Weiterentwicklung der ONR 49000-Serie zur ÖNORM D 4900-Serie

Prof. Dr. Bruno Brühwiler

Update Mai 2021

Ausgangslage

- Revision der ISO 31000 wurde 2018 abgeschlossen
- Bedürfnis nach Spezifikation von deren Inhalten
- Erfolgsgeschichte der 49000-Serie, vor allem in der Ausbildung von klinischen Risikomanagern
- Weiterentwicklung von Managementsystemen, insbesondere auch die ISO High Level Structure
- Erfahrungen in der Ausbildung und Beratung.

Vorgaben zur Weiterentwicklung der ONR 49000?

Netzwerk Risikomanagement

Euro Risk Limited

Die ONR wurde durch eine Arbeitsgruppe, bestehend aus Experten von Österreich, Deutschland und der Schweiz weiterentwickelt.

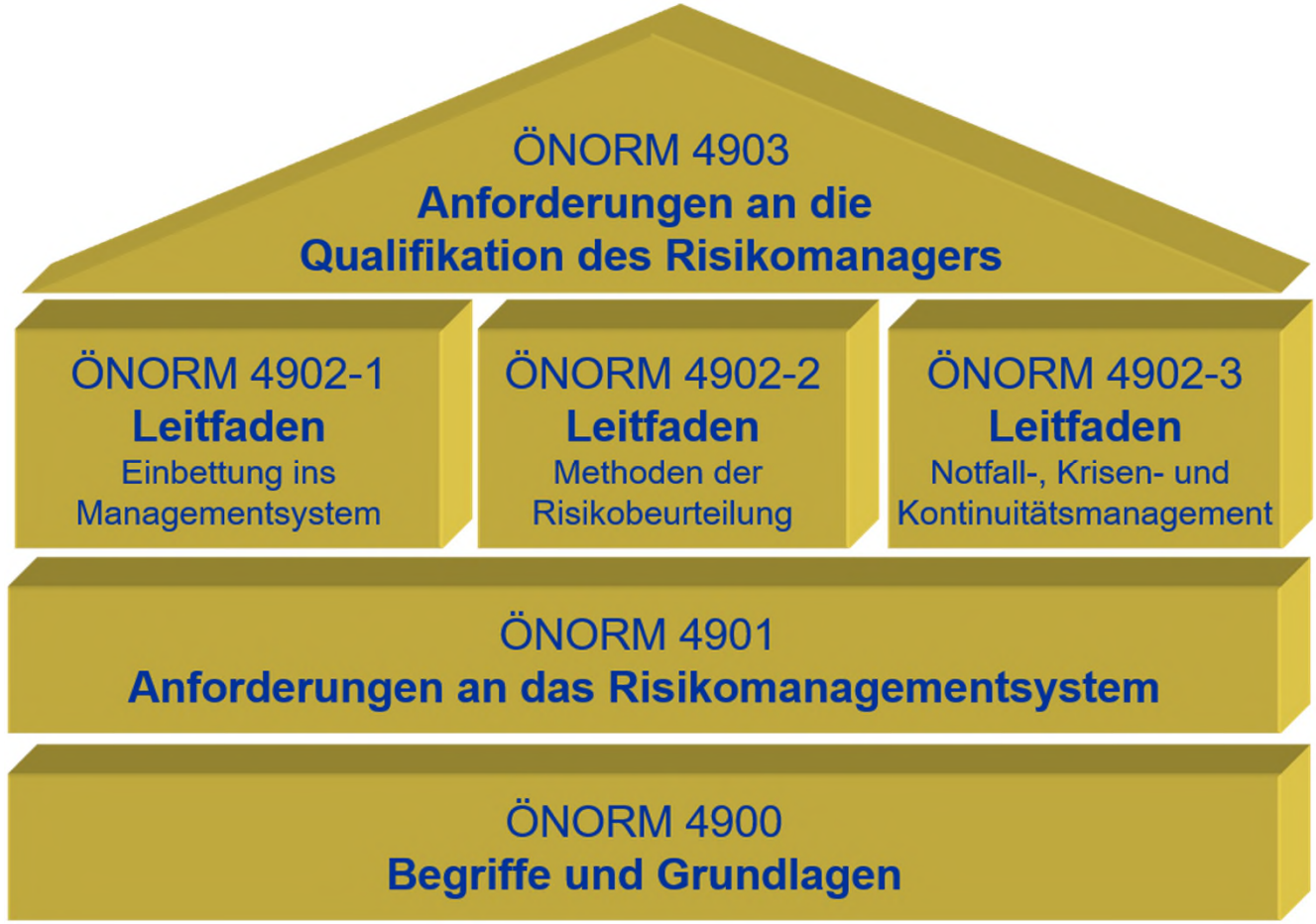
Frage 1: Wollen wir die HLS konsequent umsetzen?

