avedos
performance with integrity

Sicherheitsmanagement aus einem Guss: Zukunftsorientierte Steuerung der Informationssicherheit

T-Systems setzt weltweit auf das Informationssicherheitsmanagement-System der flexiblen Softwareplattform risk2value von avedos.

T · · Systems ·

Disclaimer

Die in diesem Dokument enthaltenen Inhalte dienen ausschließlich zur Information. Alle Inhalte wurden mit Sorgfalt und nach bestem Gewissen erstellt. Eine Gewähr für die Aktualität, Vollständigkeit und Richtigkeit sämtlicher Seiten kann jedoch nicht übernommen werden. In die Zukunft gerichtete Informationen sind Annahmen und stellen keine Zusicherung dar.

Auch wenn im Text nicht explizit ausgeschrieben, beziehen sich alle personenbezogenen Formulierungen auf weibliche und männliche Personen.

Version 2.1, Mai 2015

Inhaltsverzeichnis

Über T-Systems

T-Systems ist ein international operierender Dienstleister für Informations- und Kommunikationstechnologie (ICT). Das Unternehmen gehört zur Deutsche Telekom AG und beschäftigt in über 20 Ländern mehr als 50.000 Mitarbeiter.

Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik für multinationale Konzerne und öffentliche Institutionen. Auf dieser Basis bietet die Großkundensparte der Deutschen Telekom integrierte Lösungen für die vernetzte Zukunft von Wirtschaft und Gesellschaft. Die Mitarbeiter verknüpfen bei T-Systems Branchenkompetenz mit ICT-Innovationen, um für Kunden in aller Welt einen spürbaren Mehrwert zu schaffen.

Das Ziel von T-Systems besteht darin, das Geschäft der Kunden in wandelnden Märkten positiv und nach den jeweiligen Vorstellungen zu entwickeln, indem leistungsfähige und innovative Technologien umgesetzt werden. T-Systems versteht sich selbst dabei als „Enabler", der seinen Kunden die notwendige Handlungs- und Wettbewerbsfähigkeit sichert. Die Leistungen basieren dabei auf den drei Markenwerten des Unternehmens: Innovation, Einfachheit und Kompetenz.

Der erste Schritt zum integrierten GRC-Tool

Seit 2001 bekam T-Systems vereinzelt Kundenanfragen bezüglich Zertifizierungen im Sicherheitsmanagement. Daher wurden schrittweise die verschiedenen Standorte zertifiziert, wodurch eine Verbesserung der Nachhaltigkeit erreicht werden konnte. Die Herausforderung bestand nun darin, alle Standorte zu vereinheitlichen, um durchgängige Qualitätsstandards zu ermöglichen. Daher fiel 2006 die Entscheidung für eine Dachzertifizierung. Das bedeutet, dass alle Regelungen aus dem Sicherheitsmanagement zentral, „unter einem Dach", entwickelt und dann in der Fläche umgesetzt werden. Somit müssen die einzelnen Niederlassungen nur noch die Anwendung der Verfahren prüfen, nicht die Verfahren selbst. Dadurch konnten die Auditzeiten vor Ort dramatisch gesenkt werden, nämlich

um etwa ein Drittel. Durch das Prüfverfahren der Zertifizierung konnte ein einheitliches Sicherheitsniveau für die Kunden gewährleistet werden.

Im Jahr 2008 fand im Rahmen eines Strategiewechsels eine Bestandsaufnahme der bestehenden Regelungen statt, wobei die enorme Regelungstiefe vollumfänglich erkannt wurde. Der verantwortliche Senior Security Manager, Armin Plank, kam zu einem erstaunlichen Ergebnis:

> „Wir hatten 14,8 Gramm Papier pro Mitarbeiter, und das für damals 50.000 Mitarbeiter."

