

THEMEN:

- 01 Wie hoch ist das Risiko nicht genutzter Chancen?
- 02 Umsetzung des CRISAM® Cost Benefit Analyzers
- 03 Neues CRISAM® Report Pack verfügbar
- 04 Konzernweite Einführung von CRISAM® bei der ÖBB
- 05 RMA Österreich News, ebiz egovernment award 2009
- 06 qSkills Security Summit 2009

01

Wie hoch ist das Risiko nicht genutzter Chancen?

Sehr geehrte
Geschäftsfreunde!

Ziel unserer Entwickler ist es, CRISAM® ständig zu verbessern und mit neuen Funktionen auszustatten. Jüngste Errungenschaft ist dabei der CRISAM® Cost Benefit Analyzer. Mehr über dieses wichtige Modul zur monetären Darstellung der Risiken Ihres Unternehmens erfahren Sie in diesem Newsletter.

Ein weiterer großer österreichischer Konzern, die ÖBB, findet sich ab sofort in den Reihen der CRISAM®-User. Lesen Sie in dieser Ausgabe den Praxisbericht über die erfolgreiche konzernweite Einführung von CRISAM®.

Auch Ihnen wünsche ich einen guten Start in einen erfolgreichen Herbst,

Ihre
Mag. Anita Wenigwieser
calpana business consulting GmbH

Sie kennen die Fragen: "Wie hoch ist der Nutzen einer redundanten Serverlandschaft?", "... eines IT-Service Management Projekts", oder " ... einer Regelung für die Klassifikation von Daten?". Sie zielen alle auf den wirtschaftlichen Nutzen ab, der einer Investition oder einem monetären Aufwand des Unternehmens gegenübergestellt werden muss. Um die Frage beantworten zu können, sind Kosten und Nutzen im Sinne einer betriebswirtschaftlichen Investitionsrechnung über die Nutzungsdauer der Maßnahme zu analysieren.



DDr. Manfred Stalling, MBA
Geschäftsführer
calpana business consulting GmbH

Übersteigt der Gesamtnutzen die zu investierenden Geldmengen, so trägt die geplante Maßnahme zu einer Steigerung des Wertbeitrages für das Unternehmen bei. Übertagen die Kosten den resultierenden Nutzen, so ist aus rein monetärer Sicht kein Wertbeitragszuwachs zu erwarten. Dennoch ist Vorsicht bei einer rein monetären Bewertung geboten. Beispielsweise kann ein Imageverlust zu enormen indirekten Schäden führen. Erst eine gründliche Kosten-Nutzen (Cost-Benefit) Analyse liefert nachvollziehbare Entscheidungsgrundlagen. CRISAM® RV liefert mit dem neuen Cost-Benefit-Analyzer Modul (CBA) ein adäquates Werkzeug, um Risiken aus dem Einsatz der IT im Unternehmen monetär transparent zu machen.

An einem kleinen Fallbeispiel soll der Einsatz des CRISAM® RV CBA (Cost-Benefit-Analyzer) demonstriert werden:

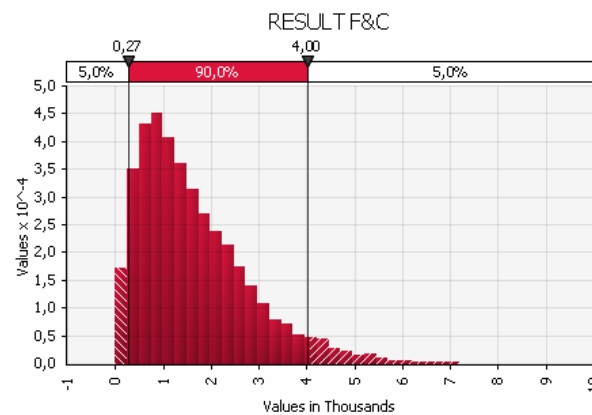
Schritt 1: Aus dem Geltungsbereich wird im Interview mit den Prozess- bzw. Bereichsverantwortlichen der maximal mögliche Schaden (Maximum Foreseeable Loss - MFL), der durch IT-Einwirkung entstehen kann, bewertet. Dieser stellt jenen Wert dar, der mit hoher Sicherheit nicht überschritten wird.