Frage 2: Wollen wir nur Empfehlungen oder verbindliche Anforderungen (zertifizierbare Norm) schaffen?

Deshalb wird die ONR (Regelwerk) zu einer ÖNORM mit der Möglichkeit der Zertifizierung weiterentwickelt.

Anforderung: Hoher Wiedererkennungswert durch Beibehaltung von Struktur und Prozess Risikomanagement.

Unveränderte Normstruktur

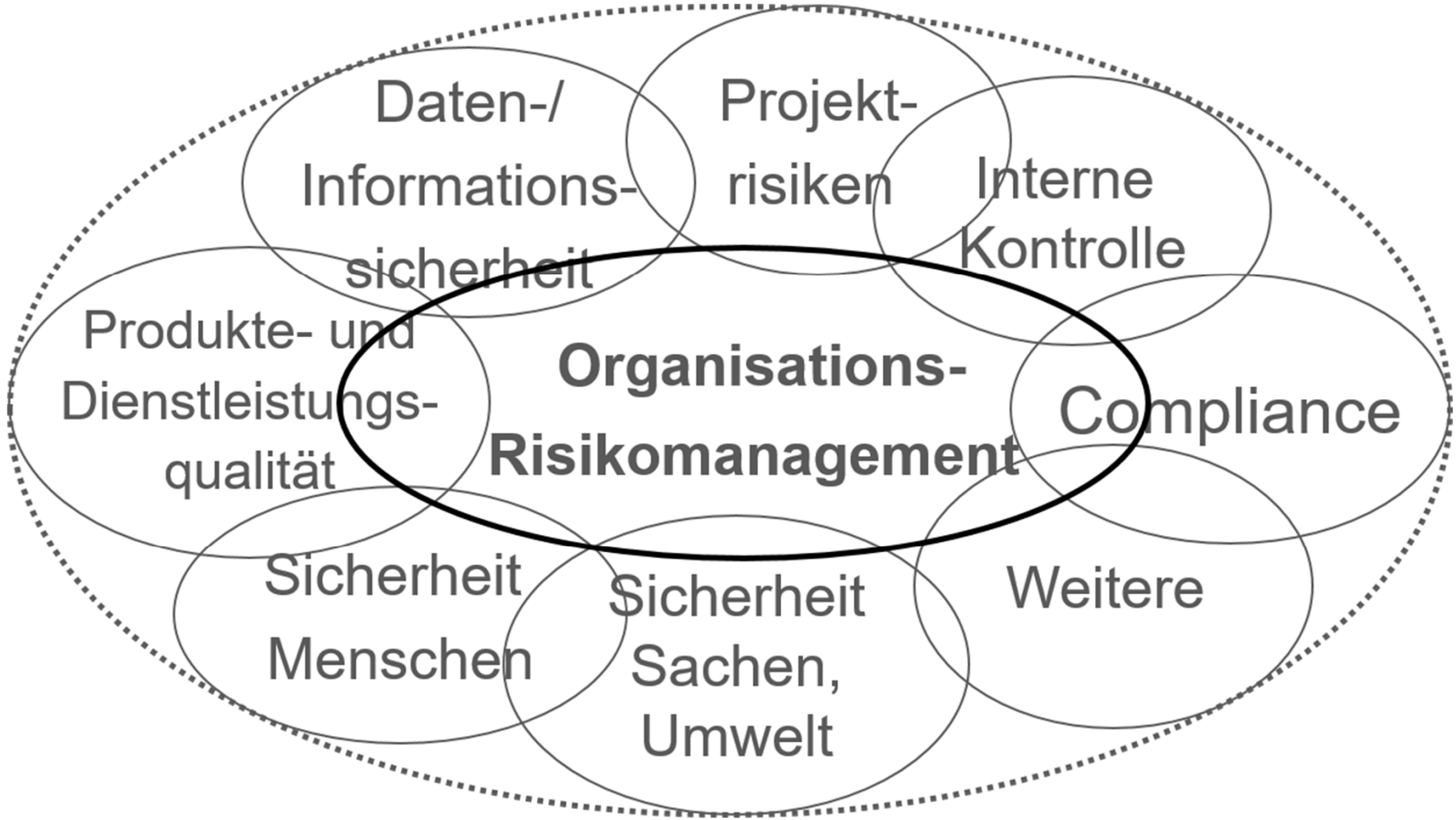


Umfang des Risikomanagementsystems

Das Risikomanagementsystem erstreckt sich nicht nur auf das Organisations-Risikomanagement, in