Die Sammlung umfasste höchst unterschiedliche Regelungen. Einerseits folgten sie internen Anforderungen: diese umfassen interne Regelungen, interne Compliance-Vorgaben und Anforderungen an das interne Reporting. Andererseits wurden externe Erfordernisse erfüllt: darunter fallen Zertifizierungen (z.B. ISO 27001), Control Mappings (z.B. COBIT) und Compliance-Auflagen. Diese internen und externen Regelungen sollten nun zusammengeführt und integriert betrachtet werden:

Die Bereiche, die bei T-Systems im Sicherheitsmanagement-System betrachtet werden, sind:

- Informationsschutz,
- IT-Sicherheit und
- physikalische Sicherheit.

Um die enorme Menge an Vorgaben effizienter verwalten zu können, wurde ein Kontrollset mit Kontrollchecklisten gebaut. Zu Beginn umfasste dieses Kontrollset 1400 Kontrollen, mittlerweile sind es weit weniger. Die Kontrollen stellen ein durchgängiges System dar, dass von der Handlungsbeschreibung für den einzelnen Mitarbeiter bis hin zu Anforderungen der Stakeholder alle notwendigen Kontrollen beinhaltet. Armin Plank dazu:

> Wir hatten anfangs knapp 1400 Kontrollen, mittlerweile sind wir durch bessere Strukturierung und Zusammenlegung von themennahen Gebieten bei etwa 900.

Optimale Nutzung der gesammelten Daten

Um die Verwaltung des Kontrollsystems leistungsfähiger zu gestalten und den Nutzen zu maximieren, begab sich das zuständige Team auf die Suche nach einem Tool, das es bei seiner Aufgabe unterstützte. Der Kontrollkatalog ist kaskadierend aufgebaut, um je nach Steuerungsanspruch mehr oder weniger weit in die Tiefe gehen zu können. Dieser spezielle Aufbau musste im Tool abgebildet werden können. Dazu Armin Plank:

> „Wir sind in 26 Ländern mit 36 Gesellschaften tätig, die etwa 96 Business Units haben – wir sprechen also von einem enorm großen Tanker, den wir steuern – mit einem nicht eindeutig definierten Katalog ist das nicht möglich."

Auch die weiteren Anforderungen verlangten nach einer sehr flexiblen und anpassungsfähigen Lösung, um alle Risiken und Chancen zu steuern und dadurch den Wert für die Stakeholder zu erhöhen:

- Verwalten des Kontrollsets und Herstellen von Bezügen zu den originären Regelungsgebern, um eine reibungslose Weitergabe der Ergebnisse sicherzustellen,
- Netzwerkverwaltung: mehrfache Nutzung von einmalig eingegebenen Daten an unterschiedlichen Stellen,
- Verwaltung der Daten ohne permanenten Support des Softwareherstellers, um die laufenden Kosten gering zu halten und um bei Änderungen der Anforderungen von externen Stakeholdern (z.B. Gesetzgeber) das Tool selbst anpassen zu können und
- Konsistenz bei Formulierungen, um Interpretationsspielraum gering zu halten und den Mitarbeitern, die das Tool nutzen, Handlungssicherheit zu geben.

Mit dem Anspruch, alle Vorgaben in einem Tool erfüllt zu bekommen, führten die Verantwortlichen bei T-Systems eine umfangreiche Marktrecherche durch, im Zuge derer eine Vielzahl von Lösungen auf ihre Tauglichkeit geprüft wurde.

Die Entscheidung der Fachabteilung fiel schließlich auf die Softwareplattform risk2value von avedos, da das angebotene Gesamtpaket die Marktbegleiter in mehreren Punkten übertraf. Das Hauptargument für die Entscheidung war die Bereitschaft von avedos, das Tool genau an die besonderen Anforderungen von T-Systems bezüglich der Darstellungsmöglichkeiten anzupassen. Armin Plank dazu:

> avedos hat sich von Beginn an sehr flexibel gezeigt, ist kundenorientiert auf die T-Systems-spezifischen Prozessanforderungen eingegangen und hat sie vollständig umgesetzt.

