antares

Whitepaper

[antares RiMIS® IKS - Internes Kontrollsystem

[Einleitung

Das vorliegende Dokument dient der Funktionsbeschreibung des IKS-Erweiterungsmoduls zur Risiko- und Chancenmanagement-Software antares RiMIS®.

antares RiMIS® ist eine Software für das Chancen- und Risikomanagement. Elementare Bestandteile dieser Standard-Software sind das Maßnahmen-Management und Berichtswesen sowie die Monte-Carlo-Simulation und Risiko-Identifikation mittels Fragebögen.

Die Software ist primär für die Industrie, Dienstleistung und Handel, Konzerne, Aktiengesellschaften und größere mittelständische Betriebe konzipiert.

Dank der vollständigen Dokumentation der Prozesskontrollen sowie der workflowgestützten Überwachung stellt antares RiMIS® IKS mit effektiven Verfahren sicher, dass Ihre Geschäftsprozesse transparent, sicher und nach definierten (Rechts-)Vorschriften ablaufen. Dabei umschließt das Verfahren alle Gesellschaftsorgane, darunter auch den Aufsichtsrat und die Geschäftsführung.

Das IKS-Modul steht ab der Version 3.7.2 zur Verfügung, welche im September 2012 erschienen ist. Dieses Modul ist nicht Bestandteil der Standard-Lizenz für antares RiMIS® und muss gesondert lizenziert werden.

[1. Zweck des Moduls

Ein internes Kontrollsystem (IKS) dient der softwaregestützten internen Prozesskontrolle sowie der Dokumentation und Überwachung von Geschäftsprozessen in Unternehmen. Es bietet zudem Schutz vor Missbrauchs- und Schadenshandlungen im Unternehmen und verhindert diese.

Zu den Hauptzielen des IKS zählen die Überwachung und Prävention von Risiken, Gewährleistung der Funktionsfähigkeit und Wirtschaftlichkeit in Geschäftsprozessen sowie der Zuverlässigkeit von betrieblichen Informationen und Vermögenssicherung. Durch umfangreiche Kontrollmaßnahmen und lückenlose Dokumentation werden wesentliche Fehlaussagen in der Finanzberichterstattung verhindert und die vollständige, korrekte Aufzeichnung des Rechnungswesens sichergestellt. Um diese Ziele zu erreichen, setzt antares RiMIS® IKS auf verschiedene Prinzipien, wie Transparenz und Mindestinformation.

Organisatorisch soll die Überwachung der Kontrollen eng mit der Überwachung der übrigen, nicht prozessimmanenten Risiken einhergehen. Da antares RiMIS® webfähig angelegt ist, können beliebig viele Personen dezentral auf das System zugreifen und sich so permanent am Prozess beteiligen oder selbstständig Informationen einholen.

[2. Begriffsdefinitionen

2.1 Prozess

Ein Geschäftsprozess stellt einen wesentlichen Ablauf in einer Gesellschaft/einem Unternehmen dar. Für das IKS-Modul stellt ein Prozess bzw. Teilprozess das Schlüsselelement für die Zuordnung von Kontrollen dar. Ein Prozess kann aus beliebig vielen Teilprozessen bestehen. Ein Teilprozess kommt nur eindeutig einmal und auch nur einmal innerhalb der Prozessstruktur vor. Die Prozessstruktur kann aus bis zu 15 Ebenen bestehen. Es muss ein Summenknoten existieren, unter dem alle Prozesse und Teilprozesse aufgeführt werden („Alle Geschäftsprozesse" o. ä.). Existiert ein ähnlicher Teilprozess in verschiedenen Prozessen, ist zu gewährleisten, dass dieser Teilprozess eindeutig wird, z. B. durch eine eindeutige ID oder einen eindeutigen Namen. Nur so kann gewährleistet werden, dass individuell verschiedene Kontrollen an einen Teilprozess adressiert werden können.

