swisscom IT services

Auftrag erfüllt?
Erfahrungsbericht Informationssicherheit

10th Symposium on Privacy and Security

Daniel Wyniger, Head of Auditing, Swisscom IT Services AG

Zürich, 31. August 2005

swisscom IT services

Agenda

1. Swisscom IT Services AG
2. Der Auftrag: Integration der Eckpfeiler unserer Informationssicherheit
3. Umsetzung der Vorgaben: Organisation und Prozesse
4. Auftrag erfüllt ? Lessons Learned und Next Steps

10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Agenda

- Swisscom IT Services AG
- Der Auftrag: Integration der Eckpfeiler unserer Informationssicherheit
- Umsetzung der Vorgaben: Organisation und Prozesse
- Auftrag erfüllt ? Lessons Learned und Next Steps

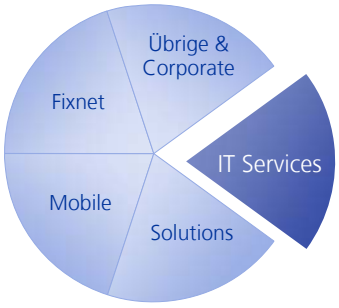
Daniel Wyniger, PRS_20050806_10th Symposium on Privacy and Security.ppt
06/09/2005
3

10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Vertrauen Sie auf einen soliden Partner

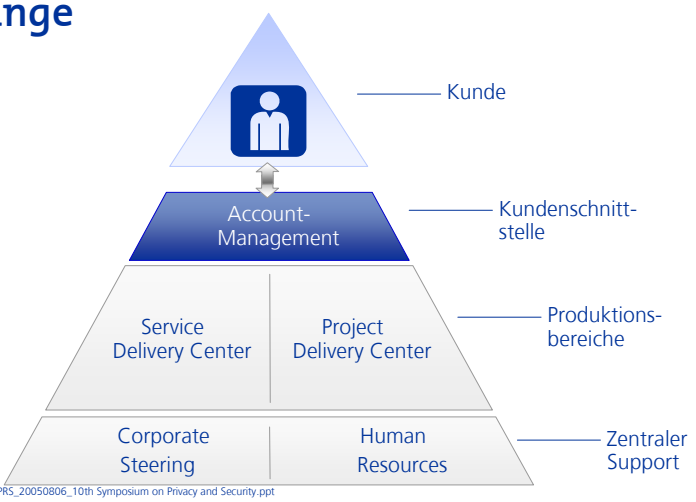
- Strategische Tochtergesellschaft von Swisscom (100%)
- Über 2'100 kompetente und motivierte Mitarbeitende
- Hauptsitz in Bern-Ostermundigen, 13 weitere Standorte in der ganzen Schweiz



Daniel Wyniger, PRS_20050806_10th Symposium on Privacy and Security.ppt
06/09/2005
4

swisscom IT services

Ihr kompetenter Ansprechpartner für alle Belange



swisscom IT services

Das ist uns wichtig: Qualität, Sicherheit und Umwelt

- Integrierte, prozessorientierte Managementsysteme für Qualität, Umwelt und Sicherheit
  Nach ISO 9001, ISO 14001, BS7799-2 zertifiziert.
  Erfüllung der Anforderungen aus dem Sarbanes-Oxley Act sind in Arbeit.
- Unser Engagement für Ökonomie, Ökologie und Soziales ist anerkannt
  Im Dow Jones Sustainability World Index (DJSI) und FTSE 4 Good Index vertreten
- Wir leben eine soziale Unternehmenskultur
- Wir verpflichten uns, die Umwelt aktiv zu schonen
- Wir bieten umweltgerechte IT-Dienste an
- Wir wählen neue IT-Geräte nach ökologischen Kriterien aus

swisscom IT services

Agenda

- Swisscom IT Services AG
- Der Auftrag: Integration der Eckpfeiler unserer Informationssicherheit
- Umsetzung der Vorgaben: Organisation und Prozesse
- Auftrag erfüllt ? Lessons Learned und Next Steps

swisscom IT services

Der Auftrag

- Aufbau eines nach BS 7799-2 zertifizierten Information Security Management Systems (ISMS) für das gesamte Unternehmen
- Integration der BS 7799-2 Controls in ein unternehmensweites Prüf- und Berichterstattungsframework
- Sicherstellung der Abdeckung möglichst vieler regulatorischer und konzerninterner Compliance Anforderungen
- Nutzung von Synergien zwischen den verschiedenen Prüfstandards und Vermeidung von ineffizienten Redundanzen
- Verständliche und verbindliche Integration der Sicherheits- und Compliance-Anforderungen in die geltenden Vertragswerke

