Information Risk Management mit einer Balanced Scorecard

Dirk Loomans
Dr. Loomans Unternehmensberatung
Mainz

Dr. Loomans
Unternehmensberatung

Warum eine Balanced Scorecard

- Erfolgreiche Sicherheit wirkt sich nicht sofort auf das Betriebsergebnis **positiv** aus
- Konsequenz: Informationssicherheit kann nicht durch Fokusierung auf die Finanzperspektive (Umsatz/Gewinn, Kosten…) erfolgreich betrieben werden keine Transparenz
- Andere Bereiche müssen ebenfalls fokussiert werden:
  - Relevante Prozesse
  - Awareness der Mitarbeiter, Kommunikation mit Partnern
  - Fortentwicklung der Sicherheit (Maßnahmen, neue Problemfelder)
  - Risikostatus und seine zeitliche Entwicklung

Dr. Loomans
Unternehmensberatung

Problem: Messbarkeit

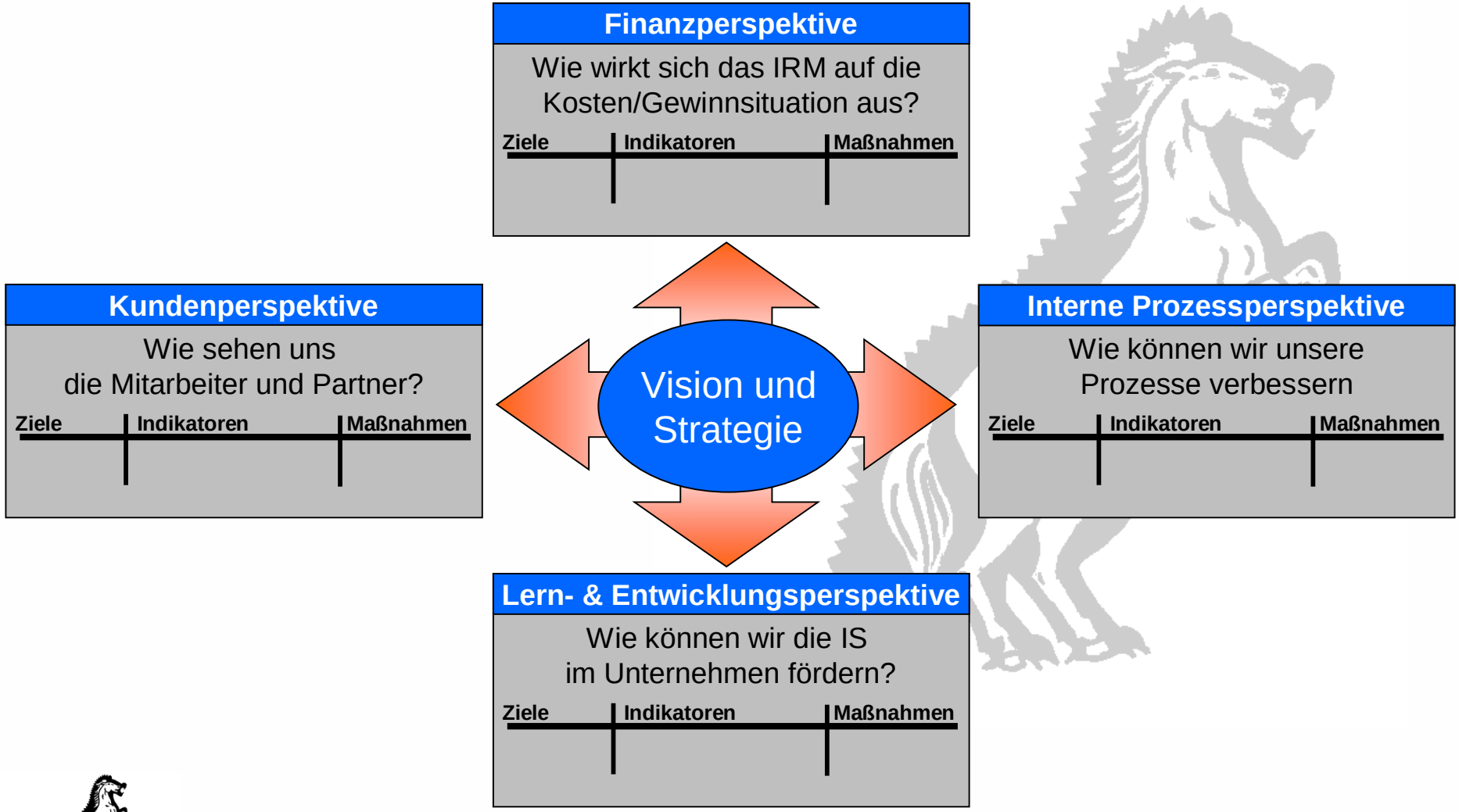
Credo: Man kann nur managen, was man auch messen kann

Das bedeutet:

- Alle Aktivitäten im IRM müssen durch Kennzahlen messbar und vergleichbar gemacht werden
  - Nur so ist ein vernünftiges Berichtswesen und Steuerung möglich
  - Nur so kann eine Basis für finanzperspektivische Betrachtungen geschaffen werden
  - Nur so entsteht die Möglichkeit einer messbaren Umsetzung von Visionen und Strategien

Dr. Loomans
Unternehmensberatung

Information Risk Scorecard IRSC



Dr. Loomans
Unternehmensberatung

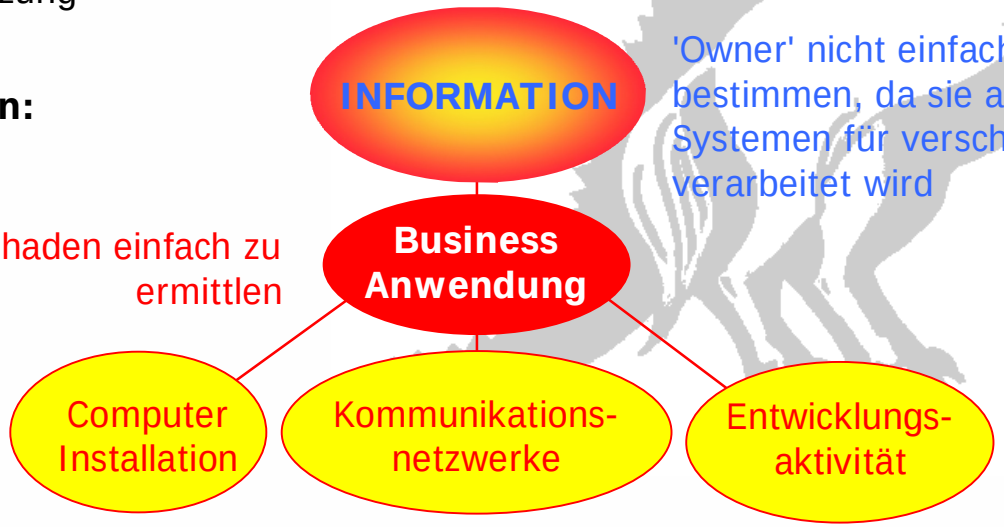
Weitere Schlüsselbegriffe

Arrangement oder Control: Eine Richtlinie, Methode, Prozess, Geräte oder programmierter Ablauf um Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen zu schützen.

