



THEMEN:

- 01 Tue Gutes und sprich darüber - Erfolge messbar machen mit Key Performance Indicators
- 02 CRISAM® FV Release 2.0
- 03 Energiehändler e&t erhebt IT-Sicherheitsbedarf mittels CRISAM®
- 04 Jahreskonferenz der RMA 2011, MEDICA 2011
- 05 Merken Sie sich bereits jetzt das nächste CRISAM® Risikomanagement Symposium vor!



01

Tue Gutes und sprich darüber - Erfolge messbar machen mit Key Performance Indicators

Sehr geehrte
Geschäftsfreunde!

Zu Beginn dieses Newsletters erläutert Ihnen Thomas Danninger, wie Sie mit entsprechenden Kennzahlen die Performance Ihres Informationssicherheits-Management-Systems (ISMS) messen können.

Anschließend präsentiert Ihnen Günther Angerbauer ausführlich die neue Version des CRISAM® FV Explorers.

Thomas Klenner berichtet danach über das erfolgreich abgeschlossene CRISAM® Projekt bei der e&t ENERGIE HANDELSGESELLSCHAFT m.b.H. und abschließend geben wir Ihnen noch einige Veranstaltungshinweise.

Im Namen des CRISAM® Teams wünsche ich Ihnen eine spannende, informative Lektüre und eine wunderschöne Herbstzeit!

Ihre
Mag.^a Anita Wenigwieser
calpana business consulting
gmbh

Die ISO27001:2005 als Informationssicherheitsmanagementsystem (ISMS) kann mittlerweile als der Sicherheitsstandard in Unternehmen angesehen werden (etwa 10.000 ausgestellte Zertifikate weltweit). Die Grundidee des ISMS basiert auf einem Management der Informationssicherheit, welches ausgerichtet ist auf dem Management der Unternehmensrisiken. Zu berücksichtigen bleibt aber, dass diese Zertifizierung nichts über Güte und Performance eines ISMS aussagt. Zur kontinuierlichen Verbesserung des ISMS kann der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) und für vorbeugende und korrigierende Maßnahmen die Norm selbst herangezogen werden; es sind aber keine Messmethoden vorhanden, mit denen Aussagen über die Abschätzung der Güte eines ISMS getroffen werden können.



Mag. Thomas Danninger
Head of Consulting, Senior Consultant
calpana business consulting gmbh

Seit 2010 steht ein weiteres Mitglied der Normenreihe 2700x zur Verfügung. Es handelt sich dabei um die ISO/IEC 27004:2009, die einen Leitfaden zur Entwicklung von Methoden zur Messung der Effektivität eines ISMS zur Verfügung stellt und natürlich entsprechende Relevanz im Rahmen einer Zertifizierung nach 27001 erlangt.

Zur Bewertung von Managementsystemen bzw. Prozessen stehen in der Literatur weitere unterschiedliche Methoden zur Messung der Performance zur Verfügung. Neben Methoden wie SPICE oder CMMI, die insbesondere die Performance über den Reifegrad von Prozessen messen, besteht eine weitere Methode, die aus vielerlei Hinsicht einer weiteren Betrachtung wert ist. Die Performance eines ISMS kann auch über entsprechende Kennzahlen (Key Performance Indicators) gemessen werden.

Key Performance Indicators sind Kennzahlen, die es ermöglichen, die entscheidenden Erfolgsfaktoren optimal ins Blickfeld zu rücken. Dabei ist es das Ziel, das Management mit den wichtigen Kennzahlen zu versorgen, damit das erkennt:

- Werden die gesteckten Ziele erreicht?
- Entstehen Abweichungen, denen möglichst rasch gegengesteuert werden muss?
- Wo liegen die Stärken und wo bestehen noch Schwächen?

Jeder Unternehmensbereich und so auch die IT sollte bei der Entwicklung seiner Key Performance Indicators darauf achten, dass erwartet wird, die geforderte Qualität ihrer Leistungen in angemessener Zeit zu möglichst geringen Kosten zur Verfügung zu stellen. Dies gilt selbstverständlich auch für ein Informationssicherheits-Management-System (ISMS).

