

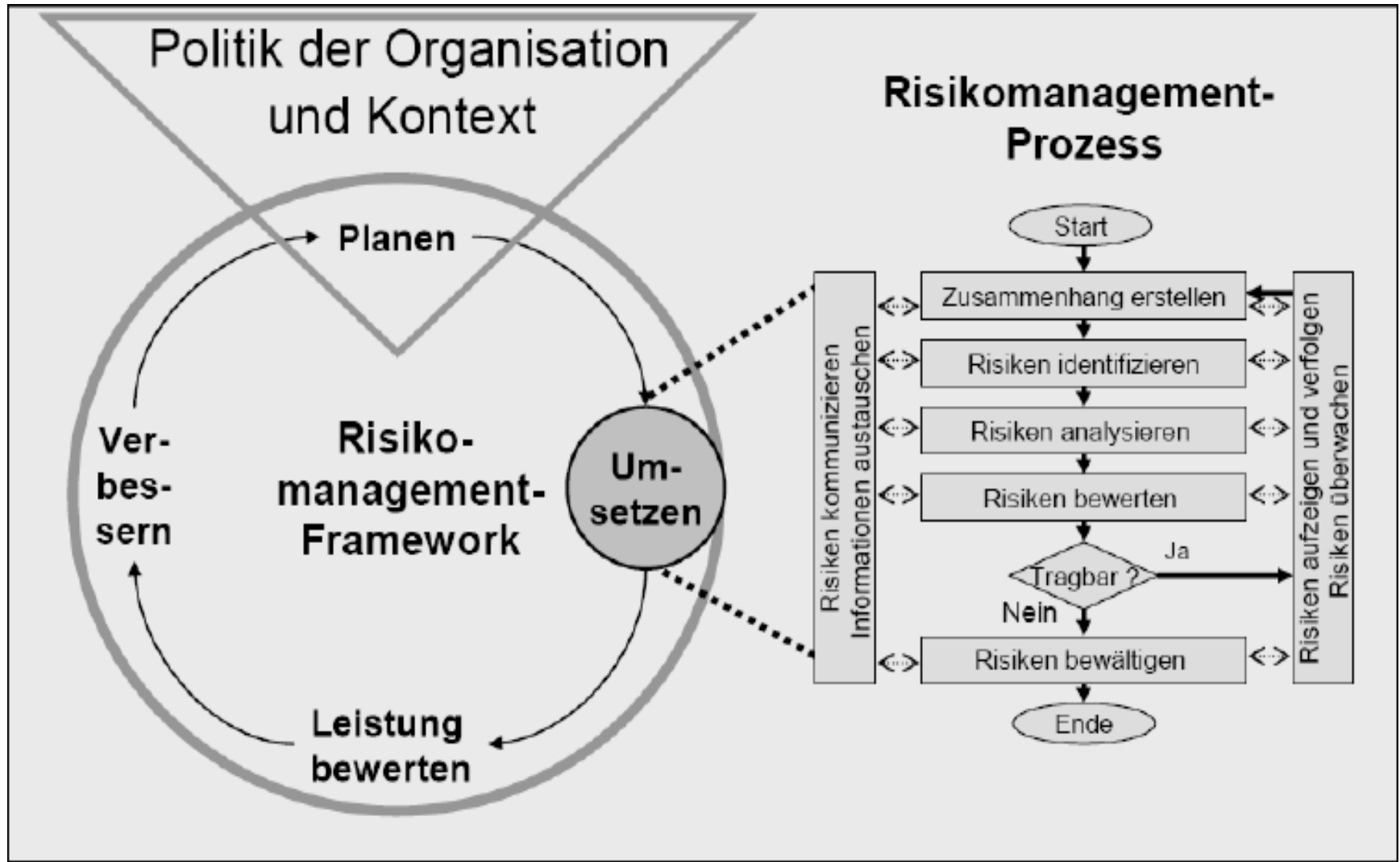
ISO 31000 – Risikomanagement: Gemeinsamkeiten und Synergien mit anderen Normen

Dr. Jürg Liechti, Neosys AG

1. ISO 31000: Inhalt + Aufbau
2. Anwendung; Einbau in ein bestehendes Managementsystem
3. Gemeinsamkeiten und Bezüge
 - ➔ ISO 9001 / ISO 14001
 - ➔ OHSAS 18011, EKAS, HACCP
4. Risikomanagement mit ISO 31000: KMU-Beispiel

- Es ist klar geworden, dass die verschiedenen „Risk-managements“ mit derselben Mathematik und mit ähnlich gelagerten Instrumenten betrieben werden.
- Corporate Governance Reformen (USA: Sarbanes-Oxley Act ; Deutschland: KonTraG; Schweiz: OR-Reform, IKS) haben die Bedeutung des Unternehmens-RM verstärkt.
- Risikomanagement-Fehlleistungen zeigen den Bedarf nach Integration in das allgemeine Management auf.

ISO 31000 = AS/NZS 4360 + ONR 49000



„Risk Management – Principles and guidelines“

1 Scope → generisch, generell, auf alles anwendbar

2 Begriffe und Definitionen → ISO/IEC Guide 73

3 Prinzipien für das Risikomanagement

4 Der Management-Rahmen für Risikomanagement

5 Der Risikomanagement-Prozess

Anhang A Eigenschaften von hochwertigem Risikomanagement



RISK (3.1)
RISK MANAGEMENT (3.2)
RISK MANAGEMENT FRAMEWORK (3.2.1)
RISK MANAGEMENT POLICY (3.2.2)
RISK MANAGEMENT PLAN (3.2.3)
RISK MANAGEMENT PROCESS (3.3)
COMMUNICATION AND CONSULTATION (3.3.1)
STAKEHOLDER (3.3.1.1)
RISK PERCEPTION (3.3.1.2)
ESTABLISHING THE CONTEXT
EXTERNAL CONTEXT (3.3.2.1)
INTERNAL CONTEXT (3.3.2.2)
RISK CRITERIA (3.3.2.3)
RISK ASSESSMENT (3.3.3)
RISK IDENTIFICATION (3.3.4)
RISK SOURCE (3.3.4.1)
EVENT (3.3.4.2)
HAZARD (3.3.4.3)
RISK OWNER (3.3.4.4)
RISK ANALYSIS (3.3.5)
UNCERTAINTY (3.3.5.1)
LIKELIHOOD (3.3.5.2)
EXPOSURE (3.3.5.2.1)
CONSEQUENCE (3.3.5.3)
PROBABILITY (3.3.5.4)
FREQUENCY (3.3.5.5)
RESILIENCE (3.3.5.6)
VULNERABILITY (3.3.5.7)
RISK MATRIX (3.3.5.8)
CONTROL (3.3.5.9)
LEVEL OF RISK (3.3.5.10)

GUIDE 73

RISK EVALUATION (3.3.6)
RISK ATTITUDE (3.3.6.1)
RISK APPETITE (3.3.6.2)
RISK TOLERANCE (3.3.6.3)
RISK AVERSION (3.3.6.4)
RISK AGGREGATION (3.3.6.5)
RISK TREATMENT (3.3.7)
CONTROL (3.3.7.9)
RISK ACCEPTANCE (3.3.7.1)
RISK AVOIDANCE (3.3.7.2)
RISK SHARING (3.3.7.3)
RISK FINANCING (3.3.7.4)
RISK RETENTION (3.3.7.5)
RISK MITIGATION (3.3.7.6)
RESIDUAL RISK (3.3.7.7)
MONITORING AND REVIEW
MONITORING (3.3.8.1)
REVIEW (3.3.8.2)
RISK REPORTING (3.3.8.3)
RISK REGISTER (3.3.8.3.1)
RISK PROFILE (3.3.8.3.2)
RISK MANAGEMENT AUDIT (3.3.8.4)

I) Prinzipien für Risikomanagement (Kapitel 3)

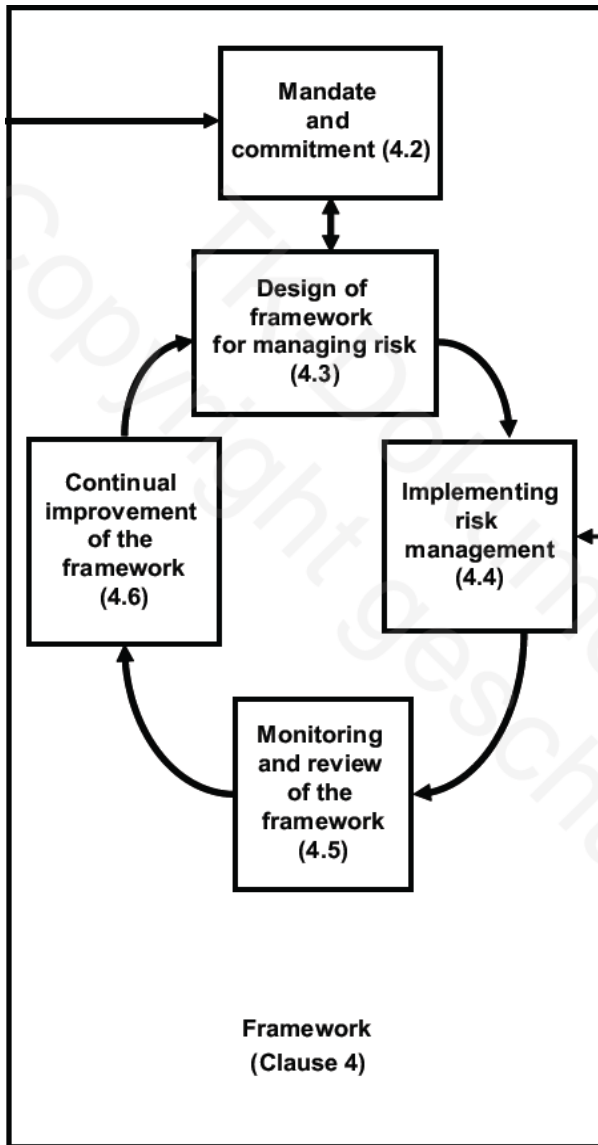
- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

Principles
(Clause 3)