Ein weiterer bedeutender Vorteil der gewählten Lösung besteht in der Garantie von avedos, dass die volle Funktionalität der Plattform in neue Versionen migriert wird. Dadurch wird sichergestellt, dass alle vorgenommen kundenspezifischen Anpassungen mit integriert werden.

Ein neuer Anfang ist gefunden

Nach einer kurzen Implementierungsphase folgte ein etwa 18 Monate dauernder Einschleifprozess von iGRCS (Integrated GRC-Service). An dessen Beginn bestand eine der wichtigsten Aufgaben darin, die Mitarbeiter von der Softwarelösung zu überzeugen. Dabei wurden vor allem Antworten auf folgende Fragen gegeben:

- Wie wird das Tool bedient?
- Was passiert mit den Daten, die eingegeben werden?
- Wie funktioniert das Reporting?

Die Mitarbeiter lernten das neue Werkzeug und die neue Art der Datenaufbereitung kennen. Der Hebel, der die Anwender von der Softwareplattform schließlich überzeugte, war die spürbare Reduktion der tatsächlichen Arbeitslast. Diese wird durch mehrere Faktoren gewährleistet:

- Aus einer Dateneingabe werden im Durchschnitt 8 belastbare Compliance-Aussagen erzeugt.
- Das Ausfüllen eines Kontrollsets generiert im Durchschnitt 22 Reports, die früher einzeln erstellt werden mussten.
- Die Dokumentation erfolgt automatisch.
- Auf Tastendruck ist sichtbar, wer die Daten bekommt und in welcher Detailtiefe die Daten weitergegeben werden.
- Die Zustellung der Reports erfolgt automatisch.
- Alle Aktionen, Vorgänge und Abläufe werden revisionssicher dokumentiert.
- Die Mitarbeiter haben Handlungssicherheit, da die Aufgabenstellungen und Erwartungen klar sind.
- Ein aktives Rück-Reporting schafft Transparenz für jeden Mitarbeiter.

Die Teilnehmerrate von iGRCS stieg kontinuierlich an und ist mittlerweile bei einem nahezu perfekten Wert angekommen. Die wenigen Ausfälle sind meist durch Funktionswechsel der beteiligten Mitarbeiter begründet. Herr Plank äußert sich zufrieden:

> Mit risk2alue haben wir es geschafft, lästige Doppelgleisigkeiten zu eliminieren und damit haben wir die Akzeptanz der Mitarbeiter gewonnen. Jeder Einzelne hat gesehen, dass bei ihm persönlich Synergien ankommen.

In einer Umfrage unter den etwa 200 Usern von risk2value wurde abgefragt, inwieweit die Mitarbeiter Verbesserungen bzw. Verschlechterungen in verschiedenen Bereichen sehen:

- Performance der Assessments
- Benutzerfreundlichkeit des Tools
- Anzahl der Controls
- Redundanzen innerhalb der Controls
- Funktionalität des Reportings
- uvm.

Das Ergebnis bestätigte, dass die Mitarbeiter in nahezu allen Bereichen erhebliche Verbesserungen feststellen konnten. Vor allem die Ergebnisse in den Bereichen „Performance der Assessments" und „Benutzerfreundlichkeit des Tools" waren überzeugend, da 100% der Befragten eine Verbesserung erkannten.