IS-Vorfall (information incident): Ein Ereignis (oder Ereigniskette), das die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen verletzt, z.B. durch:

- Hardware- oder Softwarefehlfunktionen
- Verlust von Mitarbeitern, Ausrüstung oder Standorte
- Überlast
- Menschliches Versagen
- Unvorhergesehene Auswirkungen von Änderungen
- Zugriffsschutzverletzung

IT-unterstützte Informationsressourcen:



Dr. Loomans Unternehmensberatung

Die **FIRM** Methode

FIRM *ist eine ausgereifte Methode um unternehmensweit Informationsrisiken zu managen:*

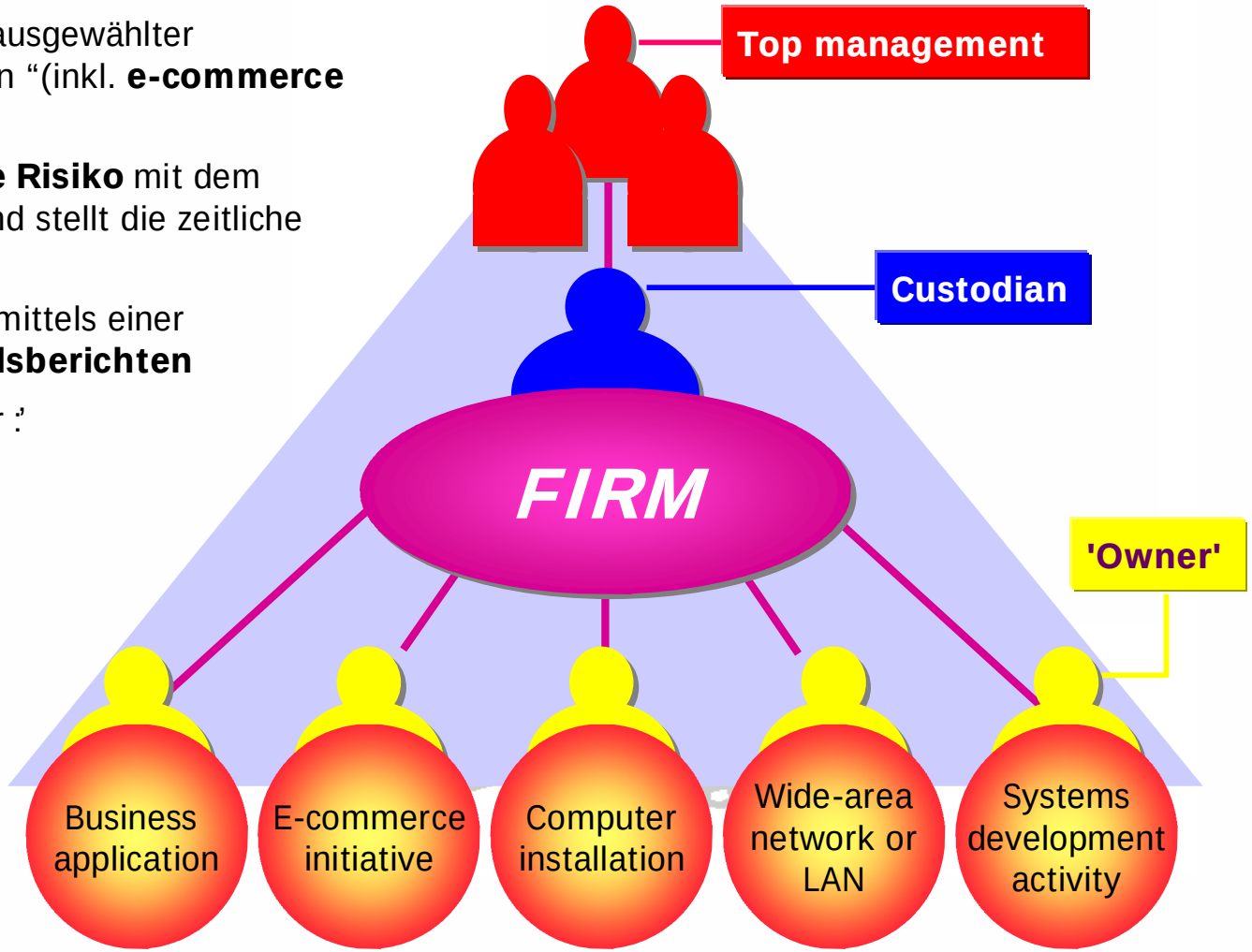
- Ein bahnbrechender, **quantitativer** und **Maßnahmen basierter** Ansatz
- Veröffentlicht durch das Information Security Forum (ISF) –einem Verein mit 250+ Mitgliedern (Globale Firmen und Organisationen, die in diesem Verein Forschung im Bereich Informationssicherheit unterstützen und gegenseitigen Erfahrungsaustausch fördern) SF
- Basierend auf statistischen Analysen der umfangreichen ISF-Daten
- Wurde von den ISF Mitglieder mit großem Interesse aufgenommen
- Unterstützt BS7799 und ISO 17799 sowie den „Forum's Standard of good practice "
- Umfassend dokumentiert und mittlerweile auch für nicht ISF-Mitglieder zugänglich

Dr. Loomans
Unternehmensberatung

Organisation und Prozesse

FIRM:

- Überwacht die Risiken ausgewählter „Informationsressourcen “(inkl. **e-commerce** Initiativen)
- Vergleicht das **aktuelle Risiko** mit dem **akzeptablen Risko** und stellt die zeitliche Entwicklung dar
- Erhebt die Risikodaten mittels einer **Scorecard** und **Vorfallsberichten**
- Erstellt für jeden „owner “:
  - einen 1-seitigen **risk status report**
  - **guidance on driving down risk**
  - Einen **Action-plan**
- Ebenso werden erstellt:
  - Risiko Ranglisten
  - andere high-level Berichte
  - Vorfallsstatisitken



Die **FIRM** Methode wird herausgegeben durch das Information Security Forum, London.

