Befragung zur Informationssicherheitskultur in CH-Unternehmen

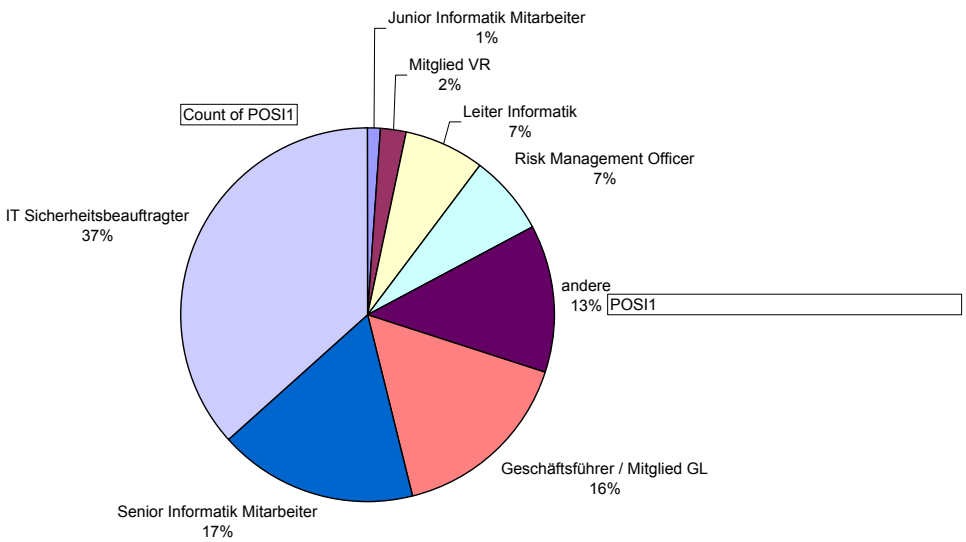
September / Oktober 2004

Arbeitsgruppe Informationssicherheitskultur der FGSec (information security society switzerland)
www.fgsec.ch/ag/isk.html

