GRUNDLEGENDES ZUR VERFAHRENS- UND COMPLIANCE DOKUMENTATION V

Governance Dokumentation

S. Mack

Vorbemerkung
Zunächst soll der Begriff der Governance pragmatisch auf ein engeres Bedeutungsfeld eingeschränkt werden. Hierfür werden einige, zum Teil widersprüchliche Wikipedia-Zitate herangezogen.

Z1: *Governance*, aus dem französischen *gouverner*, „verwalten, leiten, erziehen“, abgeleitet, wird oft als Regierungs-, Amts- bzw. Unternehmensführung –, auch Lenkungsform, bezeichnet. Hierbei wird allgemein das Steuerungs- und Kontrollsystem im Sinn von Strukturen (Aufbau- und Ablauforganisation) einer politisch-gesellschaftlichen Einheit wie Staat, Verwaltung, Gemeinde, privater oder öffentlicher Organisation. Governance wird auch im Sinne von Lenkung oder Führung einer jeglichen Organisation (etwa einer Gesellschaft oder eines Betriebes) benutzt.

Z2: Unter *Corporate Governance* versteht man die Kontroll- und Steuerungsstruktur innerhalb, gelegentlich – bezüglich rechtlicher Regelungen – auch außerhalb privatwirtschaftlicher Unternehmen. Governance bezieht sich ausschließlich auf Strukturen sowie institutionelle respektive prozessuale Elemente einer politischen oder gesellschaftlichen Einheit, wodurch deren Management unterstützt und verbessert werden soll.

Z3: *Corporate Governance* (deutsch: Grundsätze der Unternehmensführung) bezeichnet den Ordnungsrahmen für die Leitung und Überwachung von Unternehmen. Der Ordnungsrahmen wird durch Gesetzgeber und Eigentümer bestimmt. Die konkrete Ausgestaltung obliegt dem Aufsichtsrat und der Unternehmensführung. Das unternehmensspezifische Corporate Governance-System besteht aus der Gesamtheit relevanter Vorgaben. Dies relevante Gesetze, Richtlinien, Kodizes, Absichtserklärungen, Unternehmensleitbild, und Usus der Unternehmensleitung und -überwachung.
Zu beachtende Prinzipien: Accountability (Rechenschaftspflicht), Responsibility (Verantwortlichkeit) und Transparency (Offenheit und Transparenz von Strukturen bzw. Prozessen).

Im vorliegenden Text soll Governance als Kontroll- und Lenkungsinstanz verstanden werden, die die Gestalt des Unternehmens bestimmt; Corporate Governance ist hier nicht Gegenstand der Diskussion.

Die Kontroll- und Lenkungsinstanz der Governance soll nachfolgenden Governance Corpus **GC** bezeichnet werden.

Daten und Aufbewahrungspflicht

Um sich möglichst anschaulich und elementar an die Bedeutung des hier verwendeten Begriffs der Governance heranzuarbeiten, beginnen wir mit einem Rückblick auf Daten und Aufbewahrungspflichten, bzw. auf die Archivierung. Es liegt auf der Hand, zum Zweck der Dokumentation der Governance die Daten als Ausgangspunkt zu wählen, sie stellen schließlich das wichtigste und einzige Mittel der abstrakten Repräsentation der Situation eines Unternehmens dar. Unter Daten sollen Datenobjekte aller Art verstanden werden, gleich ob digital oder auf Papier, Mikrofilm oder sonstigen Medien aufgebracht.

Daten werden erzeugt, verarbeitet, gespeichert und schließlich irgendwann vernichtet. Mit anderen Worten: Es gibt Prozesse der Entstehung, Verarbeitung und Speicherung. Unter Verarbeitung sollen hier alle möglichen speziellen Formen wie Übertragung, Zusammenführung, Zusammenfassung, Referenzierung usw. verstanden werden. Die Archivierung bzw. zuverlässige Vorhaltung wird als Spezialfall der Speicherung betrachtet, im Sinne des Life Cycle Management (ILM), der letzten Phase vor der Vernichtung oder das Ende des Lebenszyklus.