Dr. Loomans Unternehmensberatung

Monitoring Prozess mit positiver Rückkopplung

Die FIRM Methode beinhaltet einen 2 phasigen Monitoring Prozess, der sicherstellt, dass niemand bestraft, sondern Erfolg belohnt wird

Dr. Loomans
Unternehmensberatung

I-risk Scorecard, um Risiken zu erfassen

*Die 2-seitige **I-risk scorecard** ist optimiert für Papier und Bildschirmdarstellung*

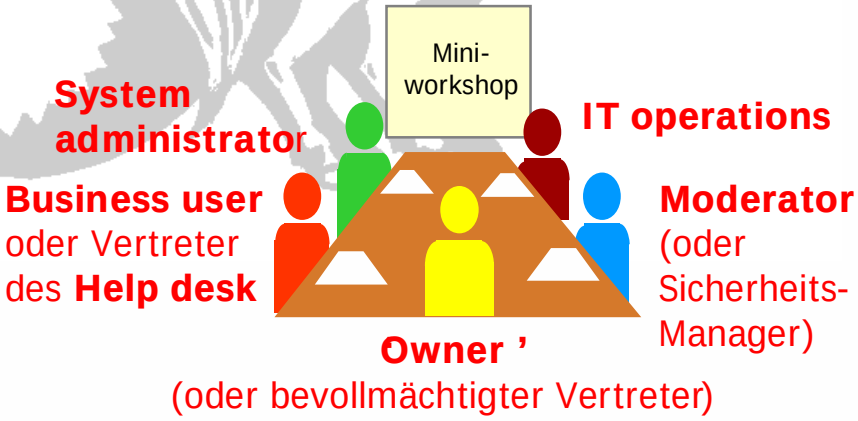
*Beim ersten Mal wird die Scorecard am besten in einem **Miniworkshop** ausgefüllt (Dauer ca. 1,5 Std.)*

*Die I-risk Scorecard misst für eine Ressource **5 Risikoindikatoren**:*

- Das Schadenspotential für das Unternehmen (**criticality**)
- Die Schwachstellen in 17 Bereichen (**control weakness**)
- Besonderer Rahmenbedingungen (**special circumstance)**
- Anzahl der Vorfälle im letzten Jahr **(level of threat)**
- Die tatsächlichen Schäden, die durch Vorfälle entstanden sind (**business impact**)

Ebenso werden erfasst:

- Eine Beschreibung der Ressource (**identity**)
- Verantwortlichkeiten (**accountability**) (z.B. Owner)
- Der Status der Verbesserungsmaßnahmen (**improvement activity**), z.B. zur Beseitigung von Schwachstellen



Dr. Loomans
Unternehmensberatung

Die Scorecard misst I-Risiken realistisch

Die Scorecard vermittelt ein stringentes Verständnis dafür, was Risiken nach oben oder unten treibt

Statistisch bedeutend

Betriebsw. bedeutend

Criticality: Ein Maß für den maximalen Schaden, der durch einen Vorfall entstehen kann. Je größer der Wert, desto höher der Schutzbedarf

Vulnerability: a) Status of arrangements: Ein Maß für Schwachstellen auf verschiedenen Gebieten. Je mehr Schwachstellen auftreten, desto größer ist die Wahrscheinlichkeit für einen Vorfall

Vulnerability: b) Special circumstances: Ein Maß für besondere Rahmenbedingungen. Je mehr zutreffen, desto höher die Vorfallswahrscheinlichkeit

Level of threat: Ein Maß für die Anzahl der tatsächlich aufgetretenen Vorfälle. Je größer die Anzahl, desto höher die Wahrscheinlichkeit für einen schweren Vorfall. (Auch ein Kontrollinstrument für die Angaben zu den Schwachstellen)

Business impact: Ein Maß für Schadensart und –höhe der beobachteten Vorfälle. Es beweist, dass Vorfälle eine reale und greifbare Bedrohung sind. So werden betriebswirtschaftliche Bewertungen möglich und detaillierte Vorfallsberichte angestoßen

Dr. Loomans Unternehmensberatung

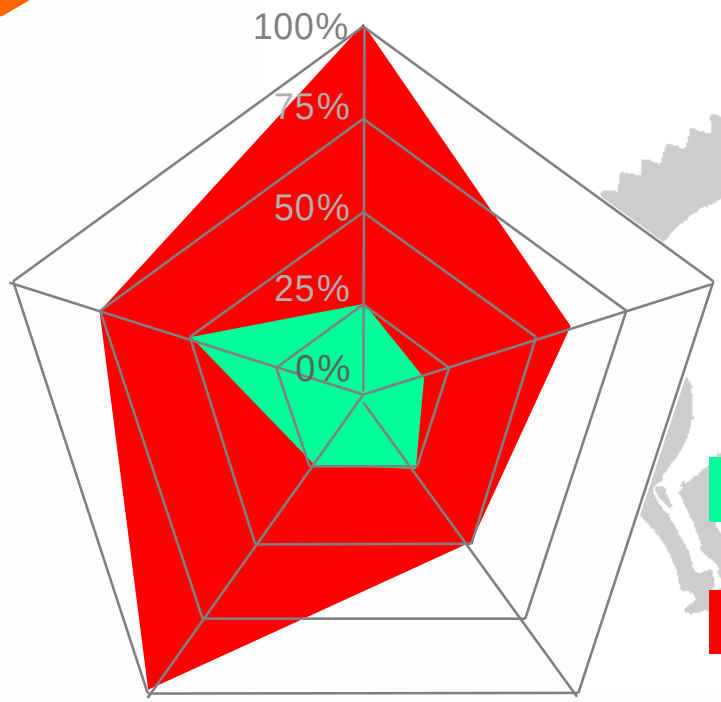
Wie werdem Risiken einer individuellen Anwendung dargestellt

Die vom System erzeugten Risiko Charts heben die Bereiche mit nicht akzeptablen Risikoniveau hervor und ermuntern ***Risiken zu minimieren***

Hier ergeben sich die meisten Möglichkeiten zur Risikoreduktion

Control weaknesses

Schwachstellen



Criticality

Special circumstances

Alle Kennzahlen werden auf eine gemeinsame Skala abgebildet (0-100%). Der äußere Rand markiert das maximal mögliche Risiko.

