

ISO 27001 bei der SpaceNet AG

Sebastian v. Bomhard, 25.6.2008

ISO 27001

Wieso tut man sich so was an?

Altes Testament: im Anfang war das Chaos

ΧΑΟΣ

Neues Testament: im Anfang war das Wort

ΛΟΓΟΣ

Die SpaceNet AG in Kürze

- Internetprovider
- gegründet 1993 (als GmbH)
- heute ca. 75 Mitarbeiter
- 2000 Geschäftskunden (Mittelstand)
- ca. 9 Mio Jahresumsatz
- Schwerpunkte: Komplexes Hosting, Mail, Remote Backup, Archivierung, Rechenzentrumdienste

Ausgangssituation

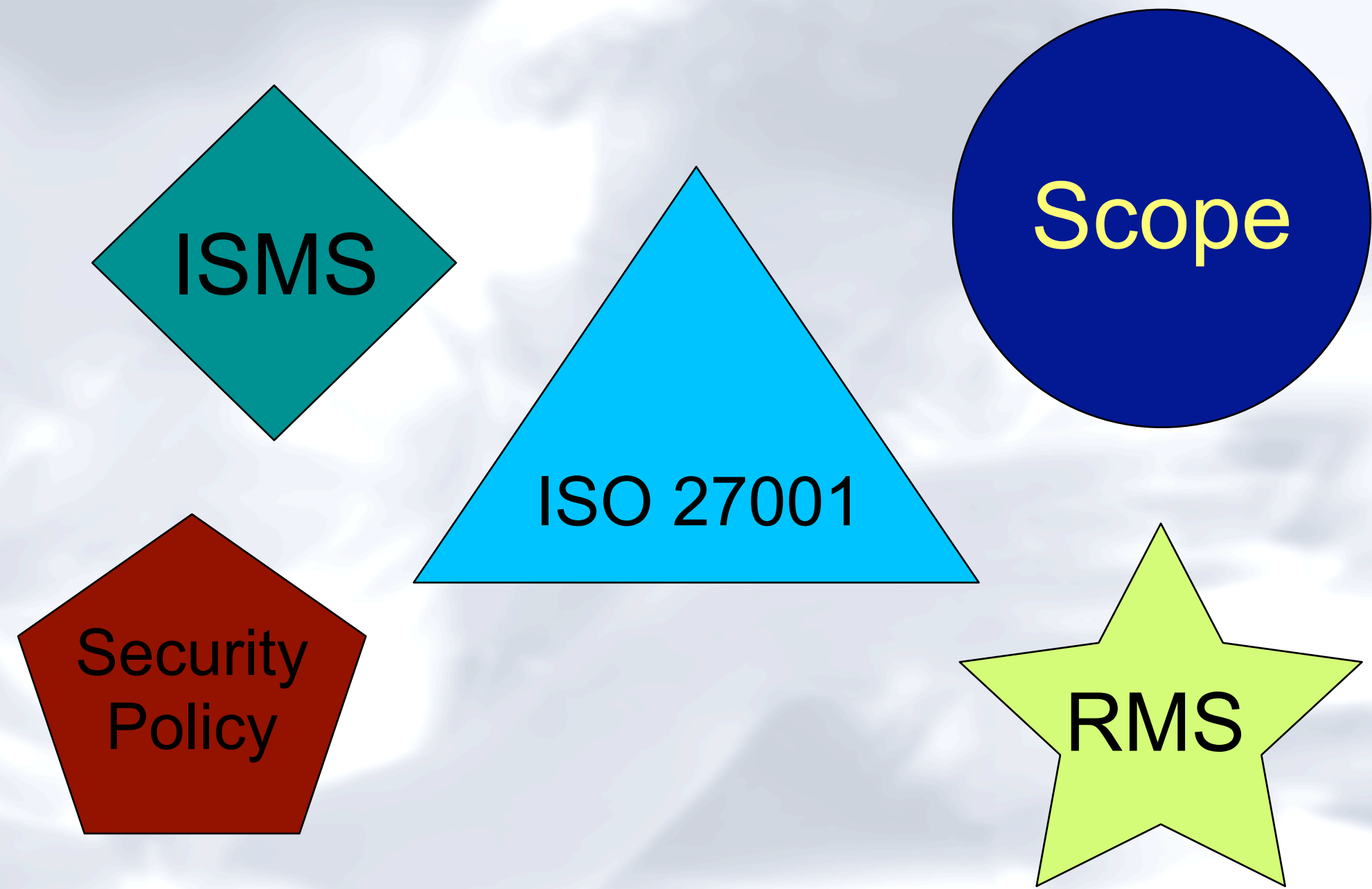
- knapp 15 Jahre „Evolution der Prozesse“
- Mitarbeiterfluktuation
- unabhängige Normen entstehen:
 - ★ disjunkte Systeme
 - ★ Inkonsistenzen treten auf
- Kraftanstrengung: Das Intranet!

