

GRC Cockpit 1. Hilfe Informationen



LETZTE AKTUALISIERUNG

24 März 2009

GRC Cockpit 1. Hilfe Informationen

Produkt: docs&rules GRC Cockpit

Inhaltsverzeichnis

EINLEITUNG	2
WEITERE INFORMATIONEN AUF WWW.GRC-COCKPIT.DE.....	2
E-MAIL	2
HOTLINE.....	2
HERSTELLER	2
ALLGEMEINE HINWEISE ZUR BEDIENUNG	3
SYSTEMANFORDERUNGEN	3
ANFORDERUNGEN CLIENTS.....	3
TECHNISCHE VORAUSSETZUNGEN	3
HERANGEHEN AN DIE EINRICHTUNG DES RISIKO-MANAGEMENTS	4
1.SCHRITT / GRUNDEINRICHTUNG	5
2. SCHRITT / EINRICHTUNG DES RISIKO-KONTROLL-ZENTRUMS.....	5
RISIKEN IDENTIFIZIEREN UND BEWERTEN	5
MAßNAHMEN ABLEITEN.....	6
AKTIVITÄTEN PLANEN UND DELEGIEREN	6
AKTIVITÄTEN ÜBERWACHEN.....	6
TIPPS & TRICKS.....	7

Einleitung

Das docs&rules GRC Cockpit richtet sich an alle Unternehmen, die durch Unternehmenssteuerung Risiken und Chancen erkennen wollen. Die Anwendung kann von den verantwortlichen Stellen für die Unternehmensstrategie, -Controlling und -Management wie auch besonders vom Risiko Management genutzt werden.

Das GRC Cockpit wurde zusammen mit erfahrenen Fachspezialisten entwickelt. Die praxisnahen und nützlichen Funktionen sind das Resultat der engen Zusammenarbeit.

Weitere Informationen auf www.grc-cockpit.de

Alles Wissenswerte zu docs&rules GRC Cockpit, wie z. B. die detaillierten technischen Anforderungen, ein Glossar und weitere Informationen zu den Funktionen bietet die Website (www.GRC-Cockpit.de). Eine detaillierte Online-Hilfe innerhalb des GRC Cockpits wird in Kürze realisiert.

E-Mail

Anfragen und Anregungen zum GRC Cockpit senden Sie bitte an folgende E-Mail-Adresse:
info@grc-cockpit.de

Hotline

Für telefonische Anfragen steht Ihnen eine Hotline zur Verfügung, welche Sie von Montag bis Freitag von 10 – 12 Uhr erreichen: Fon: +49 (30) 920383 5992 oder Fax: +49 (30) 920383 5993

Hersteller

docs&rules GmbH
Keithstraße 6
10178 Berlin
Deutschland

Allgemeine Hinweise zur Bedienung

Systemanforderungen

Das GRC Cockpit ist eine webbasierte Online Software. Für Sie heißt das, dass Sie von jedem beliebigen Arbeitsplatz, sofern ein Internetzugang vorhanden ist, mit einem eigenen Login mit dem GRC Cockpit arbeiten können.

Anforderungen Clients

Monitorauflösung:	1024*768 Pixel
Betriebssystem:	Windows 98 / 2000 / XP / Vista / MacOS / Linux
Web-Browser:	Internet Explorer ab V. 6.0
	Mozilla Firefox ab V. 2.0
	Opera ab V. 8.0
	Safari Webbrowser ab V. 3.0

Software zum Empfang von E-Mails an o. genannte E-Mail-Adresse. Mindestens eine E-Mail-Adresse für den Internet-Zugang bei unserem Hosting-Partner IBM.

Für im System hinterlegte Inhalte, wie zum Beispiel PDF-, Word- oder Excel-Dateien sollte der Leser Acrobat Adobe Reader verwenden.

Technische Voraussetzungen

Um das GRC Cockpit einzusetzen, muss Ihr Browser aus Sicherheitsgründen die 128 Bit Daten-Verschlüsselung, JavaScript und Cookies unterstützen. Falls der Betrieb mit den Browsern «Internet Explorer», «Mozilla Firefox», «Opera» oder «Safari Webbrowser» nicht funktioniert, kontrollieren und ändern Sie evtl. folgende Einstellungen im Menu des Browsers:

	Internet Explorer	Firefox
Datenverschlüsselung SSL 3.0 (Secure Socket Layer)	Menu: Extras > Internetoptionen > Erweitert > «Standard wiederherstellen» oder unter dem Punkt «Sicherheit» den Eintrag «SSL 3.0 verwenden» aktivieren	Menu: "Extras / Einstellungen / Erweitert / Verschlüsselung" unter dem Punkt "Protokolle" den Eintrag "SSL 3.0 verwenden" aktivieren
Aktivieren von JavaScript	Menu: Extras > Internetoptionen > Sicherheit > Internet > Stufe auf «Medium» setzen	Menu: "Extras / Einstellungen / Inhalt" den Eintrag "JavaScript aktivieren" selektieren
Aktivieren von Cookies	Menu: Extras > Internetoptionen > Datenschutz > Erweitert >«Automatische Cookiebehandlung aufheben» deaktivieren	Menu: "Extras / Einstellungen / Datenschutz" unter den Punkt "Cookies" den Eintrag "Cookies akzeptieren" selektieren

Herangehen an die Einrichtung des Risiko-Managements

Risiko-Management- und Interne-Kontroll-Systeme gehen typischerweise von Risiken aus. Der normale Ablauf im GRC Cockpit orientiert sich an diesem Vorgehen:

- ✓ Zuerst werden die Risiken identifiziert und bewertet. Hierzu steht ein umfangreicher Risiko-Katalog zur Verfügung. Dieser kann aber spezifisch ergänzt werden.
- ✓ Für relevante Risiken wurden oder werden Maßnahmen definiert, um diesen entgegen zu wirken
- ✓ Die Maßnahmen (z.B. eine Schulung oder eine Kontrolle) werden dann konkret als Aktivität geplant, zugewiesen und selber wieder kontrolliert.



1. Schritt / Grundeinrichtung

Die ersten Grundeinstellungen werden unter „Management“ eingestellt.

Hierzu gehört vor allem die Einrichtung der Benutzer. Mitarbeiter können nur Aufgaben bearbeiten und Artikel lesen. GRC Manager können auch das Risiko-Zentrum bearbeiten, Artikel schreiben und Management-Analysen vornehmen. Die Benutzererkennung erfolgt über eine reale E-Mail. Es kann derzeit eine E-Mailadresse nur exakt einmal im gesamten System vergeben werden! Mit Anlage eines Benutzers erhält dieser eine Informationsmail und kann sich per URL-Bestätigung aktivieren lassen.

Die Angaben unter dem Unternehmensprofil werden derzeit noch nicht ausgewertet. Sie sollen später dazu dienen, Artikel qualifizierter versenden zu können.

2. Schritt / Einrichtung des Risiko-Kontroll-Zentrums

Das Risiko-Kontroll-Zentrum wird unter Management / Risiko-Kontroll-Zentrum / Konfiguration eingerichtet.

Unter / Einstellungen kann die Bedeutung von Schäden monetär bewertet werden. Eine exakte monetäre Einschätzung ist manchmal möglich und kann explizit eingestellt werden, wenn bspw. der Wert eines Gutes, das bedroht ist, bekannt ist. Um auch in anderen Fällen eine ungefähre Klassifizierung zu ermöglichen, können auch 5 Kategorien mit Wertangaben und Bedeutungen hinterlegt werden.

Unter Funktion und Risikokategorien können außerdem die Struktur und die Angaben der Geschäftsfunktionen sowie die Risiko-Kategorien modifiziert werden.

Risiken identifizieren und bewerten

Zuerst werden die Risiken identifiziert und bewertet. Hierzu steht ein umfangreicher Risiko-Katalog zur Verfügung. Wir empfehlen die Durchführung von Interviews mit den Funktions-Verantwortlichen (z.B. dem CFO, dem CIO und dem Hausjuristen). Hierzu stehen Filter für die Geschäftsfunktion sowie für spezielle Themen zur Verfügung.

Die Risiken werden hinsichtlich ihrer Bedeutung für das Unternehmen bewertet.