Akzeptables Risikoniveau (top-management definiert)

Tatsächliches Risikoniveau der Anwendung Xnn

Level of threat

Business impact

Dr. Loomans Unternehmensberatung

"Unsicherheitskosten "

Citicus ONE *ermöglicht es, die "Unsicherheitskosten "zu quantifizieren. Dafür werden die Vorfallsberichte ausgewertet*

The 'cost of insecurity '	
Nature of impact	**Calculated amount**
Loss of sales income	$66,400,000
Unforeseen costs	$26,800,000
Total reduction in profit	**$33,430,000**
Loss of tangible assets	$1,100,000
Total reduction in the value of the business	**$34,500,00**
Average reduction in profit per individual reported incident	**$328,000**

Die oben angegebenen Zahlen basieren auf den finanziellen Schadens-angaben von 102 Vorfällen, von denen 71 mindestens schwere Schäden verursachten. Der gesamte finanzielle Schaden ist nicht bekannt, da die obigen Werte die große Anzahl kleiner Vorfälle unberücksichtigt lassen. Somit dürfte der tatsächliche Schaden deutlich größer sein.

Diese Art der Datenerhebung:

- Ist praktikabel
- Führt zu Ergebnissen, die für das Top-Management lesbar und interessant sind
- Erlaubt eine betriebswirtschaftliche Beobachtung der Trends
- Rechtfertigt Investitionen für Personal und andere Maßnahmen

Dr. Loomans
Unternehmensberatung

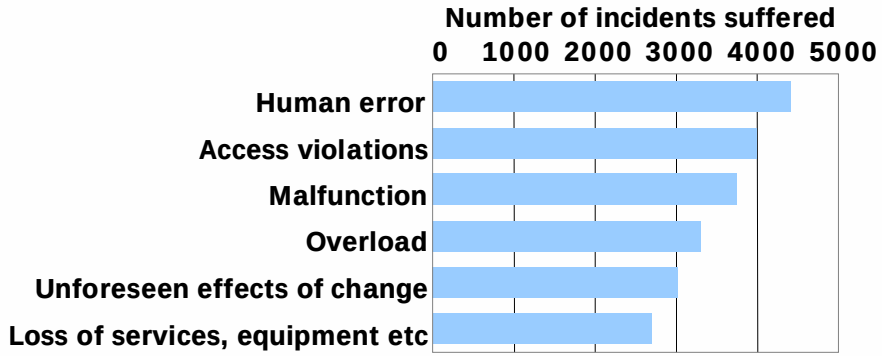
Statisitische Ergebnisse

Daten für die Planung und Priorsierung von Maßnahmen

z.B. Identifikation von:

- Den meist verbreiteten Schwachstellen
- Den häufigsten Vorfallsarten
- Den Vorfallskosten
- Den ursächlichen Gründen für Vorfälle
- Vorbildlichen Lösungen

Type of incident affecting our business-critical systems



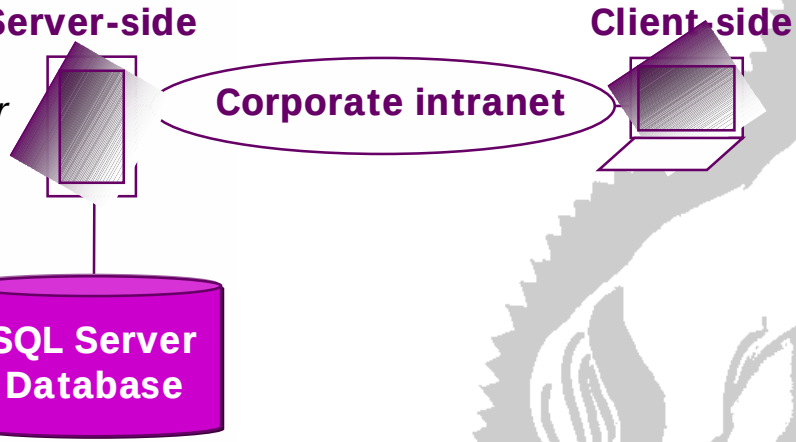
Control weaknesses affecting our business-critical systems

Dr. Loomans
Unternehmensberatung

Citicus ONE –Technische Übersicht

Citicus ONE *wurde optimiert für*:

- **Einfache Installation:** Keine Installation auf den Clients
- **Einfache Handhabung:** Die "Owner "entlasten
- **Anpassungsfähigkeit:** Kundenspezifische Einstellungen (z.B. Übernahme der eigenen Policies und Richtlinien) und Skalierbarkeit und beliebige Unternehmensstrukturen und -größen



NT4 / Windows 2000 Server
IIS 4.0 / 5.0
SQL 7.0 / SQL 2000

Nur Browser –keine zusätzliche client-seitige software

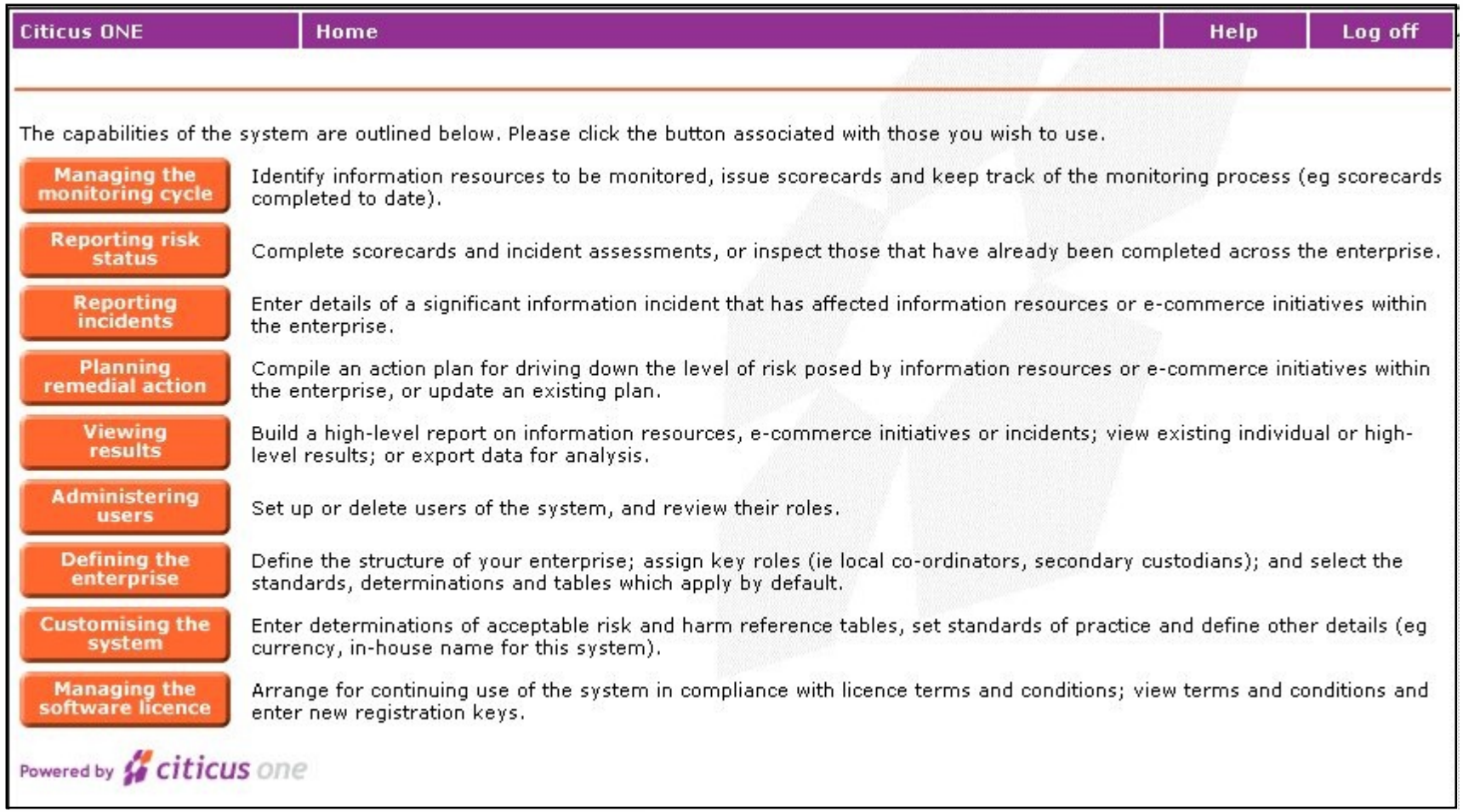
Internet Explorer v4+
Netscape Navigator v4+