Stand: 13. April 2005

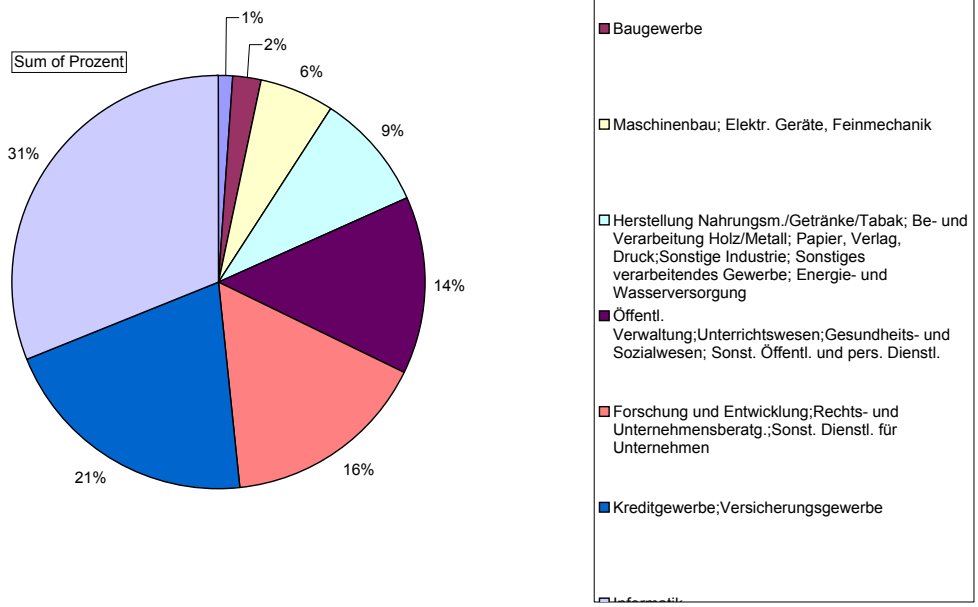
n=87

Position



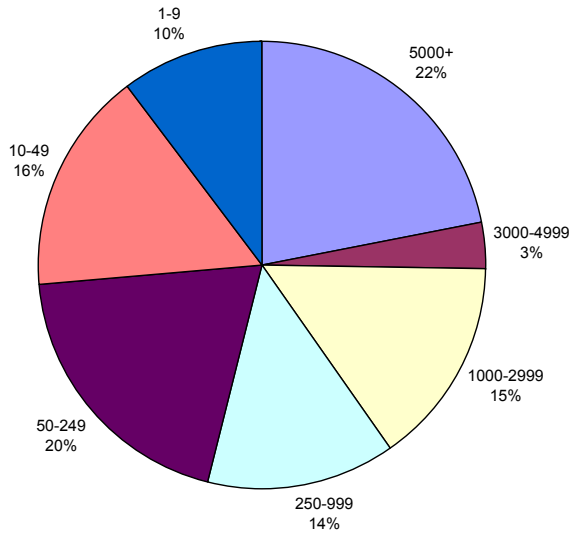
n=87

Branche



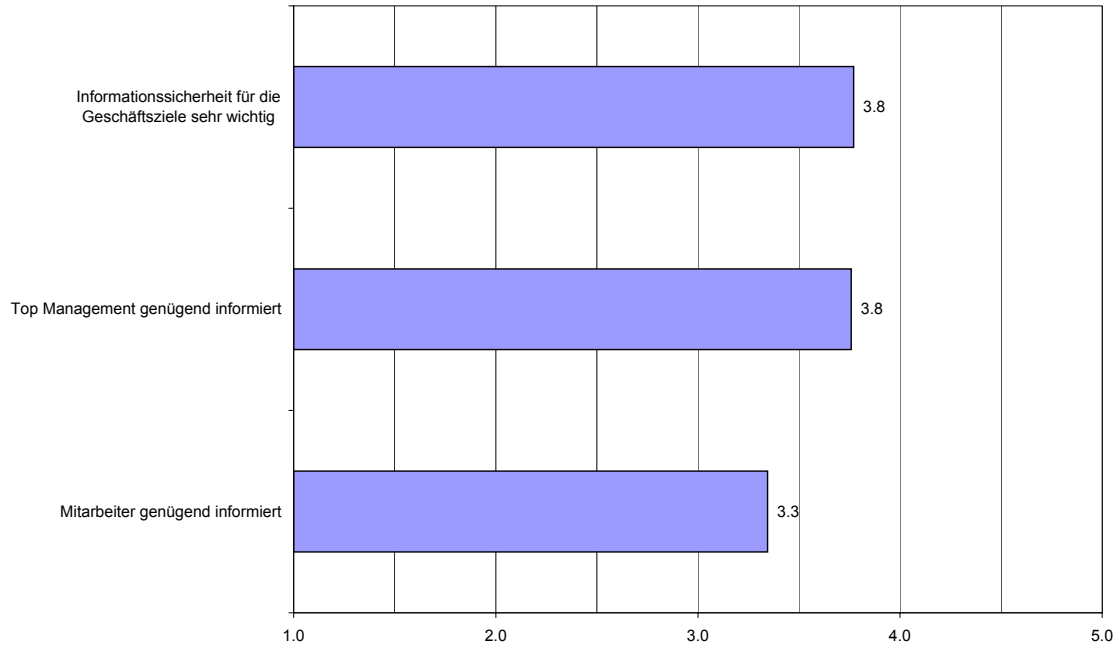
n=87

Anzahl Beschäftigte



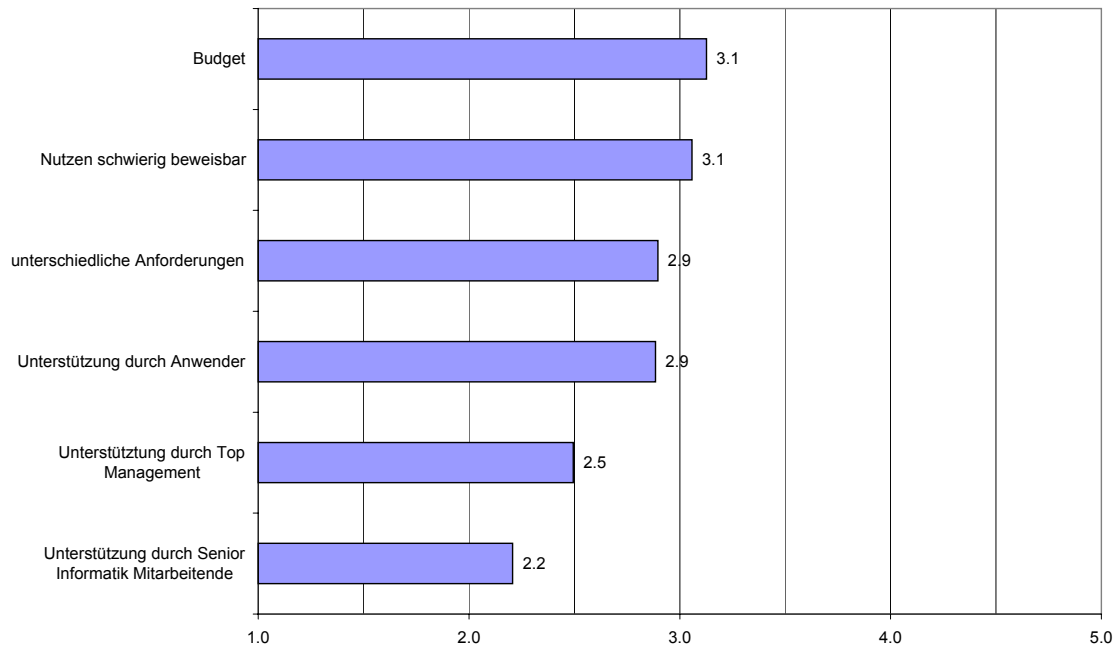
n=87

Einführung Informationssicherheitskultur



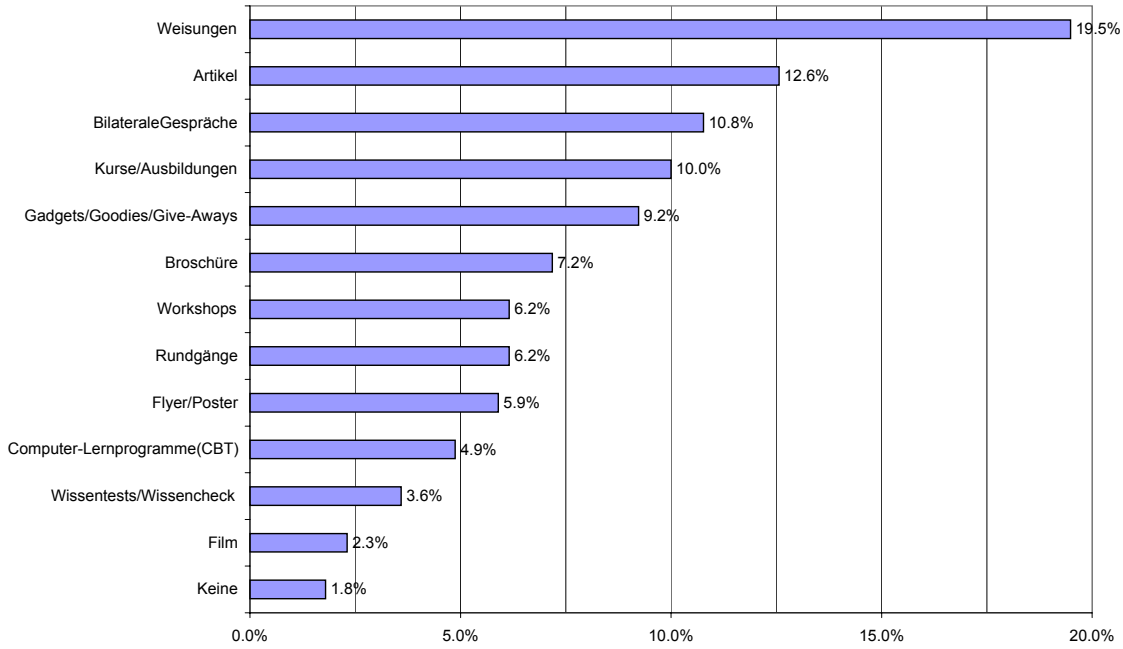
