

antares RiMIS®

[Softwarelösung für Governance,
Risk & Compliance



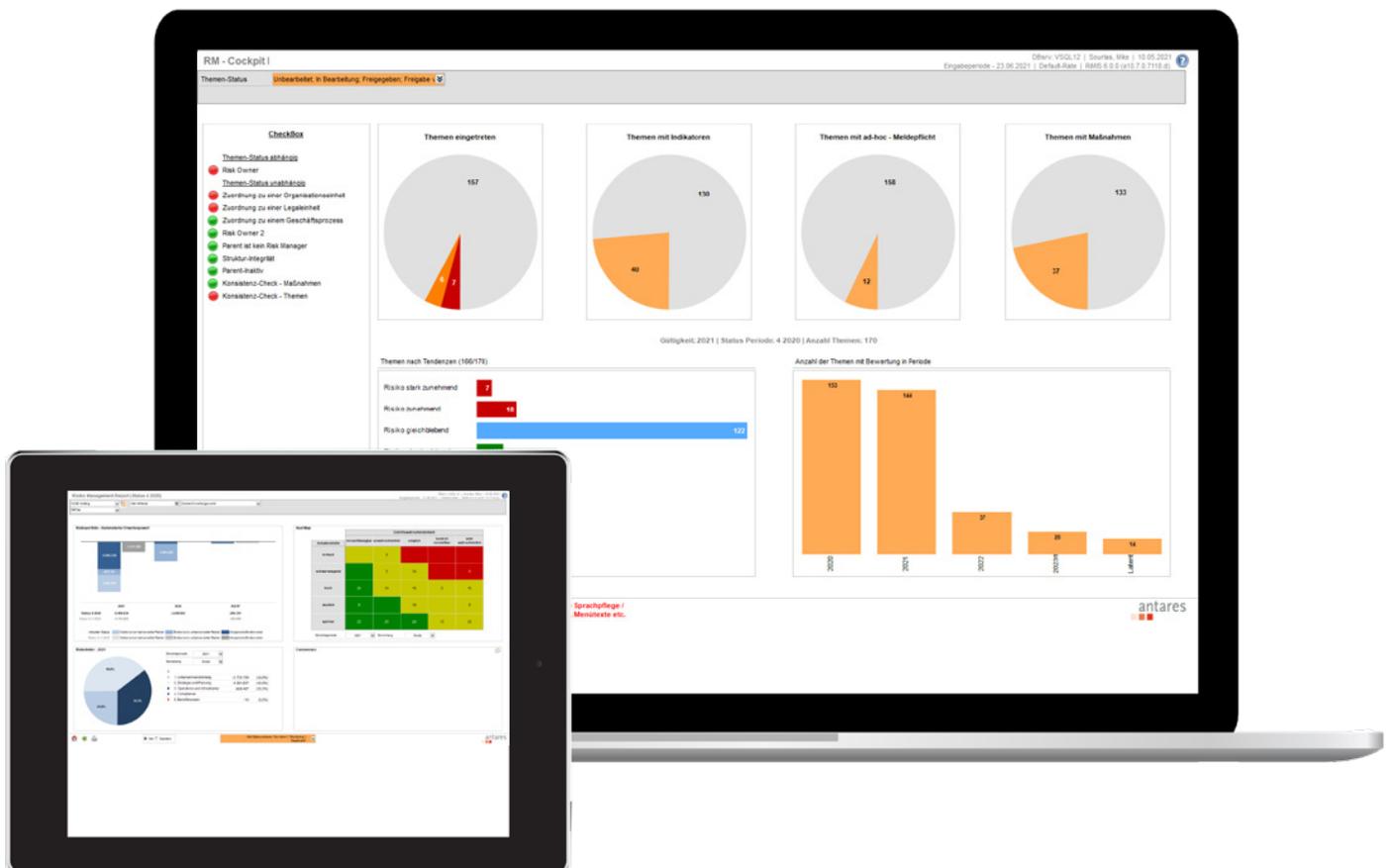
[Gefahren erkennen und Krisen bewältigen

Ein effektives Chancen- & Risikomanagement ist zu einem unverzichtbaren Teil einer erfolgreichen Unternehmensführung geworden. In Zeiten zunehmender Unsicherheit beschäftigen sich Führungskräfte und Risikomanager immer intensiver mit der Frage, wie Risiken den Geschäftsverlauf beeinflussen. Die Experten von heute entwickeln ganzheitliche Strategien zur Identifikation, Bewertung und Steuerung von Risiken über sämtliche Unternehmensbereiche hinweg.

Nur wer seine spezifischen Herausforderungen der Globalisierung und Digitalisierung kennt und auf Krisensituationen gut vorbereitet ist, kann auch die Chancen der Internationalisierung und neuer Technologien nutzen. Vor diesem Hintergrund haben wir die Softwarelösung für Chancen- und Risikomanagement antares RiMIS® entwickelt.

Mit unserer webbasierten Software haben Sie die Möglichkeit, Ihre Unternehmensrisiken frühzeitig zu erkennen, diesen wirkungsvoll entgegenzusteuern und Chancen für Ihr Unternehmen wahrzunehmen. Behalten Sie dank übersichtlicher Risikokataloge den Überblick über Ihr aktuelles Risikoportfolio und überwachen Sie dieses. Durch die Integration aller Unternehmensbereiche in den Risikomanagement-Prozess werden redundante Arbeiten vermieden und alle Aktionen, die zur Bewältigung von Risiken getroffen werden, einheitlich dokumentiert, geprüft und ausgewertet.

Die intuitive Oberflächenstruktur und der E-Mail-gestützte Workflow - von der Erfassung bis zum automatisch erstellten Risikobericht - sorgen für einen reibungslosen und effizienten Risikomanagement-Prozess. Selbsterklärende Cockpitansichten und Grafiken erleichtern den täglichen Umgang und sorgen für schnelle Ergebnisse z. B. durch Drill-Down-Methodik.



[Funktionen von antares RiMIS®

- Risikoidentifikation, Risikoanalyse, Bestimmung der Eintrittswahrscheinlichkeit für ein Risiko, Aggregation, Controlling, Risikoüberwachung und Risikobewältigung im Falle des Schadeneintritts.
- Workflowgestützte, periodische Beurteilung der Risikosituation.
Integrierte Fragebögen zur Risikoidentifikation und Selbsteinschätzung.
- Kommentierung von Themen auf "Administrator-Ebene" möglich.
- Quantitative und qualitative Bewertungsmethoden stehen zur Verfügung Erfüllung aller geltenden Vorschriften für das Risikomanagement (z. B. KonTraG, COSO II, ISO 31000, IDW (E) PS 981, IDW PS 340).
- Integrierbare Module für CIRS, IKS, ISMS, DSMS und Compliance-Management.
- Umfangreiche Customizing-Parameter für eine optimale Anpassung an individuelle Geschäftsprozesse und Anforderungen.
- Integrierter Berichtsheftgenerator: PDF oder PPT.
- Import und Export von Kennzahlen sowie E-Mail-Benachrichtigung bei Erreichen von Schwellenwerten (Push-Benachrichtigungen).
- Schnittstellen zu Vorsystemen und der Bestandsdatenimport für eine optimale Anbindung an bestehende IT-Umgebung.
- Ständige Verbesserungen des Tools durch den Wartungsvertrag.
- On-Premise- oder Cloud-basierte Lösung.