Weitere Eigenschaften:

- **Einstellbare Sicherheit:** Sie bestimmen, wie viel Schutz Sie benötigen
- **Robuste Grundlage:** data-driven, skalierbares Design, Verwendung von Standardtechniken
- **Fokus auf Integrierbarkeit (zukünftig)** z.B. mit firmenweitem Vorfallsberichtswesen, e-Mail, und Verzeichnisdiensten

Dr. Loomans
Unternehmensberatung

Citicus ONE Startseite. Darstellung der Grundfunktionen



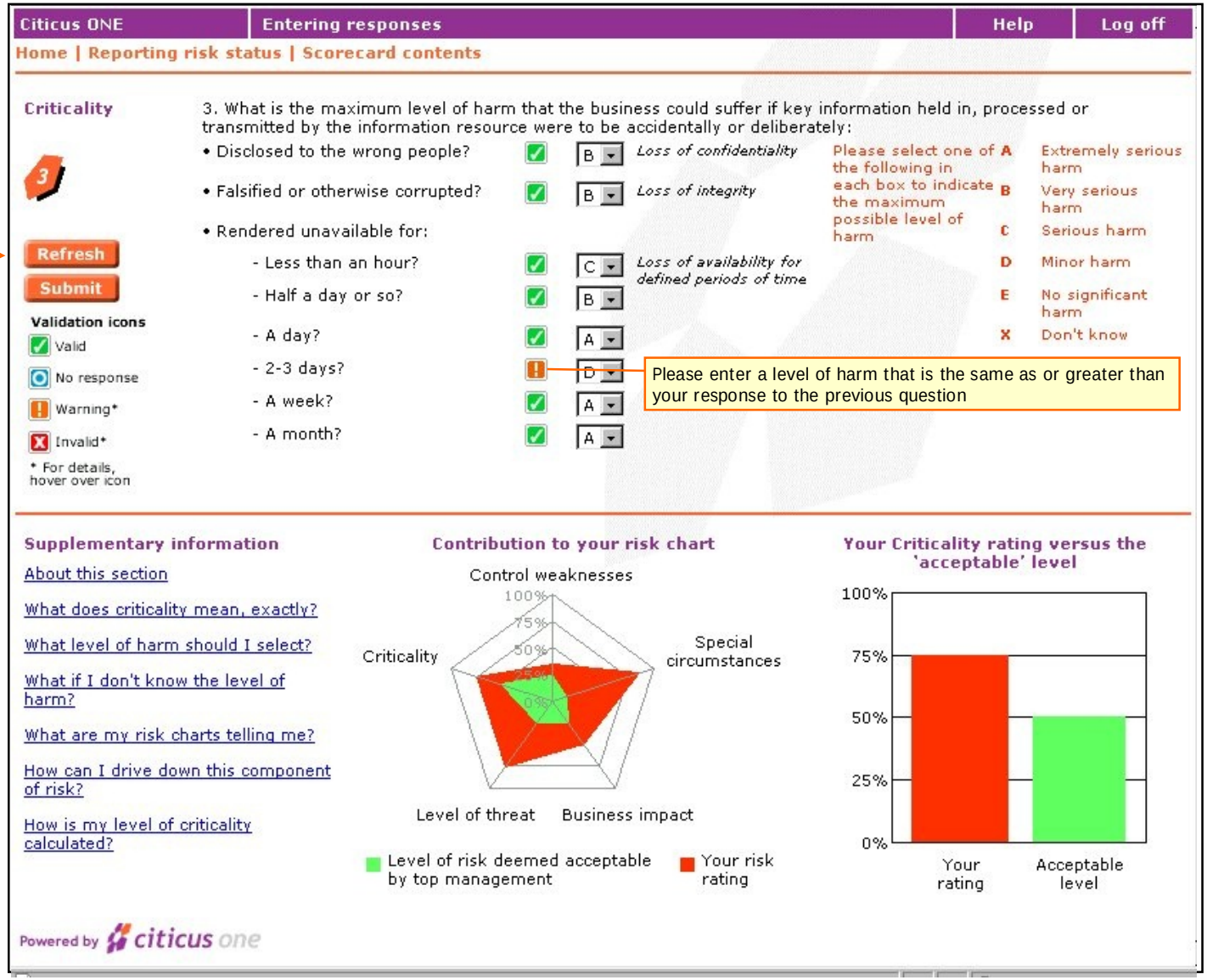
Dr. Loomans
Unternehmensberatung

Owner ’erhalten sofort eine grafische Übersicht über ihren Status

Refresh button zeigt die Auswirkungen der Angaben auf den Risikostatus

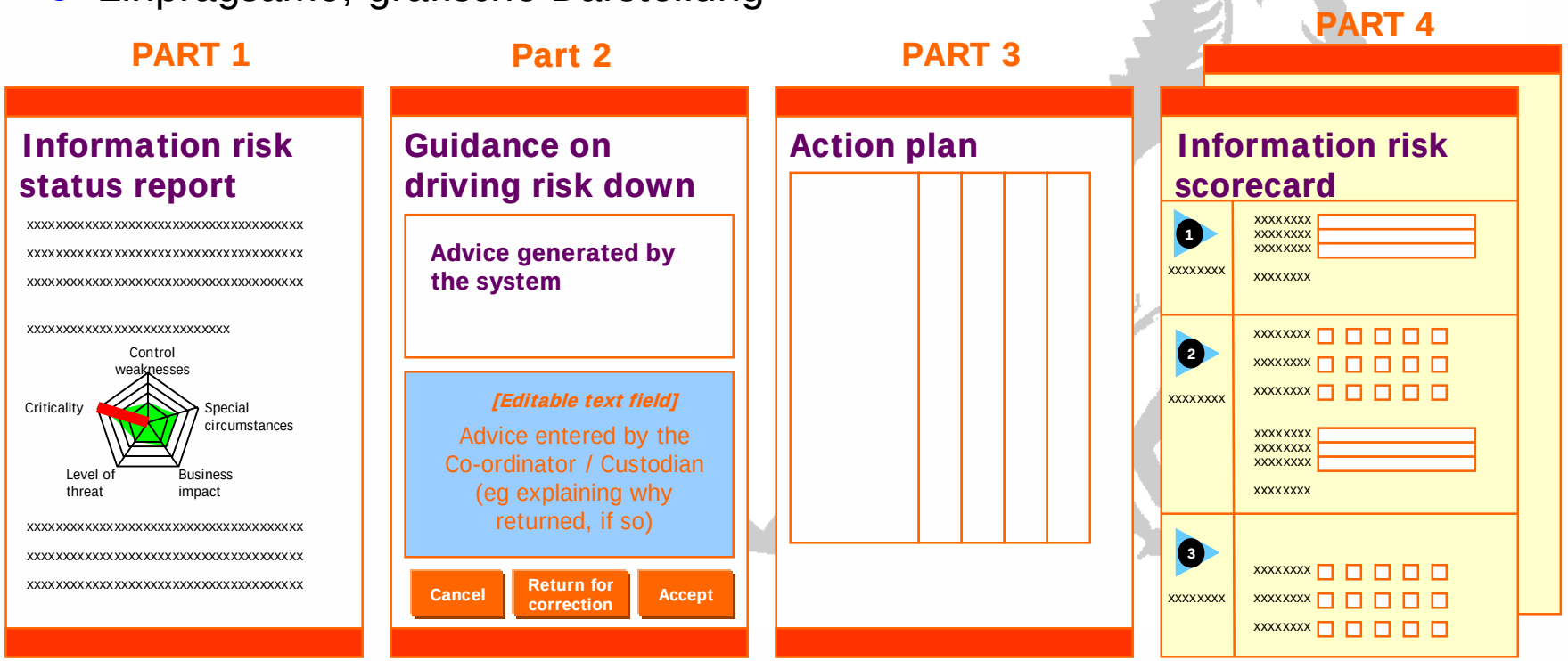
Validation icons zeigen falsche Antworten … und pop-up Fenster geben Hilfestellung

Kontext-sensitive Hilfe gibt durch einen Klick weitere Informationen



Resultate aus **Citicus ONE** für den einzelnen „Owner"

- Ausgefüllte Scorecard / incident form, sowie Ergebnisse, die dem „Owner" helfen, seine Risiken zu reduzieren
- Automatisch erstellt
- Einprägsame, grafische Darstellung



Dr. Loomans Unternehmensberatung

Citicus ONE High-level Resultate für Entscheidungsträger

- 5-teiliger, automatisch erstellter Bericht
- Basierend auf den Daten ausgewählter Informationsressourcen (oder aller)
- Einprägsame, grafische Darstellung, mit Platz für Ihre Kommentare
- Sicht auf alle Informationsrisiken in Teilbereichen oder im gesamten Unternehmen
- Alle Daten könne für weitere Analysen exportiert werden

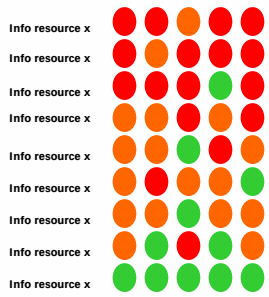
PART 1

Overall risk status

- What's been monitored
- Main results
- Greatest risks
- Progress since last period

Part 2

Risk 'league table'



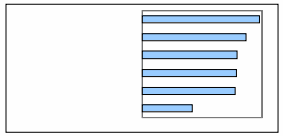
PART 3

Business impact of incidents

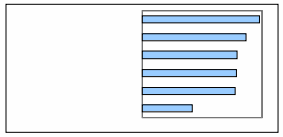
Cost of incidents

PART 4

Main vulnerabilities

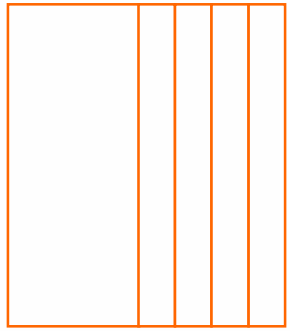


Key threats



PART 5