n=87

Hindernisse der Informationssicherheitskultur



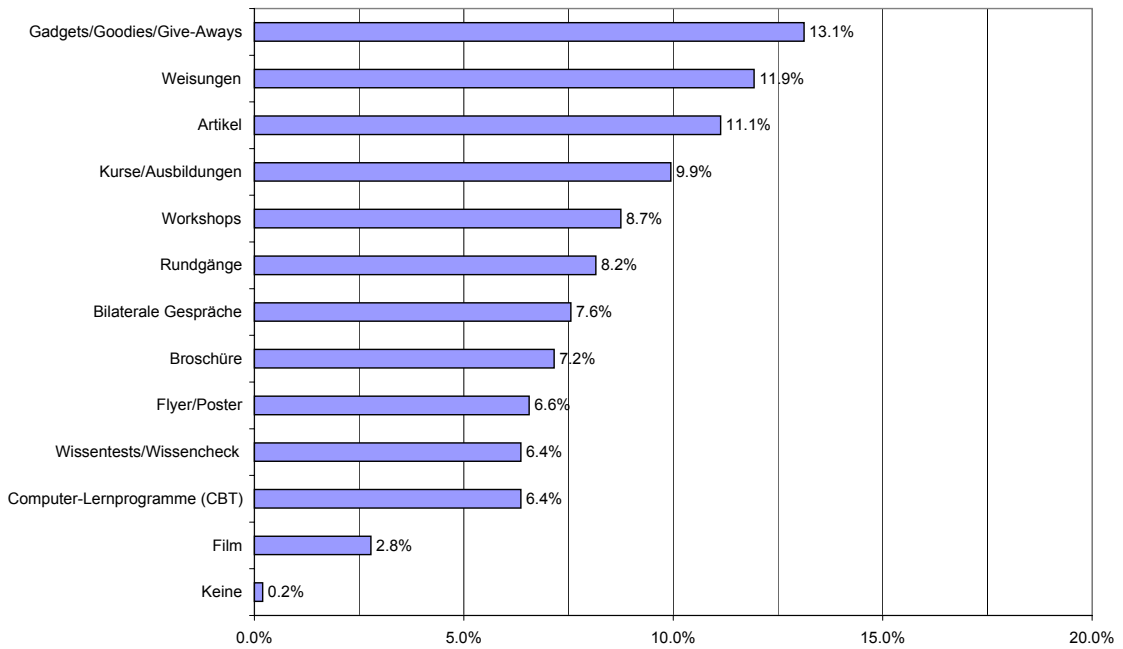
n=87

Heute eingesetzte Massnahmen



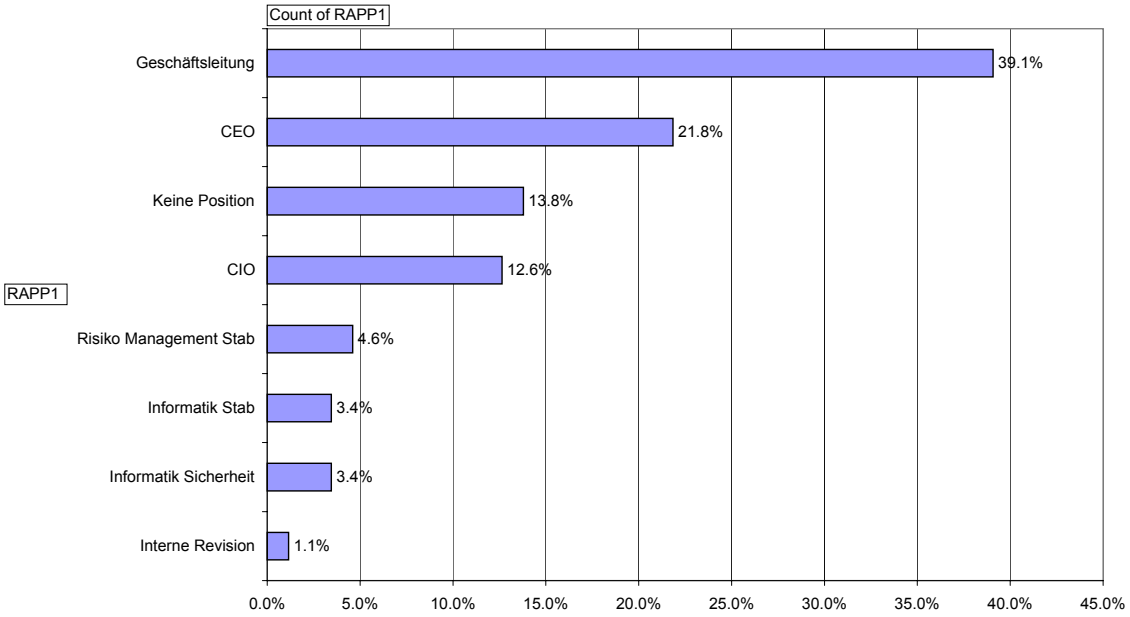
n=87

In den nächsten 2 Jahren gewünschte Massnahmen



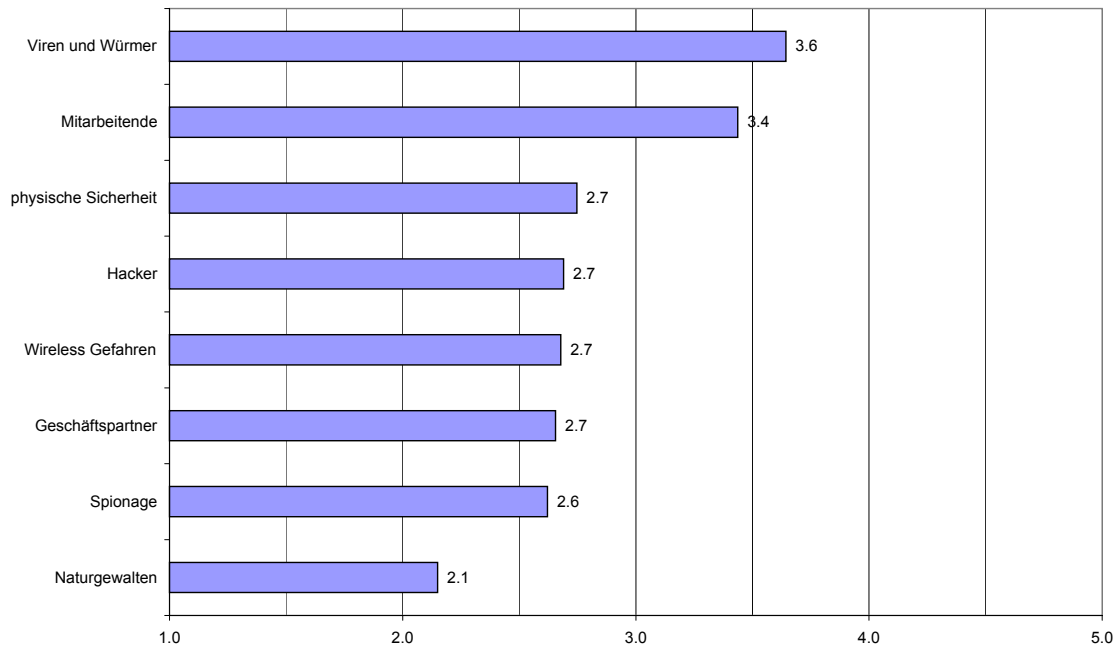
n=87

Informationssicherheitskultur-Verantwortliche rapportieren/sind unterstellt