Schritte zur Professionalisierung

Es gibt bei T-Systems 400 User und 96 Verantwortliche in den Units, die Reports abgeben. Pro Unit sind also im Durchschnitt etwa vier Personen an der Erstellung des Reports beteiligt. Jeder dieser Mitarbeiter bekommt einmal pro Quartal ein Kontrollassessment vorgelegt, das mit den Daten aus dem letzten Quartal befüllt ist, um es zu überprüfen und gegebenenfalls zu adaptieren. Diese Selfassessments werden ausgewertet und die schwächsten sowie stärksten Handlungsfelder in Bezug auf die Einheit und in Bezug auf den globalen Durchschnittswert identifiziert. Danach werden entsprechende Handlungsempfehlungen ausgegeben.
Ein weiterer Entwicklungsschritt war die erfolgreiche Übernahme des IS Riskmanagement in das iGRCS. Quartalsweise müssen hier die lokalen Risiken von 23 internationalen Geschäftseinheiten erfasst, bewertet, und konsolidiert werden. Dieser Riskmanagementprozess wurde lange Zeit mit Spreadsheets händisch abgewickelt. In einer Projektgruppe wurde dieser Prozeß Schritt für Schritt in das iGRCS integriert und immer wieder getestet. Die Implementierung konnte 2014 abgeschlossen werden, in einem letzten Schritt wurde das Risk Reporting an die Bedürfnisse der Mitarbeiter und des Management angepasst. Überzeugend waren auch hier für alle Beteiligten der hohe Einsparungseffekt an zeitraubenden Einzeltätigkeiten und dezentraler Datenhaltung zugunsten einer zentralen, integrierten Lösung für das IS Riskmanagement. Für die Zukunft sind hier noch die Einrichtung weiterer Schnittstellen zum Management der Sicherheitsarchitektur oder dem Audit Management geplant. Armin Plank:

> „Unsere Nutzer sind mit dem Riskmanagement sehr zufrieden. Dank der positiven Rückmeldungen aus den Geschäftseinheiten sind wir in der Lage vorhandene, dezentrale Applikationen zugunsten unserer iGRCS-Plattform abzulösen. Dies generiert für uns weitere Synergien."

Laufende Anpassungen in risk2value werden von T-Systems selbst vorgenommen, wohingegen die Entwicklung von sinnvoll hinterlegten Workflows ein gemeinsames Projekt mit avedos darstellt. Die kundenspezifischen Besonderheiten wurden von Beginn an berücksichtigt. Dadurch funktionierte die Umstellung der Plattform auf neue Versionen hervorragend. Außerdem wurde die Zusammenarbeit von T-Systems und avedos zunehmend effizienter. So passierten Änderungen früher auf Zuruf, wohingegen mittlerweile ein professionelles Ticketing-System genutzt wird.

Auch das Reporting wurde zur Zufriedenheit von Armin Plank weiterentwickelt:

> Mit dem Reporting in risk2value.analytics sind wir sehr zufrieden, weil die Fachabteilung auf Basis von Excel selbstständig Reports entwerfen kann. Weiters kann festgelegt werden, wie weit der einzelne Nutzer Reports eigenständig parametrisieren kann. Dadurch sinkt die Anzahl an benötigten Reporting-Templates und der Betrieb wird aufgrund von Kostenvorteilen, die in der Entwicklungszeit generiert werden, effizienter.

Der gemeinsame Weg in die Zukunft

Die nächsten strategischen Schritte umfassen eine Anknüpfung von risk2value an andere Systeme, z.B. technische Vermessungssysteme. Das bringt den Vorteil, dass Angaben nicht mehr händisch eingegeben werden müssen, sondern Daten automatisch abgelesen und ins Tool übertragen werden. Zur Umsetzung dieser Aufgabe ist von T-Systems ein gemeinsames Projekt mit avedos vorgesehen, bei dem Importschnittstellen für externe Systeme integriert werden, um die Mitverwaltung externer Daten zu erlauben. Weiters wird die Ermöglichung der mobilen Nutzung der Softwareplattform mit Smartphones und Tablets überlegt, um die Dateneingabe und das Abrufen von Reports unterwegs zu ermöglichen.
Darüber hinaus wird die Integration von anderen Bereichen ins bestehende Kontrollset angedacht. Dafür kommen Bereiche wie Prozesswesen und Qualitätsmanagement infrage, um auch dort mehr Transparenz zu schaffen. Armin Plank erklärt:

> Wir haben im Vergleich zu anderen strategischen Handlungsfeldern dank risk2value einen deutlich höheren Durchdringungsgrad in der Fläche, eine deutlich höhere Sicherstellung der Harmonisierungsaspekte und eine deutlich höhere Handlungstransparenz.