Die Prozessbeschreibung und der Prozessaufbau können sich jederzeit ändern, d. h. Änderungen sollten nachvollziehbar sein (Historie). Die Prozessbeschreibung kann in mehreren Sprachen erfasst werden. Ein Prozess hat eine eindeutige, alphanummerische ID. Ein Prozess kann aufgrund der Historisierung nicht gelöscht, sondern nur deaktiviert werden. Die Zuordnung zwischen Prozess und Teilprozess wird ebenso historisiert, folglich auch deaktiviert.

2.2 Legaleinheit

Eine Legaleinheit ist eine organisatorisch weitgehend eigenständige Einheit und eine eigenständige juristische Person. Legaleinheiten können wiederum zu einer Legalstruktur zusammengefasst werden. Beteiligungsverhältnisse werden derzeit in antares RiMIS® nicht erfasst.

Neben der Legal- und der Prozessstruktur ist es in antares RiMIS® auch möglich, eine Organisationsstruktur abzubilden. In der Legalstruktur können ebenso nicht eigenständige Einheiten, wie z. B. Produktionswerke, hierarchisch eingeordnet werden. Einzelne Einheiten können auch mittels Summenknoten zu einer regionalen Struktur zusammengefasst werden.

2.3 Zuordnung zwischen Legaleinheit und Prozess

In antares RiMIS® wird je Legaleinheit definiert, welcher Prozess in der Legaleinheit als wesentlicher Prozess der Legaleinheit anzusehen ist. Daraus leiten sich später die Standardkontrollen ab und in welcher Form die Kontrollen durchzuführen sind. Die Zuordnung kann mehrstufig erfolgen (z. B. Must/Want/Nice to have/nicht relevant).

2.4 Schadenspotenzial

Ein Prozess kann mehrere Schadenspotenziale haben, die gleichbedeutend mit potenziellen Risiken sind. Die Zuordnung zu vorgegebenen Standardrisiken dient der Integration des IKS in den Standard-Risikomanagement-Prozess und soll die Erfassung von Kontrollen und weiteren Maßnahmen erleichtern. Ein Schadenspotenzial besteht aus einer eindeutigen ID, einer Beschreibung, die mehrsprachig sein kann und einem Flag, abhängig davon, ob es sich bei dem Schadenspotenzial um ein Pflicht-Schadenspotenzial handelt (das vom Prozess abgeleitet wird). Aus individuellen Risiken können weitere Schadenspotenziale über einen Standard-Prozess innerhalb von antares RiMIS® angelegt werden.

2.5 Zuordnung zwischen Prozess und Schadenspotential

Ein Prozess bzw. Teilprozess kann mehrere Schadenspotenziale zugeordnet bekommen. Ein Schadenspotenzial kann auch verschiedenen Prozessen zugeordnet sein.

2.6 Kontrollziel und Zuordnung zur Kontrolle

Mit dem Kontrollziel soll definiert werden, was die Zielsetzung der Kontrollen hinsichtlich eines Prozesses ist. Einem Prozess werden ein bis mehrere Kontrollziele zugeordnet. Ein Kontrollziel kann z. B. die Gültigkeit (der Daten) oder die Sicherheit sein. Kontrollziele und deren Zuordnung können nur zentral und unternehmensweit angelegt werden. Ein Kontrollziel dient der späteren Wirksamkeitsprüfung der Kontrollen.

2.7 Kontrolle

Eine Kontrolle besteht aus einem Titel, einer Langtextbeschreibung und Verweisen zu internen Dokumenten wie einem Management-Handbuch, die allesamt mehrsprachig angelegt werden können. Darüber hinaus hat eine Kontrolle die Attribute Soll-Frequenz, Soll-Check-Frequenz, Art der Kontrolle, Dokumentationspflicht und die Unterscheidung, ob es sich um eine Standard-Kontrolle handelt, die Top-Down vorgegeben ist oder um eine individuelle Kontrolle, die vom dezentralen IKS-Verantwortlichen angelegt wird. Des Weiteren wird definiert, ob es sich um eine Pflichtkontrolle oder eine freiwillige Kontrolle handelt. Diese Vorgabe kann im Einzelfall noch strenger gefasst werden, eine Erleichterung bei Legaleinheiten, die per Prozesszuordnung gezwungen sind, Kontrollen durchzuführen, ist nicht vorgesehen.