Schritt 2: Aus der CRISAM® Ratingkennzahl wird die Häufigkeit möglicher IT-Fehlfunktionen ermittelt.

Schritt 3: Durch die integrierte statistische Simulation (Monte Carlo Simulation) wird der erwartete Schaden (Most Likely) sowie der Best- und Worst Case errechnet und über die Prozesshierarchie aggregiert - Ergebnis ist das erwartete sowie Best- und Worst Case IT-Risiko auf Unternehmensebene.

logbuch

01



Beispielergebnis aus einer Monte Carlo Simulation von Schaden und Häufigkeit

Schritt 4: Aus der Maßnahmenplanung werden erforderliche Investitionen und Aufwendungen, um auf das gewünschte Zielrating zu kommen, aus monetärer Sicht bewertet sowie deren Betriebskosten, eventuell auch Finanzierungskosten, berücksichtigt - sie repräsentieren den Faktor "Kosten".

Schritt 5: Schritt 3 wird für das Zielszenario wiederholt und der reduzierte Risikowert ermittelt. Vom aggregierten Risikowert aus Schritt 3 werden der verbleibende Restrisikowert und die erforderlichen Aufwendungen aus Schritt 4 abgezogen, sodass der Nettonutzwert als Ergebnis verbleibt.

Das Risiko, die Chance nicht auf den Zielwert zu reduzieren, kann mit dem Ergebnis aus Schritt 5, dem Nutzwert, beziffert werden.

In analoger Form können mehrere Alternativszenarien durch Wiederholen von Schritt 4 und 5 bewertet werden. Daraus kann sich durchaus auch ergeben, dass der Nutzwert einer Risikoreduktion auf "BBB" (wesentlich) höher ausgewiesen wird als eine Verbesserung der IT-Strukturen auf ein "A" Risikoniveau.

Der CRISAM® RV CBA (Cost-Benefit-Analyzer) ist jenes Werkzeug, das dem CIO und IT-Verantwortlichen die Übersetzung in die Sprache des CFO und Eigentümer ermöglicht!




 logbuch

02

Umsetzung des CRISAM® Cost Benefit Analyzers



Ing. Mag. Günther Angerbauer
Leiter Entwicklung
calpana business consulting GmbH

Mit dem CRISAM® Cost Benefit Analyzer (CBA) liefert calpana business consulting ein optional erhältliches Modul, mit dem Sie den Kosten/Nutzen-Nachweis für Ihre in CRISAM® geplanten Maßnahmen monetär darstellen können. Dabei werden die Kosten bzw. Einsparungen aus der Maßnahmenplanung den durch die Maßnahmen reduzierten bzw. erhöhten Risikowerten gegenübergestellt.

Der CRISAM® Cost Benefit Analyzer bedient sich bereits wesentlicher Teile des Anfang nächsten Jahres erscheinenden Produkts CRISAM® Financial Valuation. Während in CRISAM® Financial Valuation beliebige Entscheidungssituationen und Finanzmodelle modelliert und simuliert werden können, werden beim CRISAM® Cost Benefit Analyzer die Verlustverteilungen aus den in CRISAM® Explorer ermittelten Ratingkennzahlen und hinterlegten Schäden je Szenario simuliert und über den Risikobaum aggregiert.

Als Komponente zur Monte Carlo Simulation wurde das Produkt @RISK des führenden Herstellers Palisade Corporation in CRISAM® Explorer nahtlos integriert.

Die Umsetzung des CRISAM® Cost Benefit Analyzers erfolgt in drei Schritten:

>> Neuer Bericht "Risikosimulation": Mit dem Bericht Risikosimulation werden der Risikobaum bzw. Teile davon simuliert und die Risiken nach Kriterium, IT-Service bzw. Ressource, Geschäftsprozess bzw. Organisationseinheit und Unternehmen aggregiert. Der Bericht wird auf Excel ausgegeben und ermöglicht damit eine einfache Weiterbearbeitung und -verarbeitung. Die Risiken werden mit den drei monetären Werten VaC (Value at Chance oder 5% Perzentil), Erwartungswert und VaR (Value at Risk oder 95% Perzentil) sowie weiteren Parametern zur Beschreibung der resultierenden Verteilungsfunktion ausgegeben. Der Bericht Risikosimulation ist ab sofort verfügbar.