welchem sich die oberste Leitung mit den bestandsgefährdenden Risiken befasst.

Es erstreckt sich auch auf die auf dem risikobasierten Ansatz aufgebauten Teilbereiche wie Produkt- und Dienstleistungsqualität, Sicherheit für Menschen (insbes. klinisches Risikomanagement), interne Kontrollsysteme, Compliance, Datenschutz und Informationssicherheit, Projekt-Risiken und weitere Anwendungsbereiche.

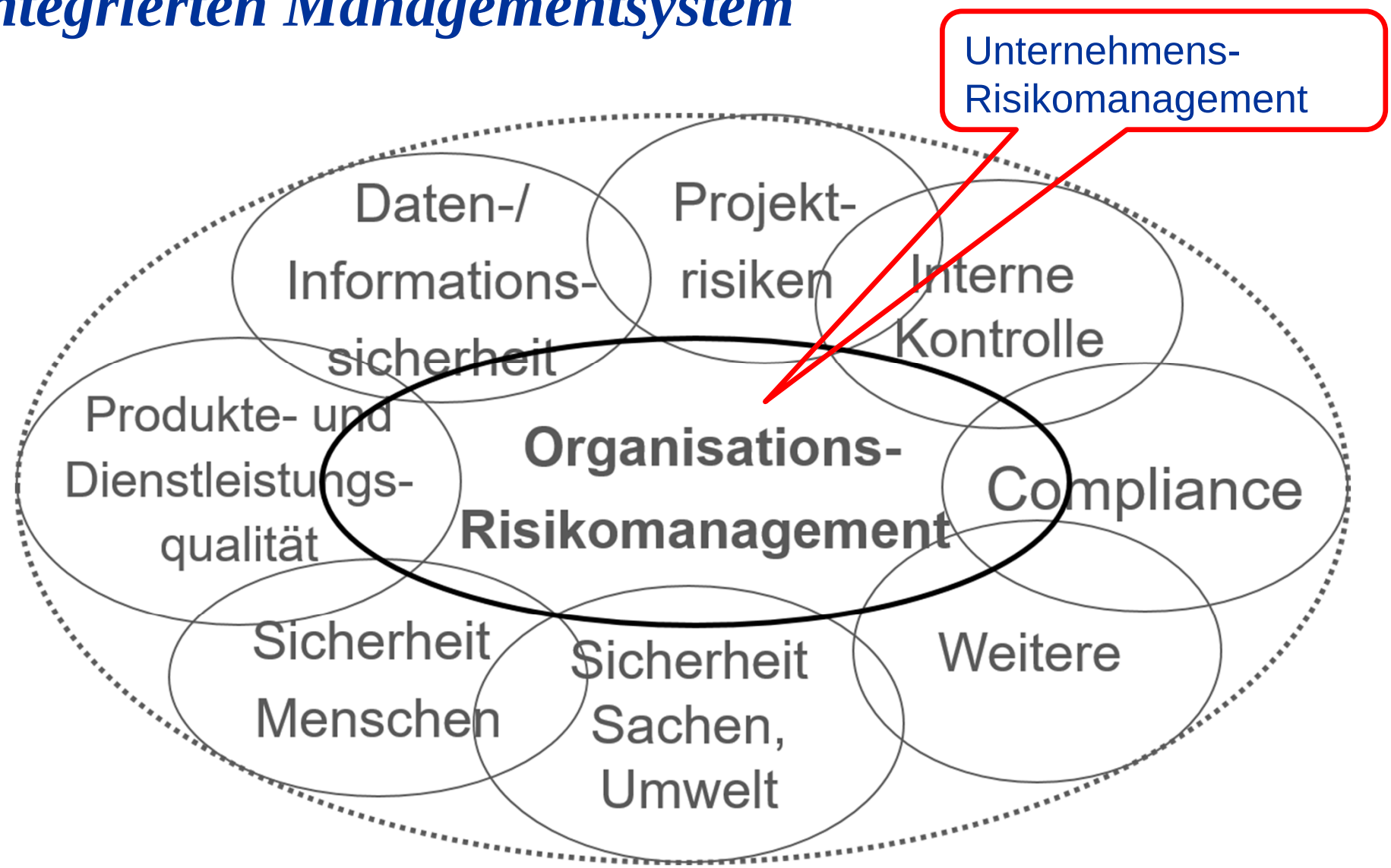
Das Grundkonzept in einem integrierten Managementsystem