Chancen- und Risikomanagement



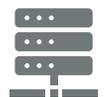
R-basierte Monte-Carlo-Simulation



Integriertes Frühwarnsystem



Modulare Erweiterbarkeit



Standardisierter Datentransfer

[Planen, analysieren und steuern leicht gemacht

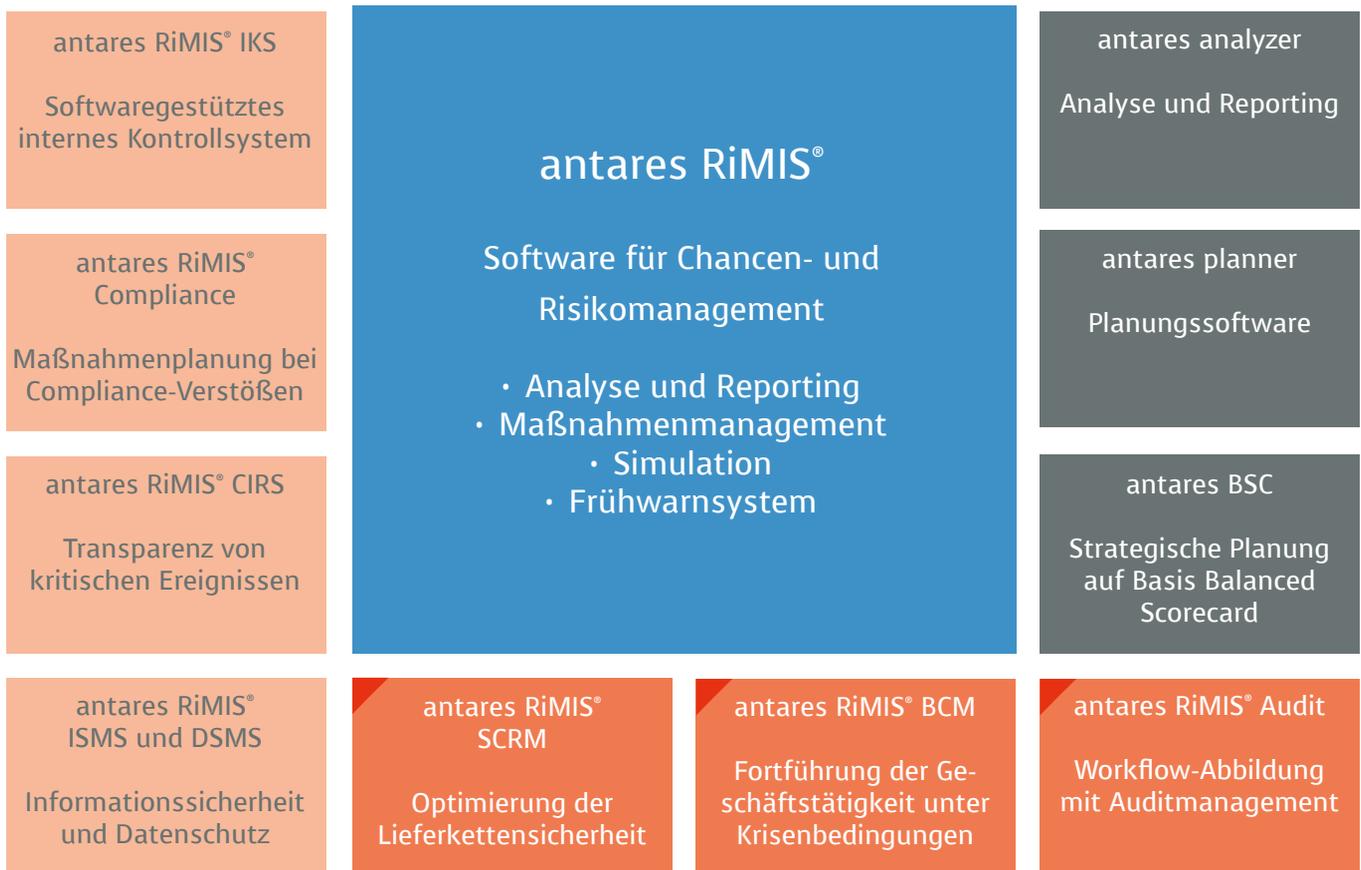
Die Software-Suite umfasst das Governance-, Risk- und Compliance-Management. Etablierte Standards werden ebenso berücksichtigt wie rechtliche und regulatorische Anforderungen. So behalten Sie stets den Überblick über Ihr aktuelles Risikoportfolio, überwachen und dokumentieren workflowgestützt interne Geschäftsprozesse und unterstützen die Organisation dabei, geltende Regeln, Gesetze und Normen einzuhalten.

Durch umfangreiche Customizing-Parameter kann die Anwendung exakt auf Ihre Unternehmensprozesse und Anforderungen angepasst werden. Der konfigurierbare Eingabe-Wizard, die intuitive Benutzeroberfläche mit vielfältigen ad hoc-Analysen sowie die integrierte Value at Risk-Simulation unterstützen Sie bei

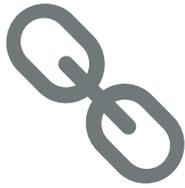
der Etablierung eines reibungslosen und revisions-sicheren Risikomanagement-Prozesses. Unsere langjährige Erfahrung bei der Entwicklung strategischer Informationssysteme garantiert eine optimale und sichere Prozessgestaltung. Benutzerfreundliche Funktionalitäten in der Anwendung und rollenbasierte Berechtigungskonzepte gewährleisten maßgeschneiderte Funktionalitäten.

Bedarfsgerecht und auf Ihren Unternehmensprozess abgestimmt, stehen Ihnen weitere Softwaremodule zur Verfügung. Diese sind sowohl integriert als auch unabhängig nutzbar.

[Modular erweiterbar – damit Sie rundum zufrieden sind



[Ihre Vorteile auf einen Blick



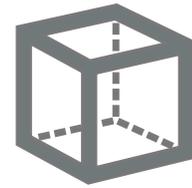
Förderung des Resilienz-Managements

Was passiert, wenn Risiken eingetreten sind? Ziel- und Strategieentwicklung zur Resilienz-Förderung. Widerstandsfähigkeit gegen Krisen. Analyse der Vulnerabilität und Anpassungsfähigkeit bei Krisensituationen. Entwicklung von Stärken zur Lösung von Problemen.



Förderung der internen Revision

IDW PS 340: Prüfung des Risiko-früherkennungssystems. Methoden zur Identifikation und Minderung der Risiken. Entwicklung von Absicherungsstrategien. Vorfälle untersuchen und Ursachen bestimmen.



Integrierte Simulation basierend auf R

Statistikorientierte Programmiersprache. Verschiedene Verteilungsfunktionen. Korrelation (inkl. Copula) und Berechnung des VaR mit Verbindung zu Ihrer GuV-Bilanz. Bestimmung von Risikoszenarien in Bezug auf ihre Eintrittswahrscheinlichkeit und Auswirkung auf die Erfolgsplanung.



Business Continuity Management (BCM)

Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung beim Geschäftsverlauf ernsthafte Schäden hervorrufen – zu schützen bzw. alternative Abläufe zu ermöglichen. Maßnahmen zur Identifikation, Überwachung und Bewältigung von Risiken bestimmen.



Zugelassen

Entspricht § 317 Abs. 4 HGB und dem Prüfungsstandard IDW PS 340, erfüllt die BilMoG-Anforderungen und bereitet den Weg, Verstößen gegen den Sarbanes-Oxley Act vorzubeugen. Berücksichtigt die Gesichtspunkte des KonTraG, ISO 31000, IDW (E) PS 981, COSO II sowie ONR 49000 und ÖNORM S 2410 und richtet sich nach der IEC 62198.



Fehlermöglichkeits- und Einflussanalyse (FMEA)

Ziel: Fehler und Risiken von vornherein vermeiden. Potenzielle Fehler- und Risikoursachen identifizieren. Kosten- und Nutzenoptimierung in der Entwicklungsphase. Präventive Fehler- und Risikovermeidung durch Ursache-Wirkungs-Diagramm.

[Transparente Prozesse mit antares RiMIS® IKS

Ein internes Kontrollsystem (IKS) dient der softwaregestützten internen Prozesskontrolle sowie der Dokumentation und Überwachung von Geschäftsprozessen in Unternehmen. Es bietet Schutz vor Missbrauchs- und Schadenshandlungen im Unternehmen und verhindert diese. Darüber hinaus beinhaltet ein IKS diverse Überwachungsmaßnahmen, die vor allem von der internen Revision durchgeführt werden.

Das IKS-Modul ist als integraler Bestandteil der antares RiMIS®-Softwarelösung konzipiert, sodass sich aus dem Zusammenspiel beider Komponenten positive Synergie-Effekte ergeben. Unter anderem können aufgrund der Webfähigkeit beliebig viele Personen dezentral auf das System zugreifen und sich permanent am Prozess beteiligen oder selbstständig Informationen einholen.

Dank der vollständigen Dokumentation der Prozesskontrollen und 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 Geschäftsorgane, darunter auch den Aufsichtsrat und die Geschäftsführung.

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. 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.



Internes Kontrollsystem



Systematischer Kontroll-Workflow



Berechtigungskonzept

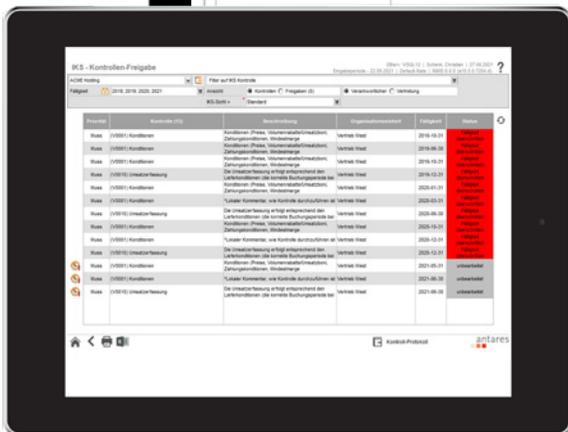
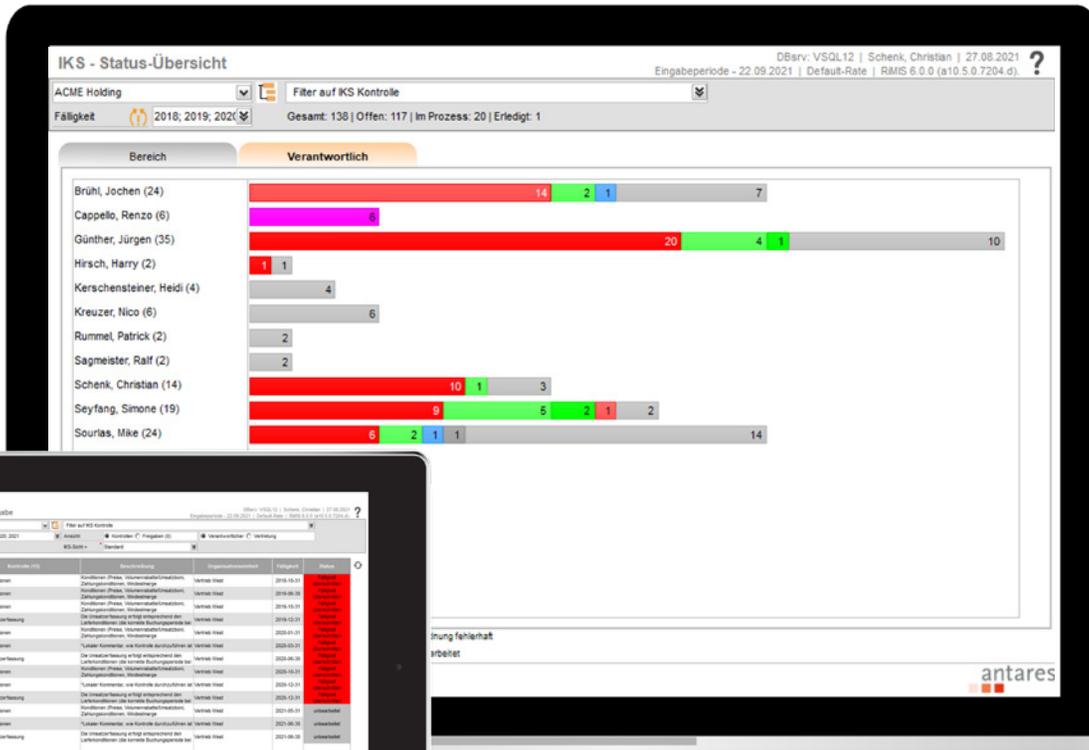


