# Information GRC im QM-Pilot

## Governance, Riskmanagement, Compliance

Governance, Risikomanagement und Compliance fasst die drei wichtigsten Handlungsebenen für die erfolgreiche Führung eines Unternehmens zusammen. Im Folgenden wird beispielhaft dargestellt, wie dies für G-R-C im QM-Pilot umgesetzt werden kann.

### Governance – interne Vorgaben steuern

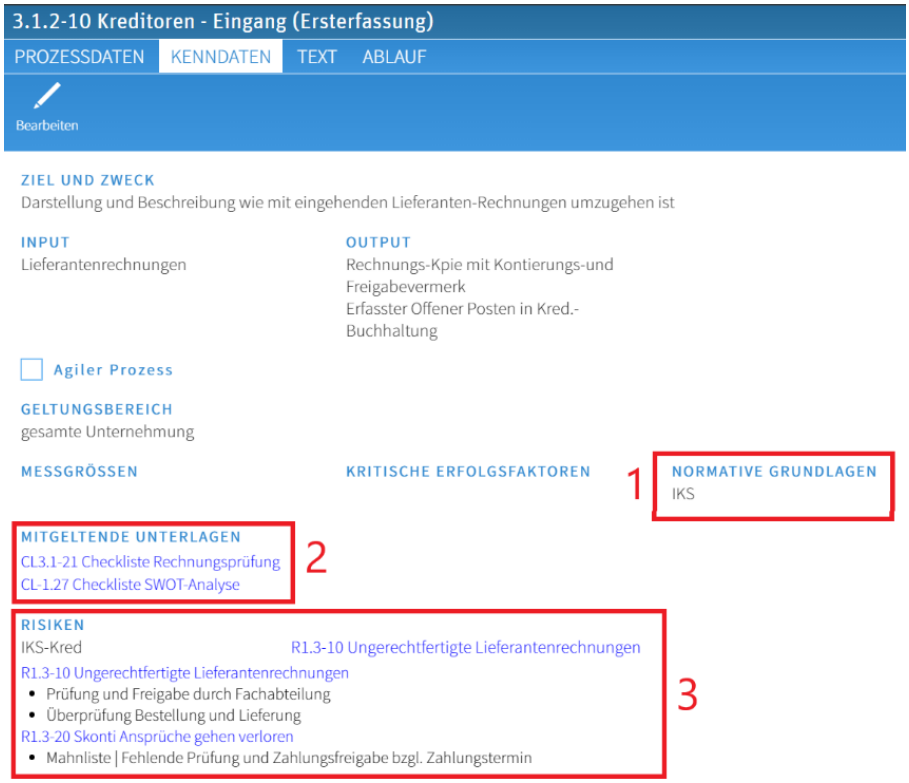
Abbilden der **Geschäftsprozesse** im Modul Prozessmanagement (siehe Produktinformationsbroschüre) inkl. der Daten aus den Modulen Dokumentenmanagement und Risikomanagement. Dies ermöglicht ein **holistisch** aufgebautes Managementsystem. Neben dem Abbilden der **Prozesslandkarte**, detaillierten Prozessbeschreibungen als **Flow-Charts** oder **BPMN-Swimlanes** können diese mit unternehmensspezifischen **Daten** angereichert werden. Die Datenfelder sind **flexibel konfigurierbar** und können unter anderem folgende Punkte abdecken und sind beliebig erweiterbar:

- **Ziele** (auf jeder Prozessebene, Detailziele oder unternehmensübergreifende Ziele)
- **Methodik** zur Umsetzung (erschliesst sich aus den Prozessen und zugehörigen Informationen)
- Angabe der notwendigen **Ressourcen** zu einem Prozess – Reporting zur Gesamtauswertung

Zusätzlich werden alle (internen) Vorgabedokumente im Dokumentenmodul (siehe Produktinformation) verwaltet, versioniert, archiviert, immer aktuell freigegeben zur Verfügung gestellt und können in **Verbindung mit Prozessen, Risiken und Compliance-Vorgaben gesetzt werden.**