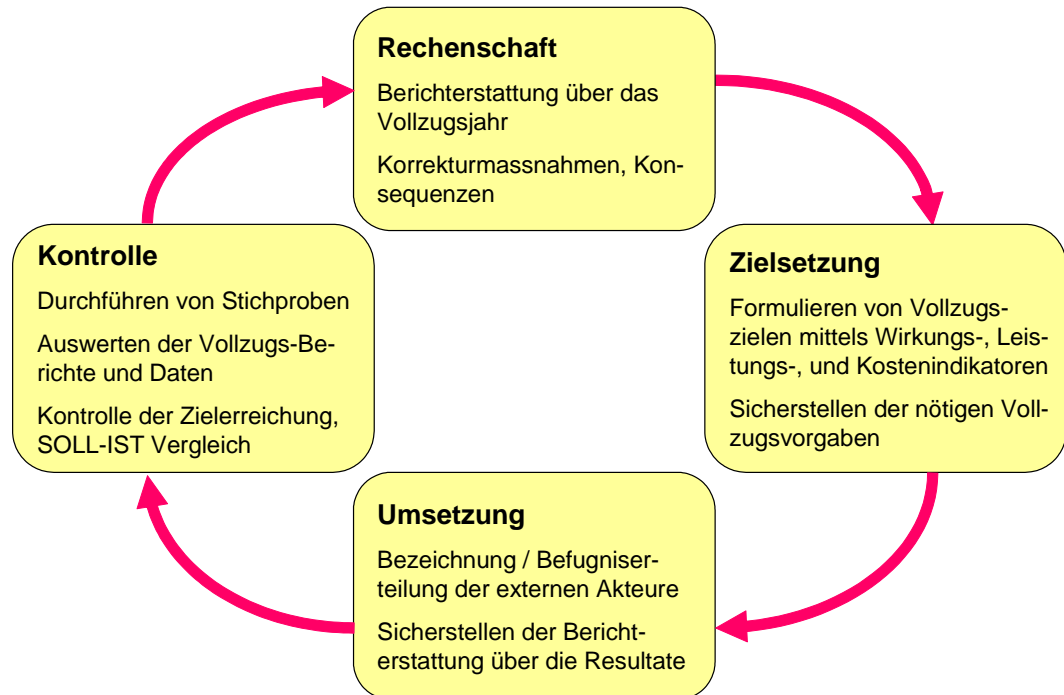
Risikomanagement

- Generiert Werte
- Ist ein integraler Teil der Prozesse
- Ist Teil des Entscheidungsprozesses
- Bezieht sich auf ungewisse Ereignisse (positive und negative)
- Ist systematisch, strukturiert und aktuell
- Basiert auf der bestmöglichen Information und Erfahrung
- Ist massgeschneidert für das jeweilige Anwendungsgebiet
- Berücksichtigt die menschlichen und kulturellen Faktoren
- Ist transparent und schliesst alle Funktionen und Stufen ein
- Ist dynamisch, iterativ und offen für Änderungen
- Unterstützt die kontinuierliche Verbesserung und Entwicklung

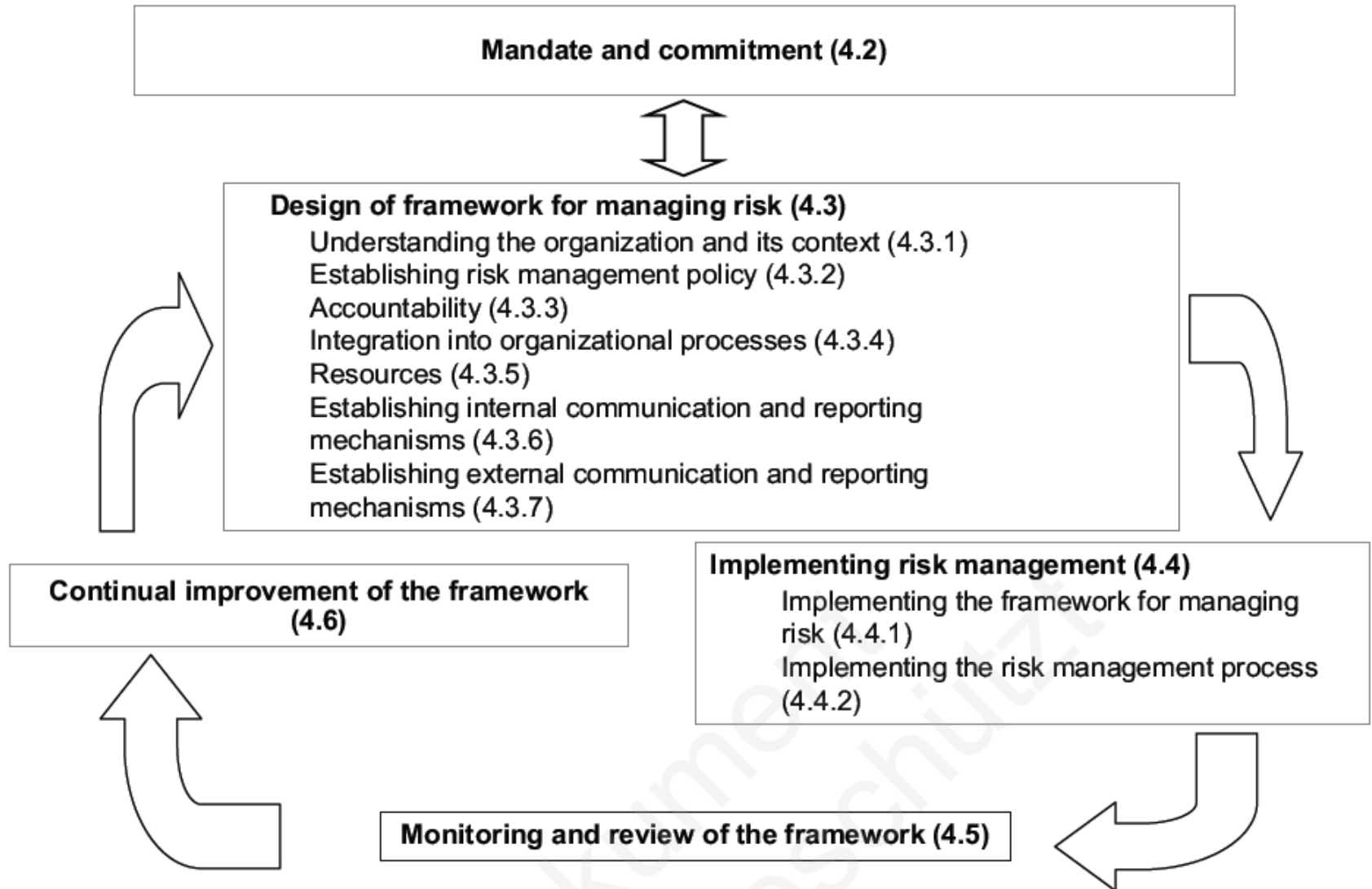
II) Management-Rahmen für Risikomanagement (Kapitel 4)



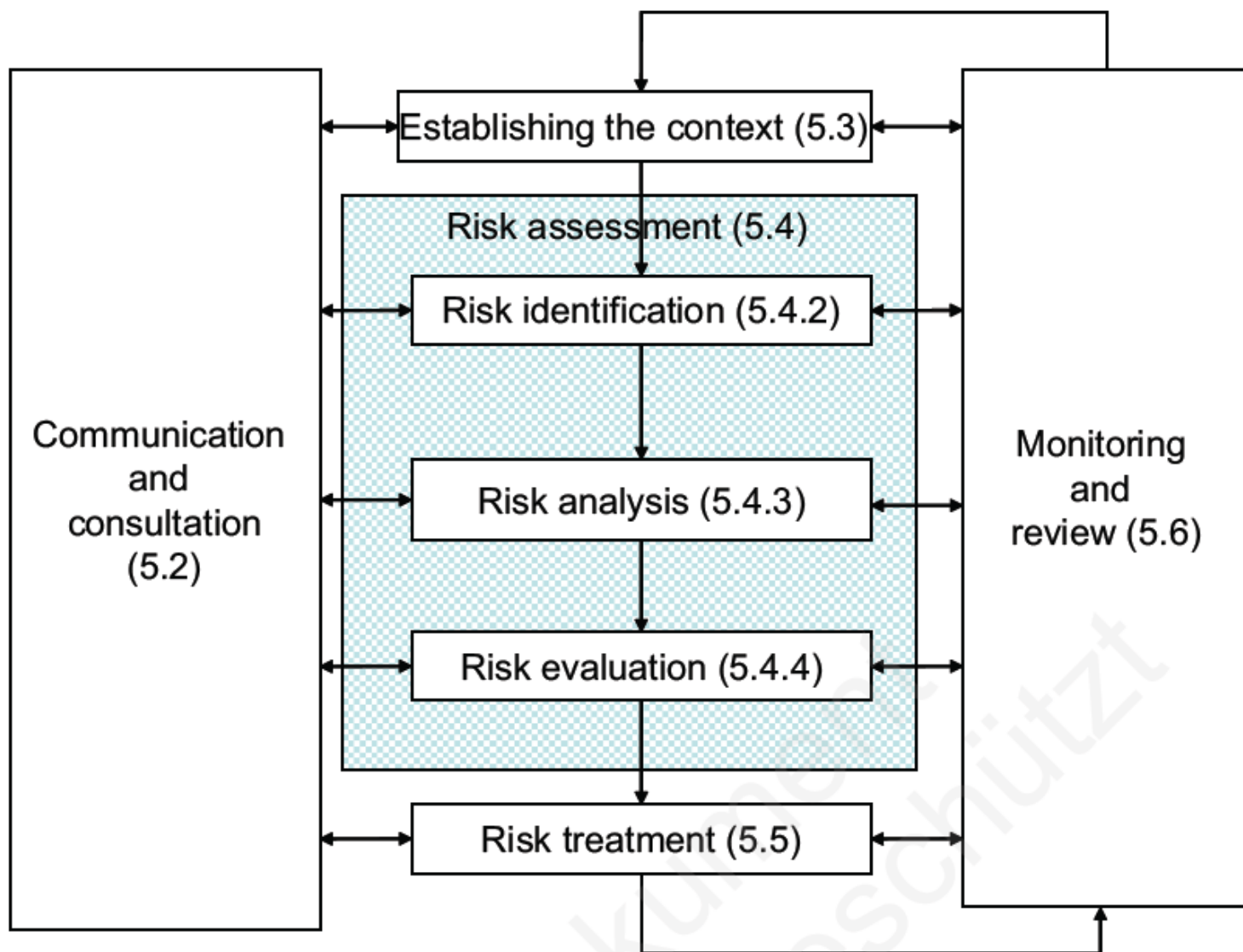
Ein typischer solcher Rahmen ist zB. ein Managementsystem nach ISO 9001, oder jedes prozessorientierte Managementsystem, das auf einem PDCA-Zyklus beruht.