Die Forderungen an die langfristige Datenvorhaltung werden durch die gesetzlichen Aufbewahrungspflichten geregelt und um unternehmensspezifische Bedürfnisse ergänzt. Für Datenobjekte gibt es zahlreiche Attribute wie Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit, Datenschutzwürdigkeit (personenbezogen), Aufbewahrungszeit und andere mehr, die teilweise Kriteriencharakter haben wie z.B. „unterliegt IKS-Kontrolle“. Mit Hilfe dieser Attribute lässt sich eine umfassende Klassifizierung durchführen wie sie z.B. für das Life Cycle Management erforderlich ist.

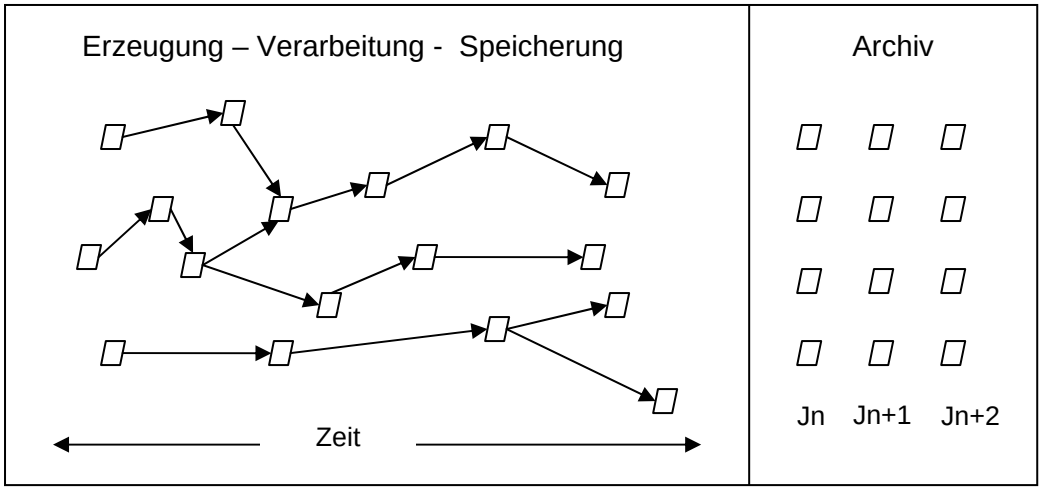

Abb. 1

Teilnehmerhierarchie

Betrachtet man den blau hinterlegten Abschnitt der unten stehenden Tabelle, erkennt man die in vielen Modellen verwendete Teilnehmerhierarchie. Die in den Feldern T1-T7 eingetragenen Klassennamen lassen sich von unten nach oben als Enabling-Hierarchie deuten; Ziel ist hierbei die Bestimmung der Governance-Objekte.

Verfügt man über eine Umgebung (Gelände, Gebäude, Raum, Schrank) lässt sich darin eine IT-Infrastruktur (passive Netzwerkelemente, technische Einrichtungen, Verkabelung

etc.) unterbringen. Mit dieser Infrastruktur werden Hardwareelemente (Server, Clienten und aktive Netzwerkelemente) verbunden. Ist die Hardware vorhanden, wird diese per Betriebssystem (oder Firmware) zum „Leben“ erweckt. Jetzt lassen sich Anwendungen installieren; sind diese installiert, können Personen können mit diesen Anwendungen interagieren. Bei diesen Interaktionen können Daten erzeugt, verarbeit und gespeichert werden. Die Klassen aus T1-T6 werden als Ressourcen bezeichnet.