Das Grundkonzept in einem integrierten Managementsystem

Netzwerk Risikomanagement

Euro Risk Limited



Der Risikomanagementprozess schliesst das Notfall-, Krisen- und Kontinuitätsmanagement ein

Der Risikomanagementprozess muss umfassen:

- die Früherkennung von Risiken (Bedrohungen, Chancen)
- die Analyse und Bewertung der Risiken,
- die Frühwarnung bei drohendem Schaden,
- die Bewältigung und Überwachung von Risiken,
- die Reaktion auf plötzlich eintretende Schadenereignisse und
- die Erkennung und Wahrnehmung von Chancen zur Organisationsentwicklung.

Warum verbindliche Anforderung?

Netzwerk Risikomanagement

Euro Risk Limited

Risikomanagement ist eine gesetzliche Aufgabe und Verpflichtung der obersten Leitung. Reine Empfehlungen sind unverbindlich und reichen deshalb nicht aus. Es braucht Anforderungen, diese müssen allerdings massgeschneidert und der Organisation angemessen sein («Kontext der Organisation»).

Die Konformität der Komponenten des Risikomanagementsystems mit den Anforderungen der Norm muss festgestellt werden können. Dies erfolgt entweder durch eine interne Bewertung (Self Assessment, internes Audit) oder durch eine zusätzliche externe Bewertung.

Die Übereinstimmung eines Risikomanagementsystems mit Anforderungen kann – sofern gewünscht – zertifiziert werden.

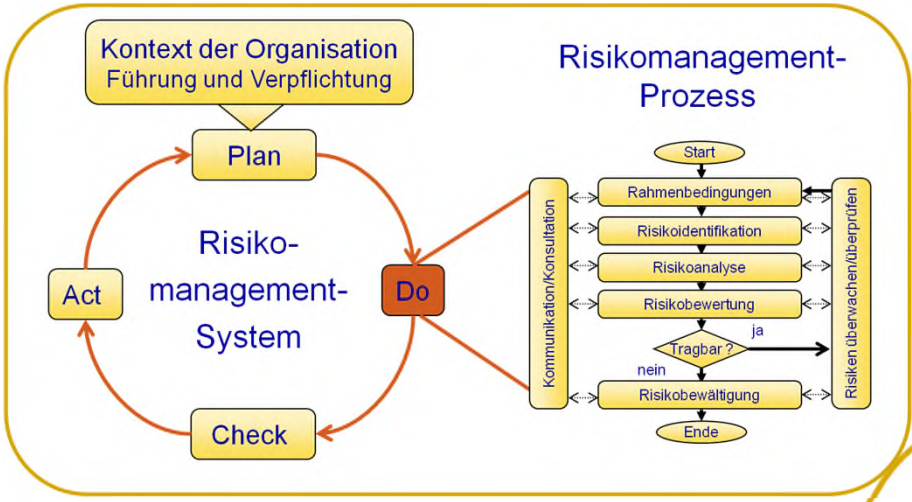
Die ISO Welt hat in den vergangenen Jahren Managementsystem-Normen durch die sogenannte «High Level Structure» vereinheitlicht.