2.8 Zuordnung zwischen Prozess & Kontrolle

Über den Prozess wird letztendlich bestimmt, welche Schadenspotenziale bei einer Legaleinheit qua Organisation existieren und wie diesen Risiken mit Kontrollen begegnet werden kann bzw. muss. Dies wird einerseits durch eine Top-Down-Vorgabe konzernseitig definiert, andererseits kann aber auch individuellen Risiken mit Kontrollen begegnet werden, die der Risikoverantwortliche für sich definiert und ausgestaltet. Diese Zuordnung stellt eine „Sollvorgabe" dar, die in der Legaleinheit personell verankert wird.

2.9 Zuordnung zwischen Kontrolle, Legaleinheit & Prozess

Aus der vorgenannten Sollvorgabe leitet sich die konkrete Verantwortung ab, welche Person (und Vertretung) für die Kontrolle fachlich verantwortlich ist, in welcher Form die Kontrolle tatsächlich durchgeführt wird sowie wie und wo die konkrete Kontrolle weiter beschrieben wird.

2.10 Durchführung der Kontrolle

Die Dokumentation der Durchführung der Kontrolle ist entsprechend der Kontrollfrequenz vorzunehmen und durch Upload eines Dokuments zu belegen.

2.11 Durchführung der Wirksamkeitsprüfung der Kontrolle

Die Kontrollen sind periodisch entsprechend der Check-Kontrollfrequenz auf deren Wirksamkeit und Nachvollziehbarkeit zu überprüfen. Dies kann mehrstufig bewertet und mit einem Freitext näher dargestellt werden.