Teilnehmer T1-T10		
10	**G**	overnance
9	**M**	anagement
8	**Pr**	ozess
7	**D**	aten
6	**Pe**	rson
5	**A**	nwendung
4	**B**	etriebssystem
3	**H**	ardware
2	**I**	infrastruktur
1	**U**	mgebung

Abb. 2

Dieser Aufbau deckt sich in etwa mit dem vom BSI definierten IT-Verbund. Versteht man die Beziehung der Punkte T8-T10 als „Beherrschung“, dann beherrscht die Governance das Management und das Management die Prozesse, und die Prozesse die darunter liegenden Daten und Ressourcen, wobei die „Beherrschung“ nach unten vererbbar ist. Hier ist zu beachten, dass die Klasse der Prozesse unter T8 die üblichen Geschäfts- und IT-Prozesse bezeichnet und für die Management und die Governance eigene Prozesse zur Anwendung kommen, die sich i. a. nicht mit den Geschäftsprozessen überschneiden. In einigen Modellen werden diese Prozesse unter einem gemeinsamen Dach „Geschäftsprozesse“ geführt.

Die Instanzen der Elemente in den Tabellenzeilen T1-T6 manifestieren sich als physische Objekte, die Daten T7 als abstrakte Objekte und in T8-T10 findet sich eine Hierarchie von Ereignissen. Hier zeigt sich die besondere Bedeutung der Daten als funktionales Bindeglied zwischen Ressourcen und Ereignissen; schließlich soll aus den aufbewahrten Daten im Rahmen einer Prüfung jeder Geschäftsvorfall rekonstruierbar sein. In diesem Zusammenhang soll angemerkt werden, dass zu den Daten, die von der Anwendung selbst erzeugt und bearbeitet werden, den inhärenten Aufzeichnungen, auch diejenigen zu zählen sind, die Daten **über** Ereignisse aufzeichnen wie z.B. Workflow- oder Monitoring-Anwendungen, die kohärente Ereignisaufzeichnungen erstellen.

Diese Betrachtung bringt vorläufig nichts neues, zeigt aber deutlich den „Durchgriff der Verantwortlichkeit“ im Rahmen der Governance bis auf die Daten und eventuell Personen, wie er von der Gesetzgebung verlangt wird. Wird Governance allgemein als Struktur des Steuerungsapparates definiert, soll hier der Begriff Kontroll- und Lenkungsapparat verwendet werden, um dem angelsächsischen Begriff „control“ besser einzudeutschen.

Regelkreis Governance

Hält man nach einem Modell Ausschau, die schon möglichst nah an die Darstellung des Wirkens der Governance herankommt und zur Dokumentation eignet, bietet sich der Regelkreis der klassischen Regelungstechnik zur Abbildung eines ähnlichen Kreislaufs an. Ziel ist hierbei nicht, eine „neues“ Modell zu konstruieren, sondern eine Darstellung, die es erlaubt, zu diskutierende Elemente anschaulich zu identifizieren. Die der nachfolgen-

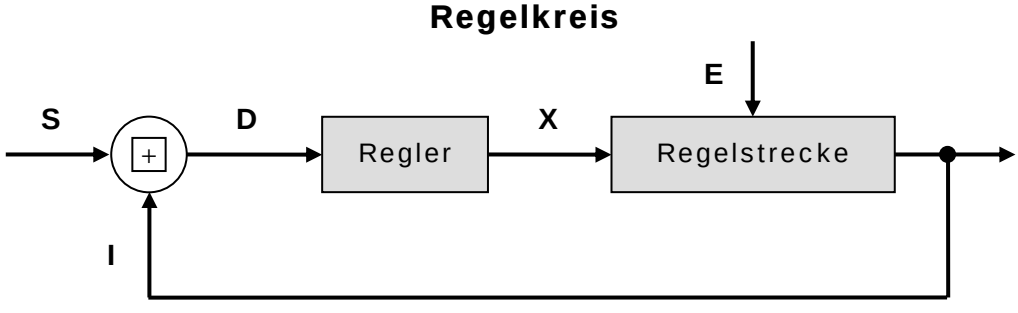

Abb. 3

den Abbildung zeigt das vereinfachte Blockschaltbild eines Regelkreises bestehend aus den Hauptteilen Regler und Regelstrecke.