Sortierung der anstehenden Kontrollen



Komfortabler Berichtsheft-generator

Einblicke in antares RiMIS® IKS



[Kritische Ereignisse, Strukturen und Prozesse erkennen mit antares RiMIS® CIRS

Ein Critical Incident Reporting System (CIRS) dient der Erfassung von sicherheitsrelevanten und kritischen Ereignissen, die durch jeden Mitarbeiter des Unternehmens anonym gemeldet werden können. Das Ziel hierbei ist es, Schwachstellen in Prozessen und Strukturen offenzulegen und negative Auswirkungen durch wirksame Maßnahmen zu vermeiden. Das System hilft außerdem dabei, die Qualität des Betriebsablaufs durch Fehlervermeidung aufzuwerten und aus Erfahrungen zu lernen.

Das Meldesystem zur Erfassung von sicherheitsrelevanten und kritischen Ereignissen basiert auf der Erkenntnis, dass zwischen leichten/schweren Vorfällen und Beinahe-Zwischenfällen ein zahlenmäßiger Zusammenhang besteht. Unerwünschte Ereignisse im Unternehmensalltag werden aufgrund ihrer hohen Eintrittswahrscheinlichkeit als zweifelhaft wahrgenommen und stellen somit ein hohes Risiko für Unternehmen dar. Die Vermeidung von kritischen Ereignissen durch Bearbeitung der CIRS-Fälle und die dementsprechende Maßnahmenplanung soll die Eintrittswahrscheinlichkeit folgenschwerer Zwischenfälle verringern.

Bei uns spielt der Schutz des Melders eine zentrale Rolle. Unser Meldesystem antares RiMIS® CIRS arbeitet auf einer komplett anonymen Basis. Da Login-Informationen nicht gespeichert werden, können weder der Meldende noch das Unternehmen oder der Geschädigte anhand der Daten zurückverfolgt werden.

Der Meldende füllt das Formular über den Vorfall anonym aus und kann bereits dort Verbesserungsvorschläge hinzufügen. Freigegebene Berichte werden tabellarisch aufgelistet und können in einer Detailansicht betrachtet werden. Die Durchführung von Kontrollen wird dem Kontroll-Manager automatisiert mitgeteilt.



Anonymes Meldesystem



Ableiten von Verbesserungen und Empfehlungen



Selbsterklärende Eingabemasken

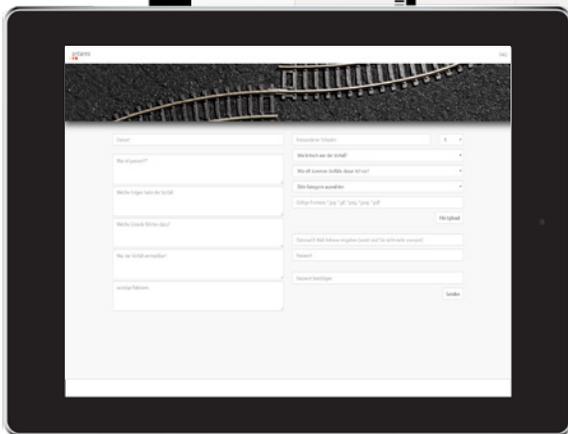
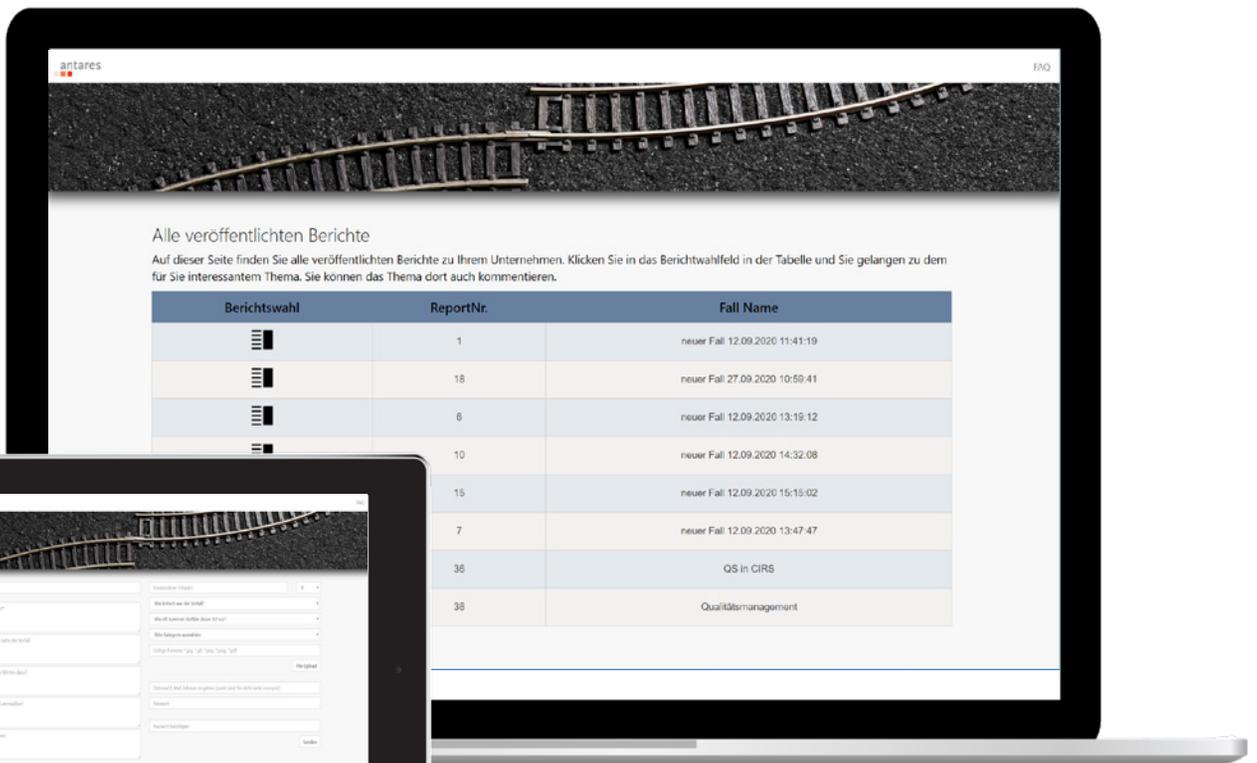
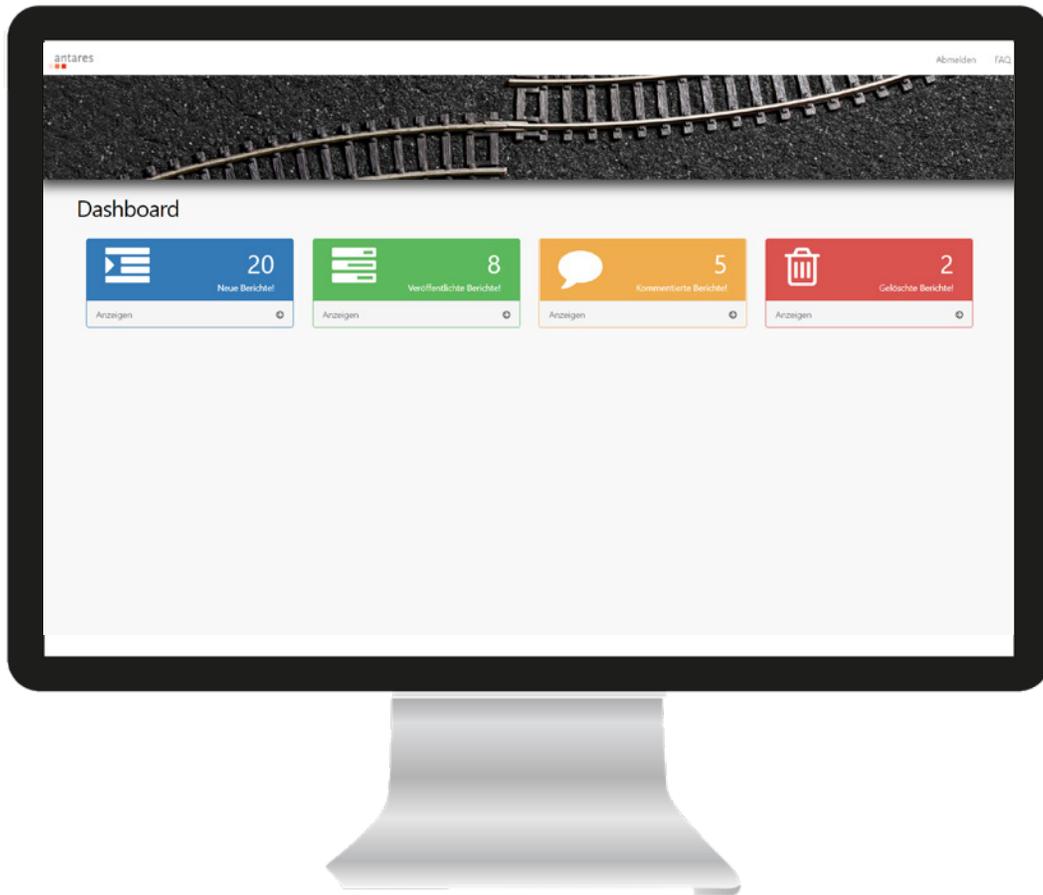