Die einheitliche ISO Managementsystem-Struktur (High Level Structure)

Netzwerk Risikomanagement

Euro Risk Limited

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. Kontext der Organisation
5. Risikomanagement als Führungsaufgabe
6. Planung des Risikomanagementsystems
7. Unterstützung des Risikomanagements
8. Betrieb des Risikomanagementprozesses
9. Bewertung der Wirksamkeit des Risikomanagementsystems
10. Verbesserung des Risikomanagementsystems

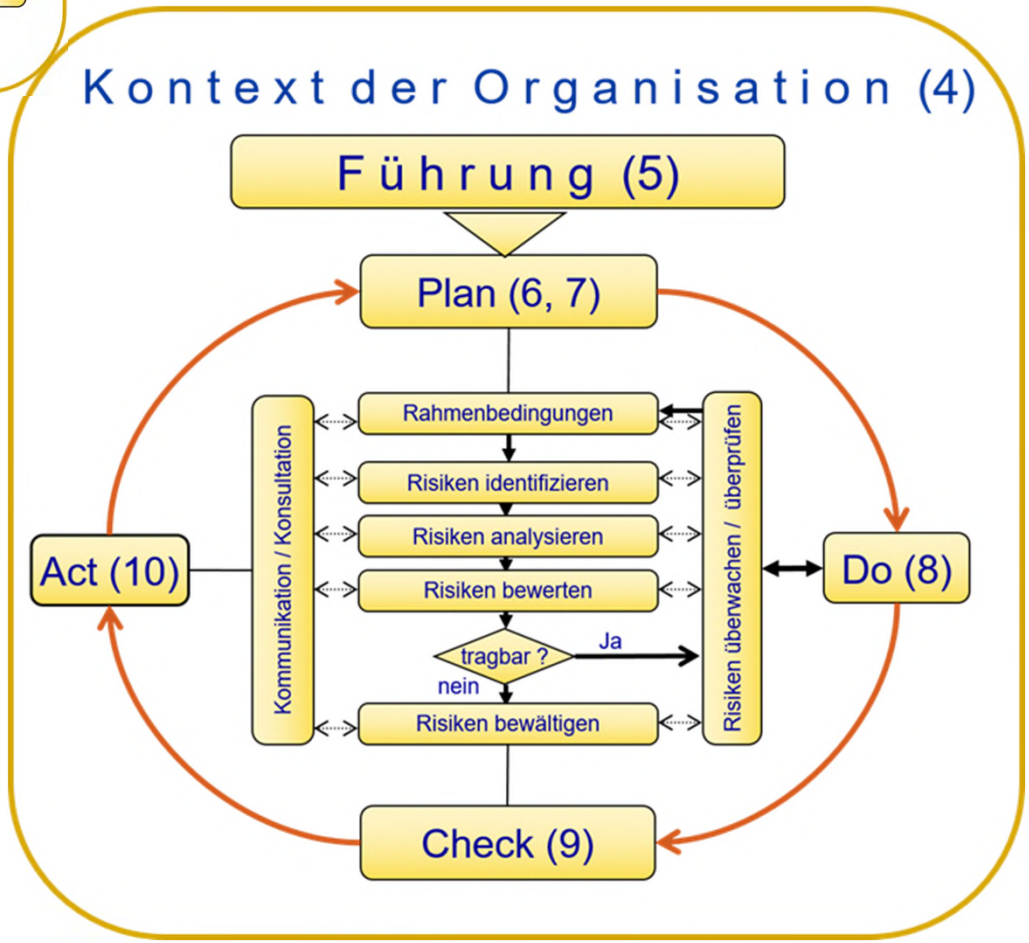


Bisher duale Gliederung

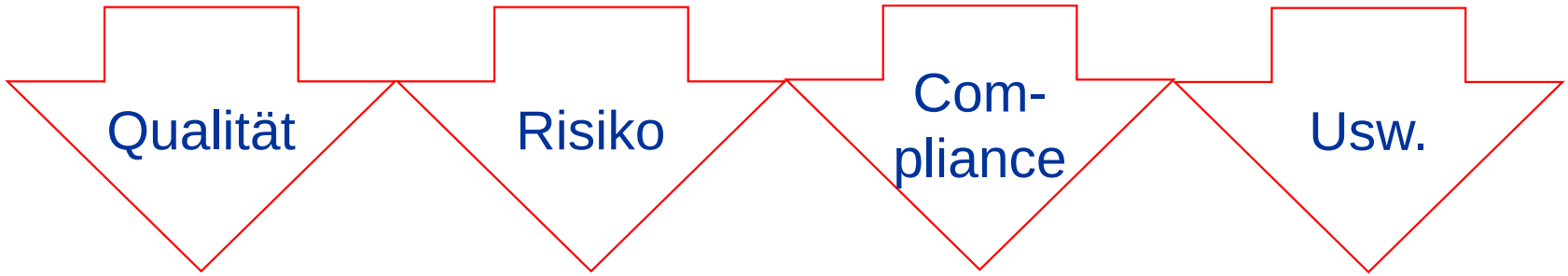
Netzwerk Risikomanagement

Euro Risk Limited

Neue Gliederung



Integration von verschiedenen Managementsystemen wird direkt unterstützt

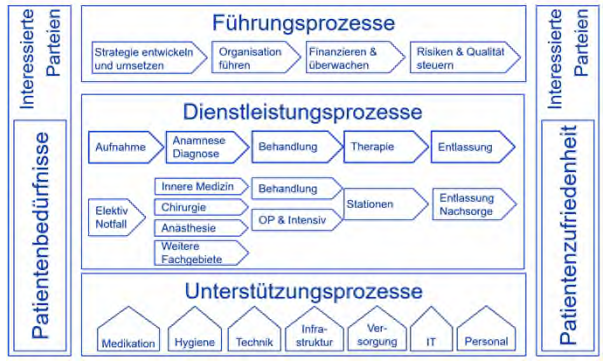


ISO Managementsystem-Struktur

«Doppelspurigkeiten sind zu vermeiden»

Anforderungen an Qualitäts- und Risikomanagement (1)

Netzwerk Risikomanagement — Euro Risk Limited

		ISO 9001	ÖNORM 4901
4	Kontext	▪ Relevante externe und interne Themen berücksichtigen ▪ Relevante Anforderungen der interessierten Parteien bestimmen ▪ Anwendungsbereich festlegen ▪ QMS aufbauen, verwirklichen, aufrecht erhalten und fortlaufend verbessern , ▪ Prozesse und ihre Wechselwirkungen bestimmen 	▪ Relevanten internen und externen Kontext berücksichtigen ▪ Relevante Anforderungen der interessierten Parteien bestimmen ▪ Organisatorische Grenzen festlegen ▪ Umfeldanalyse und Organisationsanalyse durchführen ▪ Übereinstimmung mit der Politik, der Strategie, den Zielen, den Tätigkeiten sowie den bindende Verpflichtungen