Regler: Teil des Regelkreises, der aus der Regelabweichung die Ausregelkorrekturen umsetzt.
Regelstrecke: Teil des Regelkreises, der vom Regler ausgeregelt werden soll.
Führungsgröße oder Sollwert S: Vorgegebener Wert, auf dem die Regelgröße durch die Regelung gehalten werden soll. Sie wird von außen bestimmt und zugeführt.
Regelgröße oder Istwert I: Ausgangsgröße der Regelstrecke, die zum Zweck des Regelns erfasst und zum Vergleich rückgeführt wird.
Regelabweichung D: Differenz zwischen Führungsgröße und Regelgröße **D = S - I**, bildet die Eingangsgröße des Reglers.
Stellgröße X: Ausgangsgröße der Regeleinrichtung und Eingangsgröße der Strecke. Sie überträgt die steuernde Wirkung des Reglers auf die Strecke.
Störgröße E: Von außen wirkende Größe, die eine Änderung des Istwertes der Regelgröße bewirkt und einen Regelung auslöst.

Anpassung des Blockschaltbilds

Dieses Blockschaltbild muss nun angepasst werden. Die Instanzen aller Objekte erzeugt aus T1-T9 werden unter dem Begriff Governance-Objekte (GO) zusammengefasst.

S (**Sollwert)** werden als Zielvorgaben durch die Governance formuliert. Diese werden durch Zahlen, Handlungsvorschriften und Strukturmerkmale ausgedrückt und können alle GO betreffen.
I (**Istwert)** ist der Status der GO.
D (**Regelabweichung)** bestimmt die möglichen Änderungen, die ebenfalls alle Instanzen der GO können betreffen.
Management (Regler) setzt die Korrekturmaßnahmen in Veränderungen der Struktur, Ereignisse Anweisungen usw. um. Ausgenommen sind direkte Maßnahmen, die Veränderungen des Managementpersonals betreffen.
X (**Stellgröße)** ist die Menge der Änderungsmaßnahmen.
Unternehmen (**Regelstrecke)** sind die hier die GO des Unternehmens
E ist die Menge der Informationen über äußere Ereignisse, die eine Änderung der GO bewirken oder erzwingen wie Gesetze, Konkurrenz, Marktentwicklungen usw.
B steht für die Menge der internen Berichte, mit der Menge an Daten und Fakten über Abweichungen der GO von der Führungsgröße (Qualität, Effizienz, Kosten etc.).
GC steht für Governance Corpus (Aufsichtsrat, Unternehmensleitung und evtl. wechselnde externe und interne Mitarbeiter).

Das grobe Blockschaltbild der Governance verändert sich entsprechend:

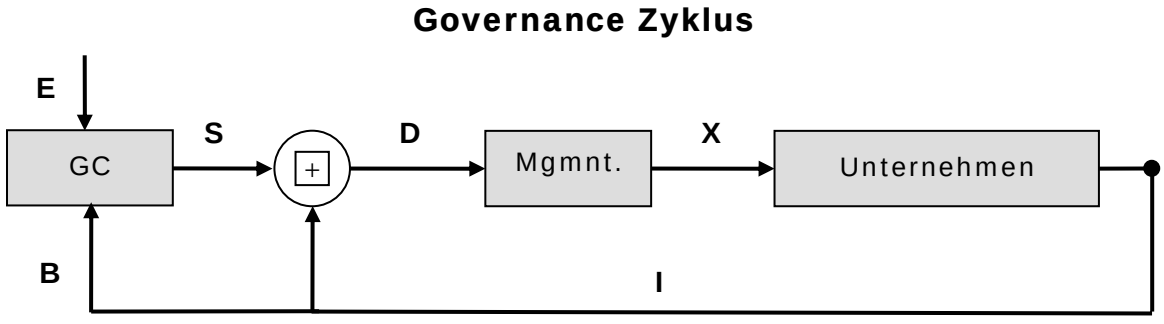

Abb. 4

Instrumente der Governance

Anhand der Pfeile und Kästen des CG-Blockschaltbildes können nun die für die Dokumentation relevanten Elemente diskutiert werden.