>> Neuer Bericht "Kosten/Nutzen Simulation": Mit diesem Bericht werden die in CRISAM® hinterlegten Maßnahmen den Risikowerten gegenübergestellt. Damit wird ersichtlich, welche Kosten/Einsparungen aus der Umsetzung geplanter Maßnahmen welche Veränderung im resultierenden Risiko bewirken. Dieser Bericht ist Anfang nächsten Jahres verfügbar.

>> Integration in die Benutzeroberfläche von CRISAM® Explorer: Die in den Berichten enthaltenen Daten werden dann direkt über die Benutzeroberfläche rasch und intuitiv abrufbar gemacht und übersichtlich angezeigt. Diese Funktion ist Anfang nächsten Jahres verfügbar.

Der CRISAM® Cost Benefit Analyzer ermöglicht es somit, über die Veränderung der resultierenden Risiken den Nutzen von Maßnahmen darzustellen. Damit wird eine vielfach geäußerte Vision von Risikomanagern Wirklichkeit: Durchführung einer Investitionsrechnung für Investitionen zur Risikobehandlung (vgl. Return of Security Investments - ROSI).


 logbuch

03

Neues CRISAM® Report Pack verfügbar



Ing. Mag. Günther Angerbauer
Leiter Entwicklung
calpana business consulting GmbH

Mit dem CRISAM® SLM Report Pack können IT-Serviceprovider ab sofort aus den Ergebnissen im CRISAM® Risikomanagement Service Level Agreements mit ihren Kunden ableiten, vereinbaren und monitoren.

Ein weiterer Schwerpunkt unserer Tätigkeit beschäftigt sich mit dem Schaffen von Synergien zwischen den verwandten Disziplinen IT-Risikomanagement und Service Level Management. Erstes Ergebnis dieser Bemühungen ist das CRISAM® SLM Report Pack.

Das CRISAM® SLM Report Pack umfasst folgende zwei Berichte:

>> Neuer Bericht "Service Level Anforderungen": Der Bericht Service Level Anforderungen ermöglicht es, die Ergebnisse aus der Business Impact Analyse je Kriterium, IT-Service und Geschäftsprozess bzw. Organisationseinheit inkl. den im Risikomanagement ermittelten Anforderungen und dem daraus resultierenden Ziel-Rating darzustellen. Der Bericht wird auf Excel ausgegeben und ermöglicht damit eine einfache Weiterbearbeitung und -verarbeitung. Der Bericht ermöglicht die Ableitung von Service Levels auf Basis der im Risikomanagement ermittelten Service-Anforderungen.

>> Neuer Bericht "Business IT-Service Report": Dieser Bericht stellt eine übersichtliche Zusammenfassung für einen bestimmten IT-Service in Bezug zu einem Geschäftsprozess bzw. einer Organisationseinheit dar. Der Bericht dient als Nachweis für einen Service-Verantwortlichen des Serviceproviders im Gespräch mit dem Kunden, welche Service Level Zielwerte vereinbart wurden, ob diese erreicht wurden und welche Abweichungen vorhanden sind.

Die Verwendung der CRISAM® Ratingkennzahlen als Service Level Zielwerte bietet mehrere Vorteile für Sie und Ihre Kunden. Einerseits werden Risikomanagement und Service Level Management Richtung Kunden effizient standardisiert und andererseits wird auch den zurzeit häufig wenig beachteten Kriterien wie Vertraulichkeit und Integrität das erforderliche Augenmerk geschenkt.

04

Konzernweite Einführung von CRISAM® bei der ÖBB

Gerade in wirtschaftlich herausfordernden Zeiten ist für Unternehmen die Kenntnis aller Unternehmensbelange und Kennzahlen von zentraler Bedeutung. Im Zusammenhang mit der IT stellt sich beispielsweise die Frage nach dem Risiko und die Möglichkeiten, dieses Risiko auf ein adäquates Niveau zu bringen und zu halten. Diese Frage- und Problemstellungen kennt wohl jeder CIO, wobei er Ihnen meist ratlos gegenübersteht, da die verwendeten Toolsets zur Risikodarstellung nicht die entsprechenden Antworten bringen.