Übersichtliches Verzeichnis aller veröffentlichten Berichte



E-Mail-Benachrichtigung beim Eingang eines Berichts

[Einblicke in antares RiMIS® CIRS



[Maßnahmenplanung bei Compliance-Verstößen mit antares RiMIS® Compliance

Das Thema Compliance betrifft alle Mitarbeiter in jedem Unternehmen! Dennoch ist die Unternehmensführung stärker im Fokus, weil die Sicherstellung gesetzeskonformen Verhaltens Bestandteil der unternehmerischen Organisationspflicht ist. Dabei geht es nicht nur um die Einhaltung von gesetzlichen und vertraglichen Regeln, sondern auch um das Einhalten unternehmensinterner Richtlinien.

Damit die Anforderungen des Compliance-Standards erfüllt werden, muss ein Unternehmen ein systematisches, unternehmensweites Compliance-Managementsystem einführen, dokumentieren, verwirklichen und aufrechterhalten. Compliance- und Datenschutz-Beauftragte sowie Beauftragte für integrierte Managementsysteme müssen geeignete Maßnahmen ergreifen, die eine ständige Aufsicht und Kontrolle ermöglichen.

Neben den unzähligen ungeschriebenen Sorgfaltspflichten gibt es Hunderte weitere Vorschriften und Regeln, die weitere Pflichten normieren, z. B. aus den Bereichen Arbeitssicherheit, IT-Compliance, Datenschutz, Finance & Tax, betrieblicher Umweltschutz oder Betriebsgenehmigungen.

Ziel unseres Compliance-Managementsystems ist es, im Unternehmen systematisch alle Voraussetzungen zu schaffen, sodass Verstöße gegen definierte Pflichten vermieden bzw. minimiert werden. Es hilft dabei, eingetretene Verstöße zu erkennen und zu behandeln. antares RiMIS® Compliance ist ein integraler Bestandteil der antares RiMIS®-Software. Aus dem Zusammenspiel mit den Lösungskomponenten IKS, ISMS, DSMS und CIRS ergibt sich eine leistungsstarke Risikomanagement-Lösung.



Compliance-
Managementsystem



Vermeidung von
Compliance-Verstößen



Erfüllung der ISO
19600-Norm

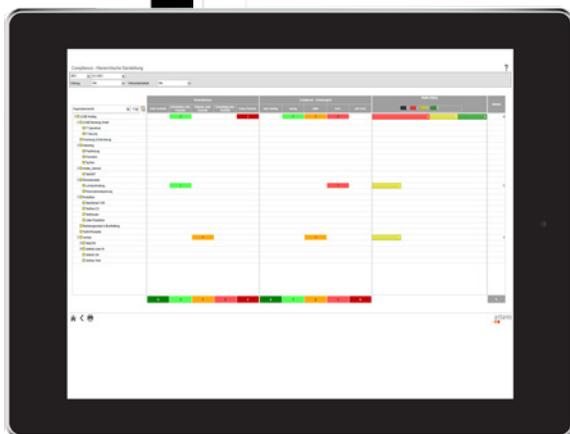
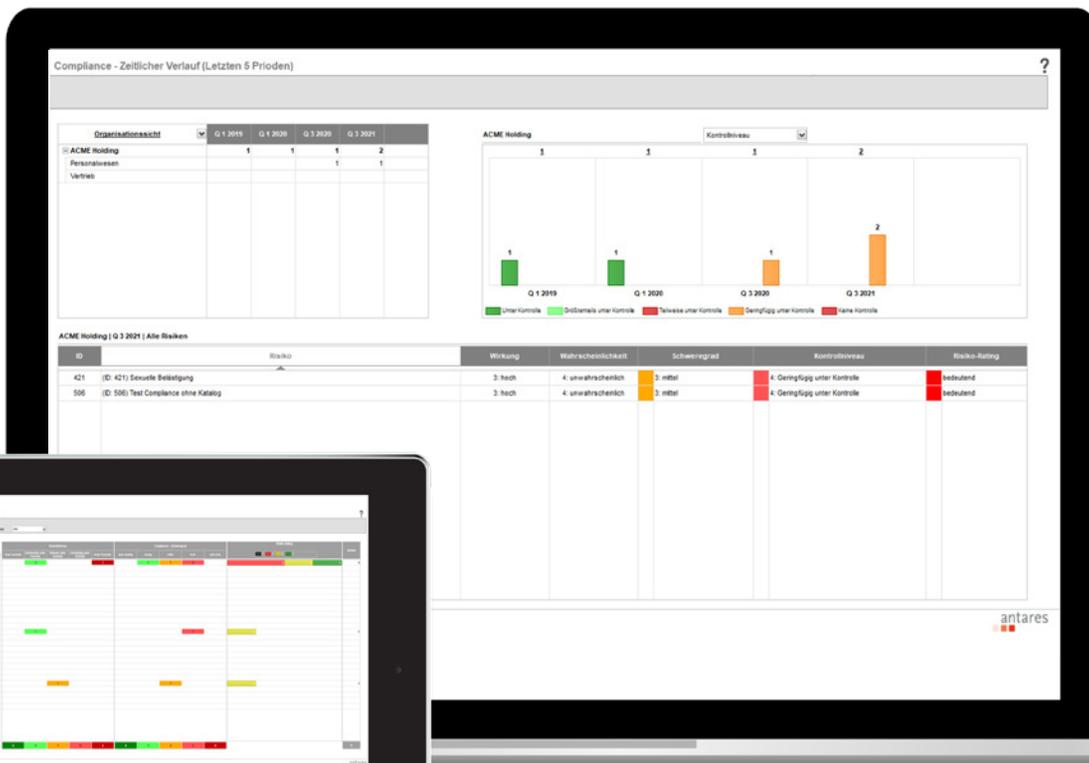
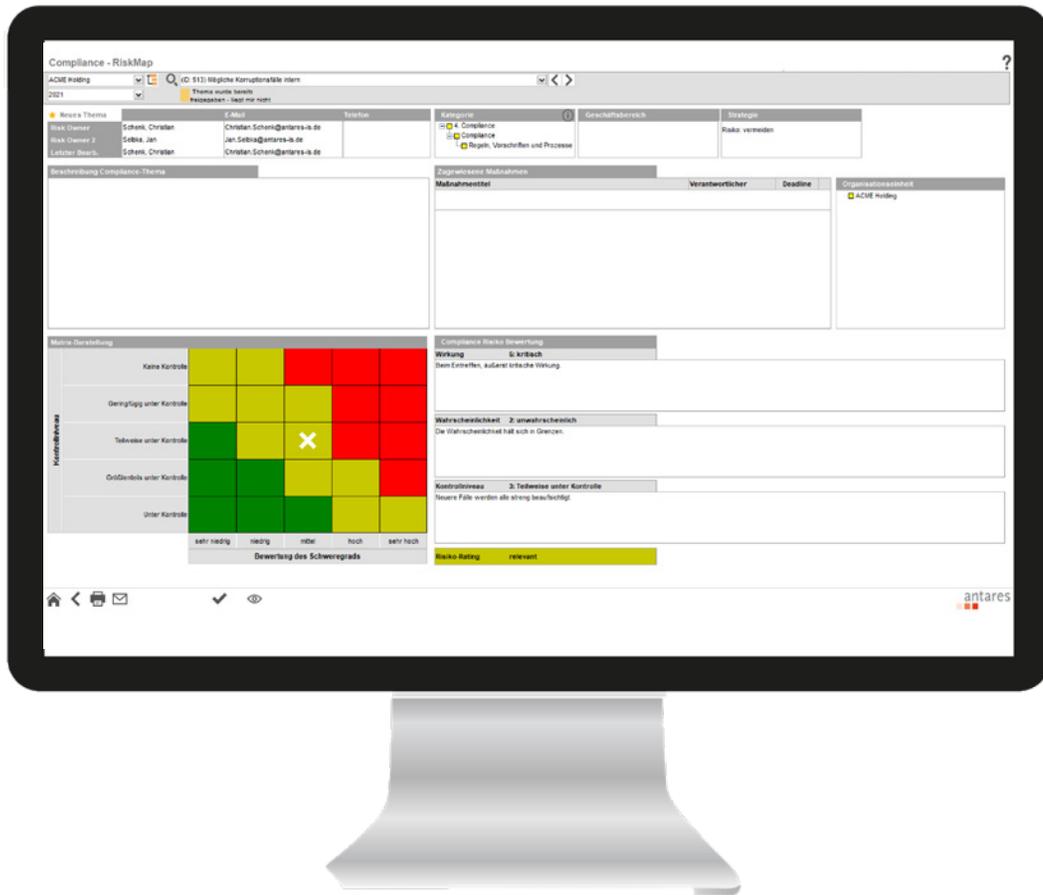