Informationsbeschaffung/-bereitstellung (Intelligence)

Voraussetzung für jegliche Aktivität des GC sind Informationen über äußere Ereignisse (**E**) und über den Status des Unternehmens und der Ereignisse im Unternehmen (**B**). Die Bereitstellung bzw. Beschaffung dieser Informationen erfolgt über Kanäle **IK(E)** und **IK(B**), die jetzt grob aufgefächert werden. Unternehmensspezifisch erfolgt eine feinere Auffächerung z.B.: Konkurrenz (Situation, Image, Patentverletzungen usw.), auf die hier nicht eingegangen werden soll.

IK(B)	IK(E)
Vorschlagswesen	Marktinformationen
IKS-Berichte, Audits	Konkurrenzinformationen
Rechnungswesen (Berichte / Auswertungen) Business Intelligence	Compliance Forderungen Gesetze wie AO, Datenschutz, Arbeitsschutz
Frühwarnberichte	Marketing Intelligence
Personalberichte	
Anonyme Hotline	
Kummerkasten	
…	…

Risikomanagement – Analyse & Entscheidung

Das zentrale Instrument der internen Informationsbeschaffung bildet das Interne Kontrollsystem. Für Aufbau und Funktion des Internen Kontrollsystems gibt es diverse Standards (z.B. COSO für ICS internal control system) oder Vorschläge nach den Stellungnahmen des IDW. Im Zusammenhang mit der CG soll hier nur die Überwachungs- und Berichtsfunktion des IKS betrachtet werden; von der Ausprägung der Kontrollen und anderen Funktionen des IKS wird hier abstrahiert. Wesentlich ist, dass alle IK(B) und IK(E) Kanäle einem Filter unterliegen, der im Bedarfsfalle die unmittelbare Einschleusung in das Risikomanagement auslöst. Die Betrachtungsweise des IKS hat sich in letzten Jahren deutlich in Richtung Risikomanagement verschoben, da dieses für die Analyse und Bearbeitung externer und interner Risiken zuständig ist. Der Risikobegriff umfasst neben externen Risiken damit auch interne Abweichungen von Norm und Zielvorgabe und kommt damit dem Bedrohungsbegriff immer näher und schließt damit auch die gesamte IT-Sicherheit ein. Das ERM (enterprise risk management nach COSO) schließt das frühere ICS (internal control system) als Untermenge ein. Bei der Bewertung positiver Berichte (z.B. Vorschlagswesen) wird das Risiko als Möglichkeit erklärt, evtl. eine Kostenminderung, Effizienzsteigerung, Produktidee usw. zu verpassen. Mit diesem Verständnis des Begriffs Risiko wird das Risikomanagement zum zentralen Instrument der Analyse und Bewertung der gewonnen Intelligence Information aus IK(B) und IK(E).

Nach der Entscheidungsvorbereitung durch das Risikomanagement wird durch die Entscheidungsvorgaben eine neue Soll-Gestalt bestimmt; Maßnahmen, die auf Grund der Entscheidungsvorbereitung getroffen werden, aber nichts mit einer Gestaltänderung zu tun haben, werden hier bei Seite gelassen.

Direktiven – Vorgaben des Generalstabs

In der Dokumentation des Geschäftsgeschehens nehmen Direktiven einen besonderen Platz ein. Unter Dokumentation wird im Kontext der rekonstruierbaren Geschäftsereignisse gemeinhin die Vereinigung von Aufzeichnungen und Beschreibungen verstanden. Die

Aufzeichnungen bestehen hierbei aus digitalen bzw. digitalisierten Objekten, aber die Beschreibungen sind intellektueller Natur, d.h. primär von Menschen gefertigt. Beschrieben werden die Objekte erzeugt aus T1-T9 und die Aufzeichnungen werden durch T7, die Daten repräsentiert. Damit sind alle Verfahrenselemente, Managementprozeduren, Ablauf- und Aufbauorganisation erfasst. Die Beschreibungen unterliegen der Historisierung nach Maßgabe der Veränderungen von T1-T9 und damit der Aufbewahrungspflicht.