II) Management-Rahmen im Detail



III) Der Risikomanagement-Prozess (Kapitel 5)

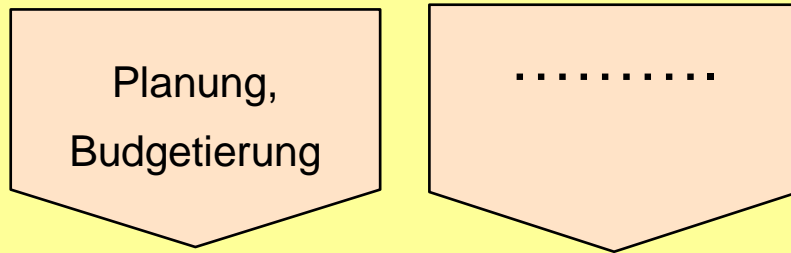


IV) Eigenschaften von hochwertigem RM (Anhang)

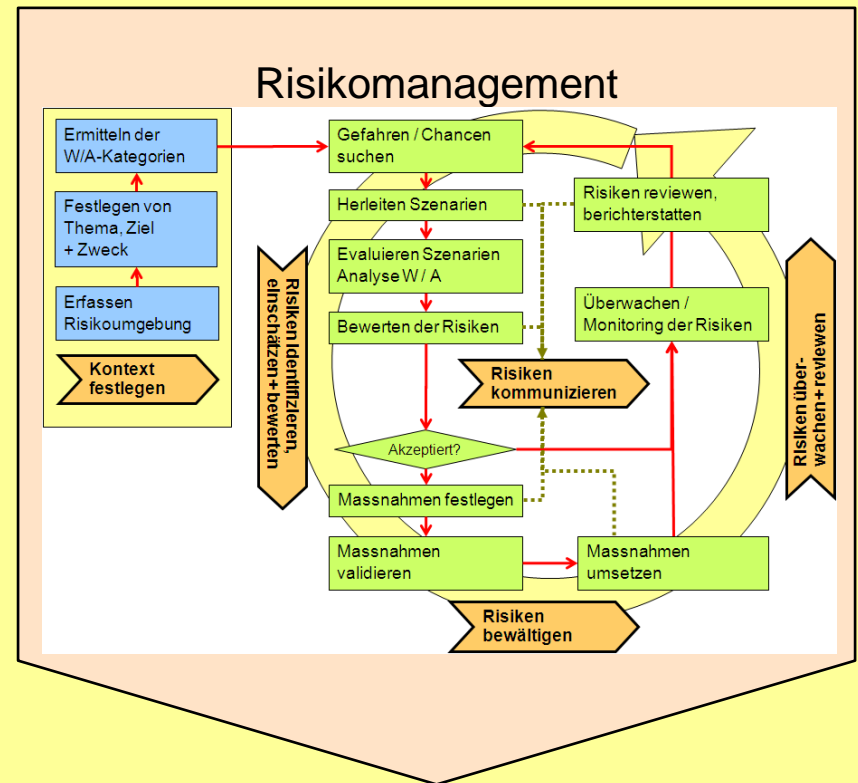
- 1 Es gibt Performance-Ziele für das Risikomanagement, welche publiziert werden**
- 2 Es gibt eine vollständige und akzeptierte / benutzte Risikobuchhaltung**
- 3 Es gibt keine Entscheidungsfindung ohne Risikobetrachtung**
- 4 Es gibt eine kontinuierliche Kommunikation / Risikoreporting mit internen und externen Stakeholdern**
- 5 Governance und Struktur der Firma basieren auf dem Risikomanagement.
Risikomanagement wird von den Managern als essentiell für die Zielerreichung betrachtet und als „Management der Unsicherheit“ wahrgenommen**

- ISO 31000 ist seit Oktober 2009 in Kraft.
- ISO 31000 ist nicht eine Zertifizierungsnorm, sondern eine Guideline.
- ISO 31000 will **nicht** ein neues, zusätzliches Managementsystem (neben ISO 9001, ISO 14001, OHSAS 18001,) werden. ISO 31000 zeigt wie das betriebliche Risikomanagement in das bestehende Managementsystem eingebaut werden kann! (Prozessebene)
- Eine Zertifizierung erfolgt wenn überhaupt, dann im Rahmen bestehender Zertifizierungen
- Dank ISO 31000 wird RM in die normalen Geschäftsabläufe integriert. Damit kann auch neuen Anforderungen (seitens Gesetzgebung oder bestimmten Normen) Rechnung getragen werden. (IKS, OR 663b, ...)

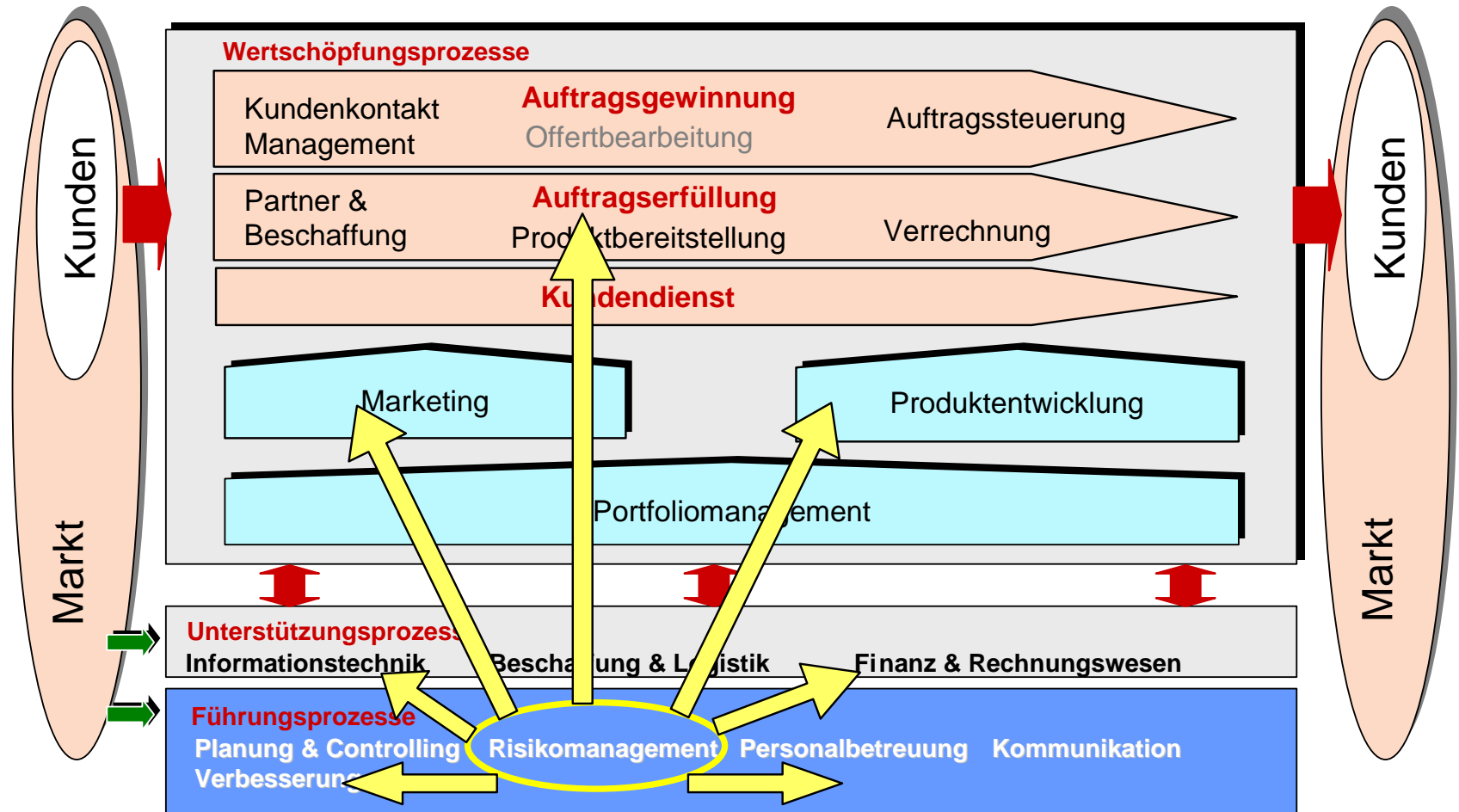
1. Ein Management-Umfeld haben, welches systematisches Management auch für Risiken ermöglicht (zB. MS ISO 9001)
2. Den Risikomanagement-Prozess in die Führung einbauen