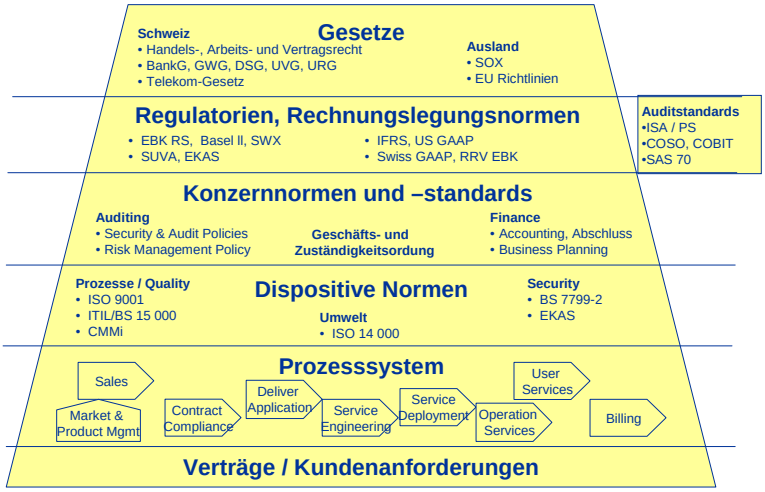
swisscom IT services

Die Herausforderungen

- Interne Prozesse und Standards müssen verschiedene Kundenkulturen und –anforderungen abdecken
- Integration verschiedener Regulatorien, Normen und Vorgaben
- hohe Mobilität von Assets, Mitarbeitern und der Anforderungen im Outsourcing-Business
- Wahl und Durchsetzung einer einem führenden IT-Unternehmen angemessenen Security Organisation

swisscom IT services

Regulatorien, Gesetze und Richtlinien



swisscom IT services

Agenda

- Swisscom IT Services AG
- Der Auftrag: Integration der Eckpfeiler unserer Informationssicherheit
- Umsetzung der Vorgaben: Organisation und Prozesse
- Auftrag erfüllt ? Lessons Learned und Next Steps

swisscom IT services

Integration der Security in ein Corporate Compliance Programm

- starker Trend zu vermehrter gesetzlichen Regulation und Intensivierung der Corporate Governance (SOX, BS7799-2, Eu-Richtlinien)
- wesentlichen Treiber sind exogen vorgegeben
- Anwendung des Sarbanes Oxley Act (SOX) für Swisscom-Konzern und wichtige Kunden
- Parallelitäten und Überlappungen der verschiedenen Normen und Standards
- Suche nach Synergien. Konzentration der Kräfte

10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Milestones und Teilergebnisse

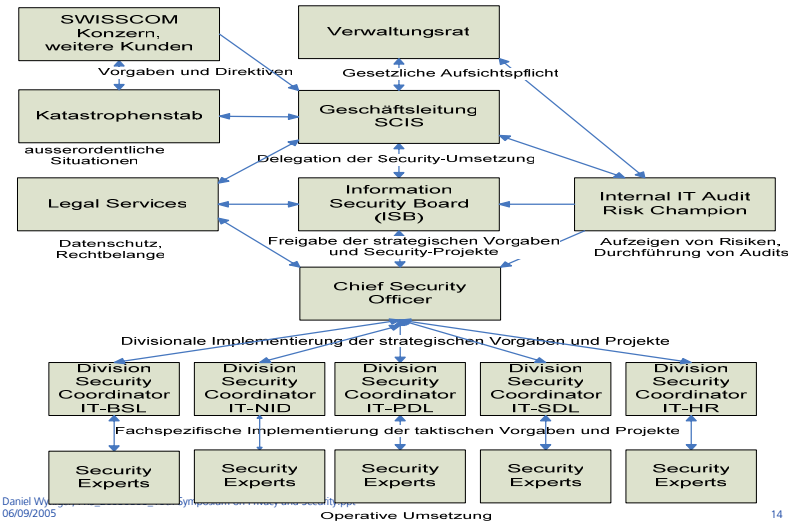
- ✓ Aufbau einer Sicherheitsorganisation mit verteilten Zuständigkeiten und Kompetenzen
- ✓ Integration der Sicherheitsaspekte in die Prozesse und Rollen
- ✓ Definition eines Standardprozesses für das Outsourcing-Geschäft
- ✓ Standardisierung im Midrange-Bereich, um verschiedene Sicherheitskulturen und –anforderungen kundengerecht abzudecken (Windows, Unix)
- ✓ Zonierung des Netzwerks (Network Connectivity Architecture)
- ✓ Regelmässige Awareness-Aktionen