Direktiven sind von Menschen gefertigte imperative Beschreibungen, die auf eine erwünschte Struktur von Sachen bzw. des Ablaufs von Ereignissen und/oder das Verhalten von Menschen abzielen. Sie werden vom GC oder dem Management oder externen Institutionen verfasst.
Typische Beispiele für Verhaltensdirektiven sind: Governance Codex, Policies, Mission Statement, Verhaltensgrundsätze (code of conduct) etc. zusammengefasst unter „Corporate Behaviour“. Sie beschreiben die Art und Weise ab, wie Unternehmensziele erreicht werden sollen und mit welchem Verhaltensbild das Unternehmen in der Außenwelt erscheinen soll (nicht mit Corporate Image zu verwechseln).

Anweisungen für die Abwicklung von Prozessen, Verhalten im Notfall, Berichtspflichten usw. werden unter „interne Direktiven“ zusammengefasst; diese bedürfen der Klassifikation und richten sich an verschiedene Personengruppen.

Die zweite Klasse von Direktiven betrifft Veränderungen der inneren Struktur. Diese Strukturdirektiven (structural directives) werden als Ergebnis eines Governance-Prozesses (Risiko/IKS) vom Management umgesetzt und betreffen die Elemente T1-T9.

Dokumentation der Governance

Nachfolgend wird wie oben erläutert das IKS als Untermenge des Risikomanagements angesehen. Gemäß dem letzten Abschnitt stellen sich die Instrumente der CG wie folgt dar:

- Intelligence
- Risikomanagement
- Direktiven

Intelligence
Die Beschreibung der Intelligence beschränkt sich auf die tabellarische Auflistung der Elemente der Kanäle IK(B) und IK(E) evtl. mit einer zweistufigen Verfeinerung. Jedem Element wird ein Dokument zugeordnet, das den Owner, die Quelle sowie die Art und Weise der Beschaffung und Bereitstellung beschreibt. Eine weitere Verknüpfung verweist auf die zugeordnete Menge aller konkreten Fallberichte. Für einige Branchen verlangt der Gesetzgeber die Angabe von Informationsquellen und die Vorhaltung der Information.

Risikomanagement
Die Beschreibung der Funktion des Risikomanagements wird i. a. vom Lieferanten oder Systemintegrator einschließlich der Darstellung der Einzelfälle geliefert. Sollte dies nicht der Fall sein, empfiehlt sich die Anlage eines RM-Kalenders, in dem das Datum des Auftretens (Bericht) geführt wird, eine Identifikation des Risikos, der Owner, das Ende der Bearbeitung und ein Verweis auf ein Risikofall-Deckblatt. Ein Basisdokument sollte die Funktion des eigenen Risikomanagements beschreiben.

Internes Kontrollsystem
Für das IKS kann eine ähnliche Vorgehensweise gewählt werden, falls kein unterstützendes System zur Verfügung steht. In einer tabellarischen Übersicht werden die einzelnen IKS-Anwendunge bzw. -Projekte aufgeführt. Jeder Eintrag ist mit einem Dokument verknüpft, das eine Beschreibung und Klassifikation etwa nach folgender Vorlage enthält. In einem IKS-Kalender werden Einträge analog zum RM-Kalender geführt.

Sowohl der RM- als auch der IKS-Kalender (elektronisch) erlauben Planungseinträge für geplante Überprüfungen, die zum fraglichen Zeitpunkt eine Email an den Owner des Kalenders auslösen.

Direktiven
Getrennt nach strukturalen und behaviouralen Direktiven werden zwei Übersichten geführt, die auf die jeweiligen Dokumente verweisen. Der Aufbau evtl. mit Kalender entspricht den Übersichten unter Risikomanagement und IKS.