Anbindung an weitere
Module



Webfähigkeit

[Einblicke in antares RiMIS® Compliance



[Datenschutz-Management nach DSGVO mit antares RiMIS® DSMS

Immer umfassender werdende Datenschutz-Regulierungen sowie stetig zunehmende Gesetze und Vorschriften stellen Unternehmen vor große Herausforderungen beim Umgang mit personenbezogenen Daten. Mit der Europäischen Datenschutz-Grundverordnung, die seit Mai 2018 verbindlich ist, haben die Themen Informationssicherheit und Datenschutz an Bedeutung gewonnen. Das bisher im Bundesdatenschutzgesetz (BDSG) enthaltene Datenschutzrecht inkl. Regelungen zur Verarbeitung personenbezogener Daten wurden somit weitgehend durch die der Grundverordnung ersetzt bzw. erweitert.

Alle Unternehmen, die personenbezogene Daten erheben und verarbeiten, sind somit verpflichtet, alle Strukturen und Prozesse zur Implementierung des EU-weit einheitlich geltenden Datenschutzes anzupassen. Im Falle einer Überprüfung muss ein Nachweis darüber erbracht werden, dass geeignete Maßnahmen zur Einhaltung der Anforderungen der Grundverordnung ergriffen werden. Bei einem Verstoß drohen empfindliche Bußgelder, im Extremfall bis zu 4 % des Jahresumsatzes.

Wir helfen Ihnen dabei, die neuen Vorgaben der Datenschutz-Grundverordnung zur Auftragsverarbeitung in Ihrem Unternehmen zu meistern sowie neue Prozesse und Strukturen zu etablieren. Hierfür bietet es sich an, die Datenschutzrichtlinien in das vorhandene Informationssicherheits-Managementsystem (ISMS) zu integrieren. Dadurch entsteht ein ganzheitliches Datenschutz-Managementsystem.

Unser DSMS auf Basis der Europäischen Grundverordnung und der ISO 27001 oder/und IT-Grundschutz etabliert anerkannte Verfahren, mit welchen Prozesse und Richtlinien in einem Unternehmen methodisch eingeführt werden. Diese Richtlinien ermöglichen die rechtzeitige Erkennung der Risiken für Datenschutzverstöße. Das Ziel dabei ist es, mithilfe aller technischen und organisatorischen Maßnahmen deren Steuerung, Kontrolle und permanente Verbesserung zu ermöglichen. Die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von IT-Systemen und -Diensten in Bezug auf die Datenverarbeitung wird dabei ähnlich wie bei einem ISMS umgesetzt.



Zuverlässiger Schutz der Unternehmensdaten



Nachhaltige, ganzheitliche Risikominimierung



Absicherung der Unternehmenswerte

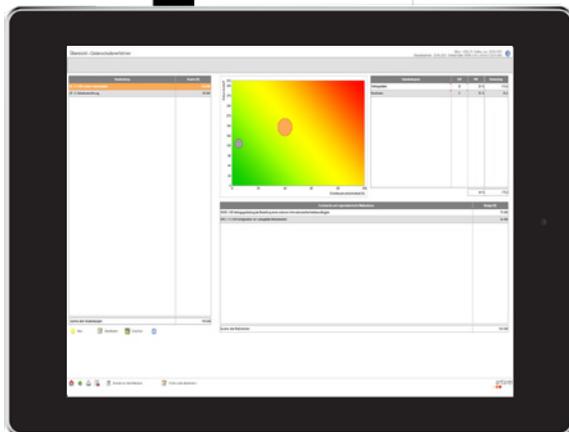
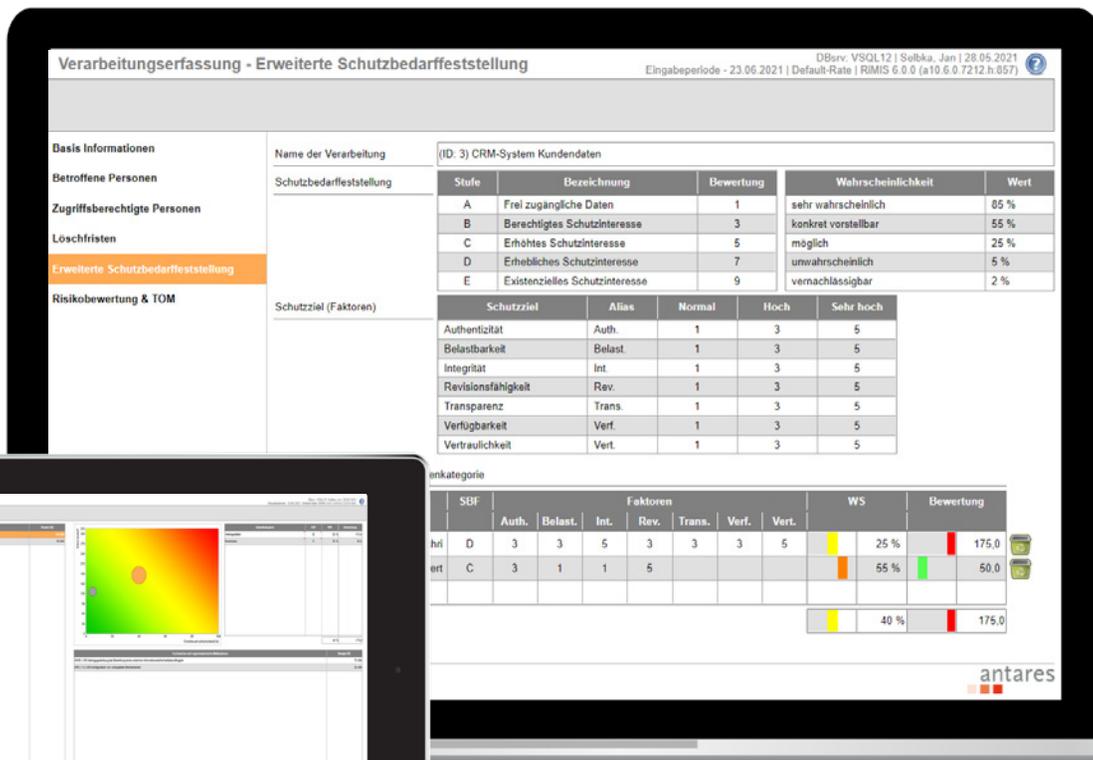
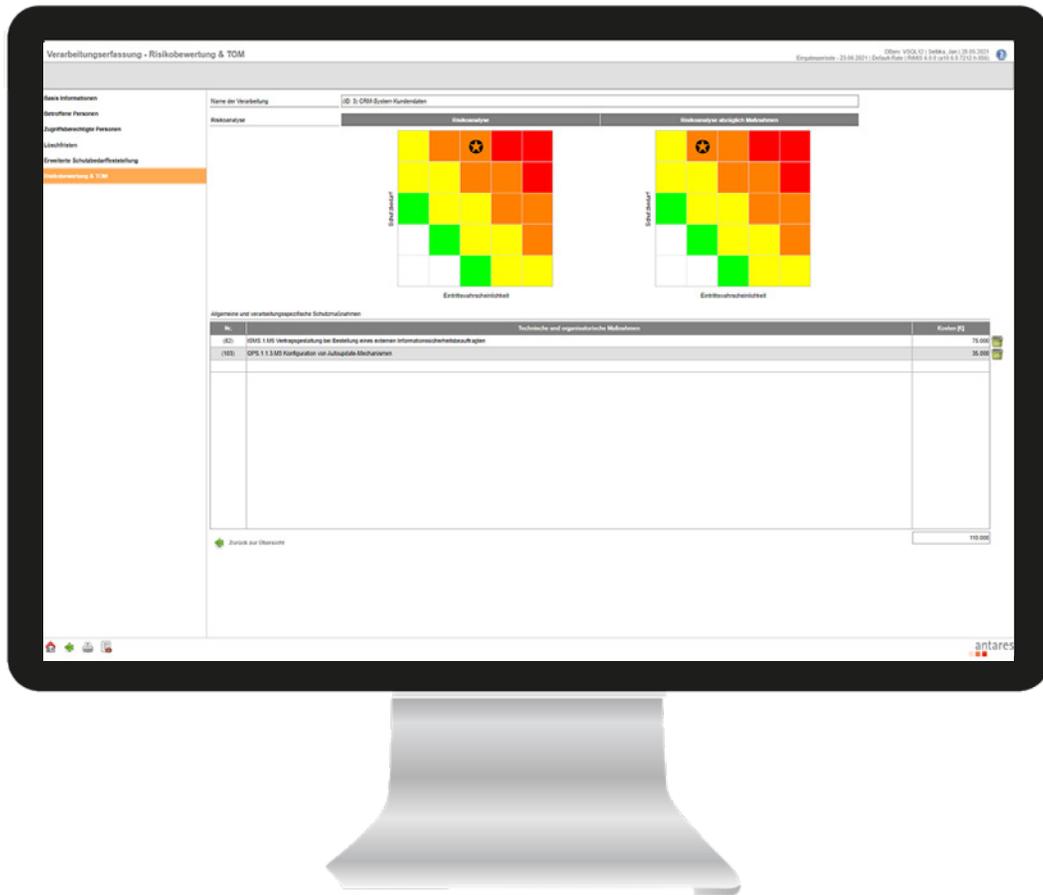


Revisionsichere Dokumentation der Aktivitäten



Compliance gegenüber Geschäftspartnern, Kunden, etc.