der Organisation feststellen ▪ Organisationsrisikomanagement für die bestands-gefährdenden Risiken, risikobasierter Ansatz für Teilbereiche des Management-systems  ▪ RMS aufbauen, verwirklichen, aufrecht erhalten und fortlaufend verbessern ▪ Wesentliche Risiken erkennen und beurteilen ▪ Risikomanagementprozess anwenden ▪ Notfall-, Krisen- und Kontinuitätsmanagement einschliessen

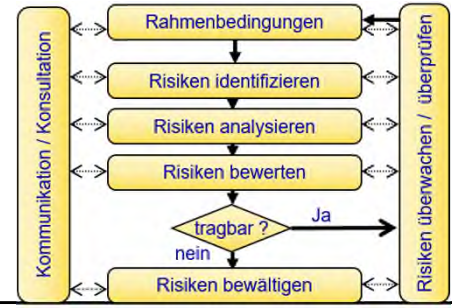
Anforderungen an Qualitäts- und Risikomanagement (2)

		ISO 9001	ÖNORM 4901
5	Führung	Führung und Verpflichtung Kundenorientierung Qualitätspolitik (allgemein) Verantwortlichkeiten und Befugnisse	Risikomanagement als Führungsaufgabe in die Organisation einbinden, ▪ Risikotragfähigkeit ▪ Bedeutende Risiken steuern ▪ Überwachungsorgane einbeziehen Risikopolitik inhaltlich spezifizieren ▪ Beauftragter der obersten Leitung ▪ Risikoeigner, Risikomanager, Auditoren
6	Planung	Berücksichtigung von Massnahmen im Umgang mit Risiken und Chancen, Aktionspläne, Anpassung bei Veränderungen	Berücksichtigung von Wertschöpfung, Risikokultur, Zielkonflikte erkennen und lösen Aktionspläne, Anpassung bei Veränderungen
7	Unter-stützung	Ressourcen, Fähigkeiten, Infrastruktur, Umgebung, Messtechnik, Wissen, Kommunikation Dokumentierte Information Dokumentenlenkung	Ressourcen, Fähigkeiten, Infrastruktur, interne und externe Risikokommunikation, einschliesslich Krisenkommunikation, ▪ Fehlermeldesysteme ▪ Beschwerdemeldungen ▪ Hinweisgebersysteme Information zum Risikomanagementprozess und zum Risikomanagementsystem dokumentieren