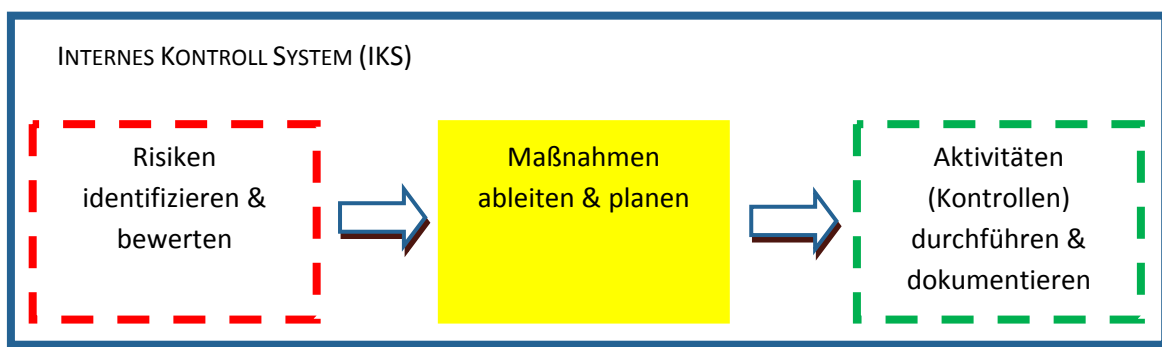
Notfallrelevanz kennzeichnet Maßnahmen und Aufgaben, die Ereignisbezogen gestartet werden sollen. In diesem Fall werden die verbundenen Maßnahmen bzw. deren Aktivitäten unmittelbar gestartet (wird derzeit noch nicht ausgewertet!)



Maßnahmen ableiten

Signifikante Risiken sollten Maßnahmen gegenüber stehen. Maßnahmen sind zunächst abstrakt, wie z.B.: Aufstellungen, Kontroll-Listen, Schulungen, Berichte oder Richtlinien. Es können aber auch eine „Leitkultur“, Leitprinzipien (z.B. generelles 4-Augenprinzip) oder „Einzelfall-Gespräche“ sein. Da hier sehr unterschiedliche Maßnahmen getroffen werden können, gibt es in dieser Sektion nur eine erste Auswahl möglicher Maßnahmen. Hier werden häufig eigene Maßnahmen zu präzisieren und zu ergänzen sein. Das Risiko wird mit einer oder mehreren Maßnahmen verbunden.

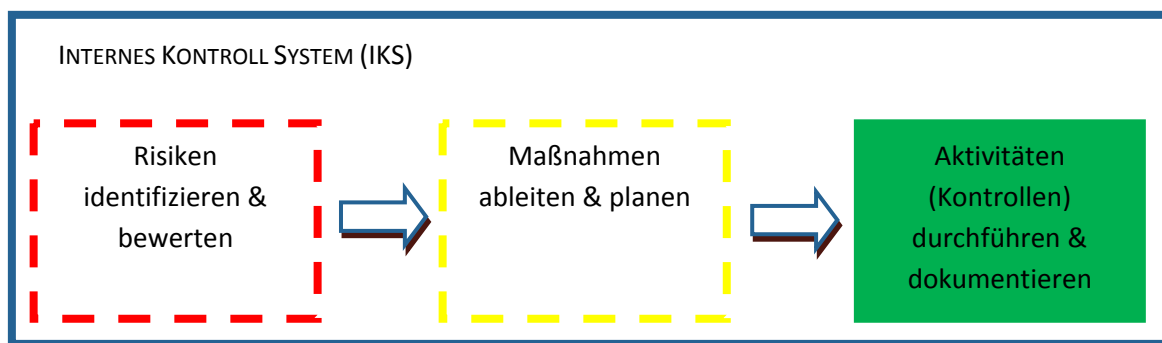
Die Kennzeichnung der Maßnahmen wird zukünftig für spezielle Auswertungen verwendet, damit auf Basis dieser Auswertungen, zentrale Inhalte eines Risiko-Berichts komfortabel generiert werden können.



Aktivitäten planen und delegieren

Besonders kritische Risiken sollten durch konkrete, d.h. Personen zugewiesene Aktionen, im Sinne eines Frühwarnsystems zyklisch überwacht werden. Hierzu kann der Verantwortliche aus der Liste der angemeldeten Benutzer ausgewählt werden.

Die Zeitspanne der geplanten Verarbeitung liegt zwischen dem Benachrichtigungszeitpunkt und der Fälligkeit (nächster Check). Der Benachrichtigungszeitpunkt wird in Bezug zum bereits eingegebenen nächsten Check gesetzt.



Aktivitäten überwachen

Unter Management / Management-Analyse lassen sich alle anstehenden Aufgaben filtern und überprüfen

Tipps & Tricks

Tipp: Konzentrieren Sie sich auf die wesentlichen Risiken! Es geht nicht darum, möglichst viele Kontrollaktivitäten zu etablieren, die Ihre Mitarbeiter von der eigentlichen Arbeit abhalten. Vielmehr geht es darum, das Risiko-Bewusstsein zu erhöhen und die wirklich wichtigen Kontrollen verlässlich umzusetzen.