>> Lesen Sie weiter auf der nächsten Seite.

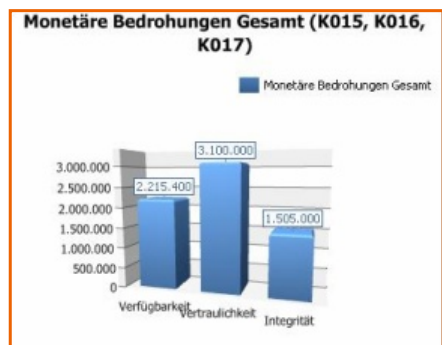


01

Wirklich gute Key Performance Indicators schaffen Vertrauen. Denn sie machen sichtbar, wie es um die Leistungsfähigkeit des ISMS bestellt ist. Ein Vorteil von Kennzahlen ist außerdem, dass sie einfach und klar sind. Sie erfordern keine umständliche Datenerhebung, in die sich viele Fehlermöglichkeiten oder Interpretationsspielräume einschleichen können. Sie lassen sich nach einem eindeutigen Schema berechnen und alle Mitarbeiter wissen, wie sie ermittelt werden und was sie aussagen.

Dabei überfordern zu viele Kennzahlen den Anwender, denn er hätte es gerne einfach, klar und übersichtlich und am liebsten nicht mehr als eine Hand voll Kennzahlen auf die er sich konzentrieren kann. Dazu wird in CRISAM® ein umfangreiches Set an möglichen Kennzahlen zur Verfügung gestellt, aus dem die für das jeweilige Unternehmen wichtigsten KPIs ausgewählt werden können.

Dabei überfordern zu viele Kennzahlen den Anwender, denn er hätte es gerne einfach, klar und übersichtlich und am liebsten nicht mehr als eine Hand voll Kennzahlen auf die er sich konzentrieren kann. Dazu wird in CRISAM® ein umfangreiches Set an möglichen Kennzahlen zur Verfügung gestellt, aus dem die für das jeweilige Unternehmen wichtigsten KPIs ausgewählt werden können.



Bereits seit Beginn der Entwicklung von CRISAM® ist es möglich, das bestehende Restrisiko für das Unternehmen aus dem Einsatz der IT zu messen. Zunächst mit Hilfe des Ratingmodells nach Standard&Poors (AAA, AA, etc.), in jüngster Vergangenheit wurde es zusätzlich möglich, die Risiken monetär darzustellen.

Auch die Standards ISO/IEC 27001 bzw. ISO/IEC 27004 fordern von Organisationen die regelmäßige Überprüfung der Wirksamkeit des ISMS unter Berücksichtigung der Effizienz-Messung und gleichzeitig die Wirksamkeit der Kontrollen zu überprüfen, um die Erfüllung der Sicherheitsanforderungen sicherzustellen. Um vergleichbare und reproduzierbare Ergebnisse zu erzielen, fordert der Standard außerdem eine Definition, wie die Wirksamkeit der definierten Kontrollen zu messen und die Wirksamkeit der jeweiligen Maßnahmen zu bewerten ist.

logbuch

01

Die wichtigsten Ziele der Messung von Informationssicherheit:

- Darstellen der kontinuierlichen Verbesserung
- Darstellen der Compliance (Einhaltung von Standards, Verträgen, SLAs, OLAs, etc.)
- Entscheidungsgrundlage für künftige Investitionen (Software, Hardware, Training, Personal, etc)
- Erfüllen der Forderung der ISO 27001 bzw. 27004
- Schaffung von Vertrauen beim Top-Management und Stakeholdern, dass implementierte Kontrollen wirksam sind

Ihr Nutzen durch den Einsatz von Key Performance Indicators:

- Einfachheit und Klarheit in der Darstellung komplexer Gegebenheiten
- Für Top-Management verständliche Aggregation
- Planung und Steuerung des ISMS wird ermöglicht bzw. zumindest erleichtert
- Erleichtert den Prozess zur Überwachung der Effektivität des ISMS
- Instrument, um mit evtl. zukünftigen Problemen proaktiv umzugehen
- Transparente und nachvollziehbare Ziele (Mitarbeitermotivation)
- Nachweis für Auditoren

Um die kontinuierliche Verbesserung zu weiteren für das ISMS unbedingt relevanten Themen bzw. in einem noch höheren Detaillierungsgrad darstellen zu können, wurde in CRISAM® das neue Key Performance Indicators – Modul implementiert und ist ab sofort verfügbar.