2.12 Mehr-Augen-Prinzip, Dokumentation

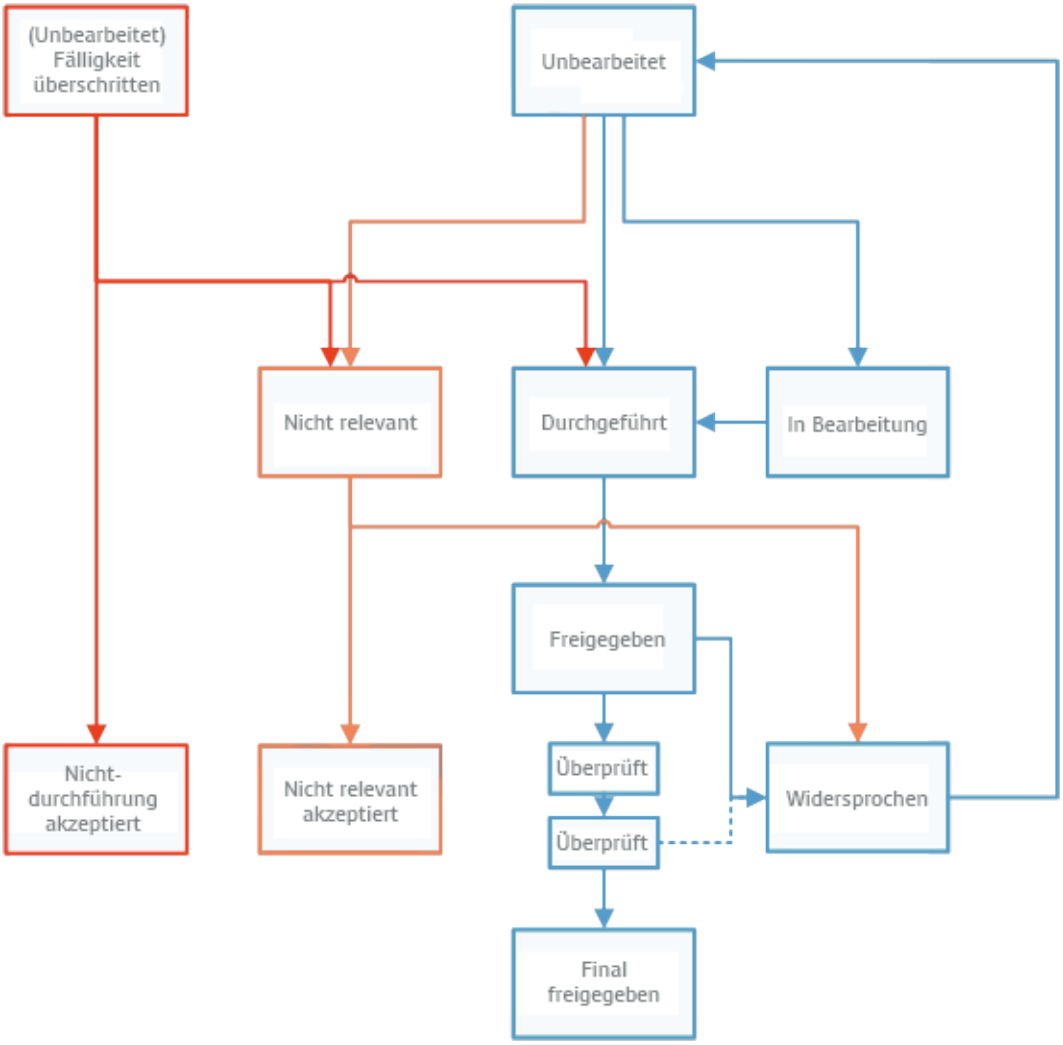
Die Durchführung einer Kontrolle wird durch einen automatischen Prozess dem Kontroll-Manager (i. d. R. der Geschäftsführer) signalisiert, der die Durchführung überwacht. Dieses Mehr-Augen-Prinzip kann über einen Freigabeprozess über bis zu 15 Stufen durchgeführt werden.

2.13 Kontroll-Frequenz

Kontrollen müssen regelmäßig periodisch wiederkehrend durchgeführt werden. Dies wird zentral in den Stammdaten der Kontrolle erfasst. Über die Kontrollfrequenz wird errechnet, wann die Durchführung der Kontrolle spätestens zu erfolgen hat, z. B. bei einer Frequenz einmal pro Quartal am 31.3, 30.6, 30.9 und 31.12 eines Jahres. Wird eine Kontrolle nicht innerhalb dieses Zeitraums durchgeführt, muss das begründet und vom IKS-Manager akzeptiert werden, wofür ein eigener Status vorgesehen ist.

[3. Workflow der Kontrollen

Die Kontrolle soll periodisch je nach Vorgabe durchgeführt werden. Der Workflow-Prozess ist wie folgt vorgesehen:



- Nach jeder Periode wird die Kontrolle in den Status „Unbearbeitet" versetzt.

- Bis zur Freigabe („Freigegeben") kann eine Kontrolle bearbeitet werden (Änderung des Kontrollkommentars, Änderung des Dokumenten-Anhangs). Sobald die Freigabe erfolgt ist, kann am Kontrollkommentar und am Dateianhang keine Änderung mehr vorgenommen werden.

- Die Ablehnung der Kontrolle („Widersprochen") erfordert die Eingabe eines Kommentars durch den Ablehnenden. Anschließend kann die Kontrolle bis zur erneuten Freigabe wieder beliebig bearbeitet werden.

- Der Freigabeprozess „Überprüft" muss jede Instanz der IKS-IKSM-Struktur durchlaufen. Zwischen den Freigaben kann eine Ablehnung erfolgen, wobei die Kontrolle dann wieder direkt beim Kontrollierenden vorliegt.