[Einblicke in antares RiMIS® DSMS



[Informationssicherheits-Management mit antares RiMIS® ISMS

Informationen sind wertvolle Unternehmenswerte, die geschützt werden müssen. Die Bedeutung von Informationen und deren Schutz ist mittlerweile höchste Priorität in Unternehmen. Nicht zuletzt wegen der zunehmenden Bedrohung durch Datendiebstahl, Hacker- und Cyber-Angriffe sowie das Inkrafttreten des IT-Sicherheitsgesetzes (IT-SiG).

Die Unternehmensleitung trägt die Verantwortung dafür, dass geeignetes Maßnahmenmanagement betrieben und damit die Erfüllung der Sicherheitsziele gewährleistet wird. Dabei geben diverse Standards, wie ISO-27001, einen Bezugsrahmen vor, um die Einführung eines Informationssicherheits-Managementsystems zu unterstützen. Wichtig ist, Informationssicherheit direkt in die Geschäftsprozesse einzubinden und dort zu beobachten, welche Informationen fließen und geschützt werden müssen.

Unser ISMS stellt Verfahren und Regeln nach ISO 27001 im Unternehmen auf, um die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten sowie fortwährend zu verbessern. Mithilfe der Anwendung lassen sich Informationssicherheitsrisiken identifizieren, bewerten und zielgerichtet reduzieren. Nutzen Sie antares RiMIS® ISMS als verlässliche Informationsbasis zur Ableitung wichtiger Schutzmaßnahmen und zur Einführung einer Informationssicherheitskultur in Ihrem Unternehmen.

Für Automobilhersteller und -zulieferer, die eine TISAX®-Zertifizierung anstreben, stellen wir antares RiMIS® ISMS mit integriertem VDA ISA-Katalog sowie dem Grundschutzkatalog des BSI zur Verfügung. Somit können bereits vor Antritt des Audits Schwachstellen festgestellt und erkannte Gaps geschlossen werden.



Managementsystem für Informationssicherheit



ISO 27001 & BSI IT-Grundschutz-Zertifizierung



Gewährleistung der Schutzziele

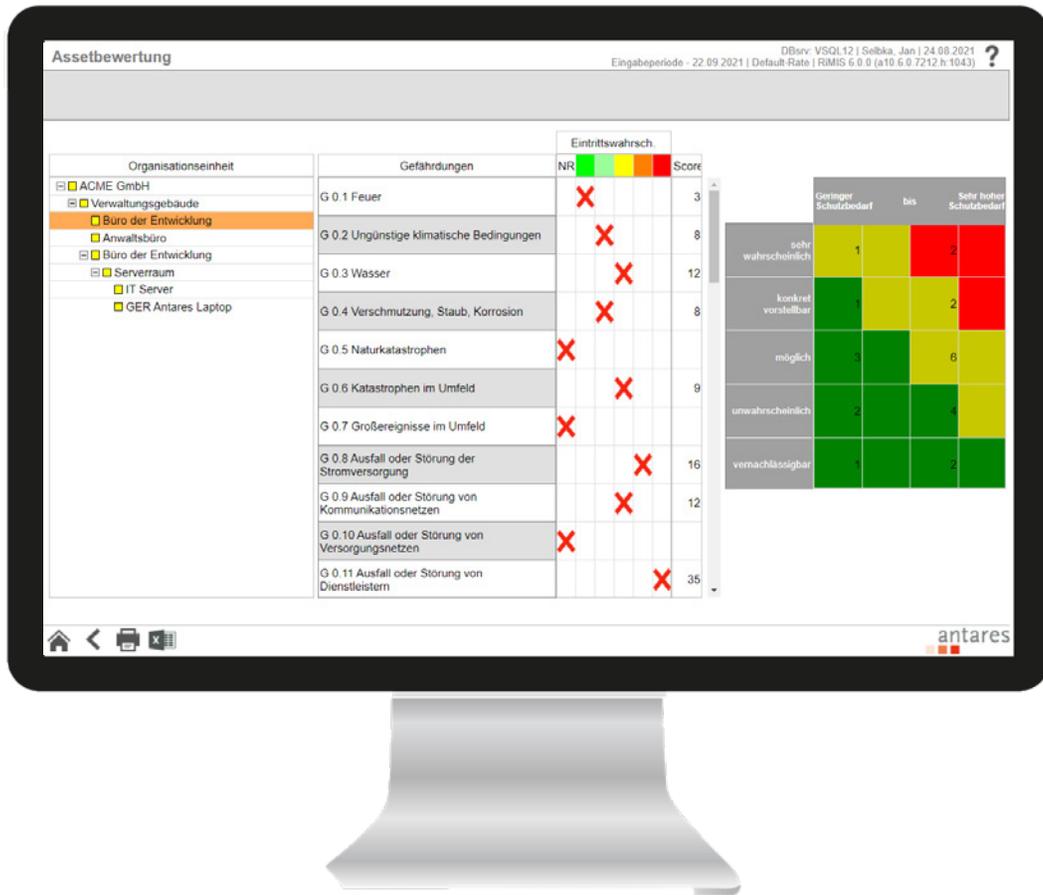


Vergabe von Berechtigungsrollen



Dezentraler Zugriff dank Webfähigkeit

[Einblicke in antares RiMIS® ISMS



Relevante Anforderungen | Eingabeperiode - 23.08.2021 | DBSV: VSQL12 | Seibka, Jan | 24.08.2021

Anforderung	Umsetzungsgrad	Wirksamkeit	Kommentar
<ul style="list-style-type: none"> APP1.1 Office-Produkte G 0.21 Manipulation von Hard- oder Software Geringer Einsatz von Erweiterungen für Office-Produkte testen neuer Versionen von Office-Produkten G 0.28 Software-Schwachstellen oder -Patches regelmäßiger Einsatz von Erweiterungen für Office-Produkte Regelung der Software-Entwicklung durch Code-Reviews testen neuer Versionen von Office-Produkten Verwendung von Virenschutz APP1.2 Videokonferenzen G 0.14 Ausfällen von Informationen (Sprache) Datensensibilität in Videokonferenzen Unterstützung sicherer Verschlüsselung der Kommunikation Verwendung des privaten Modus Verwendung von vertrauenswürdigem Zeitaltern APP2.1 Allgemeiner Videokonferenzen G 0.18 Ausfall oder Störung von Dienstleistungen Ermittlung von Zugriffsberechtigungen auf Videokonferenzen Erstellung eines Notfallplans für den Ausfall eines Videokonferenzdienstes Planung des Einsatzes von Videokonferenzdiensten Planung einer Notfallübung und Regularien im Videokonferenzdienst Sichere Konfiguration und Konfigurationsänderungen von Videokonferenzdiensten Sicherer Betrieb von Videokonferenzdiensten G 0.21 Fehlerhafte Nutzung oder Administration von Geräten und Systemen Erhöhung der Kommunikation mit Videokonferenzdiensten Ermittlung von Zugriffsberechtigungen auf Videokonferenzdienste Erstellung einer Sicherheitsrichtlinie für Videokonferenzdienste Regelmäßige Updates/Installation eines Videokonferenzdienstes Migration von Videokonferenzdiensten 	Überwiegend umgesetzt Überwiegend umgesetzt Teilweise umgesetzt Nicht umgesetzt	Mäßig wirksam Mäßig wirksam Wirkung Nicht wirksam	Automatische Updates Weitere Aktionen erforderlich Neuer Funktionen einrigig Bisher kein Ansatz gefunden MA in Urlaub Test Kommentar