Im ÖBB-Konzern stand man ebenfalls vor der Herausforderung, eine Wirtschaftlichkeitsberechnung für die IT-Risikovorsorge zu entwickeln. Man versuchte, diese Aufgabe zuerst mit dem traditionellen Ansatz ROI (Return of Invest) zu lösen. Mit dem ROI war es zwar möglich, die Wirtschaftlichkeit von Investitionen auszurechnen bzw. den Zeitpunkt zu bestimmen, ab wann sie sich rechnen.

>> weiter auf der nächsten Seite


 logbuch

04

Dieser Ansatz war jedoch nicht dafür geeignet, um IT-Sicherheitsinvestitionen zu beurteilen. Deshalb haben sich alle ÖBB-Konzerngesellschaften schließlich entschieden, CRISAM® als Instrument einzusetzen, um IT-Risiken zu identifizieren, zu bewerten und in einem kontinuierlichen Verbesserungsprozess zu steuern. Dadurch konnten die Auswirkungen der Beschaffenheit der IT-Systeme in Bezug auf die Geschäftsprozesse aufgezeigt werden. Letztendlich wurde eine Reduktion der möglichen negativen Auswirkungen durch IT-Systeme und -Prozesse auf das Geschäftsergebnis erzielt. Ein weiterer Vorteil ergab sich aufgrund der Verbindung zum allgemeinen Risikomanagementsystem im Konzern, wodurch die IT-Risiken automatisiert übernommen werden konnten. Schließlich war es mit Hilfe von CRISAM® möglich, über Simulationen die Verbesserungen der IT-Infrastruktur sichtbar und somit die Auswirkungen der empfohlenen Maßnahmen direkt nachvollziehbar zu machen, wodurch auch die Transparenz des Service Providers ÖBB-DLG IS gesteigert werden konnte. CRISAM® hat sich somit auch im ÖBB-Konzern als gutes Instrument für die Entscheidungsträger zur Unternehmenssteuerung erwiesen, denn CRISAM® bewertet die Unternehmens-IT im Kontext der unterstützten Prozesse und liefert klare und nachvollziehbare Entscheidungsgrundlagen.

ÖBB-Dienstleistungs GmbH

Aufgabe der ÖBB-Dienstleistungs GmbH ist es, den gesamten ÖBB-Konzern in zahlreichen Querschnittsfunktionen zu unterstützen. Die DLG steht den Kunden als Berater zur Seite, damit im komplexen Unternehmen ÖBB Doppelgleisigkeiten vermieden, Einsparungen durch eine effiziente Einkaufspolitik und eine bestmögliche Unterstützung durch eine qualitativ hochwertige Informationstechnologie erreicht werden können. Besonders wichtig sind auch die Schaffung und Einhaltung von einheitlichen Rahmenbedingungen zur gerechten Behandlung aller MitarbeiterInnen im Konzern. Die Kernkompetenzen der DLG umfassen die Geschäftsbereiche Personalmanagement (Human Resources), Informationstechnologie (Information Services), zentraler Einkauf sowie die Internen Dienste und Soziales. Die DLG unterstützt mit ihren hochwertigen Dienstleistungen den Konzern bei seiner zentralen Zielsetzung, eine europäische Top-Bahn zu werden.

"Mit der Umsetzungen dieses konzernübergreifenden Projektes ist es gelungen ein IT-Risikomanagementsystem zu etablieren, das nicht nur die bestehenden IT-Risiken aufzeigt, sondern auch die Wirkung der vorgeschlagenen Verbesserungsmaßnahmen auf das Restrisiko visualisiert und diese Daten dem Enterprise Risikomanagement direkt zur Verfügung stellt."

(Ing. Bruno Fegerl, Projektleiter bei der ÖBB-DLG Information Services)




 logbuch

05

RMA Österreich NEWS

Am 30. Juli 2009 fand die erste Sitzung des RMA Österreich-Arbeitskreises "Enterprise Risk Management (ERM)" in Salzburg statt. Es wurde ein Vortrag zum Thema "Enterprise Risk Management - Quo vadis?" abgehalten und entwicklungsfähige Themen für den Arbeitskreis diskutiert und priorisiert. Abschließend wurden Themengruppen gebildet und die nächsten Schritte besprochen. Die Teilnehmer berichteten einander über ihre Überlegungen und Erfahrungen, wodurch jeder von diesem Tag diverse Anregungen und Denkanstöße mitnehmen konnte. Am 21. September 2009 trafen sich die Teilnehmer des RMA Österreich-Arbeitskreises "Information Risk Management (IRM)" bei der Kapsch BusinessCom AG in Wien bereits zum zweiten Mal, wo die ersten Ergebnisse aus den einzelnen Arbeitsgruppen präsentiert und diskutiert wurden. Nach dem erfolgreichen Start werden auch schon Aktivitäten für die weitere Vernetzung der RMA Österreich-Mitglieder geplant.