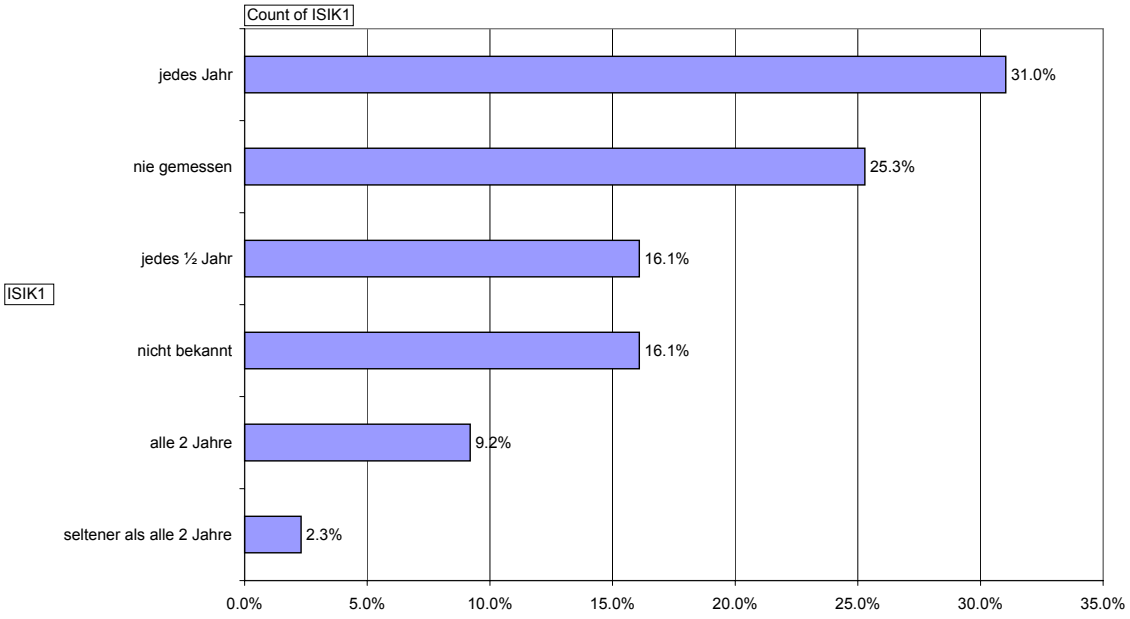
n=87

Bewertung der Informationssicherheits-Risiken



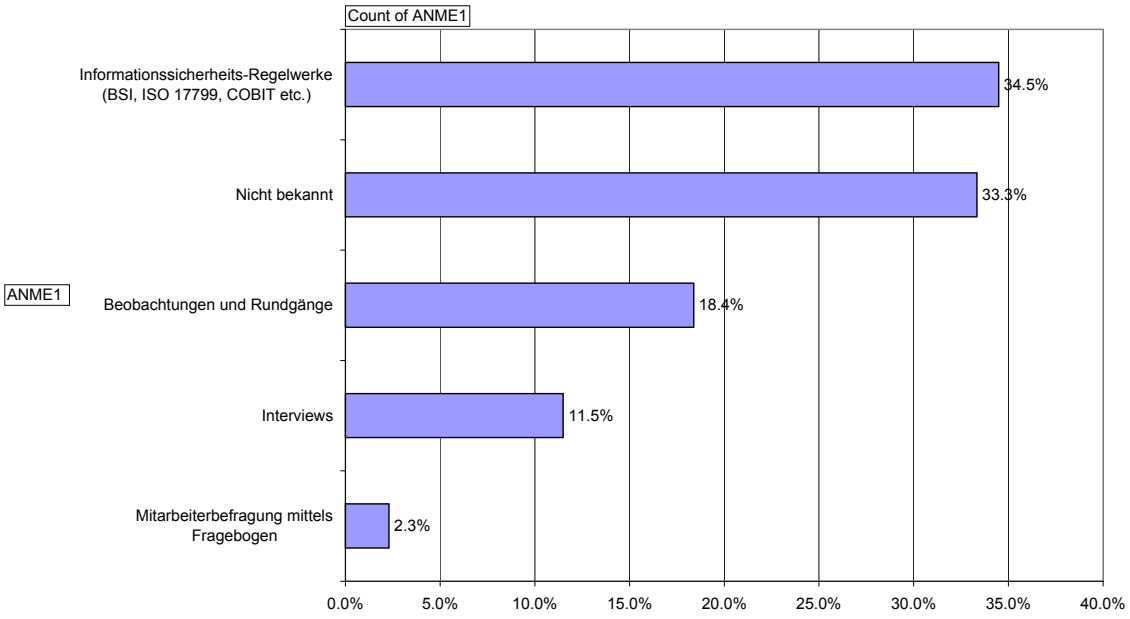
n=87

Wie häufig wird Informationssicherheitskultur gemessen/analysiert



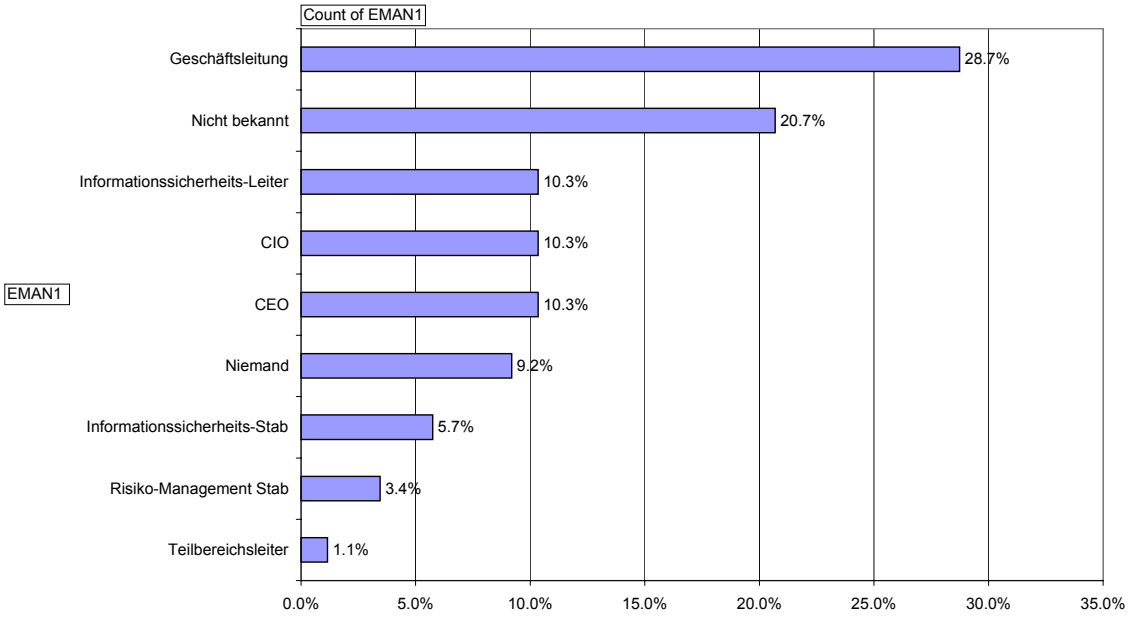
n=87

Mit was für Hilfsmitteln



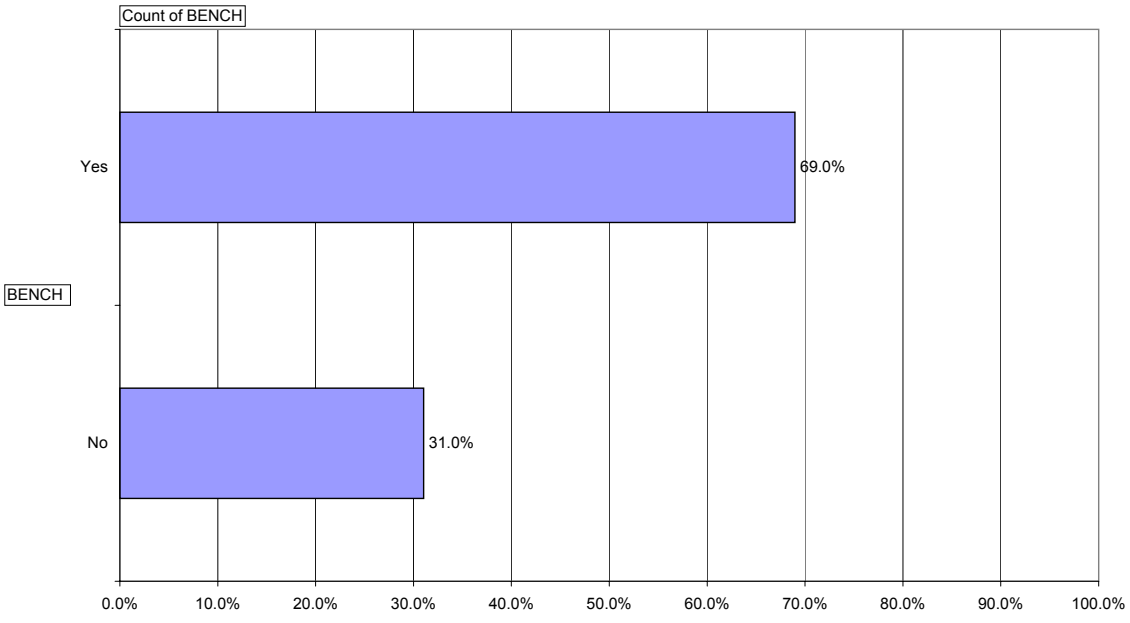