Daniel Wyniger, PRS_20050806_10th Symposium on Privacy and Security.ppt
06/09/2005 13

10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Organisation Information Security

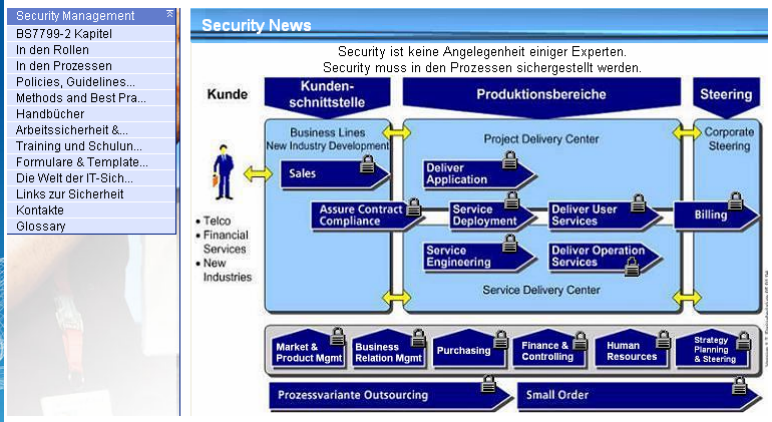


Daniel Wyniger, PRS_20050806_10th Symposium on Privacy and Security.ppt
06/09/2005 14

10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Das Prozessmodell: Übersicht



10th Symposium on Privacy and Security, Zürich, 31. August 2005

swisscom IT services

Agenda

- Swisscom IT Services AG
- Der Auftrag: Integration der Eckpfeiler unserer Informationssicherheit
- Umsetzung der Vorgaben: Organisation und Prozesse
- Auftrag erfüllt ? Lessons Learned und Next Steps

swisscom IT services

Auftrag erfüllt?

- **Ja,** wichtige Milestones erreicht:
  - Zertifizierung für das gesamte Prozessystem von Swisscom IT Services nach BS 7799-2 erreicht
  - Das Prozesssystem hat einen hervorragenden Ausbaugrad mit hoher Akzeptanz bei den Mitarbeitenden erreicht
  - Awareness ist heute auf einem befriedigenden Level
  - Abstimmung mit SOX-Vorbereitung ist erfolgt
- **Nein**, Überführung ISMS im operatives Tagesgeschäft geht weiter
  - Überarbeitung und Ergänzung gesamtes Vertragsframeworks
  - Klassifikation der Werte ist eine nicht zu unterschätzende Daueraufgabe in einem volatilen Geschäftsfeld
  - Awareness von Mitarbeitenden und Management hoch halten
  - Berichterstattung für unterschiedliche Kundensegmente über vorhandenes Security- und Compliance-Niveau aufbauen

swisscom IT services

Lessons Learned

- Integration der Sicherheit ins operative Tagesgeschäft ist nur mit einem maturen Prozessmodell zu bewältigen
- Standardisierung von Prozessen und Produkten ist die Grundvoraussetzung
- kein wirksames und wirtschaftliches Security Management ohne unmissverständliche Anforderungsdefinition in Verträgen und SLA
- Motivation und Awareness der Mitarbeitenden
- Security findet im operativen Geschäft statt, die IT Security Organisationseinheit als Enabler und Eskalationsinstanz
- die Evaluation eines geeigneten Tools ist ein irreführender Nebenschauplatz