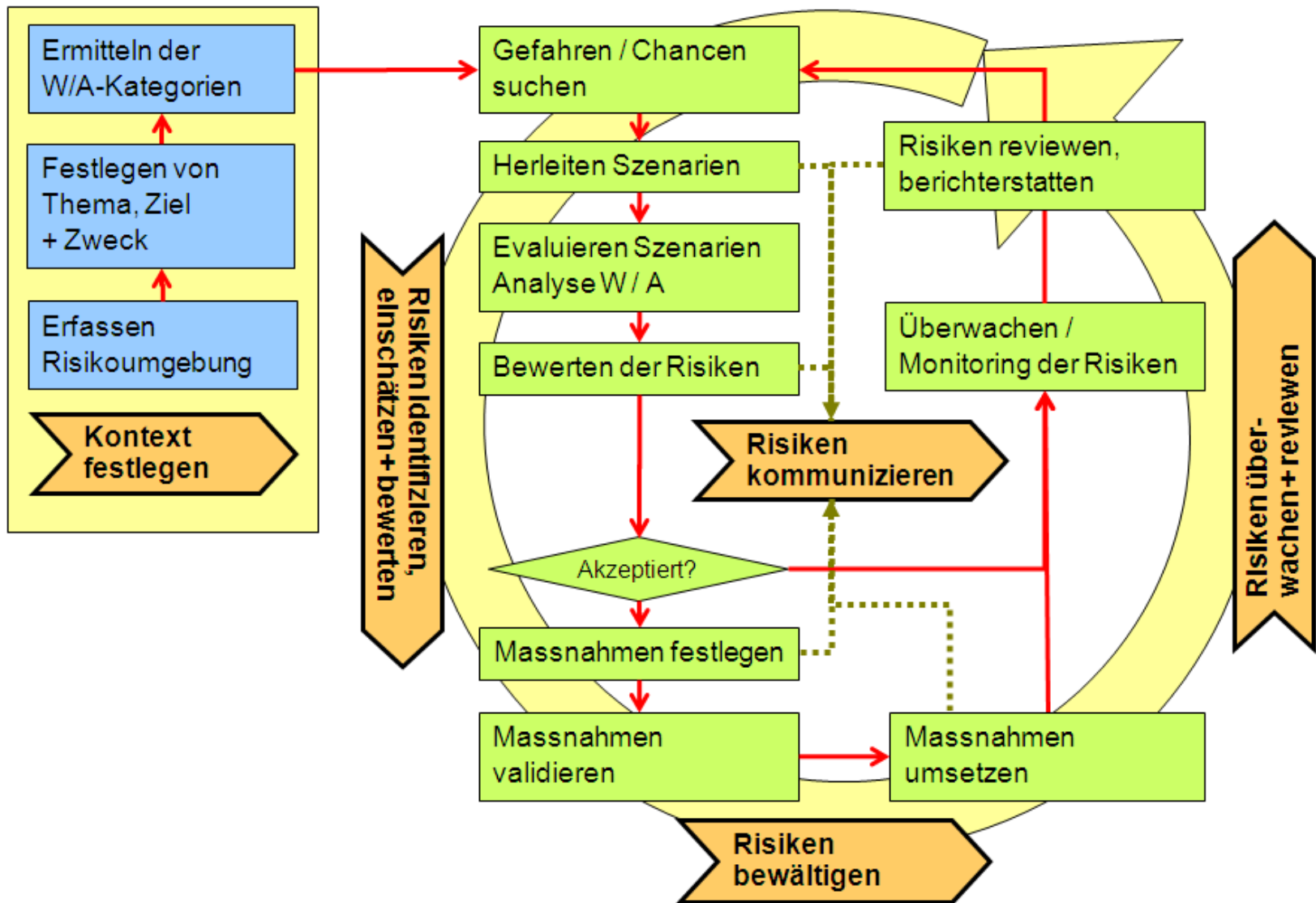
Führungsprozesse

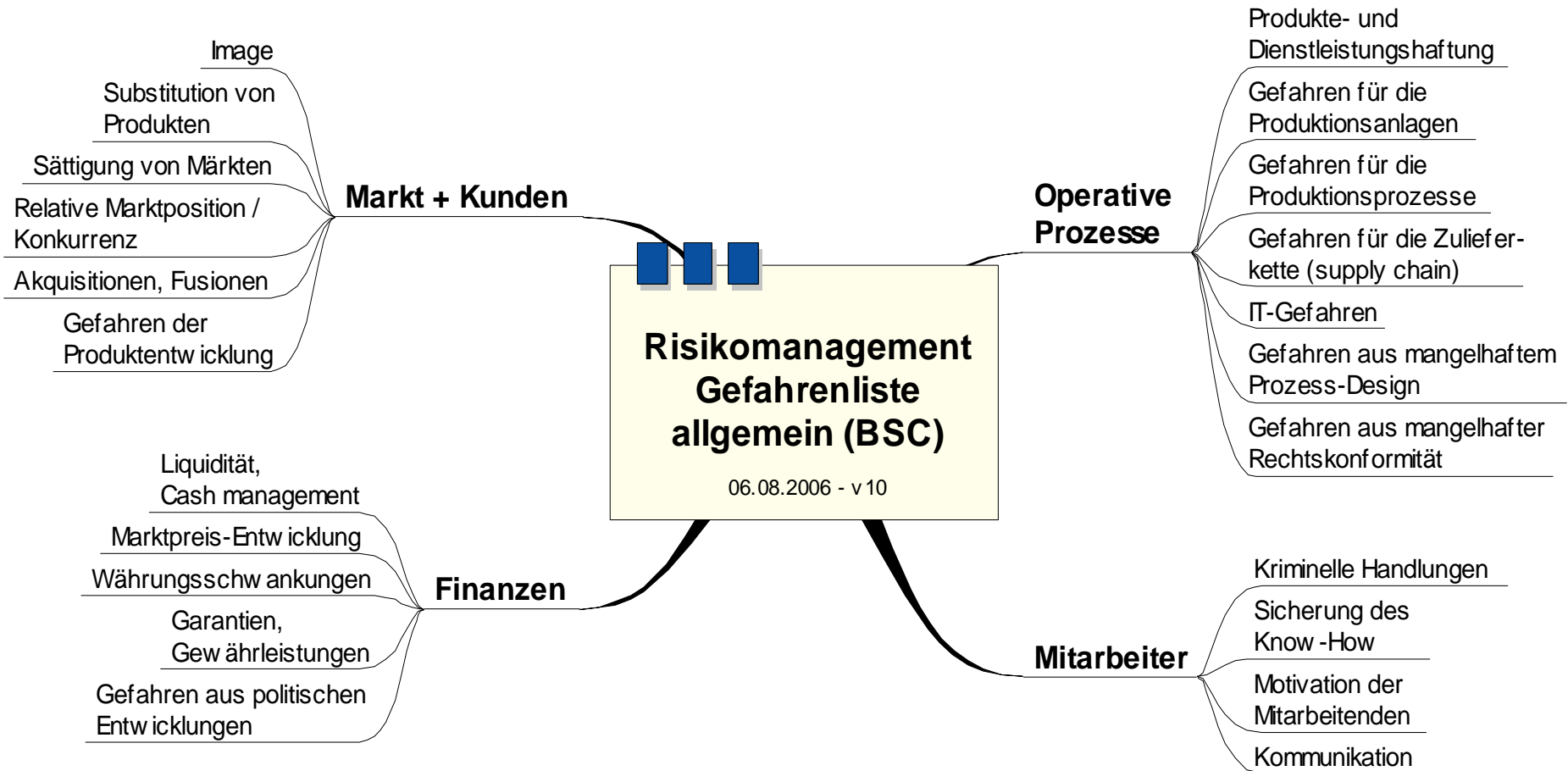


3. Den Risikomanagement-Prozess auf die nötigen anderen Prozesse anwenden



Im Detail: Darstellung Risikomanagement-Prozess





GEFAHREN BESCHAFFUNG

1/2

Ungenügende Liefersicherheit

- Bei Lieferausfall steht zeitgerecht kein Ersatzlieferant zur Verfügung. Es drohen Produktionsausfälle
- Die Pufferkapazität des Lagers ist der Liefersicherheit nicht angepasst (zu gross oder zu klein)
- Es fehlen vertragliche Liefergarantien seitens des Lieferanten
- Es fehlen Pufferlager auf der Seite des Lieferanten
- Es bestehen spezielle Importrisiken (Ausfuhr- / Einfuhrgenehmigungen etc.)
- Es bestehen spezielle Transportrisiken

Ungenügende Lieferantenwahl / ungenügende Kenntnis des Lieferanten. Inakzeptable Produktionsbedingungen beim Lieferanten

- Der Lieferant ist wenig solvent und kann vertraglich festgelegte Sanktionen gar nicht tragen
- Der Lieferant ist nicht liefersicher und/oder liefert stark schwankende Qualitäten
- Der Lieferant ist unbeständig und könnte die Produktlieferung plötzlich unterbrechen
- Der Lieferant ist zu teuer. Es gäbe günstigere gleichwertige Alternativen
- Der Lieferant ist nicht termintreu
- Der Lieferant wendet ökologisch unakzeptable Produktionsverfahren an
- Der Lieferant produziert unter sozial inakzeptablen Produktionsbedingungen (insb. Schwellen- und Entwicklungsländer)

Ungenügende Beschaffungsspezifikationen

- Sicherheitsrelevante Eigenschaften des beschafften Produkts sind zuwenig explizit gefordert
- Qualitätsrelevante Eigenschaften des beschafften Produkts sind zuwenig explizit gefordert
- Die Spezifikationen erwähnen "Selbstverständliches" nicht, das im Umfeld des Lieferanten u.U. nicht selbstverständlich ist.
- Es fehlt eine Analyse des Produkts, welche die sicherheits- und qualitätsrelevanten Forderungen an die Teile klar ermittelt (zB. Lieferkonditionen und Preise sind zuwenig genau spezifiziert
- Die Spezifikationen sind zu umfassend und verteuern das Produkt unnötig

Instrument: Das W-A – Diagramm

Roter Bereich:
Inakzeptable Risiken

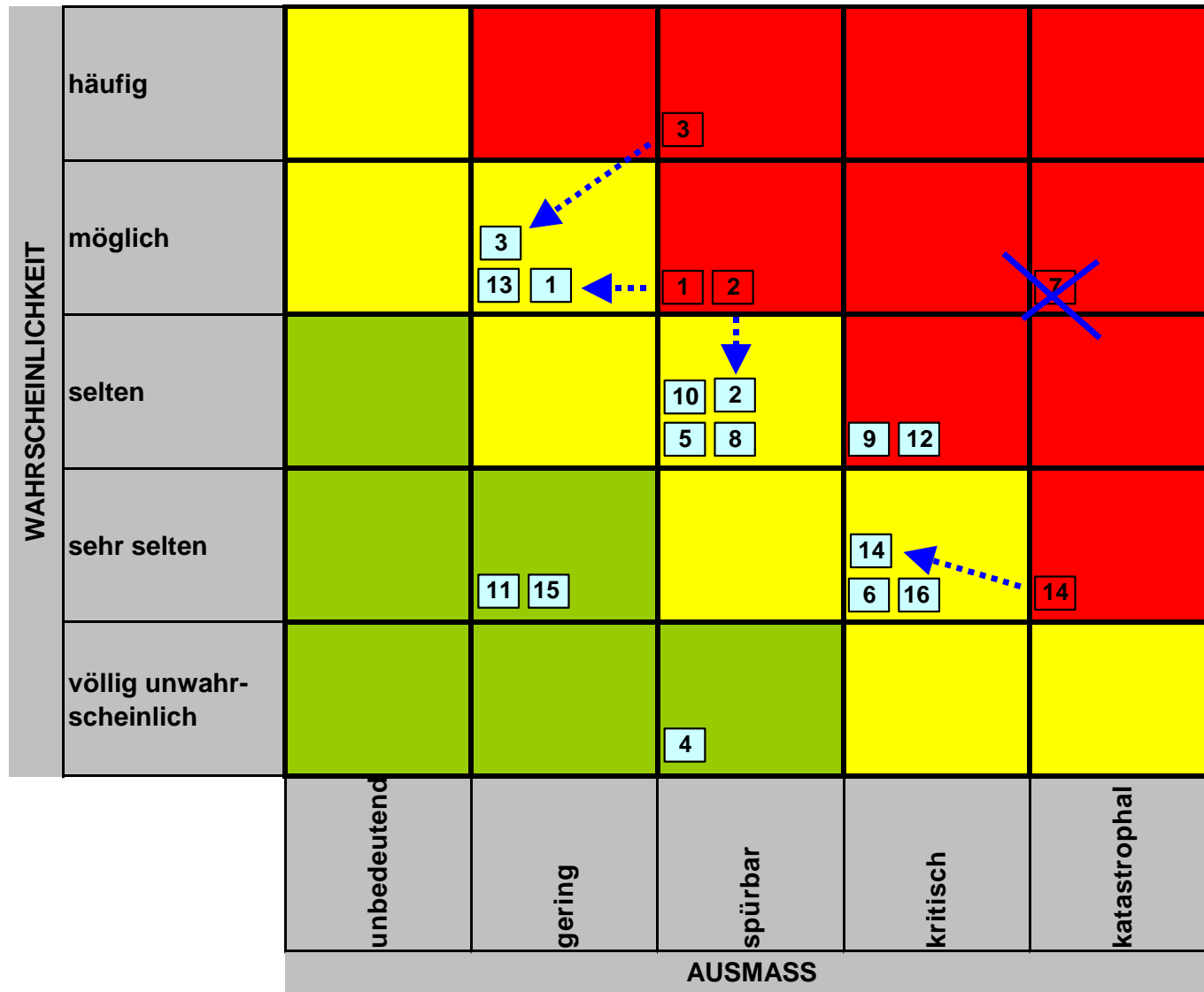
Gelber Bereich:
Bedingt akzeptable
Risiken