Tun Sie weiterhin Gutes und sprechen Sie jetzt darüber!





logbuch

02

CRISAM® FV Release 2.0



Ing. Mag. Günther Angerbauer
 Head of Development, Senior Consultant
 calpana business consulting gmbh

Mit der neuen Version von CRISAM® FV Explorer setzt calpana neue Maßstäbe für das Management von Risiken in Unternehmen. Der CRISAM® FV Explorer bietet Ihnen ein Höchstmaß an Flexibilität wenn es darum geht, einfach und schnell zu beginnen, um dann kontinuierlich den Reifegrad Ihres Risikomanagement Prozesses zu steigern.

Key features and benefits

- Anpassbare Abbildung Ihres Risikomanagement-Prozesses.
- Flexible Modellierung und Risikoidentifikation.
- Integrierte Simulation und Aggregation.
- Aussagekräftige Ergebnisanalyse.
- Flexibles Reporting.
- Risikosteuerung und Frühwarnsystem.
- Integrierte Sicherheit.

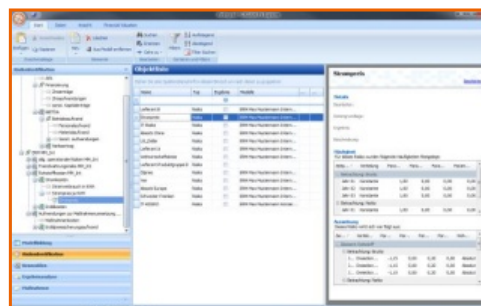
Anpassbare Abbildung Ihres Risikomanagement-Prozesses

Über den Navigationsbereich sind die zentralen Aufgaben im Risikomanagement-Prozess übersichtlich abgebildet. Damit werden Risikomanagement-Prozesse entsprechend ISO/IEC 31000, ONR 49000 oder dem COSO ERM Framework unterstützt. Besonderer Wert wurde auf die durchgängige Anpassbarkeit der Anwendung für unterschiedliche Reifegrade Ihres Risikomanagement-Prozesses gelegt. Sie können somit im aktuellen Prozessreifegrad Ihres Unternehmens beginnen und die Prozessqualität ohne Systembrüche laufend weiter verbessern.

Flexible Modellierung u. Risikoidentifikation

Die Modellbildung und Risikoidentifikation sind zentrale Bestandteile von CRISAM® FV. Je nach Reifegrad können einfache Risikolandschaften bis hin zu komplexen Finanzmodellen modelliert werden. Über Vorlagen wird der Start beschleunigt, mit Drag&Drop sind Erweiterungen und Änderungen am Modell einfach möglich. Wenn Sie Werte modellieren, die im jeweils betrachteten Zeitbereich unsicher sind, können diese mit ihrer Volatilität über eine statistische Verteilung belegt werden. Bei der Identifikation von Risiken können Häufigkeit und Auswirkung ebenfalls als konstant oder veränderbar über die entsprechende Verteilung hinterlegt werden.

Wenn Sie im ersten Schritt mit einem einfachen Modell zur Inventarisierung der Risiken starten, können Sie später jederzeit die bestehenden Daten auch in anderen Modellen wieder verwenden.



>> Lesen Sie weiter auf der nächsten Seite.