- Für die Freigabe-Schritte kann eine „Sammelfreigabe" erfolgen, mehrere Kontrollen können in einem Schritt als „Überprüft" markiert werden.

- Kontrollen können vom Kontroll-Verantwortlichen als „nicht relevant" markiert werden, was jede Kontrollperiode erneut zu erfolgen hat und vom Nächsthöheren im Freigabeprozess akzeptiert werden muss.

- Sollten Kontrollen in einer Kontrollperiode nicht durchgeführt worden sein, werden sie als „Nicht durchgeführt" in der aktuellen Periode fortgeführt. Die Kontrolle kann im Nachhinein durchgeführt werden oder der nächste im Freigabeprozess akzeptiert die Nichtdurchführung.

Die durchzuführenden Kontrollen werden in einem filterbaren/durchsuchbaren und sortierbaren Übersichtsbildschirm dargestellt. Hierbei werden nur die Kontrollen angezeigt, die vom angemeldeten User durchzuführen sind. Über ein Kontextmenü werden spezifische Optionen angeboten. Dies ist unter anderem: Durchführung der Kontrolle (via Dialog-Maske) und Detail-Informationen zur Kontrolle (via Dialog-Maske). Über eine andere Ansicht des Übersichtsbildschirms werden die zu prüfenden Kontrollen dargestellt. Über die Sortierung wird wiederum gewährleistet, dass die aktuell anstehenden Prüfungen am Anfang der Tabelle genannt werden. Für den jeweiligen Status kann parametrisiert werden, ob ein Dokument oder Kommentar notwendig ist.

[4. Risiken und Kontrollen

In antares RiMIS® existiert per se bereits ein umfangreiches Maßnahmenmanagement mit Statusüberwachung der Maßnahmen, Prüfung der Effizienz einer Maßnahme und teilautomatischer Ableitung der Netto-Bewertung eines Risikos. Maßnahmen können verschieden typisiert werden, z. B. Notfallplanung, regelmäßige Wartung oder einmalige Aktion. In diesem Umfeld stellt eine Kontrolle eine Art regelmäßig durchzuführende Präventionsmaßnahme dar. Die Besonderheit einer Kontrolle besteht jedoch darin, dass je Legaleinheit in einem Top-Down-Prozess vorgegeben wird, welche Kontrollen durchzuführen sind, was sich aus den in der Legaleinheit vorhandenen und mehr oder weniger stark ausgeprägten Geschäftsprozessen ergibt.

Aus diesen Vorgaben ergeben sich „Pflichtrisiken" und damit verbundene Kontrollen. Neben der Durchführung der Kontrolle ist individuell auch das Risiko zu beschreiben, zu bewerten etc., worauf an dieser Stelle jedoch nicht näher eingegangen wird. Die Top-Down vorgegebenen Kontrollen können durch individuelle Kontrollen beliebig durch den Risikoverantwortlichen ergänzt werden. Es können zudem auch weitere Maßnahmen definiert werden, die keinen Kontrollcharakter innehaben.

[5. Individualisierung von Kontrollen

Dezentrale Einheiten haben die Möglichkeit, einzelne Kontrollen in folgenden Ausprägungen zu individualisieren:

- Verschärfung der Notwendigkeit zur Durchführung einer Kontrolle (z. B. von Soll auf Muss).
- Kommentierung der Kontrolle, z. B. wie wird eine Kontrolle konkret bei der Tochtergesellschaft durchgeführt/umgesetzt/dokumentiert.
- Erhöhung der Kontrollfrequenz, z. B. von einmal pro Quartal auf monatlich.
- Darstellung, ob eine Kontrolle automatisch durch ein System erfolgt (Verweis auf das System) oder manuell.