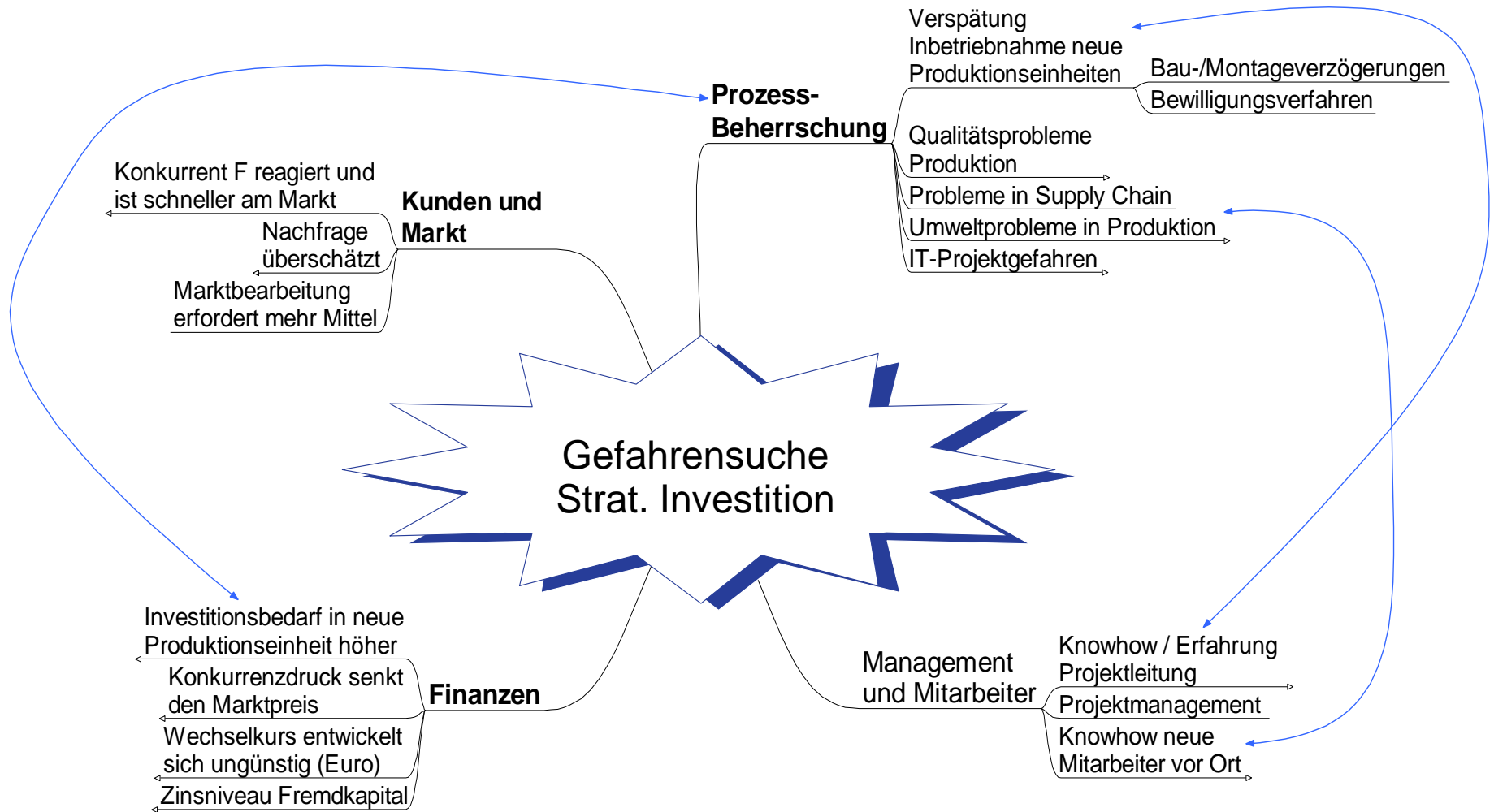
Grüner Bereich:
Akzeptable Risiken

WAHRSCHEINLICHKEIT	häufig			3		
	möglich		13	1 2		7
	selten			10 5 8	9 12	
	sehr selten		11 15		6 16	14
	völlig unwahrscheinlich			4		
		unbedeutend	gering	spürbar	kritisch	katastrophal
		AUSMASS				

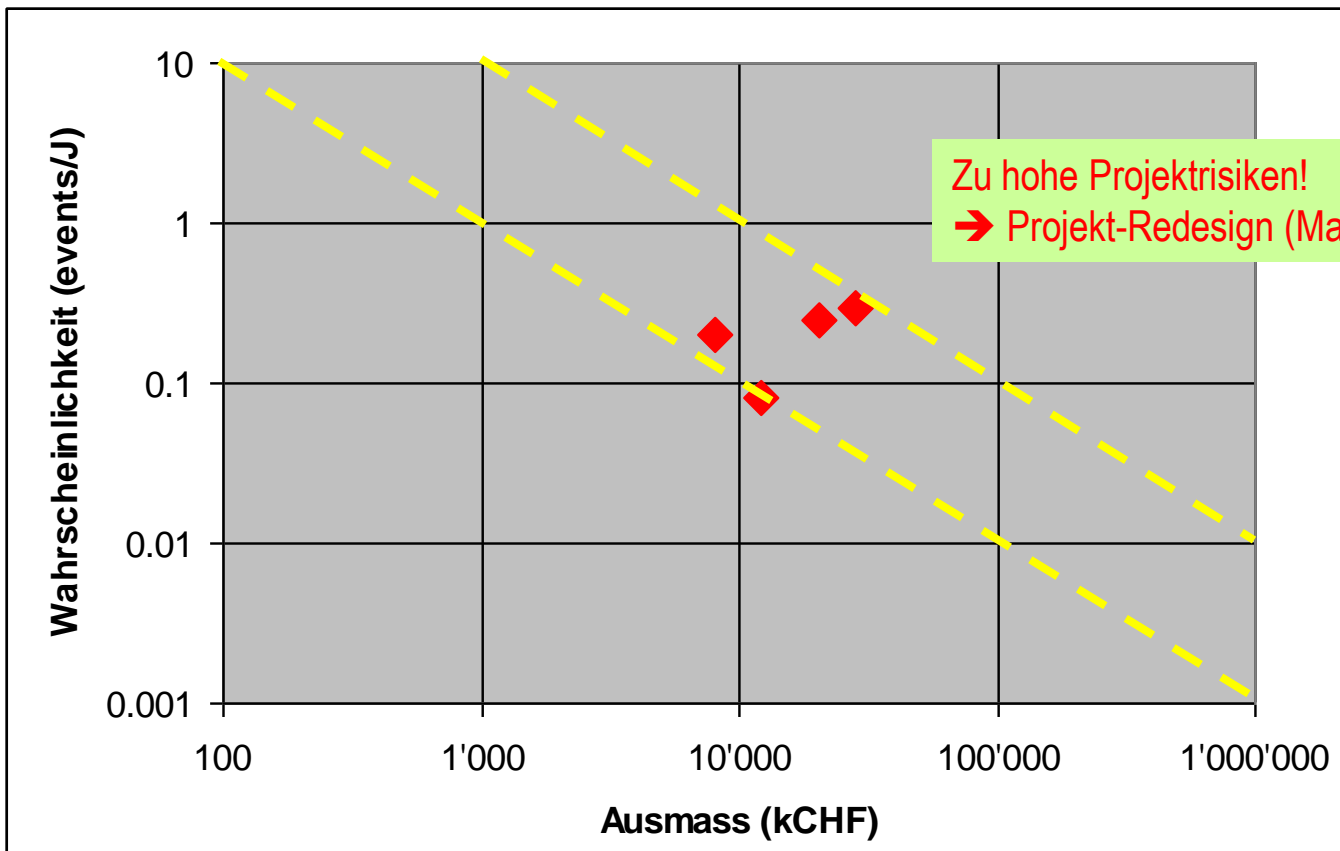
Thema				Szenario Nr.	9
Finanz bezogene Prozesse: Wertberichtigung Produktion / Lager					
Szenario					
Aufgrund von Veränderungen am Markt verlieren bestimmte Anlagen oder Lagerbestände an Wert. Sie müssen in der Bilanz wertberichtigt werden, unter Inkaufnahme ausserordentlicher Abschreibungen.					
Abschätzung im IST-Zustand				W-Klasse	selten
Die Produktionsanlagen sind mit CHF 22.5 Mio in der Bilanz. Dazu kommen CHF 5.8 Mio Rohwaren-Lagerbestände und CHF 1.5 Mio Fertigwaren. In einem schlimmen aber möglichen Fall würde der Zusammenbruch der Nachfrage nach Produktreihe HS Entwertungen der Lagerbestände von ca. CHF 3.5 Mio verursachen. Die Produktionsanlagen wären auf andere Produkte umrüstbar, es wäre aber mit Kosten zu rechnen. W-Klasse: 0.1/J; A-Klasse: 5 Mio CHF				A-Klasse	kritisch
				Risikoklasse	500'000 CHF/J
Synergien					
Querverbindung zu anderen Szenarien				Behandlung	
==> Operative Prozesse: Lagerbewirtschaftung: Lager tief fahren bringt Gefahren betreffend Liefersicherheit!				Parallel behandeln. Güterabwägung	
Massnahmen					
Massnahme	Status	Termin	Verantwortlich	IST-Zustand	
Projekt "Optimale Lagerbewirtschaftung"	bestehend	30.11.2007	abcde	gestartet 1.4.2007	
Abschätzung im SOLL-Zustand (nach Massnahmen)				W-Klasse	selten
„Szenario-Fiche“				A-Klasse	spürbar
				Risikoklasse	50'000 CHF/J