Action plan



Dr. Loomans Unternehmensberatung

Andere High-Level Berichte beinhalten Vorfallslisten

Incidents are ranked by business impact:

- Nimda Virus (BIA70)
- Main computer room was flooded (BIA4)
- A breach of licensing arrangements (BIA66)
- Loss of captured signatures on system (BIA2)
- Web site compromised - credit card details stolen (BIA19)
- Failure of hardware component caused system outage (BIA12)
- Customer stole userID and password to access another customer's system/data. (BIA94)
- Code Red Virus (BIA97)
- Website security breach –confidential customer information obtained (BIA44)
- Loss of connectivity to Certificate Authority (CA) database for PKI. (BIA103)
- Wrong temporary configuration caused serious delays for several hours. Network completely stuck. (BIA41)
- File with payments went accidentally from acceptance environment into production (BIA48)
- Planned process to create new seasonal plans had to be aborted due to incorrect results. Recovery to previous correct state not possible. (BIA5)
- Breach of Web-site security (BIA24)
- Nimda Virus Infection (BIA71)
- Private Internet business run using our corporate resources (BIA31)

Dr. Loomans
Unternehmensberatung

Citicus ONE Einführung: Kosten / Nutzen

Die Vorteile einer erfolgreichen **Citicus ONE** Einführung:

- Schlüsselrisiken werden erkannt und verstanden
- Die Aufmerksamkeit richtet sich auf die Informationsressourcen, die das größte Risiko bergen und auf allgemeine Schwachstellen die behoben werden müssen
- "Owner "kennen das akzeptable Risikoniveau und sind motiviert, ihre Risiken entsprechend zu verringern
- Verringerung von Schwachstellen führt zu einer messbaren Verringerung von:
  - Der Anzahl IS-Vorfällen, die Ihr Unternehmen schwächen
  - Der Wahrscheinlichkeit, dass Ihre Organisation Opfer eines schweren Vorfalls wird
  - Den jährlichen "Unsicherheitskosten "Ihres Unternehmens