n=87

Wer bekommt diese Analyse-Resultate



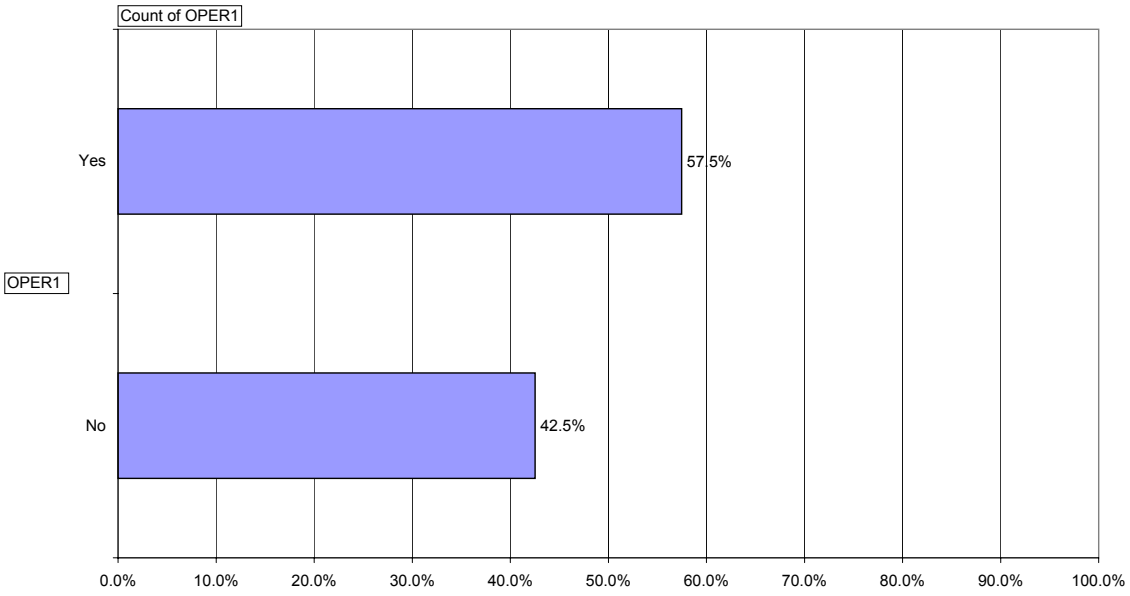
n=87

Interesse an einem anonymen Vergleich der Informationssicherheitskultur (Benchmarkig)



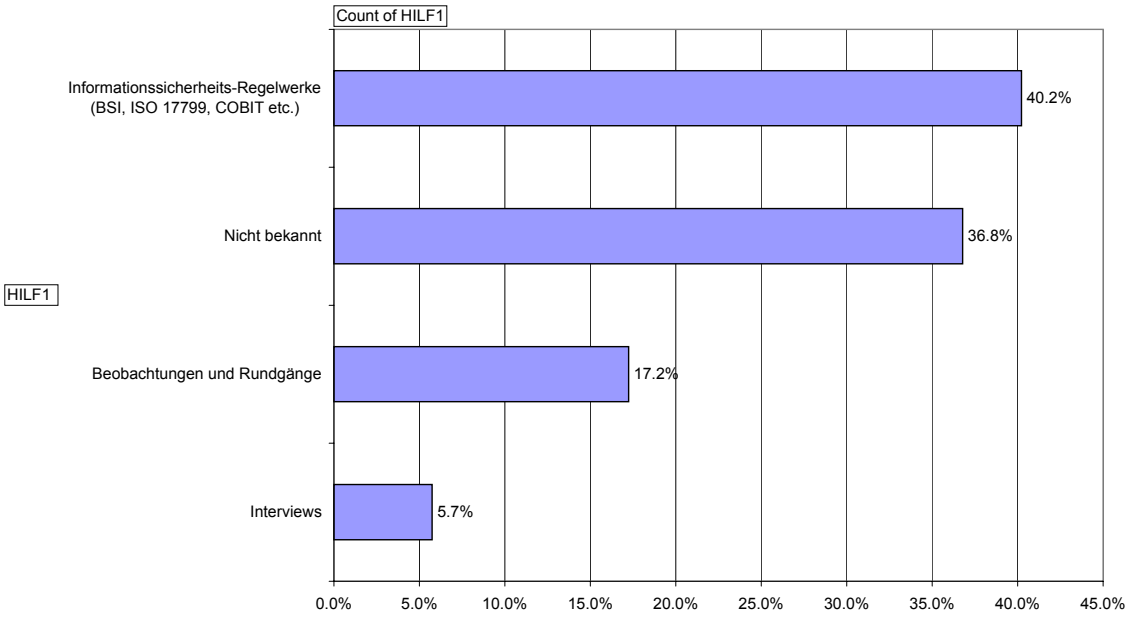
n=87

Existieren Prozesse zur regelmässigen Identifikation von Informationssicherheits-Fehlern und -Problemen