Kompetenzen

Standard	Beschreibung
ISO 27001:2017	Informationssicherheitsmanagement
ISO 27002:2017	Informationssicherheitsmaßnahmen
ISO 27005:2018	Informationssicherheitsrisikomanagement
ISO 27031:2018	Informationssicherheitsresilienz
ISO 27032:2018	Informationssicherheitspersönlichkeit
ISO 27033:2018	Informationssicherheitsgesetzgebung
ISO 27034:2018	Informationssicherheitssoftwareentwicklung
ISO 27035:2018	Informationssicherheitsvorfälle
ISO 27036:2018	Informationssicherheitsbeziehungen
ISO 27037:2018	Informationssicherheitsforensik
ISO 27038:2018	Informationssicherheitsgesetzgebung
ISO 27039:2018	Informationssicherheitsgesetzgebung
ISO 27040:2018	Informationssicherheitsgesetzgebung
ISO 27041:2018	Informationssicherheitsgesetzgebung
ISO 27042:2018	Informationssicherheitsgesetzgebung
ISO 27043:2018	Informationssicherheitsgesetzgebung
ISO 27044:2018	Informationssicherheitsgesetzgebung
ISO 27045:2018	Informationssicherheitsgesetzgebung
ISO 27046:2018	Informationssicherheitsgesetzgebung
ISO 27047:2018	Informationssicherheitsgesetzgebung
ISO 27048:2018	Informationssicherheitsgesetzgebung
ISO 27049:2018	Informationssicherheitsgesetzgebung
ISO 27050:2018	Informationssicherheitsgesetzgebung
ISO 27051:2018	Informationssicherheitsgesetzgebung
ISO 27052:2018	Informationssicherheitsgesetzgebung
ISO 27053:2018	Informationssicherheitsgesetzgebung
ISO 27054:2018	Informationssicherheitsgesetzgebung
ISO 27055:2018	Informationssicherheitsgesetzgebung
ISO 27056:2018	Informationssicherheitsgesetzgebung
ISO 27057:2018	Informationssicherheitsgesetzgebung
ISO 27058:2018	Informationssicherheitsgesetzgebung
ISO 27059:2018	Informationssicherheitsgesetzgebung
ISO 27060:2018	Informationssicherheitsgesetzgebung
ISO 27061:2018	Informationssicherheitsgesetzgebung
ISO 27062:2018	Informationssicherheitsgesetzgebung
ISO 27063:2018	Informationssicherheitsgesetzgebung
ISO 27064:2018	Informationssicherheitsgesetzgebung
ISO 27065:2018	Informationssicherheitsgesetzgebung
ISO 27066:2018	Informationssicherheitsgesetzgebung
ISO 27067:2018	Informationssicherheitsgesetzgebung
ISO 27068:2018	Informationssicherheitsgesetzgebung
ISO 27069:2018	Informationssicherheitsgesetzgebung
ISO 27070:2018	Informationssicherheitsgesetzgebung
ISO 27071:2018	Informationssicherheitsgesetzgebung
ISO 27072:2018	Informationssicherheitsgesetzgebung
ISO 27073:2018	Informationssicherheitsgesetzgebung
ISO 27074:2018	Informationssicherheitsgesetzgebung
ISO 27075:2018	Informationssicherheitsgesetzgebung
ISO 27076:2018	Informationssicherheitsgesetzgebung
ISO 27077:2018	Informationssicherheitsgesetzgebung
ISO 27078:2018	Informationssicherheitsgesetzgebung
ISO 27079:2018	Informationssicherheitsgesetzgebung
ISO 27080:2018	Informationssicherheitsgesetzgebung
ISO 27081:2018	Informationssicherheitsgesetzgebung
ISO 27082:2018	Informationssicherheitsgesetzgebung
ISO 27083:2018	Informationssicherheitsgesetzgebung
ISO 27084:2018	Informationssicherheitsgesetzgebung
ISO 27085:2018	Informationssicherheitsgesetzgebung
ISO 27086:2018	Informationssicherheitsgesetzgebung
ISO 27087:2018	Informationssicherheitsgesetzgebung
ISO 27088:2018	Informationssicherheitsgesetzgebung
ISO 27089:2018	Informationssicherheitsgesetzgebung
ISO 27090:2018	Informationssicherheitsgesetzgebung
ISO 27091:2018	Informationssicherheitsgesetzgebung
ISO 27092:2018	Informationssicherheitsgesetzgebung
ISO 27093:2018	Informationssicherheitsgesetzgebung
ISO 27094:2018	Informationssicherheitsgesetzgebung
ISO 27095:2018	Informationssicherheitsgesetzgebung
ISO 27096:2018	Informationssicherheitsgesetzgebung
ISO 27097:2018	Informationssicherheitsgesetzgebung
ISO 27098:2018	Informationssicherheitsgesetzgebung
ISO 27099:2018	Informationssicherheitsgesetzgebung
ISO 27100:2018	Informationssicherheitsgesetzgebung
ISO 27101:2018	Informationssicherheitsgesetzgebung
ISO 27102:2018	Informationssicherheitsgesetzgebung
ISO 27103:2018	Informationssicherheitsgesetzgebung
ISO 27104:2018	Informationssicherheitsgesetzgebung
ISO 27105:2018	Informationssicherheitsgesetzgebung
ISO 27106:2018	Informationssicherheitsgesetzgebung
ISO 27107:2018	Informationssicherheitsgesetzgebung
ISO 27108:2018	Informationssicherheitsgesetzgebung
ISO 27109:2018	Informationssicherheitsgesetzgebung
ISO 27110:2018	Informationssicherheitsgesetzgebung
ISO 27111:2018	Informationssicherheitsgesetzgebung
ISO 27112:2018	Informationssicherheitsgesetzgebung
ISO 27113:2018	Informationssicherheitsgesetzgebung
ISO 27114:2018	Informationssicherheitsgesetzgebung
ISO 27115:2018	Informationssicherheitsgesetzgebung
ISO 27116:2018	Informationssicherheitsgesetzgebung
ISO 27117:2018	Informationssicherheitsgesetzgebung
ISO 27118:2018	Informationssicherheitsgesetzgebung
ISO 27119:2018	Informationssicherheitsgesetzgebung
ISO 27120:2018	Informationssicherheitsgesetzgebung
ISO 27121:2018	Informationssicherheitsgesetzgebung
ISO 27122:2018	Informationssicherheitsgesetzgebung
ISO 27123:2018	Informationssicherheitsgesetzgebung
ISO 27124:2018	Informationssicherheitsgesetzgebung
ISO 27125:2018	Informationssicherheitsgesetzgebung
ISO 27126:2018	Informationssicherheitsgesetzgebung
ISO 27127:2018	Informationssicherheitsgesetzgebung
ISO 27128:2018	Informationssicherheitsgesetzgebung
ISO 27129:2018	Informationssicherheitsgesetzgebung
ISO 27130:2018	Informationssicherheitsgesetzgebung
ISO 27131:2018	Informationssicherheitsgesetzgebung
ISO 27132:2018	Informationssicherheitsgesetzgebung
ISO 27133:2018	Informationssicherheitsgesetzgebung
ISO 27134:2018	Informationssicherheitsgesetzgebung
ISO 27135:2018	Informationssicherheitsgesetzgebung
ISO 27136:2018	Informationssicherheitsgesetzgebung
ISO 27137:2018	Informationssicherheitsgesetzgebung
ISO 27138:2018	Informationssicherheitsgesetzgebung
ISO 27139:2018	Informationssicherheitsgesetzgebung
ISO 27140:2018	Informationssicherheitsgesetzgebung
ISO 27141:2018	Informationssicherheitsgesetzgebung
ISO 27142:2018	Informationssicherheitsgesetzgebung
ISO 27143:2018	Informationssicherheitsgesetzgebung
ISO 27144:2018	Informationssicherheitsgesetzgebung
ISO 27145:2018	Informationssicherheitsgesetzgebung
ISO 27146:2018	Informationssicherheitsgesetzgebung
ISO 27147:2018	Informationssicherheitsgesetzgebung
ISO 27148:2018	Informationssicherheitsgesetzgebung
ISO 27149:2018	Informationssicherheitsgesetzgebung
ISO 27150:2018	Informationssicherheitsgesetzgebung
ISO 27151:2018	Informationssicherheitsgesetzgebung
ISO 27152:2018	Informationssicherheitsgesetzgebung
ISO 27153:2018	Informationssicherheitsgesetzgebung
ISO 27154:2018	Informationssicherheitsgesetzgebung
ISO 27155:2018	Informationssicherheitsgesetzgebung
ISO 27156:2018	Informationssicherheitsgesetzgebung
ISO 27157:2018	Informationssicherheitsgesetzgebung
ISO 27158:2018	Informationssicherheitsgesetzgebung
ISO 27159:2018	Informationssicherheitsgesetzgebung
ISO 27160:2018	Informationssicherheitsgesetzgebung
ISO 27161:2018	Informationssicherheitsgesetzgebung
ISO 27162:2018	Informationssicherheitsgesetzgebung
ISO 27163:2018	Informationssicherheitsgesetzgebung
ISO 27164:2018	Informationssicherheitsgesetzgebung
ISO 27165:2018	Informationssicherheitsgesetzgebung
ISO 27166:2018	Informationssicherheitsgesetzgebung
ISO 27167:2018	Informationssicherheitsgesetzgebung
ISO 27168:2018	Informationssicherheitsgesetzgebung
ISO 27169:2018	Informationssicherheitsgesetzgebung
ISO 27170:2018	Informationssicherheitsgesetzgebung
ISO 27171:2018	Informationssicherheitsgesetzgebung
ISO 27172:2018	Informationssicherheitsgesetzgebung
ISO 27173:2018	Informationssicherheitsgesetzgebung
ISO 27174:2018	Informationssicherheitsgesetzgebung
ISO 27175:2018	Informationssicherheitsgesetzgebung
ISO 27176:2018	Informationssicherheitsgesetzgebung
ISO 27177:2018	Informationssicherheitsgesetzgebung
ISO 27178:2018	Informationssicherheitsgesetzgebung
ISO 27179:2018	Informationssicherheitsgesetzgebung
ISO 27180:2018	Informationssicherheitsgesetzgebung
ISO 27181:2018	Informationssicherheitsgesetzgebung
ISO 27182:2018	Informationssicherheitsgesetzgebung
ISO 27183:2018	Informationssicherheitsgesetzgebung
ISO 27184:2018	Informationssicherheitsgesetzgebung
ISO 27185:2018	Informationssicherheitsgesetzgebung
ISO 27186:2018	Informationssicherheitsgesetzgebung
ISO 27187:2018	Informationssicherheitsgesetzgebung
ISO 27188:2018	Informationssicherheitsgesetzgebung
ISO 27189:2018	Informationssicherheitsgesetzgebung
ISO 27190:2018	Informationssicherheitsgesetzgebung
ISO 27191:2018	Informationssicherheitsgesetzgebung
ISO 27192:2018	Informationssicherheitsgesetzgebung
ISO 27193:2018	Informationssicherheitsgesetzgebung
ISO 27194:2018	Informationssicherheitsgesetzgebung
ISO 27195:2018	Informationssicherheitsgesetzgebung
ISO 27196:2018	Informationssicherheitsgesetzgebung
ISO 27197:2018	Informationssicherheitsgesetzgebung
ISO 27198:2018	Informationssicherheitsgesetzgebung
ISO 27199:2018	Informationssicherheitsgesetzgebung
ISO 27200:2018	Informationssicherheitsgesetzgebung