- Dokumente können direkt mit Prozess-Schritten oder in den Kenndaten (**2**) verknüpft werden und stehen immer nur in der aktuell freigegebenen Version zur Verfügung
- Dokumente/Prozesse können mit Risiken verknüpft werden (**3**)
- Normative Grundlagen können mit Dokumenten verknüpft werden (**1**)
- Alle Verbindungen/Abhängigkeiten können dargestellt/nachvollzogen werden

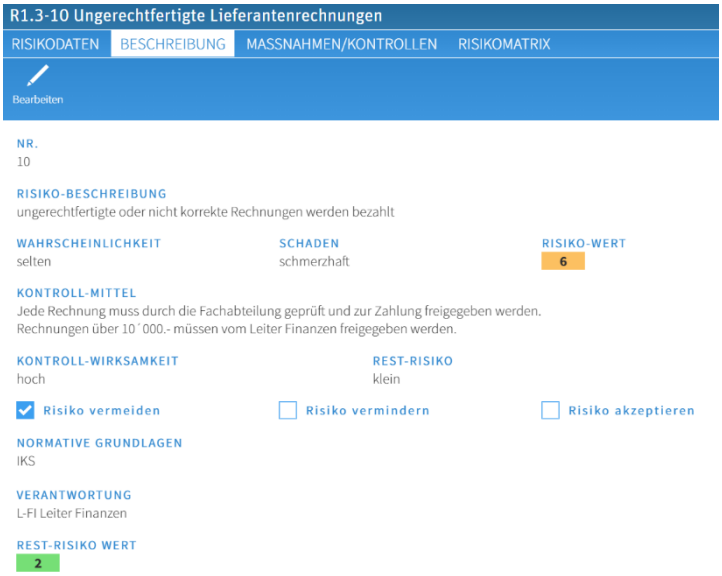
**Beispiel Kenndatenerfassung zum Prozess inkl. Verknüpfung zu Dokumenten und Risiken:**



**R**iskmanagement

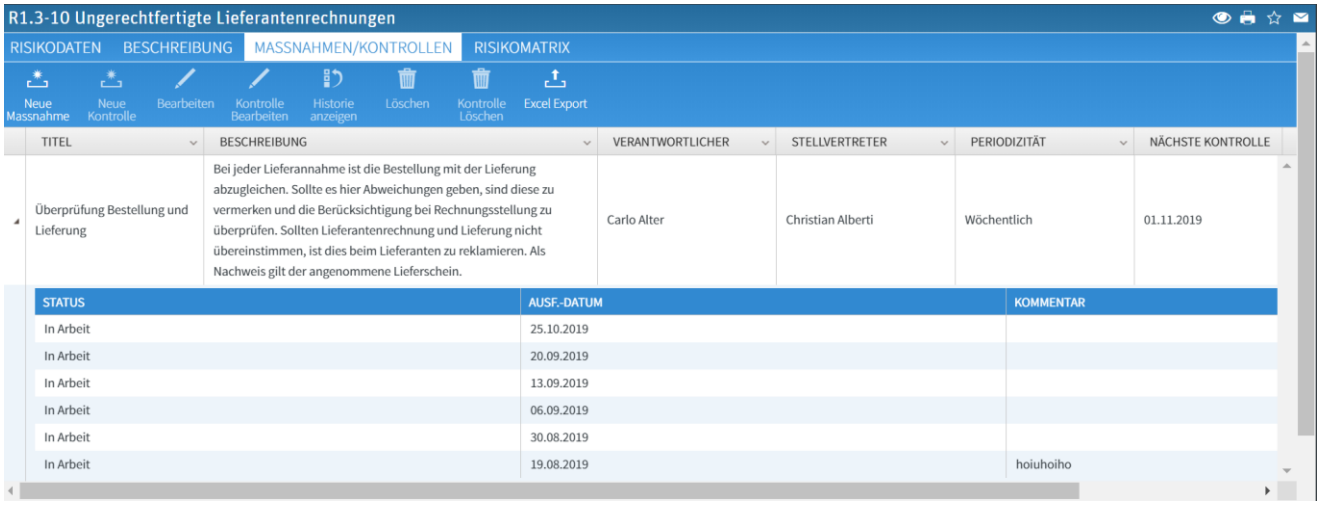
Riskmanagement ist eine Führungsaufgabe, im Rahmen derer die Risiken einer Organisation identifiziert, analysiert und bewertet werden. Für einen holistischen Ansatz ist es wichtig, dass das Riskmanagement nicht für sich alleinsteht, sondern in den gesamten unternehmerischen Rahmen mit Governance und Compliance in Verbindung gebracht wird.