Integrierte Simulation und Aggregation

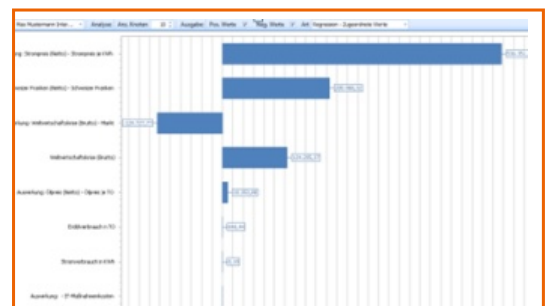
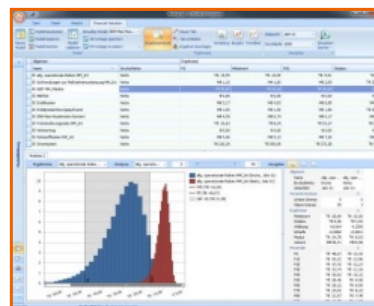
CRISAM® FV errechnet bei der Monte Carlo Simulation potentielle Ergebniswerte aufgrund der im Modell hinterlegten Werte und Risiken. In dieser Simulation werden tausende, mehr oder weniger wahrscheinliche, jedoch mögliche Realsituationen in kürzester Zeit durchgespielt. Daraus ergeben sich jene Ergebniswerte als sehr wahrscheinlich, die in der Simulation am häufigsten erreicht wurden.

Mit der nahtlos in CRISAM® FV integrierten Simulationskomponente @Risk von Palisade Corporation profitieren Sie von mehr als 25 Jahren Erfahrung dieses führenden Herstellers.

Die Aggregation erfolgt über die im Rahmen der Modellbildung verwendeten Funktionen. Neben den Standardfunktionen können mit dem Formeleditor weitere, eigene Funktionen erstellt werden.

Aussagekräftige Ergebnisanalyse

Die Ergebnisse stehen Ihnen nach der Simulation in der Ergebnisanalyse zur Verfügung. Sie können die Ergebnisse als Histogramme, Verteilungen, Boxplots oder zur Visualisierung von zeitlichen Änderungen über Trendlinien darstellen.



Weitere Auswertungen wie die Sensitivitätsanalyse, die Perzentil-Analyse und das mit Version 2.0 neu eingeführte „Risikoportfolio“ sind für den Risikomanager unverzichtbare Instrumente zur Kommunikation. Das Risikoportfolio dient dazu, auf einem Blick alle hohen bzw. hoch volatilen Risiken erkennen zu können.

Flexibles Reporting

Die enthaltenen Standardreports wurden in der Version 2.0 um zwei weitere Berichte erweitert. Ein Management-Bericht, der die Daten aus der Vorperiode inkl. Tendenz anzeigt und ein Detailbericht, der für die Risikogespräche mit den Risiko-Ownern ausgelegt ist.

Mit der Version 2.0 erstmals ausgeliefert wird der Berichtsdesigner – damit können die Standardreports durch den Kunden umfangreich bearbeitet und angepasst werden. Neben Anpassungen bei der Formatierung (Schriftart, Farbe, Logo, etc.) kann auf sämtliche Daten aus den bereitgestellten Datenquellen zugegriffen und auf Ihre individuellen Erfordernisse angepasst werden.

>> Lesen Sie weiter auf der nächsten Seite.