[6. Top-Down-Vorgaben

6.1 Definition der Prozesse

Die Definition, bei welcher Legaleinheit die verschiedenen Prozesse und damit Kontrollen umzusetzen sind, wird von einem zentral verantwortlichen IKS-Manager durchgeführt. Hierbei wird sowohl in der Prozess- wie auch in der Legalstruktur die Definition bei mehrstufigen Hierarchien vererbt, sodass der Pflegeaufwand möglichst gering gehalten wird. Die Umsetzungspflicht-Definition selbst kann mehrstufig erfolgen (Pflichtprozess, möglicher Prozess etc.).

6.2 Definition von Kontroll-Verantwortlichen

Die Kontrollverantwortung muss manuell je Legaleinheit festgelegt werden, wobei je Organisationseinheit, Legaleinheit und Prozess unterschiedliche Verantwortliche je Kontrolle definiert werden können. Neben dem Verantwortlichen kann auch eine Vertretung vorgesehen werden. Die Personenzuordnung kann entweder zentral oder auch dezentral, z. B. durch einen Bereichsverantwortlichen, definiert werden. Die Vorgabe, welche Kontrolle durch welchen Kontroll-Verantwortlichen durchgeführt werden soll, wird über eine zentrale Administrationsmaske vorgenommen. Diese Maske steht auch dezentralen Verantwortlichen in Beteiligungen/Gesellschaften zur Verfügung, die für ihre jeweilige Berechtigung die Verantwortung definieren können.

6.3 Definition der IKS-Owner/IKS-Manager-Struktur

Je Kombination aus Legaleinheit, Organisationseinheit und Prozess kann für jeden IKS-Owner ein IKS-Manager zugeordnet werden. Die Legal-/Org-/Prozess-Kombination muss dabei nicht auf unterster Ebene erfolgen, sondern kann auch ein Knoten sein, der wiederum auf alle untergeordneten Knoten vererbt wird. Bei dieser Zuordnung wird die Eingabe durch eine Multiselektion erleichtert. Diese Zuordnung bestimmt letztendlich, welcher IKS-Manager die Durchführung der Kontrolle zu überwachen hat.

6.4 Definition von Kontrollen zu Prozessen

Je Prozess können beliebig viele Kontrollen ausgewählt und zugewiesen werden, die vom Kontrollierenden in einer Legaleinheit durchgeführt werden müssen.

6.5 Schadenspotentiale zu Prozessen

Zu jedem Prozess können verschiedene Schadenspotenziale angelegt werden, aus denen Risiken abgeleitet werden können. Ein Schadenspotenzial kann das Merkmal „Pflichtrisiko" erhalten. Diese Risiken sind per Definition in jeder Legaleinheit, die dem Prozess (siehe 5. a) zugeordnet ist, vorhanden und müssen periodisch bewertet und freigegeben werden. Kontrollen ergeben sich aus der Zuordnung des Risikos zu diesem Prozess.

[7. Wirksamkeitsprüfung

In regelmäßigen Abständen (Kontroll-Check-Frequenz), die je Kontrolle definiert werden, sollen Kontrollen auf Ihre Wirksamkeit, Nachvollziehbarkeit und Zielerfüllung überprüft werden. Hierzu dient ein weiterer Übersichtsbildschirm. Die Wirksamkeit und Nachvollziehbarkeit ist in verschiedenen Klassen bewertbar. Darüber hinaus können Kommentare bei der Überprüfung erfasst werden. Zielsetzung der Wirksamkeitsprüfung ist ein periodischer Review der Kontrollen darüber, ob diese geeignet sind, auf die Kontrollziele positiv einzuwirken und so dem hinterlegten Risiko entgegenzuwirken.