Schlussbemerkung

Die hier gewählte minimalistische Darstellung verwendet zahlreiche „black boxes“ wie Intelligence, Risikomanagement und IKS, in denen sich teilweise hochkomplexen Aufgabenstellungen verbergen. Dies rechtfertigt sich damit, dass für die Zwecke der Dokumentation nur interessant ist, was in die Box hineingeht und was „hinten herauskommt“.

Für interessierte Leser steht unter http://compliance-consult.eu eine kostenlose Web-Anwendung zur Verfügung, die, obgleich mit einem Inhaltsverzeichnis für die Erstellung der Verfahrensdokumentation nach dem PK-DML Standard versehen und primär für die Erstellung einer Verfahrensdokumentation ausgelegt, eine einfache Anpassung über eine MS-Excel-Datei an eine einfach überschaubare Dokumentation der Governance nach den geschilderten Konzepten erlaubt.

S. Mack
Dortmund, August 2011

Risiko-Objekt

Risikoidentifikation

Name
Risikofeld
Risikoklasse
Risiko-Owner (Person)

Wird bei IT-Risiken durch Auswahl gesetzt

IT-Risiko-Objekt

Objektauswahl für IT-Risiko

Geschäftsvorfall
Systemereignis
Prozess
IT-System
IT-Anwendung
Mitarbeiter
Abteilung

Risikobeschreibung

Tragweite

qualitative Beschreibung

Quantifizierung

Signifkanz & Wahrscheinlichkeit

Risikotoleranz/ Appetit

Gewinn-/ Verlustpotenzial mit Wahrscheinlichkeit & Wert

Kontrollinstrumente

RW-Listen und Auswertungen, Revision Analysen, lfnd. Informationsbeschaffung

Risikominderung

Maßnahmen und Empfehlungen

Risikobeurteilung

Gefahren und Möglichkeiten - Finanz. Auswirkungen

Einschätzung-GM: hoch > €

Wert

Eintrittswahrscheinlichkeit/-horizont

Gefahr/Chance: Gefahr

Wahrscheinlichkeit: sehr hoch >75%

Eintrittshorizont

Zahlenangabe mit M=Monate J=Jahre

Risikoanalyse - Methoden

Analyse-Methodik

Risikoprofil

Risiko-Owner(Abtlg.)
Projekt-Start: 25.10.2007
Projekt-Horizont: Monate
Projekt-Ende
R-Bedeutsamkeit: sehr hoch
Prim. R-Priorisierungstool
Prim. R-Kontrollinstrument
Investition R-Kontrolle: erhöhen

Risikobewertung

Mögliche Kosten
Mögliche Leistungen
Rechtliche Auflagen
sozio-ökonom. Faktoren
weitere Einflußfaktoren

Risikobehandlung (Art der Maßnahme)

Kontrolle
Eindämmung
Vermeidung
Transfer
Finanzierung

Kostenrentabilität

Durchführungskosten der Kontrollmaßnahme bezogen (/) auf Risikosenkungsnutzen

Rentabilität
Unterlassungsverlust
Entscheidung für Kontrolle: ja

Risikoberichterstattung

Vorstand: ja
Stakeholder: ja
Management: ja
Andere

Bei Projekt-Ende show auf ein setzen

show ☑

Klassifikations - und Dokumentations- Modell des IKS

Definition IKS: Das Interne Kontrollsystem (IKS) ist das Management-Werkzeug der unternehmensinternen betriebswirtschaftlichen Überwachung. Dieses Werkzeug wird in Form einer Fragestellung auf **Kontroll-Objekte** des Unternehmens angewandt; bei der Anwendung werden Kontroll-Ziele der **Zielfelder des IKS** verfolgt und als Ergebnis **IKS-Instrumente** geliefert. Das IKS wird auf das Unternehmen angewandt und selbst zu einem Kontroll-Objekt erklärt.