[Unsere Success Story: INTERSPORT – Risikomanagement im Sportfachhandel

Aufgabenstellung

Vor der Einführung von antares RiMIS® wurde das Risikomanagement bei INTERSPORT über eine Excel-Lösung abgebildet.

Nach langjährigem Einsatz der relativ aufwendigen zu bedienenden Microsoft-Variante hat INTERSPORT 2012 nach einer geeigneten und flexiblen Software gesucht, die zum Unternehmen passt und alle Anforderungen am besten abdeckt.

Lösung

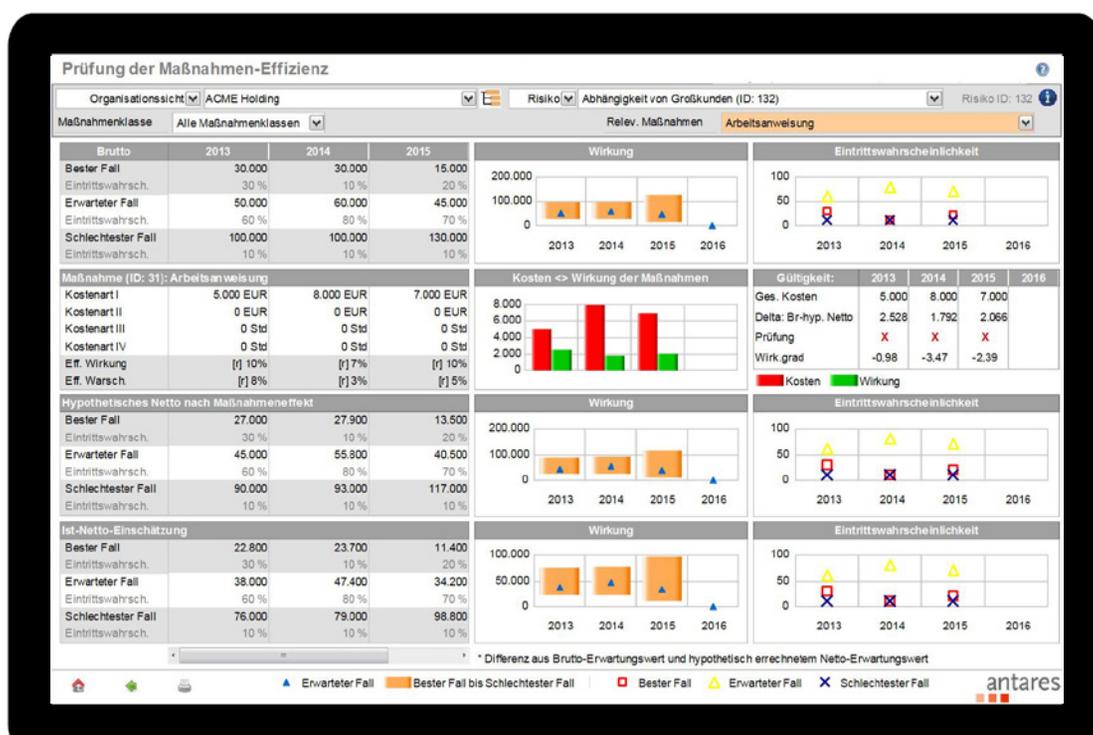
Nach intensiver Auswahlphase hat sich INTERSPORT für antares RiMIS® entschieden, zumal die Software den größten Deckungsgrad zu den gestellten Anforderungen hatte.

Die Flexibilität der Einstellungen war ein wichtiger Faktor bei der Entscheidungsfindung.

Umso wichtiger hat das hohe kundenorientierte Servicelevel von Anfang an überzeugt. Der direkte Draht zum Support und zur Entwicklung half dabei, neue Anforderungen in den Standard einzubauen.

Die vorgedachten Prozesse kommen aus der Praxis und sind zudem flexibel anpassbar. Eine Softwarelösung braucht einen „roten Faden“ und genau hier setzt antares RiMIS® an.

Ein Wizard leitet durch die einzelnen Menüs. Am Ende der Eingaben steht die Freigabe des Themas an und der Workflow läuft weiter. Natürlich hat der verantwortliche Risikomanager die größte Auswahl an Auswertungen und muss den Überblick behalten. Die Anwender verfügen über eine übersichtliche und für die Arbeit notwendige Menge an relevanten Menüpunkten.



[Das sagen unsere Kunden



„Wir konnten unseren Risikomanagementprozess mit klar definierten Rollen und Verantwortlichkeiten in antares RiMIS® durch ein sehr flexibel konfigurierbares Berechtigungskonzept und einem mehrstufigen Freigabeprozess abbilden.“

„antares RiMIS® hat uns nicht nur mit seinem komfortablen und individuellen Berichtswesen überzeugt, sondern auch mit dem intuitiven User Interface. Die Anwendung ließ sich sehr schnell erlernen, sodass keine Lücken im Arbeitsprozess entstanden.“

Svenja Olejak
GF Corporate Controlling
BA & F / Risk Management
LANXESS AG

[Unsere zufriedenen Kunden



[Wir stellen uns vor

Das machen wir

Wir sind ein mittelständisches, unabhängiges und auf professionelle Software spezialisiertes Unternehmen. Seit unserer Gründung im Jahr 1994 entwickeln und vermarkten wir strategische Informationssysteme.

Langjährige Expertise in den Themen Analyse, Planung und Unternehmenssteuerung sowie Governance, Risk und Compliance sind Garanten für den Auf- und Ausbau der fortschrittlichen antares-Softwarelösungen.

Das sind wir

Modernste Technologie, Innovation und anwenderoptimierte Lösungen prägen unsere Produkte. Leidenschaft, Zuverlässigkeit und Professionalität sind die Leitlinien im Umgang mit unseren Kunden und Partnern. Der kompetente und zuverlässige Support steht bei uns an erster Stelle. Um das zu gewährleisten, arbeiten wir konsequent an der Weiterentwicklung unserer etablierten Softwarelösungen, übernehmen das professionelle Projektmanagement und bieten darüber hinaus umfassende Dienstleistungen - von Schulungen und Webinaren bis hin zu Coachings.

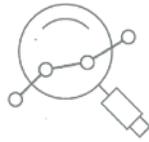
Das bieten wir

Wir zählen mittlerweile mehr als 300 Unternehmen aller Branchen und Größenordnungen zu unseren Kunden, darunter namhafte Unternehmen aus den Bereichen Industrie, Handel und Dienstleistung. Sie alle profitieren von einem erfahrenen BI-Unternehmen mit flachen Hierarchien, professioneller Partnerschaftlichkeit und Kundennähe.

Das ist unser Ziel

Unser Ziel ist es, unseren Kunden stets eine sichere, benutzerfreundliche Informationsbasis zu verschaffen, damit bewusste und sichere Entscheidungen getroffen werden können.

[Über 25 Jahre Erfahrung bei der Entwicklung von Business Intelligence-Softwarelösungen



Analysieren. Planen. Steuern.

Integration Ihrer Daten und Aufbereitung von Wissen. Gewinnen Sie wichtige Erkenntnisse, um Entscheidungen sicher und fundiert zu treffen.



Governance. Risk. Compliance.

Mit unserer ganzheitlichen Risiko- und Chancenmanagement-Software erkennen Sie systematisch Risiken, analysieren, bewerten, überwachen und kontrollieren diese, um Unternehmenschancen wahrzunehmen.



Individuelle BI-Software

Wir implementieren seit über 25 Jahren BI-Softwarelösungen, um Sie so bei der Entscheidungsfindung im ganzen Unternehmen zu unterstützen. Perfekt auf Ihre Bedürfnisse und Prozesse abgestimmt.



Software-Consulting

Wir bieten ein umfangreiches Dienstleistungsportfolio, welches sich von der Zusammenstellung Ihrer Software-Anforderungen, über die Implementierung und begleitende Anwenderschulungen bis hin zur Wartung nach Abschluss des Projektes erstreckt.

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