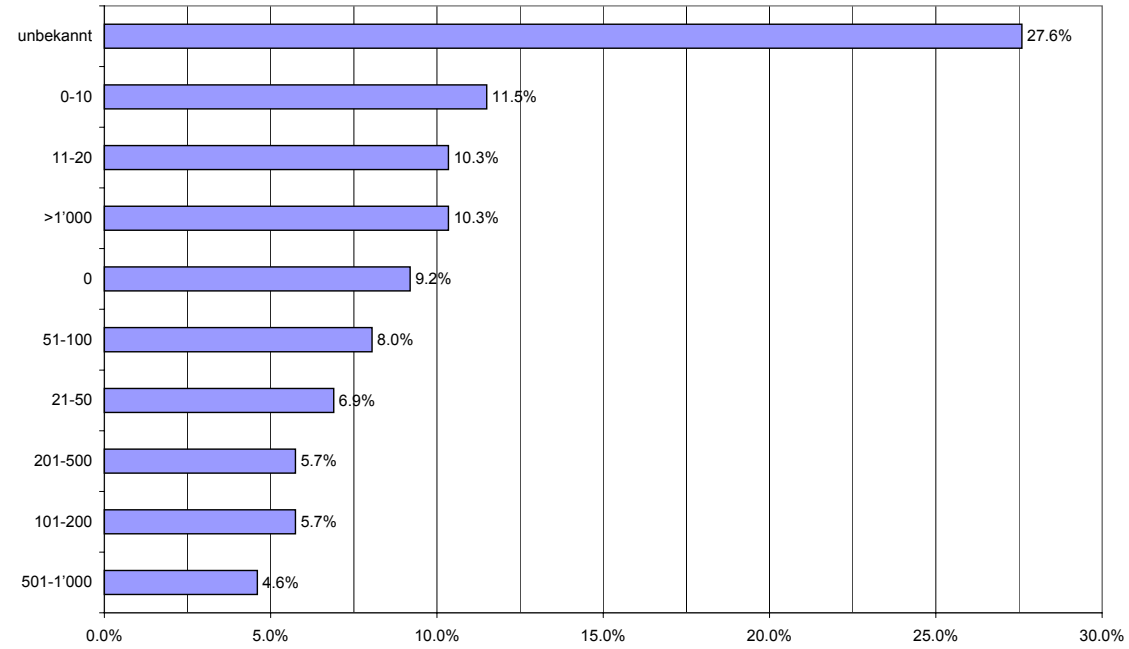
n=87

Mit was für Hilfsmitteln



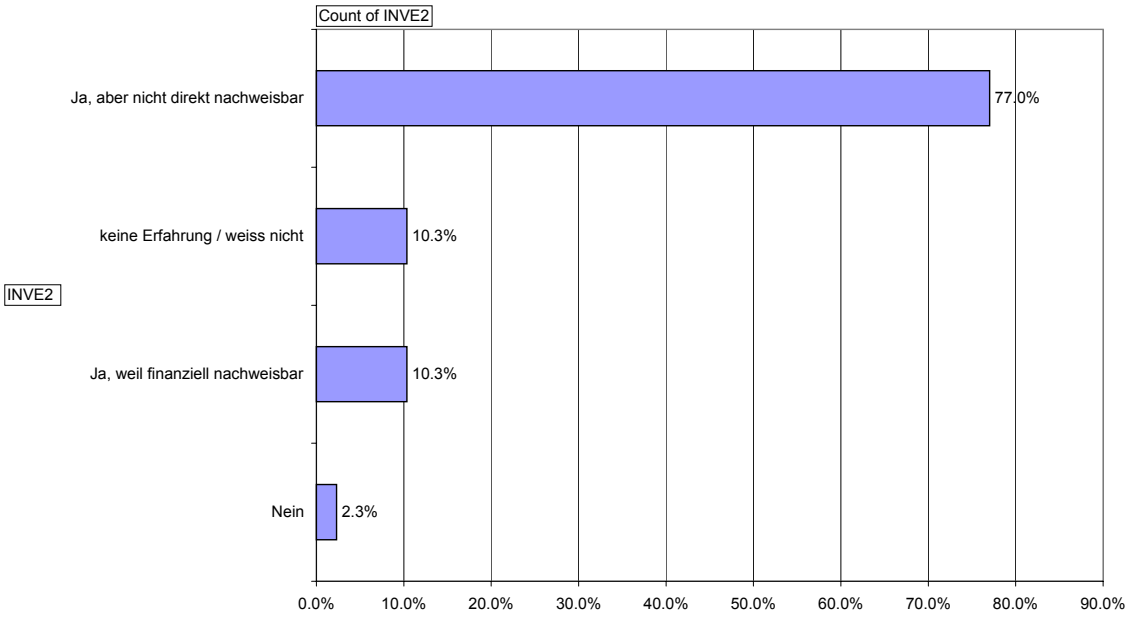
n=87

Investitionen in Sensibilisierungs-Kampagnen pro Jahr und Kopf



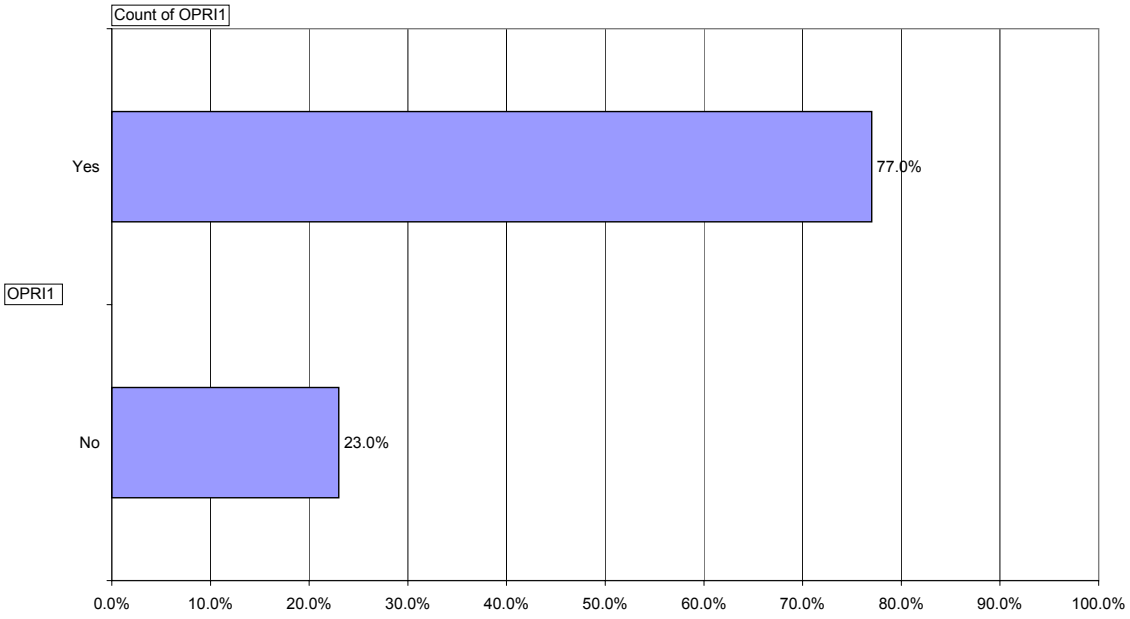
n=87

Lohnen sich Investitionen in eine geeignete Informationssicherheitskultur



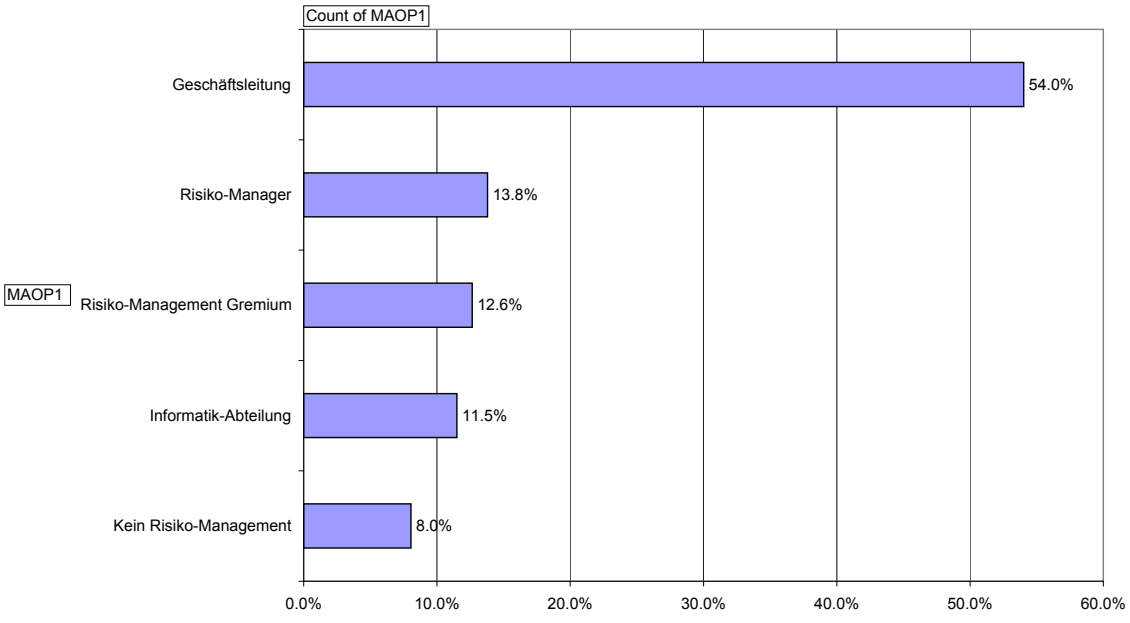
n=87

Informatiossicherheitsrisiko wird als Teil des opertationellen Risikos betrachtet



