicherheitsbeauftragten OFG. Seine Aufgaben sind nachfolgend aufgezählt:

Ausführung	**Risikomanagement:** Der Risk Officer OFG koordiniert den Prozess der periodischen Überarbeitung der Risikokataster für die Gruppe und für die einzelnen Divisionen. Er leitet dazu die ROD so an, dass der Prozess in abgestimmter Form nach zweckmässiger Methodik durchgeführt wird. Er beurteilt die divisionalen Resultate und greift bei Bedarf korrigierend ein. Er erstellt in Zusammenarbeit mit dem CEO den Risikokataster der Gruppe. **IKS Prüfungen**: Der Risk Officer OFG schlägt dem VR Ausschuss AC im letzten Quartal des Jahres einen Prüfplan für das Folgejahr vor. Nach Freigabe durch den VR-Ausschuss AC sorgt er für die zeitgerechte und inhaltlich richtige Umsetzung. Er beurteilt die Ergebnisse der erfolgten

	Prüfungen und macht zuhanden des CEO's konkrete Vorschläge zur Behebung von Schwachstellen. Er begleitet den Folgeprozess bis zum erfolgreichen Abschluss der Umsetzungsmassnahmen.
Kontrolle	In Absprache mit den Linienvorgesetzten und in Zusammenarbeit mit den ROD nimmt der Risk Officer OFG folgende Aufgaben wahr: **Compliance:** (Unter Compliance wird die Einhaltung von unternehmensinternen Weisungen und Reglementen, aber auch von Gesetzen, Verordnungen und weiteren öffentlich verbindlichen, nationalen und internationalen Bestimmungen verstanden). - Der Risk Officer OFG überwacht, ob die geltenden internen Weisungen, Reglemente, Prozessbeschreibungen etc. von den betroffenen Mitarbeitenden eingehalten werden. Er stellt sicher, dass bei Bedarf Massnahmen zur Einhaltung der Vorgaben ergriffen werden. - Er überprüft, ob die Mitarbeitenden die ihre Tätigkeit betreffenden gesetzlichen Bestimmungen kennen und sich über Änderungen auf dem Laufenden halten. - Er sorgt für die regelmässige Überprüfung von Vorgaben auf Klarheit, Vollständigkeit, Zweckmässigkeit und Korrektheit. **Prozesse:** Der Risk Officer OFG überprüft, ob die den Leistungs- und Produktionsprozessen inhärenten Risiken identifiziert und erfasst wurden, ob Betrugsrisiken durch geeignete Kontrollmechanismen (Geeignete Definition auszuführender Kontrollen als Soll-Ist-Vergleich, Vier-Augen-Prinzip, Unterschriftenregelung, etc.) abgedeckt sind, ob vertrauliche Informationen eindeutig klassifiziert und gehandhabt werden und periodisch untersucht werden.
Reporting	**Periodisches Reporting an VR, VR AC, GL OFG, CEO und an den Sicherheitsbeauftragten OFG:** Der Risk Officer OFG stellt sicher, dass Dokumente und Aktivitäten laufend aktualisiert werden und dass die Berichterstattung stufengerecht gemäss Vorgaben erfolgt. **Ereignisbezogenes Reporting an CEO:** Der Risk Officer OFG erstattet über risikomanagementrelevante Ereignisse in der Gruppe dem CEO Bericht.
Unterstützung	**Beratung:** Der Risk Officer OFG berät den CEO und die GL OFG in Fragen des Risikomanagements. **Empfehlungen:** Der Risk Officer OFG empfiehlt dem CEO und dem VR AC Anpassungen bei Prozessen, Weisungen, Reglemente und Risikomanagement. **Expertenbeizug:** Im Bedarfsfall zieht der Risk Officer OFG Experten bei.