### Risikoerfassung (Risikodaten, Beschreibung, Massnahmen/Kontrollen, Risikomatrix)




Die gezeigten Felder sind kundenspezifisch konfigurierbar. Daten wie bspw. die **Risiko-beschreibung**, **Bewertung**, **Risiko-appetit**, **Normative Grundlagen** und **Verantwortlichkeiten** sind einfach zu erfassen und über das Reporting auszuwerten. Berechnete Risikowerte können auf der Risiko-Matrix dargestellt werden. Alle Abhängigkeiten zu anderen Systeminhalten (bspw. Prozess-Schritte im IKS) können ausgewertet werden.

**Bewertungsschemata** können in Stammdaten-tabellen hinterlegt und bei der Risikobeschreibung über Auswahllisten zur Verfügung gestellt werden. Darüber lässt sich auswerten, welche Kriterien in welchen Risiken angegeben sind.




Zu jedem Risiko können beliebig viele Massnahmen erfasst und die zugehörigen Kontrollen vom System automatisch angelegt werden. Verantwortlichkeit und Stellvertreter können hier eindeutig zugeordnet werden. Zur Dokumentation im System werden die Kontrollen von den Usern mit einem Status (in Arbeit, Erledigt, Abgelehnt, Erledigt mit Mangel) dokumentiert und in der Historie abgelegt.

### Reporting

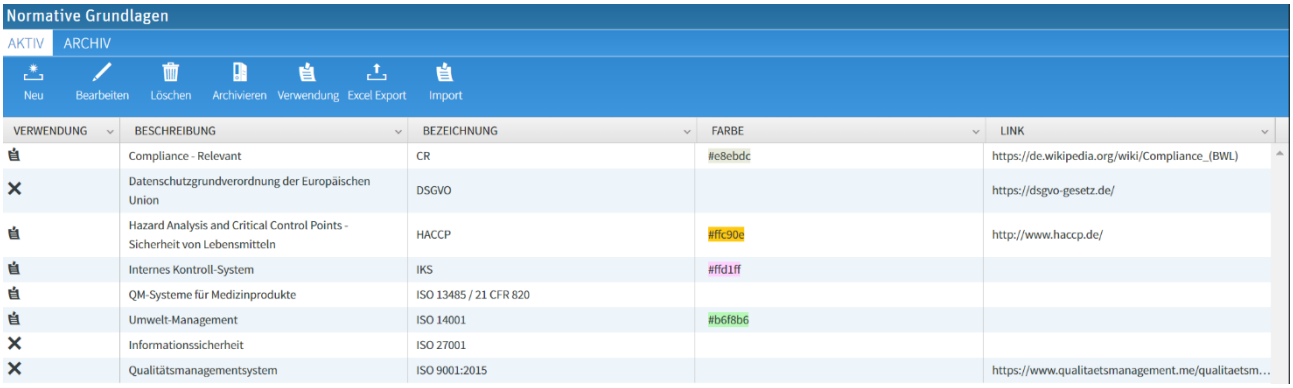
Neben einer Vielzahl an Standardberichten (Risikoliste, Risiken mit Beschreibung, Massnahmenliste, Kontrollen, IKS Risiko-Kontrollmatrix uvm.) können für spezielle Reporting-Bedürfnisse spezifische Berichte durch Abel Systems angefragt und hinterlegt werden.