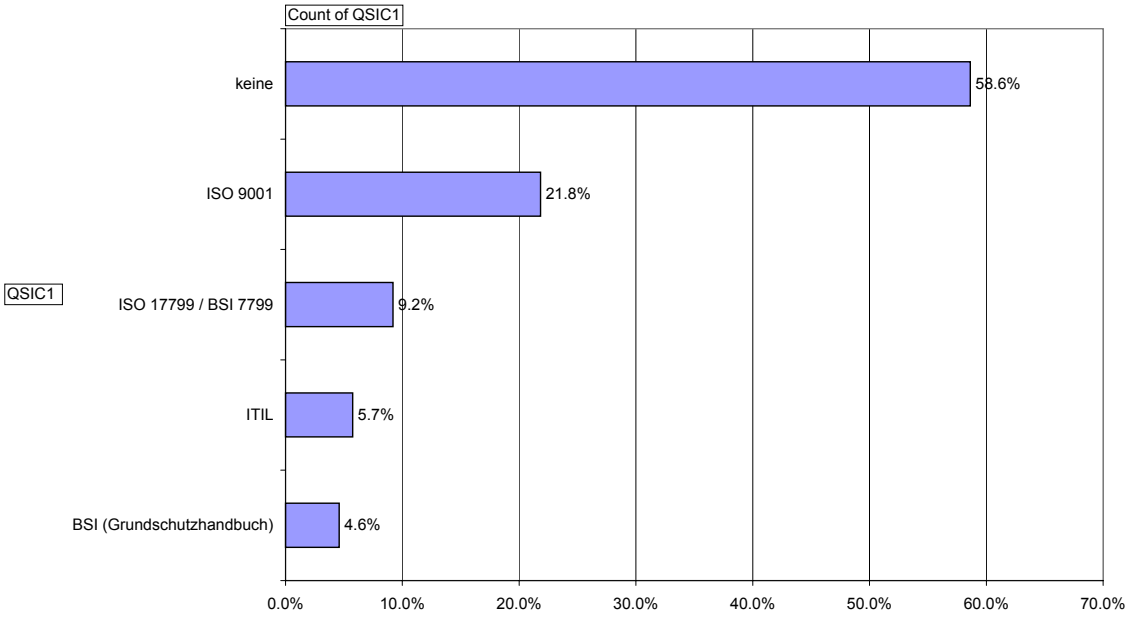
n=87

Wo findet das Management des operationellen Risikos statt



n=87

Welche Zertifikate besitzt die Organisation



Informationssicherheitskultur In CH-Unternehmen

Befragung der AGISIK / FGSec
Arbeitsgruppe Informationssicherheitskultur
Sept.-Okt. 2004

Questions marked with a * are required.

Einführung Informationssicherheitskultur

Informationssicherheitskultur umfasst „die Gesamtheit der tradierten, wandelbaren, zeitbedingten und (teilweise) beeinflussbaren kollektiven Werte, Normen und Wissensbestände der Informationssicherheit eines Unternehmens, welche mit emotionalem Engagement gehalten werden und sich in vielfältigen Artefakten äussern, und die das Verhalten der Betriebsangehörigen und damit letztlich den Erfolg der Informations-sicherheit sowie das Erscheinungsbild des Unternehmens nach aussen beeinflussen." (Brandao, R. IT-Sicherheitskultur im Unternehmen. Diplomarbeit. IFI. Zürich, Universität Zürich: 110. 1994.)

***1.** Informationssicherheitskultur Wahrnehmung. Skala/Metrik: Trifft überhaupt nicht zu (1) bis trifft voll und ganz zu (5).

	1	2	3	4	5
Die Mitarbeiter unseres Unternehmens sind genügend über die Risiken der Informationssicherheit informiert.	○	○	○	○	○
Das Top Management (GL / VR) unseres Unternehmens ist genügend über die Risiken der Informationssicherheit informiert	○	○	○	○	○
Das Top Management (GL / VR) unseres Unternehmens ist überzeugt, dass Informations-sicherheit für die Erreichung der Geschäfts-Ziele sehr wichtig ist.	○	○	○	○	○

***2.** Hindernisse:Bewerten Sie die nachfolgenden Gründe, die in Ihrer Organisation die Umsetzung einer effektiven Informationssicherheitskultur behindern, auf einer Skala von 1 (kleinstes Hindernis) bis 5 (grösstes Hindernis).

	1	2	3	4	5
Begrenztes Budget	○	○	○	○	○
Schwierig, den finanziellen Nutzen der Informationssicherheitskultur zu Beweisen	○	○	○	○	○
Das Geschäftsumfeld verfügt über zu unterschiedliche Anforderungen gegenüber der Informationssicherheit (alles ist offen und schnell)	○	○	○	○	○
Fehlende Unterstützung durch Anwender	○	○	○	○	○
Fehlende Unterstützung durch das Top Management	○	○	○	○	○
Fehlende Unterstützung durch Senior Informatik Mitarbeiter	○	○	○	○	○

***3.** Welche Massnahmen werden in Ihrer Organisation momentan zur Förderung der Informationssicherheitskultur eingesetzt?

- ☐ Weisungen z.B. Begleitung von Besuchern, sichere Passworte etc.
- ☐ Broschüre
- ☐ Flyer / Poster
- ☐ Film
- ☐ Artikel auf dem Intranet oder in der Hauszeitschrift
- ☐ Bilaterale Gespräche
- ☐ Workshops
- ☐ Kurse / Ausbildungen
- ☐ Computer-Lernprogramme (CBT)
- ☐ Wissentests / Wissencheck
- ☐ Gadgets, Goodies, Give-Aways
- ☐ Rundgänge, z.B. zur Überprüfung der clear desk policy
- ☐ Keine

***4.** Welche Massnahmen zur Förderung der Informationssicherheitskultur sollten Ihrer Meinung nach in den nächsten 2 Jahren in ihrer Organisation eingesetzt werden?