logbuch

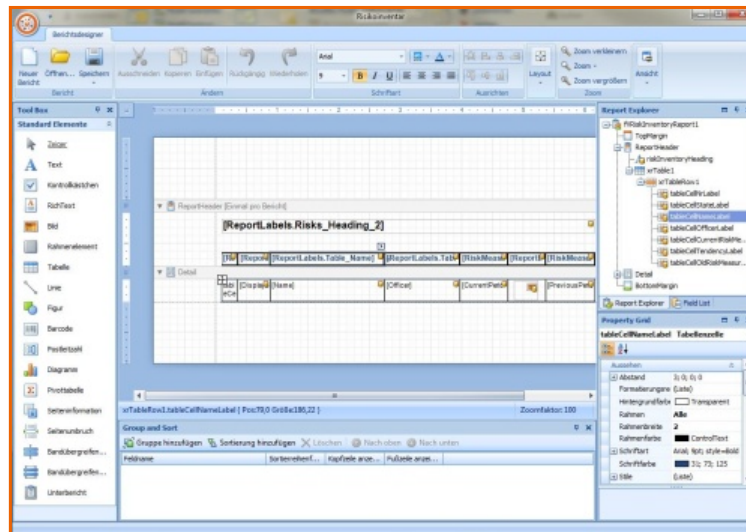


Abbildung: Neuer Berichtsdesigner

Risikosteuerung und Frühwarnsystem

Die Steuerung der Risiken erfolgt über Maßnahmen, die in CRISAM® FV verwaltet werden. Die Auswirkung der Maßnahmen auf die Risiken wird ebenfalls hinterlegt. Damit ergeben sich nun zwei unterschiedliche Betrachtungsweisen. Einmal unter der Annahme, dass keine Maßnahmen umgesetzt wurden (Brutto) oder unter der Annahme, dass die Maßnahmen implementiert wurden (Netto). In der Ergebnisanalyse kann so der Nutzen der Maßnahmen einfach ermittelt werden.

CRISAM® FV inkludiert ein Frühwarnsystem, mit dem zulässige Grenzwerte hinterlegt und überwacht werden. Das ermöglicht Ihnen eine sofortige Erkennung von Abweichungen, z.B. wenn der Value at Risk (VaR) für das gesamte Unternehmen einen bestimmten Schwellwert überschreitet.

Integrierte Sicherheit

Ebenfalls neu in der Version 2.0 ist die Integration des CRISAM® FV Explorers in das bewährte und ausgereifte Rollenkonzept des CRISAM® Enterprise Servers. Das Rollenkonzept ermöglicht eine dreistufige Rollenzuweisung von Active Directory Benutzern oder Gruppen am CRISAM® Enterprise Server. Die dreistufige Rollenzuweisung erlaubt globale Rollen für alle Daten in einem Server, projektbezogene Rollen für ein Projekt in einem Server und bereichsbezogene Rollen für einen Teil in einem CRISAM® Projekt.

Damit können unterschiedlichste Anforderungen aus mehreren Unternehmen, in Konzernstrukturen oder Service Provider Umgebungen realisiert werden. Die Berechtigungsadministration ist im Client vollständig integriert, sodass hier keine zusätzlichen Werkzeuge erforderlich sind.

Risikomanagement war noch nie einfacher, präziser und nachvollziehbarer. Machen Sie mit!



logbuch

03

Energiehändler e&t erhebt IT-Sicherheitsbedarf mittels CRISAM®



Mag. Thomas Klenner
 Risk Controlling
 e&t ENERGIE HANDELSGESELLSCHAFT
 m.b.H.

Mit dem Ziel der Erhebung des IT-Risikos in der e&t Energie Handelsgesellschaft m.b.H. wurde das Unternehmen Calpana von e&t im Jahr 2009 beauftragt. Unter der Voraussetzung, dass sich e&t eines IT-Dienstleisters für die Betreuung der geschäftsnotwendigen IT-Ressourcen bedient, welche hochverfügbar zur Verfügung gestellt werden müssen, wurde das Projekt angegangen.

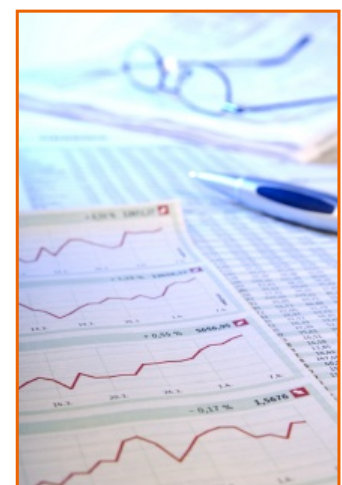
e&t ist das Energiehandelshaus der Energieallianz. Als dieses nimmt es eine wichtige Position im Energiegroßhandel für seine Gesellschafter bzw. Kunden ein. IT-Risiken stellen hinsichtlich Verfügbarkeit, Integrität, Rechtskonformität und Vertraulichkeit wesentliche Risiken dar. Hohe Ansprüche an die IT-Infrastruktur erfordern vielfach ein hohes Niveau an IT-Sicherheit, Standardtechnik kann dabei oftmals als nicht ausreichend erachtet werden.