Kostenfaktoren

Lizenzkosten plus Service und Wartung

Prozessdurchführung (eine Halbtagskraft plus dem Aufwand der lokalen Koordinatoren und "owner")

Vorteile für das Geschäft

Nachvollziehbare Einsparungen und Produktivitätssteigerung

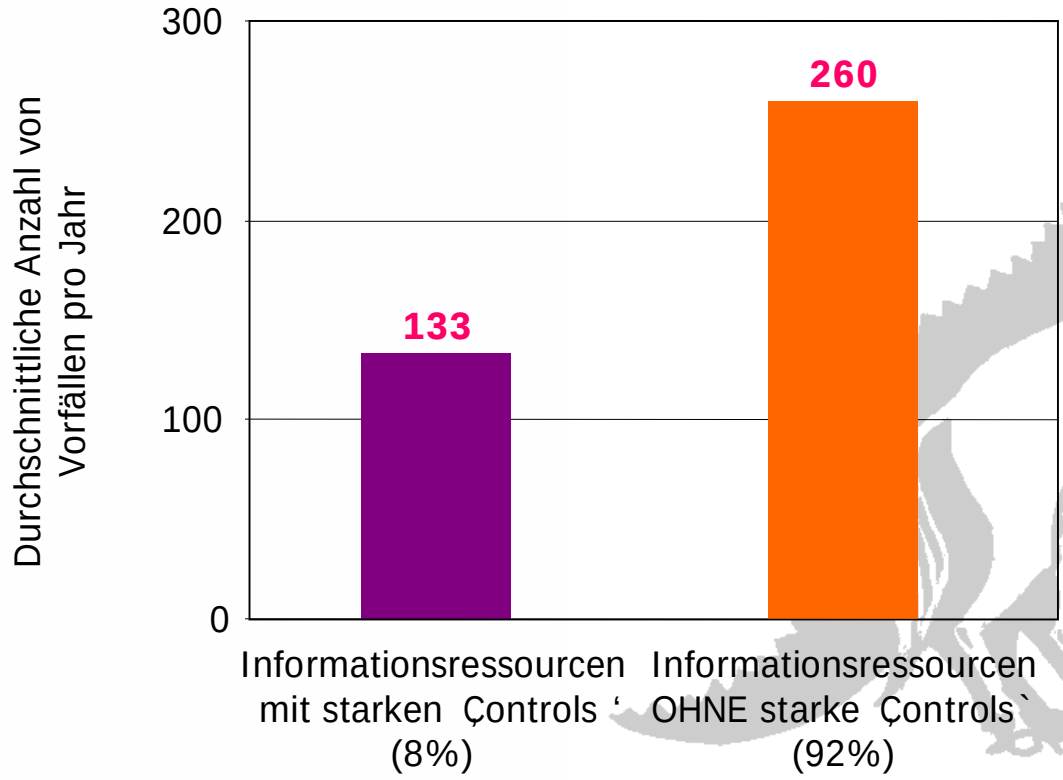
Verringertes Risiko

Verbesserte Kontrolle der IT-Prozesse

Dr. Loomans Unternehmensberatung

Ergebnisse: Gute Controls verringern die Anzahl von Vorfällen

Die durchschnittliche Anzahl der Vorfälle pro Jahr wird halbiert, wenn die `Controls ' „gut und sauber "aufgesetzt sind

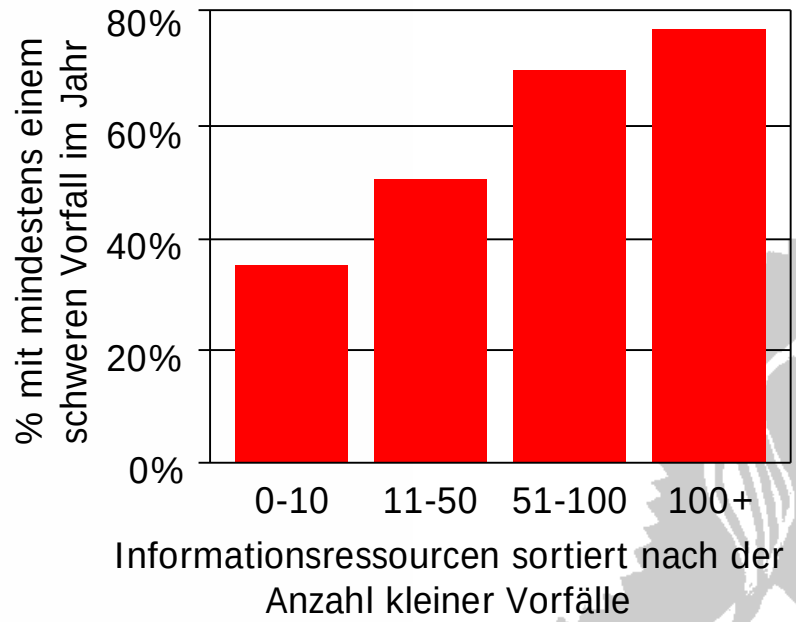


Basierend auf ca. 62.000 Vorfällen in 969 Informationsressourcen
Siehe *Driving information risk out of the business*, Information Security Forum, April 1999.

Dr. Loomans Unternehmensberatung

Ergebnisse: Die Anzahl der kleinen Vorfälle sollte verringert werden

Kleine Vorfälle sollten vermieden werden, da mit ihnen die Wahrscheinlichkeit für einen großen Vorfall direkt verknüpft ist