Anforderungen an Qualitäts- und Risikomanagement (3)

Netzwerk Risikomanagement

Euro Risk Limited

		ISO 9001	ÖNORM 4901
8	Betrieb	▪ Anforderungen an Produkte und Dienstleistungen (Kriterien, Ressourcen, Konformität, Steuerung, Dokumentierung) ▪ Kommunikation mit Kunden, Information über Produkte und Dienstleistungen, Kundenreklamationen ▪ Entwicklung von Produkten und Dienstleistungen steuern ▪ Beschaffung, Outsourcing einbeziehen ▪ Produktion unter beherrschten Bedingungen durchführen ▪ Produkten und Dienstleistungen freigeben ▪ Nicht konformer Ergebnisse korrigieren ▪ Dokumentierte Information gewährleisten	▪ Rahmenbedingungen ▪ Kommunikation / Konsultation ▪ Risiken identifizieren ▪ Risiken analysieren ▪ Risiken bewerten ▪ Risiken bewältigen ▪ Risiken überwachen / überprüfen 
9	Bewer-tung	▪ Bewertung Leistung und Wirksamkeit, einschliesslich Wahrnehmung der Kunden ▪ Interne Audits ▪ Managementbewertung	▪ Bewertung Leistung und Wirksamkeit ▪ Interne Audits ▪ Managementbewertung
10	Verbes-serung	▪ Verbesserung von Produkten und Dienstleistungen ▪ Verbesserung Wirksamkeit des Systems ▪ Behebung von Nonkonformitäten	▪ Verbesserung der Wirksamkeit des Risikomanagementsystems

Individuelle Bestimmung des Anwendungsbereichs

Netzwerk Risikomanagement

Euro Risk Limited

Die Organisation muss die organisatorischen Grenzen und die inhaltliche Anwendbarkeit ihres Risikomanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

Dabei muss die Organisation

- den internen und externen Kontext,
- die Erwartungen und Anforderungen der interessierten Parteien und
- die strategischen Ziele, operativen Tätigkeiten und bindenden Verpflichtungen beachten.

Dabei ist sicherzustellen, dass die wesentlichen Risiken berücksichtigt werden.

Rollen im Risikomanagement

- Oberste Leitung und Überwachungsorgane
- Risikoeigner
- Risikomanager
- Auditoren (Revisoren)

Führung und Verpflichtung der obersten Leitung

Die oberste Leitung muss sicherstellen, dass das Risikomanagement gemäss dem Anwendungsbereich in die Organisation eingebunden wird, indem sie

a. die Rechenschaftspflicht für das Risikomanagementsystems übernimmt,
b. die Komponenten des Risikomanagementsystems angemessen gestaltet, umsetzt, bewertet, laufend verbessert und weiterentwickelt,
c. eine Risikopolitik erlässt und eine Vorgehensweise festlegt, welche dem Kontext der Organisation, ihren Zielen, Tätigkeiten und Anforderungen entspricht,
d. …..

Führung und Verpflichtung der obersten Leitung

Die oberste Leitung muss sicherstellen, dass das Risikomanagement gemäss dem Anwendungsbereich in die Organisation eingebunden wird, indem sie …

d. die Risikotragfähigkeit der Organisation angemessen festlegt,
e. sicherstellt, dass die notwendigen Ressourcen dem Risikomanagement zugeteilt werden,
f. die Befugnisse und Verantwortung den entsprechenden Stufen in der Organisation zuweist,
g. die bedeutendsten Risiken der Organisation regelmäßig in den dafür verantwortlichen Gremien behandelt und steuert und
h. die Überwachungsorgane, falls solche gegeben sind, in das Risikomanagement angemessen einbezieht.