Instrumente: IKS-Instrumente werden einer der folgenden Kategorien zugeordnet**:**

D1 Grundsätze	Policies, Richtlinien; Vorkehrung
D2 Organisation	Aufbau: Organisationsplan/Vorkehrung
D3 Einrichtungen	Inst. tech. Elemente, Kontr./Vorkehrung
D4 Verfahren	Prozesse – Anweisungen - Kontrollen
D5 Massnahmen	Mgmnt. Gestaltungseingriff

IKS-Instrumente sind die Folge von Untersuchungen und Aktionen des IKS. Erst nach ihrer Installation werden Instrumente als **IKS-Anwendungen** in Form von Kontrollen, Vorkehrungen, Berichten etc. laufend angewandt.

Zielfelder: Das IKS wird angewandt werden zur Erzielung von:

T1 Rechtskonformität	Einhaltung der rechtlichen Vorschriften (Compliance)
T2 Strategie-Adhärenz	Einhaltung der definierten Geschäftsstrategie
T3 Bilanz-Qualität	Ordnungsmäßigkeit der Rechnungslegung
T4 Prozess-Qualität	Sicherheit, Effizienz, Wirksamkeit betrieblicher Prozesse
T5 Asset-Schutz	Schutz von Gütern, Vermögen, Daten und Informationen

Komponenten: Die Operationsfelder des IKS werden als Komponenten (IDW, COSO) bezeichnet:

K1 Kontrollumfeld	Problembewusstsein, Unternehmenskultur
K2 Risikoerkennung	Erkennung & Analyse von Unternehmensrisiken
K3 Kontrollaktivitäten	Kontrollen (integriert, intellektuell), IKS-Kalender
K4 Information/ Kommunikation	Richtlinien, Handbücher, Berichte, Kontakte
K5 Überwachung des IKS	Beurteilung der Wirksamkeit des IKS

Ende Definition IKS

Bausteine & Projekte: Das auf ein konkretes Kontroll-Objekt anzuwendende Werkzeug heißt Baustein[1]. Der Baustein stellt eine Fragestellung dar. Diese wird auf ein Kontroll-Objekt angewandt und liefert ein Instrument bzw. eine Instrumentenmenge:

Baustein => KOB => {Instrument(D_i)}; (i Є 1..5)

Die Fragestellung verfolgt ein Kontrollziel aus einem Zielfeld t Є {T1..T5} und klassifiziert damit den Baustein. Das Ergebnis der Untersuchung ist eine Instrumentmenge; jedes Instrument lässt sich einer Kategorie zuordnen. R_j=> {D1 .. D5}

Der Baustein wird durch eine Fragestellung, ein Kontroll-Objekt, einem Kontrollziel und einem entsprechenden Klassenbezeichner aus den Zielfeldern Tx bestimmt. Die Ermittlung der Ergebnis-Instrumente erfolg im Rahmen eines **IKS-Projekts**.

Instrumente: Als Instrumente des IKS werden bezeichnet: Implementierte Instrumente wie Vorkehrungen und Kontrollen, und alle Elemente aus K2 – K5, der IKS-Kalender und die Aktionen der Beauftragung. Im IKS-Kalender werden Anwendungen, Berichte, Projekte und freie Termine für Kontroll-Objekte eingetragen.

Kontroll-Objekte
Governance - Gestaltung
IKS (Di/Ki) (i=1-5) Organisation (Gestalt) Grundsatz – Einrichtung – Verfahren - Maßnahme
Ereignisse – (Ablauf–Gestalt)
Organisation (Ablauf) IT-Prozess IT-Ereignis Geschäftsprozess Geschäftsvorfall int. Leist.-Prozess
Ressourcen – (Aufbau-Gestalt)
IT-Verbund (allgemein) Raum - IT-System IT-Link - IT-Anwendung Organisation (Aufbau) Abteilung – Rolle - Person Daten-Objekte Stammdaten - Dokumente – Belege – Konten - Journale - Protokolle

[1] **Anmerkung:** Baustein wird hier gewählt, um in der Bezeichnungweise analog zur Terminologie des BSI beim GSHB zu bleiben.