## Compliance

Das Compliance Management beschreibt den Grundsatz sowie Massnahmen zur Einhaltung von Gesetzen, Richtlinien und internen Kodizes sowie die Vermeidung von Regelverstössen.

Die Gesamtheit dieser Gesetze, Normen, Richtlinien sowie internen und externen Vorgaben muss zunächst als Übersicht in einem GRC-System erfasst werden. Dies erfolgt über eine Stammdatentabelle, welche mit zusätzlichen Informationen ergänzt werden kann (Geltungsbereich, Links auf Dokumente uvm.).

**Beispiel Stammdatentabelle Normative Grundlagen**

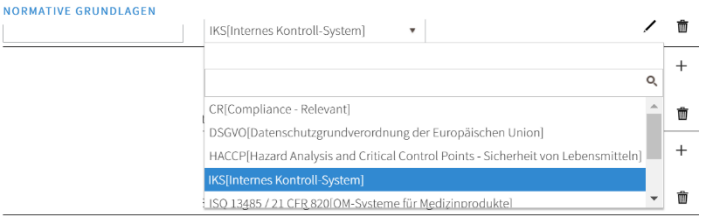



| VERWENDUNG | BESCHREIBUNG | BEZEICHNUNG | FARBE | LINK |
|---|---|---|---|---|
| ✓ | Compliance - Relevant | CR | #e8ebdc | https://de.wikipedia.org/wiki/Compliance_(BWL) |
| ✗ | Datenschutzgrundverordnung der Europäischen Union | DSGVO | | https://dsgvo-gesetz.de/ |
| ✓ | Hazard Analysis and Critical Control Points - Sicherheit von Lebensmitteln | HACCP | #ffc90e | http://www.haccp.de/ |
| ✓ | Internes Kontroll-System | IKS | #ffd1ff | |
| ✓ | QM-Systeme für Medizinprodukte | ISO 13485 / 21 CFR 820 | | |
| ✓ | Umwelt-Management | ISO 14001 | #b6f8b6 | |
| ✗ | Informationssicherheit | ISO 27001 | | |
| ✗ | Qualitätsmanagementsystem | ISO 9001:2015 | | https://www.qualitaetsmanagement.me/qualitaetsm... |

Diese Tabelle lässt sich beliebig konfigurieren und erweitern. Für alle Abhängigkeiten lässt sich die Verwendung der Einträge anzeigen. Dadurch entsteht ein Gesamtbild, an welchen Stellen (Prozesse, Dokumente, Risiken) ein bestimmtes Gesetz/Norm/Richtlinie Compliance-relevant ist.

**Abhängigkeit zu Prozessen, Dokumenten und Risiken darstellen**

Wie im Abschnitt Governance am Beispiel Prozesskenndaten ersichtlich, lässt sich die Abhängigkeit zwischen Normativer Grundlage und Prozess/Dokument/Risiko mittels Kenndatenfeld herstellen. Zugegriffen wird mittels Auswahlliste auf die in der Stammdatentabelle erfassten Daten:




Jede verknüpfte Abhängigkeit lässt sich über die Anzeige der Verwendung auswerten und darstellen. Änderungen können zentral in der Stammdatentabelle vorgenommen werden. Bei spezifischen Auswertungen zu einzelnen Normen/Gesetzen/Richtlinien lassen sich alle Compliance-relevanten Inhalten per Klick anzeigen.

**Fazit**

Der QM-Pilot kann als GRC-Tool aufgebaut werden. Ein holistischer Denkansatz und Aufbau des Systems wird durch Datenbankverknüpfungen und entsprechende visuelle Darstellung im User Interface gewährleistet. Als normorientiertes System werden Funktionen wie Versionierung, Prüf- und Freigabeworkflow sowie die Sicherstellung des Zugriffs auf ausschliesslich freigegebene Inhalte gewährleistet. Umfangreiche Modulbeschreibungen befinden sich in der Produktbroschüre des QM-Pilot. Diese Zusatzinformationen stellen lediglich gewisse Aspekte des GRC-Systems heraus.