Mittels des Tools CRISAM® wurde nach den Vorgaben der Geschäftsleitung betreffend dem erwarteten Sicherheitsniveau sowie den Schadensklassen, in einem intensiven Prozess mit den Mitarbeitern der e&t sowie dem Calpana-Projektteam, alle Kernprozesse analysiert und die dafür nötigen Applikationen bewertet. In einem zweiten Schritt wurden die Ressourcen mit dem IT-Dienstleister analysiert.

Die Ergebnisse aus dem Projekt liefern die Basis zur Erweiterung und Adaption des Servicelevels, welche mit dem IT-Dienstleister vereinbart wurden. Als Calpana Kunde profitiert e&t von den aus dem Projekt abgeleiteten Maßnahmen, welche den hohen geforderten IT-Standard erhalten und laufend ausbauen sollen.

"Durch die durchgeführte Business Impact Analyse, basierend auf dem CRISAM® Leitfaden, und die anschließende Risikoanalyse konnten wir uns einen sehr guten Überblick verschaffen, welche Abhängigkeiten von den einzelnen IT Services vorliegen bzw. welche negativen Auswirkungen bei Nichtverfügbarkeit für die Geschäftsbereiche der e&t zu erwarten sind."

Mag. Thomas Klenner, Risk Controlling
e&t ENERGIE HANDELSGESELLSCHAFT m.b.H.





logbuch

04

Jahreskonferenz der Risk Management Association e. V. 2011



Die diesjährige RMA-Jahreskonferenz hat am 19. und 20. Oktober in Ismaning bei München stattgefunden. Zum Thema "Enterprise Risk Management: Sicher navigieren in turbulenten Zeiten" haben die Teilnehmer umfangreiche Informationen, Erfahrungsberichte und Best-Practice-Beispiele aus dem Risikomanagement in Industrie- und Handelsunternehmen erhalten.

Auch die calpana business consulting gmbh war wieder als Aussteller mit einem CRISAM® Stand vertreten und Dr. Manfred Stallinger hielt einen interessanten Vortrag zum Thema "Risikomanagement - ein Instrument zur strategischen und operativen (Unternehmens-) Steuerung", der großen Anklang beim Publikum fand!



MEDICA 2011



Gemeinsam mit der Firma pascom Kommunikationssysteme GmbH sind wir Aussteller auf der Medica, der weltweit größten Medizininmesse vom 16. bis 19. November in Düsseldorf. pascom ist Anbieter von Produkten und System-Lösungen für das Gesundheitswesen rund um Patientenentertainment, Betriebsdatenerfassung, bargeldlosen Zahlungsverkehr und Alarmierungssysteme.

Wir würden uns freuen, Sie auf unserem Stand in Halle 14/B31 begrüßen zu dürfen! Dr. Manfred Stallinger informiert Sie gerne über Risikomanagement mit CRISAM® im Medizintechnikbereich bzw. zum Thema ISO 80001!



05

Merken Sie sich bereits jetzt das nächste CRISAM® Risikomanagement Symposium vor!

Wir freuen uns, Sie informieren zu dürfen, dass das nächste CRISAM® Risikomanagement Symposium am **26. Jänner 2012 ab 9:00 Uhr im Wissensturm Linz** (Kärntnerstraße 26) stattfinden wird.

Entsprechend dem Motto: „Sicher auf Kurs!“ erwarten Sie jeweils parallel informative Vorträge und Praxisberichte zu den Themen Information Risk Management und Enterprise Risk Management. Es werden Ihnen natürlich auch wieder einige Neuheiten der CRISAM® Software und Kataloge präsentiert. Für einen Erfahrungsaustausch und eine Diskussion mit den anderen Teilnehmern ist genügend Zeit eingeplant.

Das Programm mit näheren Informationen erscheint rechtzeitig vor dem Event. Wenn Sie vorab Fragen dazu haben, dann stehen wir unter office@calpana.com gerne zu Ihrer Verfügung!