Nominierung für den "ebiz egovernment award 2009 Oberösterreich"

Der "ebiz egovernment award" zeigt die Möglichkeiten von Informationstechnologie (IT) bei der Neugestaltung von Geschäftsprozessen auf und stellt den Wandel des Wirtschaftens dar, der durch die Digitalisierung eintritt. Die Ausschreibung hat zusätzlich den Schwerpunkt E-Government, um den Nutzen und den Effekt innovativer Services und Projekte in der Verwaltung öffentlich darzustellen. Der Wirtschaftspreis wird seit 2005 in jedem Bundesland vergeben. Das Bundeskanzleramt, Plattform Digitales Österreich, sowie weitere Sponsoren und Partner haben sich gemeinsam mit dem Report Verlag zum Ziel gemacht, Benchmark-Lösungen zu finden und auszuzeichnen sowie das Bewusstsein für neue Möglichkeiten zu schärfen. Jene Unternehmen, die IT und E-Business zu ihrem Vorteil gewinnbringend nutzen, werden ins Rampenlicht geholt. Auch die calpana business consulting gmbh war mit dem Projekt "ISO 27001-Zertifizierung bei der Verbund-Austrian Power Grid AG" für den "ebiz egovernment award 2009 Oberösterreich" nominiert. Die Vorstellung der nominierten Projekte und Unternehmen sowie die Prämierung der Sieger von Oberösterreich und Salzburg hat am 22. September 2009 bei der Galaveranstaltung im Linzer Landhaus stattgefunden.


 logbuch

06

qSkills Security Summit 2009



Am 12. Oktober 2009 findet in Nürnberg der zweite qSkills Security Summit statt. Im Fokus des diesjährigen Security Summit steht das Thema Risikobewertung, Quantifizierungsmodelle und IT-Sicherheitsstrategien. Wie die wirtschaftlichen Turbulenzen der letzten Monate verdeutlichen, sind neue Methoden und vor allem die Eingliederung eines Risikomanagements in das unternehmensweite Gesamtkonzept erforderlich. Vertreter namhafter Unternehmen und renommierte Experten sprechen über die Vorteile und Chancen strategisch angelegter Konzepte und aktuelle Entwicklungen von zukunftsweisenden Sicherheitsstrategien. Treffen Sie die Besten und profitieren Sie von deren Erfahrungen!

Zu den Vortragsschwerpunkten zählen unter anderem:

Risikomanagement	(Austrian Airlines - Dr. Wolfgang Henle, Österreichische Bundesbahn - Ing. Bruno Fegerl, calpana business consulting - Dr. Manfred Stallinger, Swisscom - Jörg Jungblut, RiskNet - Frank Romeike)
ISO 31000	(Steinbeis-Transferzentrum - Dr. Peter Meier)
Cloud-Computing	(icomsoft - Dennis Zimmer, Rödl & Partner - Dr. Christiane Bierehoven)
Soziale Netze	(Heise Security - Jürgen Schmidt)
Auditing	(Secuomic - Martin Freiss)
Sensible Daten	(cirosec - Stefan Strobel)
(Un)Sichere SAP-Programmierung	(Virtual Forge - Dr. Markus Schumacher)
Podiumsdiskussion	(Frank Romeike / Dr. rer. nat. Böhmer)

Veranstaltungspauschale: 195,- € - inkl. VIP-Package

Das VIP Package beinhaltet eine Übernachtung, ein Abendessen am 12.10.09, eine Gastkarte zur it-sa Securitymesse sowie eine Gastmarke für it-sa VIP-Lounge.

Nähere Informationen dazu finden Sie unter www.qskills-security-summit.de