- ☐ Weisungen z.B. Begleitung von Besuchern, sichere Passworte etc.
- ☐ Broschüre
- ☐ Flyer / Poster
- ☐ Film
- ☐ Artikel auf dem Intranet oder in der Hauszeitschrift
- ☐ Bilaterale Gespräche
- ☐ Workshops
- ☐ Kurse / Ausbildungen
- ☐ Computer-Lernprogramme (CBT)
- ☐ Wissentests / Wissencheck
- ☐ Gadgets, Goodies, Give-Aways
- ☐ Rundgänge, z.B. zur Überprüfung der clear desk policy
- ☐ Keine

*5.	Wer ist für die Informationssicherheitskultur in Ihrer Organisation verantwortlich (Position / Abteilung / Organisationseinheit)?

*6.	Zum wem rapportiert diese Person bzw. wem ist sie unterstellt?

- CEO
- Geschäftsleitung
- Informatik Stab
- Informatik Sicherheit
- CIO
- Interne Revision
- Risiko Management Stab
- Keine Position

Next Page

Informationssicherheitskultur In CH-Unternehmen

Befragung der AGISIK / FGSec
Arbeitsgruppe Informationssicherheitskultur
Sept.-Okt. 2004

Questions marked with a * are required.

Frühwarnindikatoren und Messung

Die frühzeitige Risikoidentifikation setzt die Existenz von Frühwarnindikatoren voraus. Frühwarnindikatoren für die Informationssicherheit können z.B. Anzahl von Fehlern/Problemen, Verlust von vertraulichen Informationen oder fehlende Vorgaben sein. Die Ergebnisse einer Risikoidentifikation und -bewertung werden in einem rechnerun-terstützten Risikoinventar gesammelt und erlauben eine Messung der Risikosituation.

*7. Bewerten Sie auf einer Skala von 1 (kleinstes Risiko) bis 5 (grösstes Risiko) folgende Informationssicherheits-Risiken bezogen auf Ihr Unternehmen.

	1	2	3	4	5
Hacker	○	○	○	○	○
Viren und Würmer	○	○	○	○	○
unloyale Geschäftspartner	○	○	○	○	○
Spionage	○	○	○	○	○
Eigene Mitarbeitende	○	○	○	○	○
Naturgewalten	○	○	○	○	○
Physische Sicherheit	○	○	○	○	○
Wireless Gefahren	○	○	○	○	○

*8. Die Informationssicherheitskultur wird in unserem Unternehmen wie folgt analysiert / gemessen :

- jedes ½ Jahr
- jedes Jahr
- alle 2 Jahre
- seltener als alle 2 Jahre

- nie gemessen
- nicht bekannt

***9.** Analyse- / Messmethode :

- Interviews
- Informationssicherheits-Regelwerke (BSI, ISO 17799, COBIT etc.)
- Mitarbeiterbefragung mittels Fragebogen
- Beobachtungen und Rundgänge
- Nicht bekannt

***10.** Empfänger der Informationen einer solche Analyse:

- Informationssicherheits-Leiter
- Informationssicherheits-Stab
- Teilbereichsleiter
- CIO
- Risiko-Management Stab
- CEO
- Geschäftsleitung
- Niemand
- Nicht bekannt

***11.** Würde Sie ein anonymer Vergleich (Benchmarking) ihrer Informationssicherheitskultur mit demjenigen ihrer Mitbewerber oder anderer Industrien interessieren?

- Yes
- No

***12.** Haben Sie operative und betriebliche Prozesse, mit dene Sie Informationssicherheits-Fehler und -Probleme regelmässig identifizieren und sammeln?

- Yes
- No

***13.** Falls ja, was für Hilfsmittel benutzen Sie, um diese operativen und betrieblichen Probleme/Fehler in der Informationssicherheit zu erheben?

- Interviews
- Informationssicherheits-Regelwerke (BSI, ISO 17799, COBIT etc.)
- Mitarbeiterbefragung mittels Fragebogen
- Beobachtungen und Rundgänge
- Nicht bekannt

Finanzieller Aspekt: Fragen zum Budget und zu den Investitionen in die Informationssicherheitskultur.

***14.** Wie viel CHF investiert Ihr Unternehmen schätzungsweise in Sicherheitssensibilisierungs-Kampagnen pro Jahr und Kopf?

- 0
- 0-10
- 11-20
- 21-50
- 51-100
- 101-200
- 201-500
- 501-1'000
- >1'000
- unbekannt

***15.** Lohnen sich Investitionen in eine geeignete Informationssicherheitskultur für ihre Organisation?

- Ja, weil finanziell nachweisbar
- Ja, aber nicht direkt nachweisbar
- Nein
- keine Erfahrung / weiss nicht

***16.** Begründung Ihre Antwort auf Frage 16

Next Page

Informationssicherheitskultur In CH-Unternehmen

Befragung der AGISIK / FGSec
Arbeitsgruppe Informationssicherheitskultur
Sept.-Okt. 2004

Questions marked with a * are required.

Integration in Risikomanagement

***17.** Wird in Ihrer Organisation das Informationssicherheitsrisiko als Teil des operationellen Risikos betrachtet?

- ○ Yes
- ○ No

***18.** Wo findet in Ihrer Organisation das übergeordnete Management des operationellen Risikos statt?

- ○ Informatik-Abteilung
- ○ Risiko-Manager
- ○ Risiko-Management Gremium
- ○ Geschäftsleitung
- ○ Kein Risiko-Management

***19.** Verfügt Ihre Organisation über eine IT-Governance, Qualitäts- oder Sicherheitszertifizierung?

- ○ ISO 9001
- ○ ISO 17799 / BSI 7799
- ○ BSI (Grundschutzhandbuch)
- ○ ITIL
- ○ keine

Demographische Indikatoren

***20.** Was haben Sie für eine Führungsposition?

- ○ Mitglied VR
- ○ Geschäftsführer / Mitglied GL
- ○ Risk Management Officer
- ○ Leiter Informatik
- ○ IT Sicherheitsbeauftragter
- ○ Senior Informatik Mitarbeiter
- ○ Junior Informatik Mitarbeiter
- ○ andere

***21.** Wo sitzt Ihre Organisation / Firma

***22.** Anzahl Beschäftigte in Ihrer Firma:

- ○ 1-9
- ○ 10-49
- ○ 50-249
- ○ 250-999
- ○ 1000-2999
- ○ 3000-4999
- ○ 5000+

***23.** Branche

- ○ Herstellung Nahrungsm./Getränke/Tabak
- ○ Be- und Verarbeitung Holz/Metall
- ○ Papier, Verlag, Druck
- ○ Maschinenbau
- ○ Elektr. Geräte, Feinmechanik
- ○ Sonstige Industrie
- ○ Sonstiges verarbeitendes Gewerbe
- ○ Energie- und Wasserversorgung
- ○ Baugewerbe
- ○ Grosshandel
- ○ Detailhandel
- ○ Gastgewerbe

- Kreditgewerbe / Finanzdienstleitung
- Versicherungsgewerbe
- Immobilienwesen
- Informatik
- Verkehr, Nachrichtenübermittlung
- Forschung und Entwicklung
- Öffentliche. Verwaltung
- Unterrichtswesen
- Gesundheits- und Sozialwesen
- Rechts- und Unternehmensberatung.
- Sonstige Dienstleistungen. für Unternehmen
- Sonstige. öffentliche. und pers. Dienstleistungen.
- Beratungsunternehmen

Submit Survey