[8. Auswertungen

Auswertungen werden im Standard bereits mit ausgeliefert:

- Übersicht über durchgeführte Kontrollen, Kontrollen im Verzug, Kontrollen, die im Freigabeprozess hängen mit Drill-Down-Möglichkeit.
- Aggregierte Sicht aus Prozess-, Legal- und Organisationsperspektive (Anzahl Kontrollen nach Priorität, Status, Anzahl dokumentationspflichtiger Kontrollen etc.).
- Wirksamkeitsauswertung: Darstellung der Wirksamkeitsbewertungen. Daneben kann innerhalb der Risikoauswertungen an diversen Stellen zu zugeordneten Kontrollen gesprungen werden, um deren Status zu prüfen und Detail-Informationen einzuholen.

[9. Benachrichtigung

antares RiMIS® bietet bereits zahlreiche, ereignisgesteuerte Benachrichtigungen, die für das IKS um folgende Benachrichtigungen erweitert werden:

- Automatische Benachrichtigung bei nahendem Kontrolltermin.
- Automatische Benachrichtigung bei Überschreitung des Kontrolltermins.
- Automatische Benachrichtigung bei deutlicher Überschreitung des Kontrolltermins.
- Manuelle Benachrichtigungsfunktion zur Kontaktierung des Kontroll-Verantwortlichen und des jeweiligen IKS-Managers. Diese Benachrichtigungen können vom Administrator aktiviert/deaktiviert werden. Die Parameter der Benachrichtigung, z. B. Karenzzeiten, werden zentral gepflegt.

[10. Berechtigung und Freigabeprozess

Die umfangreichen Berechtigungsfunktionen von antares RiMIS® werden auch im IKS-Bereich verwendet. So können User auf Legal-, Organisationseinheiten und Prozesse berechtigt werden. Hierbei wird wiederum eine Vererbung ermöglicht. Daneben werden pro User für die Default-Einstellung jeweils ein Prozess, eine Legaleinheit und eine Organisationseinheit definiert. Der IKS-Freigabeprozess unterscheidet sich von dem Freigabeprozess der Risiken, da es für einzelne Kontrollen, die ein User durchzuführen hat, verschiedene zuständige IKS-Manager geben kann. Die Unterscheidung kann in einer oder in mehreren Strukturen vorgenommen werden. So kann z. B. für den Einkaufsprozess ein anderer IKS-Manager zuständig sein als für den Verkaufsprozess, die Kontrolle aber von derselben Person durchgeführt werden.

[11. Berichtsheft-Integration

Für das in antares RiMIS® vorhandene Berichtsheft werden spezielle Versionen der Auswertungen geschaffen, mit denen entweder ein eigenständiges IKS-Berichtsheft erstellt werden kann oder aber der IKS-Bereich in den Risikomanagement-Bericht integriert wird. Dies obliegt dem User, der das Berichtsheft definiert.

[12. Ausblick

antares RiMIS® wird permanent weiterentwickelt. Zahlreiche Verbesserungsvorschläge von Kunden fließen in jede neue Version ein, Gleiches gilt natürlich für alle Erweiterungsmodule. Weitere Schritte bei der Entwicklung des IKS-Moduls können in folgende Richtungen gehen:

- Bewertung der Kosten und des Nutzens von Kontrollen, um die Effizienz zu prüfen und ggf. einzelne, nicht rechtlich bindende Kontrollen, durch effizientere Kontrollen zu ersetzen.
- Erweiterung der Auswertungsmöglichkeiten, um die Erfahrungsweitergabe zwischen verschiedenen legalen Einheiten zu erleichtern.
- Einführung eines Prozesses zum Vorschlagswesen, um aus individuellen Kontrollen einer Legaleinheit Standard-Kontrollen zu definieren.
- Erweiterung der dezentralen Administrationsfunktionen.

antares

[Software für sichere Entscheidungen]

[Software für sichere Entscheidungen]

antares Informations-Systeme GmbH
Stuttgarter Str. 99
D-73312 Geislingen

Tel. +49 7331 3076-0
Fax +49 7331 3076-76

www.antares-is.de
info@antares-is.de