Im Detail: Tool Risikomonitoring im W-A - Diagramm









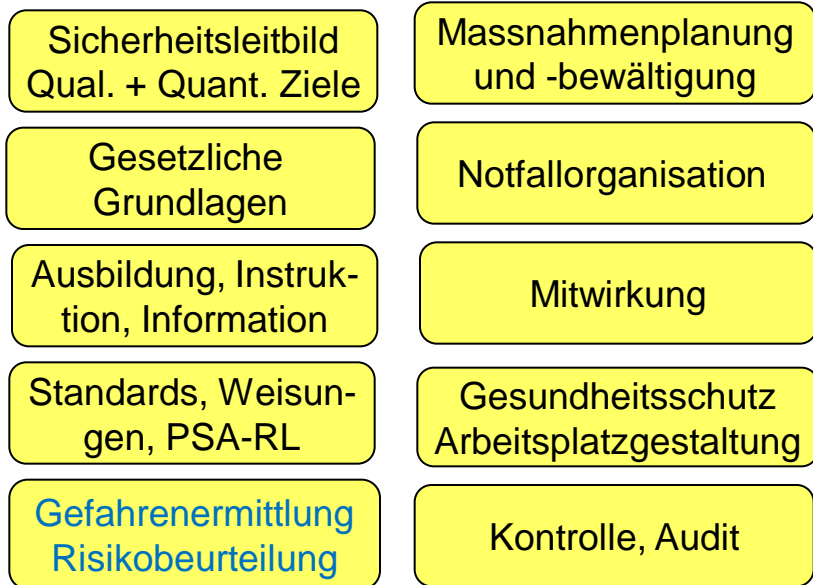
Nr	Beschrieb	Auswirkung	WK (events/J)	Risikokosten
1	Investitionsbedarf bis zu 20% höher	28'000	0.3	8'400
2	Bauverzögerung um 6 Mt	20'250	0.25	5'063
3	Nachfrage überschätzt (bis -20%)	8'100	0.2	1'620
4	Konkurrenzdruck senkt Marktpreis (bis -30%)	12'150	0.08	972
5	Euroschwankung	0	0	0

Gemeinsamkeiten und Bezüge: ‚Andockstellen‘ bei ISO 9001 / 14001 / OHSAS

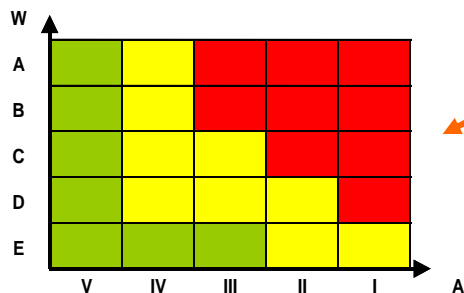
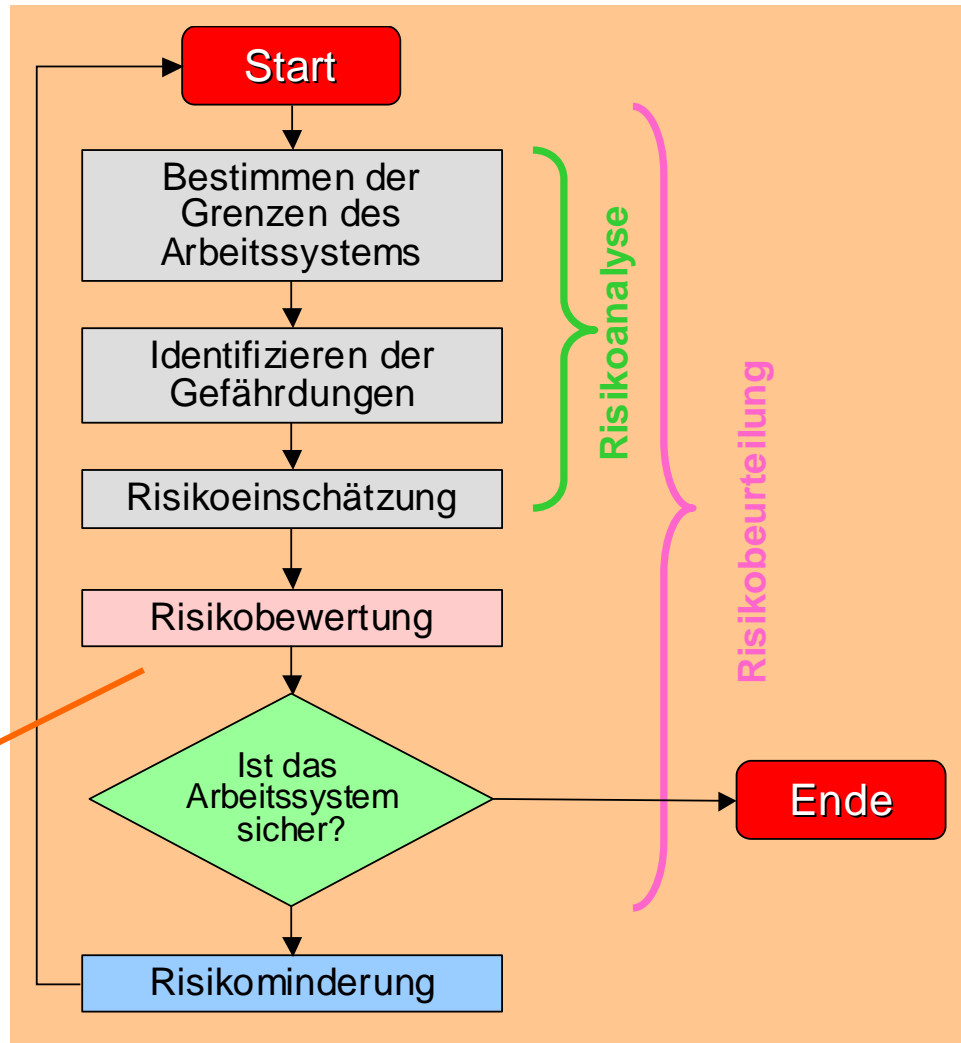
ISO 31000	ISO 9001	ISO 14001 / OHSAS 18001
4.2 Mandate and commitment		
Riskmanagement-Politik haben	Q-Politik haben	U / S Politik haben
RM-Politik auf die Firmenkultur abstimmen	Q Politik auf die Relevanz abstimmen	U / S Politik auf die Relevanz abstimmen
Passende RM-Performance-Indikatoren haben	Q-Indikatoren und Prozessmessgrössen haben	U / S Indikatoren haben
Passende RM-Ziele haben	Q-Ziele haben	U / S Ziele haben
Legal Compliance sicherstellen		Legal Compliance sicherstellen
RM Verantwortlichkeiten und -Kompetenzen zuweisen	Q Verantwortlichkeiten und -Kompetenzen zuweisen	U/S Verantwortlichkeiten und -Kompetenzen zuweisen
Ressourcenbereitstellung gewährleisten	Ressourcenbereitstellung gewährleisten	Ressourcenbereitstellung gewährleisten
4.3 Design of framework for managing risk		
4.3.1. Die Organisation und ihr Umfeld verstehen	Die Kundenbedürfnisse verstehen	Die Umweltrelevanz / AS-Risiken verstehen
4.3.2. Fordeurngen an die RM-Politik	Fordeurngen an die Q-Politik	Fordeurngen an die U/S-Politik
4.3.3. Verantwortliche Risiko-Eigner identifizieren		
Einen Verantwortlichen für die Entwicklung RM haben	Einen Q-Systemleiter haben	Einen U-Systemleiter haben
4.3.4. RM soll in die Unternehmensprozesse eingebettet sein	Prozesslenkung / Ablauflenkung	Prozesslenkung / Ablauflenkung
4.3.5. Angemessene Ressourcen haben (Leute, Methoden,	Angemessene Ressourcen haben	Angemessene Ressourcen haben
4.3.6. Interne Kommunikation und Reporting	Interne Kommunikation	Interne Kommunikation / Mitwirkung
4.3.7. Externe Kommunikation (Stakeholder)	Externe Kommunikation (Kunden)	Externe Kommunikation (Stakeholder)
4.4 Implementing risk management		
4.3.1. Den Management-Rahmen für RM in Gang setzen	!	!
4.3.2. Dem RM-Prozess implementieren	!	!
4.5 Monitoring and review of the framework		
Messen von Daten und Indikatoren	Überwachung und Messung	Überwachung und Messung
Periodische Prüfungen, ob Bedingungen ok.	Internes Audit	Internes Audit
Review der Risikosituation und der Wirksamkeit RMS	Management Review	Management Review
4.6 Continual improvement of the framework		
Kontinuierliche Verbesserung des RM-Rahmens	Kontinuierliche Verbesserung Q	Kontinuierliche Verbesserung U