2.10 Aufgaben der Risk Officers der Divisionen

Der ROD stellt auf Stufe Division die Umsetzung und Funktionsfähigkeit des Risikomanagements- und IKS sicher. Nebst der Pflege der Systeme stellt er das Reporting zum Risk Officer OFG sicher. Der ROD erledigt auch divisionsspezifische Aufgaben nach Weisung des DivL. Seine Aufgaben sind nachfolgend aufgezählt:

Ausführung	**Risikokataster:** Der ROD stellt den Risikokataster der Division gemäss Vorgaben des Risk Officer OFG zusammen und stellt laufend sicher, dass Beschreibung und Auswertung der Risiken aktuell sind. **Risikomanagement:** Der ROD stellt im Rahmen der gruppeweiten Vorgaben die Vollständigkeit und Zweckmässigkeit des divisionalen Risikomanagements sicher. **IKS Vorhaben**: Der ROD identifiziert und schlägt vor, welche Themen und Punkte im kommenden Kalenderjahr geprüft werden sollen. Er stellt laufend sicher, dass der Stand der Dokumentation der laufenden Arbeiten aktuell ist. Sämtliche Aufgaben werden in Abstimmung mit dem Risk Officer OFG und den Divisionsleiter ausgeführt.
Kontrolle	**Compliance:** Der ROD prüft, ob die geltenden internen Weisungen, Reglemente, Prozessbeschreibungen etc. von den betroffenen Mitarbeitenden eingehalten werden. Er klärt bei Fehlverhalten ab, ob dieses auf Unkenntnis der Weisung, auf überholte Vorschriften, auf Nachlässigkeit oder anderes zurückzuführen ist. Er definiert Massnahmen zur Sicherstellung der Einhaltung der Vorgaben. - Er überprüft, ob die Mitarbeitenden die ihre Tätigkeit betreffenden gesetzlichen Bestimmungen kennen und sich über Änderungen auf dem Laufenden halten. - Er sorgt für die regelmässige Überprüfung von Vorgaben auf Klarheit, Vollständigkeit, Zweckmässigkeit und Korrektheit. **Prozesse:** Der ROD überprüft, ob die den Leistungs- und Produktionsprozessen inhärenten Risiken identifiziert und erfasst wurden, ob Betrugsrisiken durch geeignete Kontrollmechanismen (Genaue Definition auszuführender Kontrollen als Soll-Ist-Vergleich, Vier-Augen-Prinzip, Unterschriftenregelung, etc.) abgedeckt sind und ob schützenswerte Informationen adäquat klassifiziert und gehandhabt werden.
Reporting	**Periodisches Reporting an DivL (Kopie an Risk Officer OFG):** Der ROD aktualisiert Dokumente und Aktivitäten laufend auf der gemeinsamen Ablage und rapportiert regelmässig an den DivL. **Ereignisbezogenes Reporting an DivL:** Der ROD führt Protokoll über risikomanagementrelevante Ereignisse in der Division und stellt die Information des DivL und des Risk Officer OFG sicher.
Unterstützung	**Beratung:** Der ROD berät den DivL und Kaderangehörige der Division in Fragen des Risikomanagements. **Empfehlungen:** Der ROD empfiehlt dem DivL und dem Risk Officer OFG Anpassungen bei Prozessen, Weisungen und Risikomanagement. **Expertenbeizug:** Im Bedarfsfall zieht der ROD in Absprache mit dem Risk Officer OFG und dem DivL Experten bei.

Organisation ROD

Anforderungen: Der ROD kann seine Funktion im Nebenamt ausüben, sofern der DivL sicherstellt, dass der ROD ausreichende Kapazität und das nötige Fachwissen für die Ausübung der Risikomanagement- und IKS Aufgaben zur Verfügung hat. In der Regel ist er Mitarbeitender der Division. Der ROD muss für die ihm übertragenen Aufgaben zeitlich verfügbar sein, über analytische und betriebswirtschaftliche Fähigkeiten verfügen und sich durch Unabhängigkeit im Urteil und Handeln auszeichnen.

Unterstellung: Der ROD rapportiert in seiner Aufgabe direkt an den DivL und wird durch diesen in Absprache mit dem Risk Officer OFG ernannt. Fachlich wird der ROD vom Risk Officer OFG geführt.

Zusammenarbeit mit DivL: Der ROD unterstützt den DivL massgeblich bei der Umsetzung des Risikomanagements. Er handelt in der Regel aus eigenem Antrieb, kann aber auch im Auftrag des DivL aktiv werden. Der ROD spricht seine Aktivitäten im Voraus mit dem Risk Officer OFG und dem DivL ab und erstattet beiden Bericht.

Zusammenarbeit mit dem Risk Officer OFG: Der ROD unterstützt den Risk Officer OFG bei der Ausführung seiner Aufgaben. Der Risk Officer OFG führt fachlich die ROD, hat bei Fachfragen Weisungsrecht gegenüber dem ROD und überwacht die Qualität und Effizienz der Arbeit des ROD durch Kontrollen in Absprache mit dem DivL.