Die Konsolidierung verschiedener Management-Domänen ist für T-Systems eine der bedeutsamsten Herausforderung für die Zukunft. Um eine Annäherung zu ermöglichen, werden verschiedene Fachbereiche Verfahren anpassen und ein kombiniertes Kontrollset verwenden. avedos ist auf diesem Weg ein zuverlässiger Partner für Armin Plank, der den Nutzen von risk2value für seine Zukunftspläne beschreibt:

> Die Stärken von risk2value liegen ganz klar in der einfachen Modellierung, der raschen Implementierbarkeit und der vorhandenen Generik, um verschiedene Management-Domänen zu vereinen.

So steht einer weiteren Zusammenarbeit und einem langen gemeinsamen Weg von T-Systems und avedos nichts im Weg.

Über avedos

avedos ist ein europäischer Softwareanbieter, der sich auf Governance, Risk und Compliance (GRC) spezialisiert hat. Das Unternehmen bietet seinen Kunden flexible Softwarelösungen, mit denen GRC-Prozesse dargestellt und verwaltet werden. Dadurch werden Synergiepotenziale geschaffen, Risiken frühzeitig erkannt und Chancen optimal genutzt.

Das zugrunde liegende Konzept für die Softwareplattform risk2value wurde von Samuel Brandstätter, einem der Inhaber und Geschäftsführer von avedos, entwickelt. risk2value bietet umfangreiche Anwendungsmöglichkeiten im GRC-Bereich und verfolgt einen richtungsweisenden Ansatz, der die individuellen Kundenanforderungen flexibel abbildet. Zu den wichtigsten Bereichen zählen vor allem Enterprise Risk Management, Internes Kontrollsystem, Compliance Management, Audit Management und Informationssicherheitsmanagement.

Das Unternehmen avedos verschreibt sich seit 2005 der kontinuierlichen Weiterentwicklung der Softwareplattform risk2value, um seinen Kunden eine anpassungsfähige, integrierte GRC-Suite zur Verfügung zu stellen. avedos arbeitet branchenneutral. Zu den Kunden zählen beispielsweise die weltweit größten und erfolgreichsten Energieversorger, Versicherungen, Telekommunikations- und Handelsunternehmen. Darüber hinaus konnten Kooperationen mit bewährten Beratungspartnern nachhaltig etabliert werden, um die gesamte GRC-Value Chain für den Kunden abzudecken. Die avedos Softwarelösungen fungieren als Bindeglied zwischen operativen Ebenen und dem Top-Management. Sie ermöglichen risikobewusste und nachvollziehbare Entscheidungen in einer komplexen Unternehmensumwelt durch objektive Argumentation und Dokumentation. risk2value schafft somit die Grundlage für eine proaktive Unternehmensführung in einem vielschichtigen Wirtschaftsumfeld.

Weitere Informationen unter: www.avedos.com

Unser Erfahrungsvorsprung

Zahlreiche nationale Unternehmen und internationale Konzerne, aus unterschiedlichsten Branchen, arbeiten seit vielen Jahren mit der GRC-Lösung risk2value. Hier ein Auszug unserer Referenzkunden:

Webinare

Bleiben Sie mit unseren Themen- und Spezialwebinaren laufend informiert über aktuelle Entwicklungen in den Bereichen:

- Governance, Risk und Compliance
- Risikomanagement und IKS
- Informationssicherheit

avedos GRC GmbH
Franz-Klein-Gasse 5
1190 Vienna, Austria
T: +43 1 3670876-0
F: +43 1 3670876-999

office@avedos.com
www.avedos.com

avedos GRC Deutschland GmbH
Peter-Mueller-Straße 3
40468 Duesseldorf, Germany
T: +49 211 42471-5638
F: +49 211 42471-5678

office@avedos.de
www.avedos.com

DVR: 4016544