Gemeinsamkeiten und Bezüge: EKAS/OHSAS ist ISO 31000 bezogen auf AS

EKAS-System

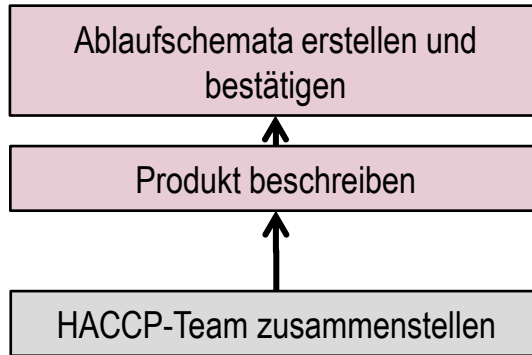


Prozess

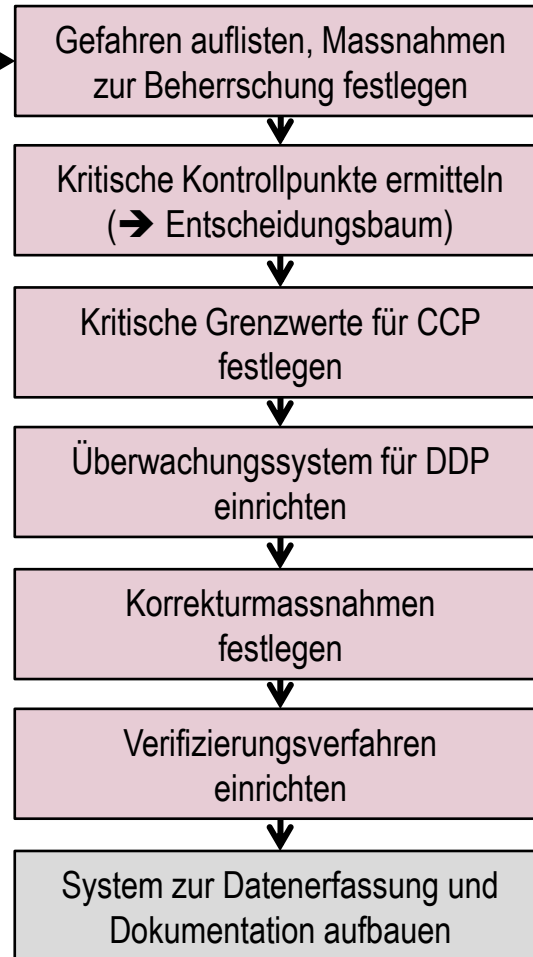


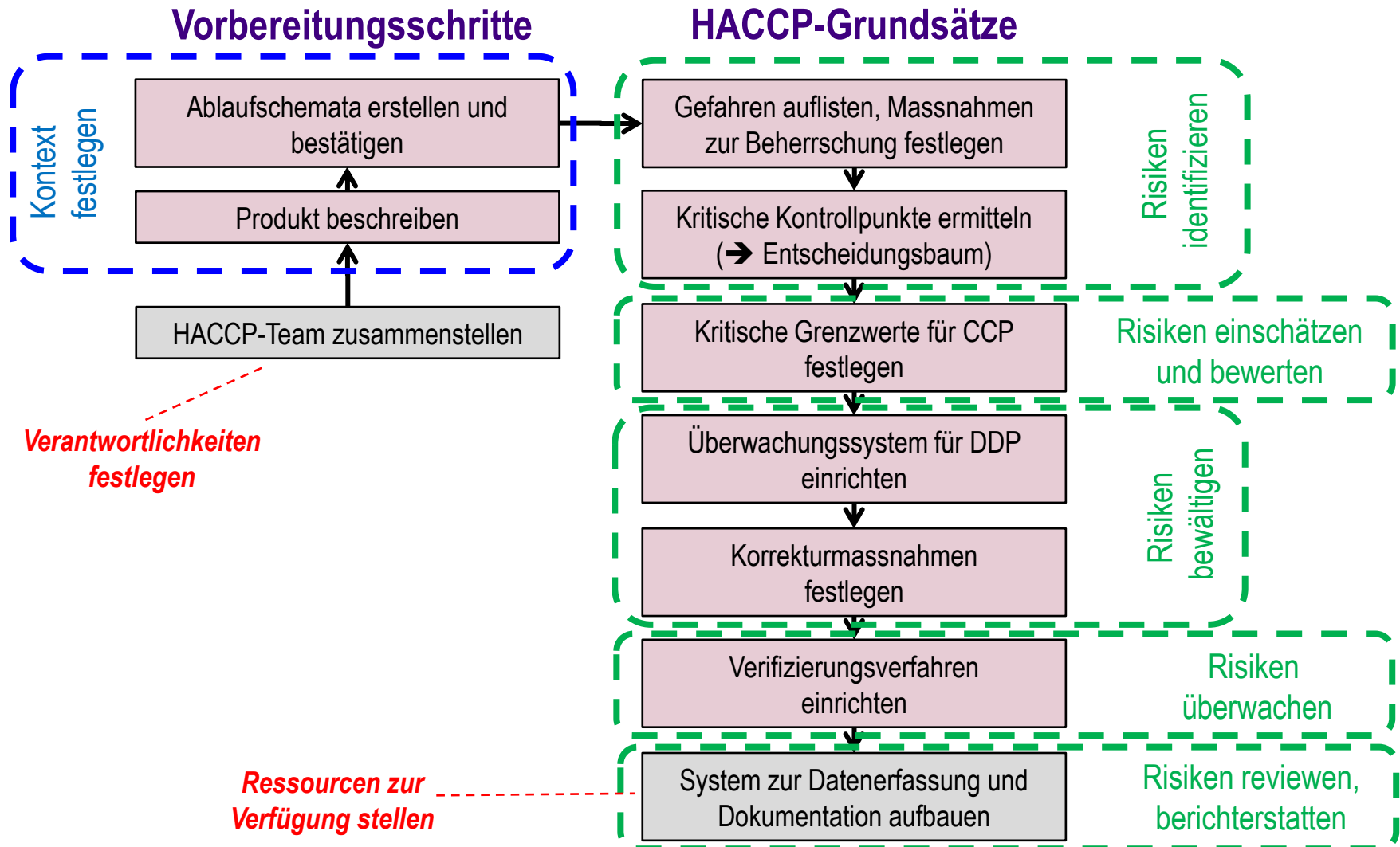
Gemeinsamkeiten und Bezüge: HACCP:

Vorbereitungsschritte

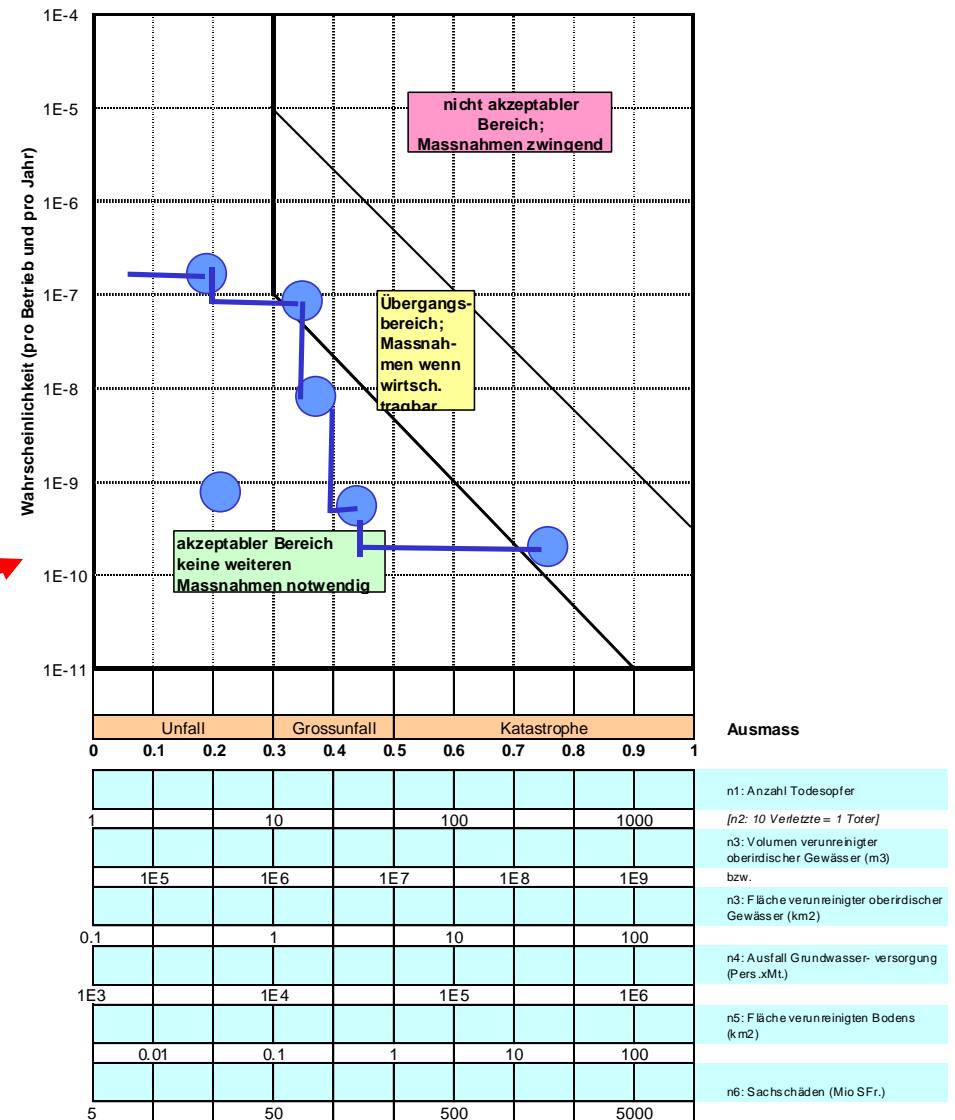
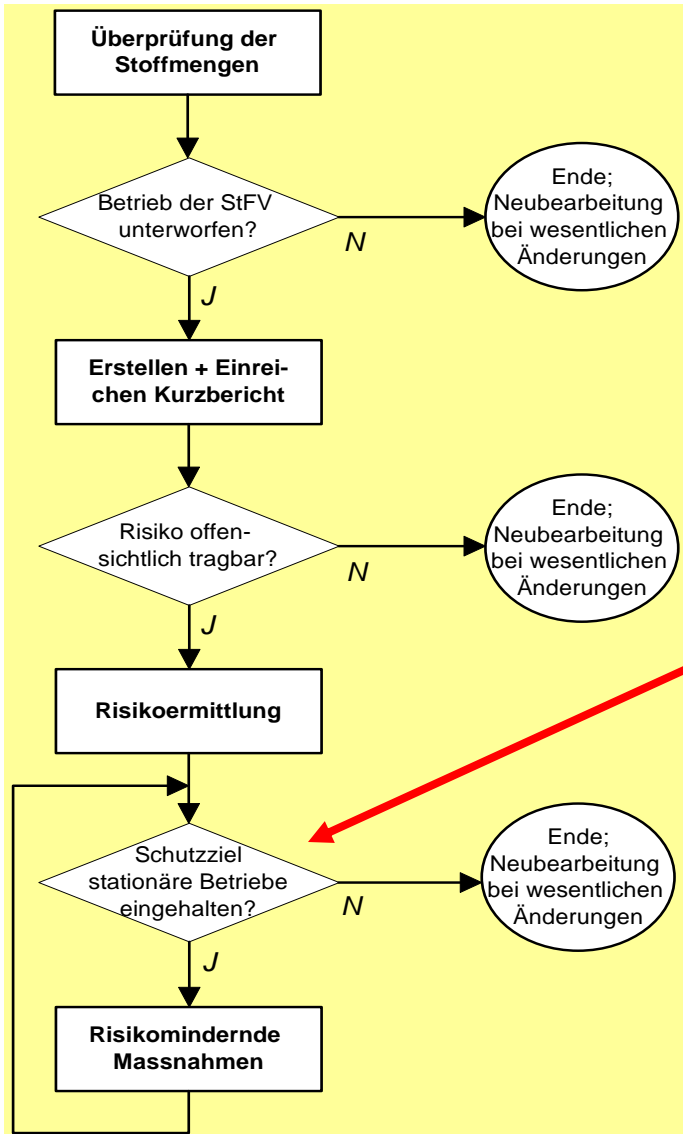