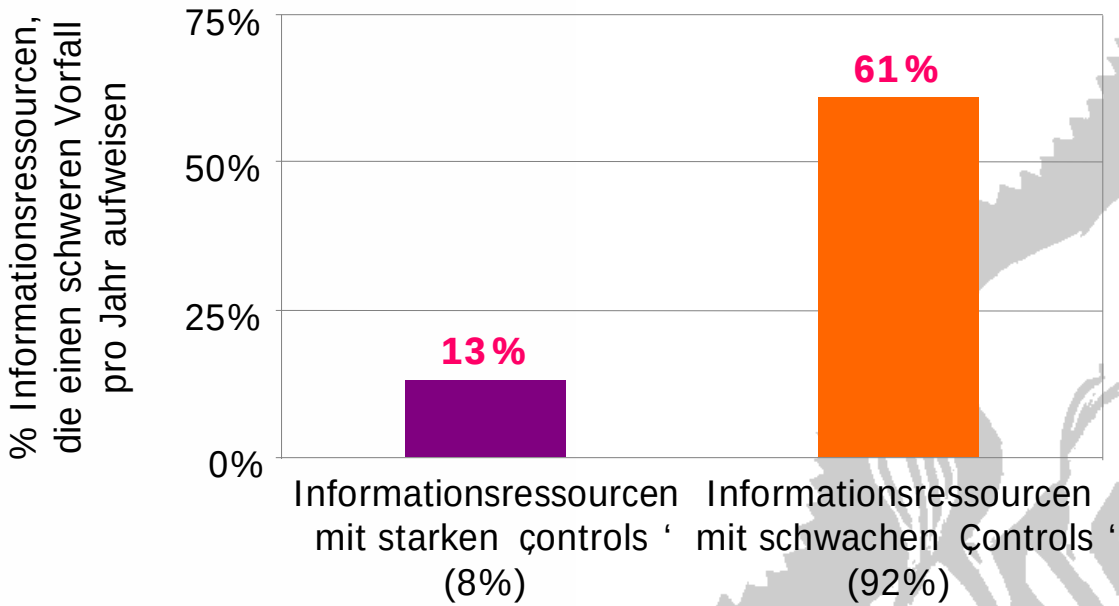


Basierend auf der Analyse von 922 Informationsressourcen, siehe
FIRM *Implementation Guide*, Information Security Forum, March 2000.

Dr. Loomans
Unternehmensberatung

Ergebnisse: Gute `Controls`verringern die Anzahl schwerer Vorfälle

Starke Çontrols ‘verringern die Wahrscheinlichkeit für einen schweren Vorfall auf weniger als ein Viertel

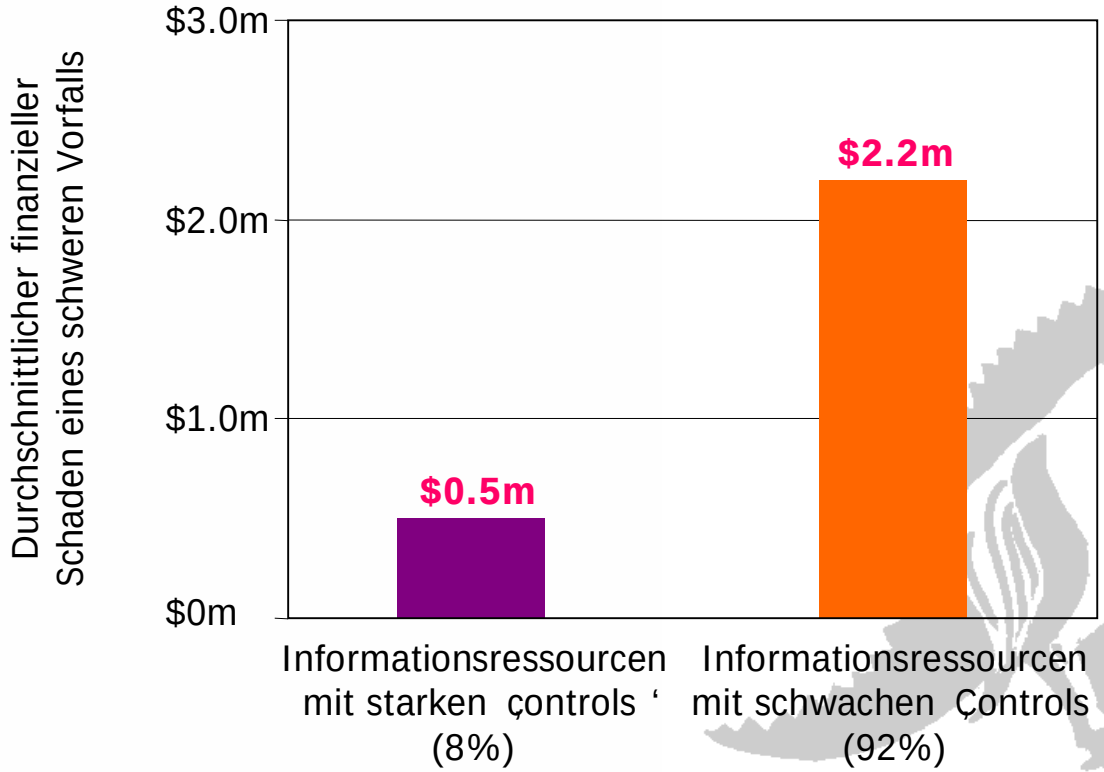


Basierend auf der Analyse von Vorfälle auf 969 Informationsressorucen Siehe *Driving information risk out of the business*, Information Security Forum, April 1999.

Dr. Loomans Unternehmensberatung

Ergebnisse: Starke `Controls` sparen Kosten

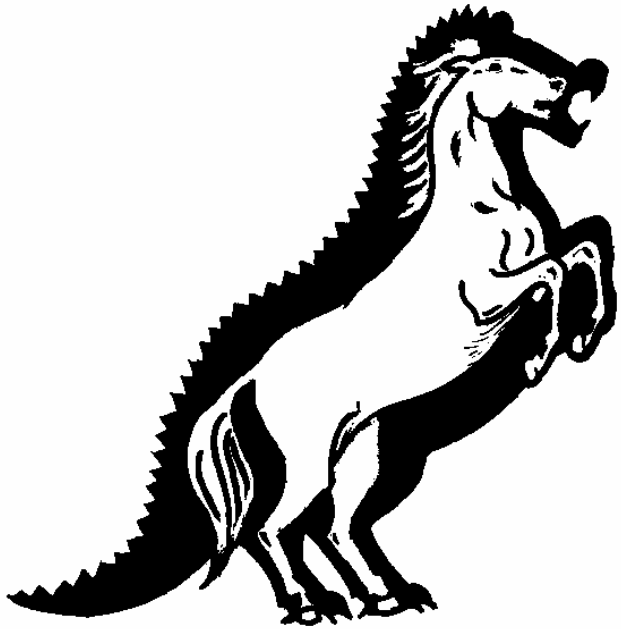
Starke `Controls` sorgen auch dafür, dass sich die Kosten für einen schweren Vorfall dramatisch reduzieren lassen



Basierend auf der Anylyse von 253 schweren Vorfällen, für die ein finanzieller Schaden ermitelt wurde. Results published in *Driving information risk out of the business*, Information Security Forum, April 1999. See also *Information risk reference guide*, Information Security Forum, September 1999.

Dr. Loomans Unternehmensberatung

Kontakt



Dr. Loomans Unternehmensberatung
Dr. Dirk Loomans

Gross-Gerauer Str. 36a
55130 Mainz
Tel.: +49 (06131) 2 77 99 79
Fax: +49(06131) 617 608
mobil: +49 (0163) 6 372 273

dirk.loomans@loomans.de