Risikoeigner und Risikomanager

Risikoeigner:
Person mit der Entscheidungskompetenz und Verantwortung, hinsichtlich eines Risikos zu handeln.

Risikomanager:
Der Risikomanager kann den Risikomanagement-prozess anwenden und in Organisationen umsetzen.

Auditoren (Revisoren)

Auditoren prüfen die Wirksamkeit des Risikomanagements in objektiver und unabhängiger Art und berichten die Ergebnisse der obersten Leitung bzw. den Überwachungsorganen. Es kann sich dabei um interne Personen und Organe oder um externe Personen bzw. Organisationen handeln.

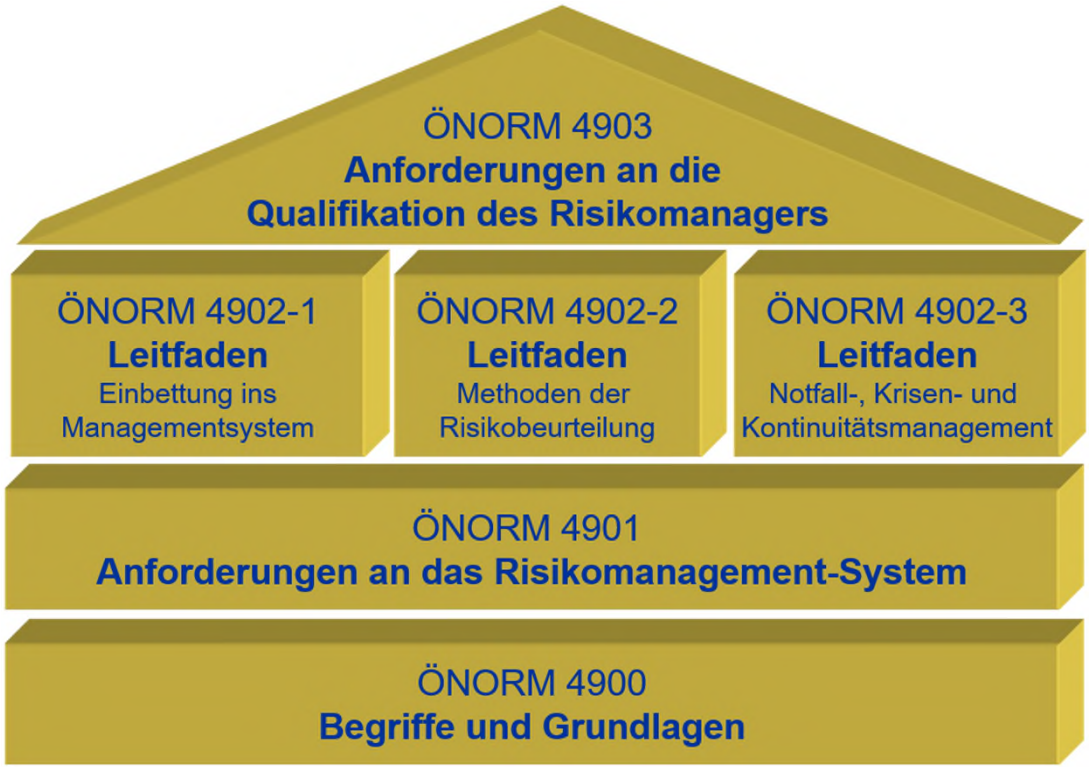
Externe Auditoren von nachweislich befähigten Zertifizierungsstellen können Konformitätsprüfungen bzw. ein externes Audit mit anerkannter Zertifizierung durchführen.

Analog zu Auditoren, die Managementsysteme bewerten, nehmen oft auch Revisoren im Sinne der Wirtschaftsprüfer diese Aufgabe wahr.

Die ÖNORM-4900-Serie ist seit Januar 2021 verfügbar.

Netzwerk Risikomanagement

Euro Risk Limited



Ausblick: Nicht mehr nur Empfehlungen, sondern überprüfbare Anforderung

ISO 31000 und die bisherige ONR 49000 enthalten Empfehlungen mit erklärenden Beschreibungen, worum es beim Risikomanagement geht.

Die «neue Welt» der ÖNORM 4901 besteht aus Anforderungen, die verbindlich formuliert und damit konkret überprüfbar sind. Die Zeit der empfehlenden Regelwerke für das Risikomanagement geht zu Ende.