HACCP-Grundsätze



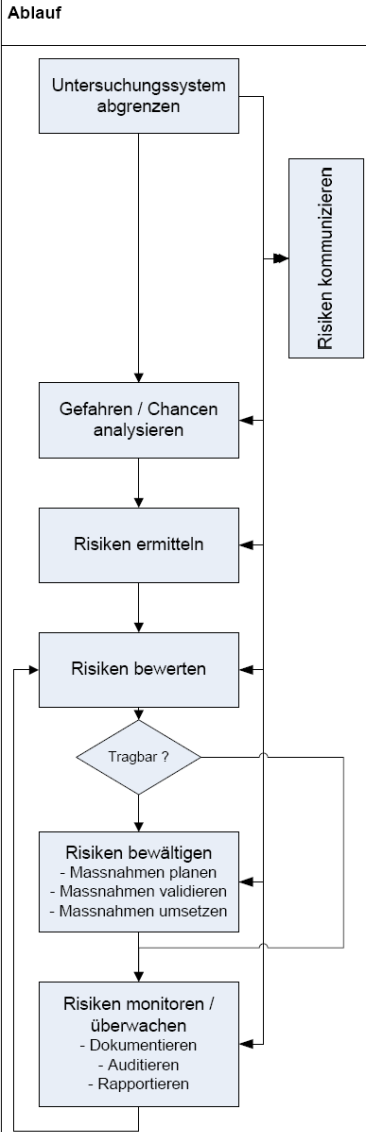


Gemeinsamkeiten und Bezüge: Störfallschutz ist auch eine ISO 31000-Anwendung



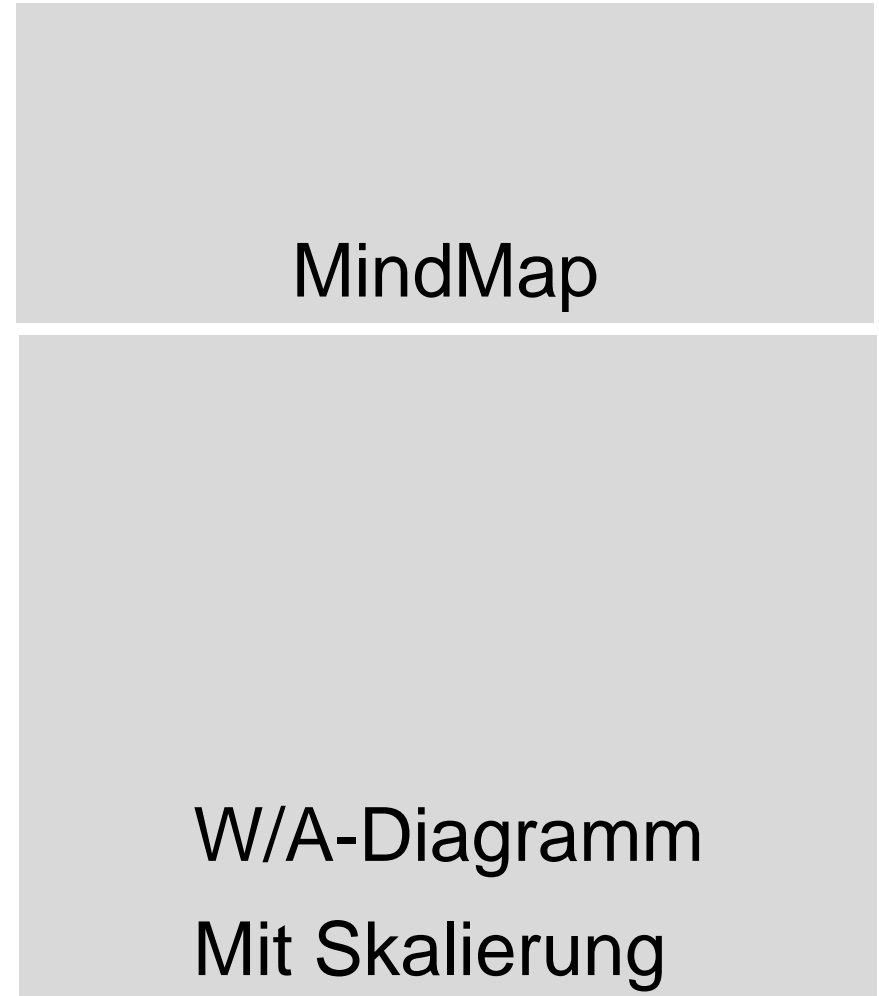
ISO 31000 Einführungsbeispiel KMU: Einführung RM-Prozess

- Es gibt einen neuen Führungsprozess im MS (ISO 9001 zertifiziert)
- Die Art der Prozessbeschreibung wird vom MS übernommen

Ablauf	Merkpunkte	Grundlage	Verantwortlich	Input Output
 <pre> graph TD A[Untersuchungssystem abgrenzen] --> B[Gefahren / Chancen analysieren] B --> C[Risiken ermitteln] C --> D[Risiken bewerten] D --> E{Tragbar?} E --> F[Risiken bewältigen] F --> G[Risiken monitorieren / überwachen] G --> A G --> D G --> H[Risiken kommunizieren] H --> B H --> C H --> D H --> E H --> F H --> G </pre>	<ul style="list-style-type: none"> - Gegenstand und Ziel der RA definieren - Skalenbereiche für Häufigkeit + Wirkung festlegen - Einflussbereiche / Risikoumgebung festhalten 		Risikoeigner	<ul style="list-style-type: none"> ► RM-Bedarf, Anlass, Ereignis Perimeter, W/A-Skalen ►
	<ul style="list-style-type: none"> - Stufengerecht - Systematisch 	Kommunikationskonzept, AW 25-100	Risikoeigner	Informationen am Ziel ►
	<ul style="list-style-type: none"> - MindMap-Darstellungen nutzen. Gefahren / Chancen dokumentieren 	FO 27-202.X	Risikoeigner	
	<ul style="list-style-type: none"> - Wahrscheinlichkeit bzw. Häufigkeit und Wirkung grössenordnungsmässig einschätzen 		Risikoeigner	
	<ul style="list-style-type: none"> - W/A-Diagramm mit Bereichen (grün, gelb, rot) benutzen - Risiken dokumentieren 	AW 27-201 FO 27-203	Risikoeigner	Risikoportfolio ►
	<ul style="list-style-type: none"> - Massnahmenplanung im IQ-Soft dokumentieren 		Risikoeigner	
	<ul style="list-style-type: none"> - Risikoportfolios benutzen und aktualisieren 	FO 27-203	Risikoeigner	<ul style="list-style-type: none"> Risikoportfolio rev. ► Auditberichte ► Risikoreportings ►

- Risikoeigner sind definiert
- Verantwortlicher RM ist definiert
- Risiko-Reporting ist festgelegt (Jahresbericht = Risiko-Management-review)
- Prozesse, auf welche RM systematisch anzuwenden ist, sind definiert:
 - Policy Deployment
 - Projektmanagement bei Projekten mit > 100 kCHF Kostenwirkung
 - Produktentwicklung bei Projekten mit > 10kCHF Kostenwirkung
 - Beschaffung bei kritischen Materialien
 - Umweltplanung
 - Lebensmittelsicherheit
- Kommunikationskonzept wurde angepasst
- Systemdokumentation wurde überarbeitet, so dass alle neuen RM-bezogenen Festlegungen darin aufgenommen sind

- Risikoidentifikation mit MindMap
- Risikoeinschätzung und –bewertung mit W/A-Diagramm
- Massnahmenplanung für die nächste Planungsperiode
- Aufaktualisierung / Review jährlich im Frühling



**Kommentar,
Massnahmen**

- ISO 31000 sagt, wie man Risikomanagement in ein MS integrieren soll.
- In einigen speziellen Fällen (Arbeitssicherheit, Lebensmittel, Medizinalgeräte, ...) gab es vorher schon Normen, die das sektorspezifisch geregelt haben.
Mit diesen ist ISO 31000 nicht im Widerspruch. Vielmehr ist ISO 31000 eine Verallgemeinerung davon für beliebige Risikoarten.
- ISO 31000 stellt weitgehend analoge Forderungen zu ISO 9/14 etc. – bezogen auf allgemeines Risikomanagement.
- Eine Zertifizierung von ISO 31000 ist nicht nötig / sinnvoll. Das Zertifikat hat seinen Platz bei der Anwendung auf ein konkretes Gebiet (zB. OHSAS, ISO 27000, ISO 14971, ...)

NB.: Wenn das Risikomanagement nicht bis ins Management vordringt ...

Die Ereignisse der jüngsten Finanzkrise haben schier unglaubliche Fehlleistungen im Risikomanagement von Finanzinstituten aufgedeckt. Dabei lag das Versagen weniger in der Analyse, sondern in der mangelnden Bereitschaft, Erkenntnisse über Risiken umzusetzen (Management).



Danke für Ihre Aufmerksamkeit !