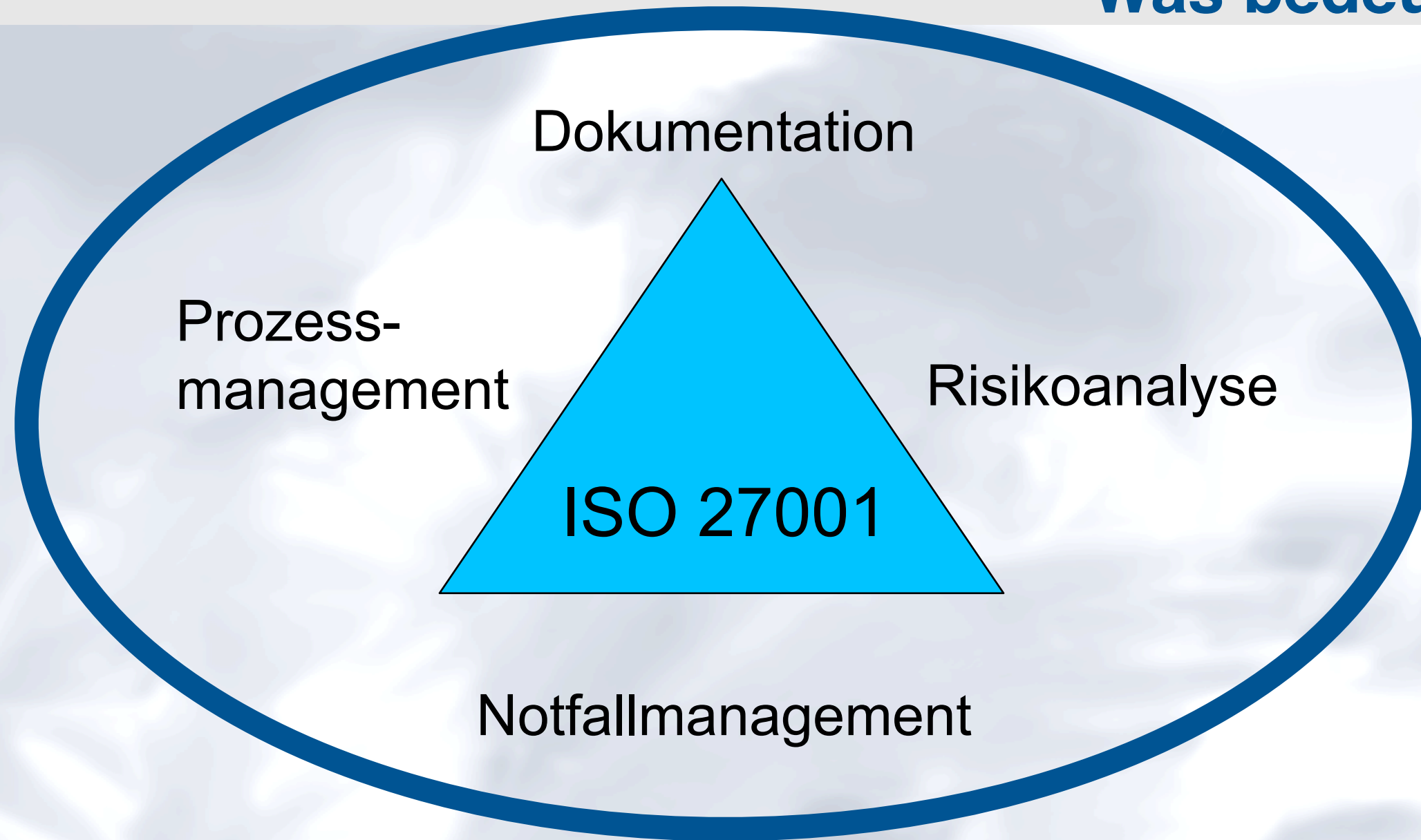
Das Intranet

- Nach drei Jahren: Nochmal von vorne
- Diesmal funktioniert es
- aber wie beweise ich es den Kunden?
- Und wie schaffe ich es, das Thema dauerhaft vom Tisch zu kriegen?

ISO 27001 ist eine externe Norm

Was bedeutet ISO 27001?





Reichweite (scope)

ISO 27001 beginnt im „Kopf“

ISO 27001 beginnt im „Kopf“

Das Management muß:

- die Gesamtverantwortung übernehmen,
- Informationssicherheit integrieren, steuern und aufrechterhalten,
- realistische Ziele setzen,
- die Kosten nicht aus den Augen verlieren und
- Vorbild sein

Zwei Phasen:

- * Vor der Prüfung
- * Vor der nächsten Prüfung

Schritt 2: Ist-Zustand

Wo stehen wir auf einer Skala von 0 bis 100?

- Fachabteilung spontan: 100! Na gut: 98!!
- Nach kurzer Diskussion: 0!!! Na gut: 2!!!!
- Nach Einbindung einer externen Beratungsgesellschaft und einer Fit/Gap-Analyse: 70%
- Entschluss: Wir brauchen weiter externe Hilfe.
- Partner: @sec

Die Arbeit fängt an.....

PDCA

CISO

Lauter neue Begriffe

LISO

ISMS

Schritt 3: Konsolidierung der Dokumentation



Schritt 3:

- **Die Mitarbeiter**
- **Das Team**
- **Die Gremien**
- **Die Kunden**
- **Die Berater**

Schritt 3:

Die Mitarbeiter

- ★ Motivation
- ★ Zieldefinition
- ★ Background: Worum geht's?

Das Team

Die Gremien

Die Kunden

Die Berater

Schritt 3:

- Die Mitarbeiter
- Das Team
 - ★ Laterale Führungskompetenz
 - ★ Sprachliche Fähigkeiten
 - ★ Projekterfahrung
- Die Gremien
- Die Kunden
- Die Berater

Schritt 3:

- Die Mitarbeiter
- Das Team
- Die Gremien und Funktionen
 - ★ CISO
 - ★ LISO
 - ★ Security Forum
- Die Kunden
- Die Berater

Schritt 3:

- Die Mitarbeiter
- Das Team
- Die Gremien
- Die Kunden
 - ★ Hier ist der Point of No Return
 - ★ Die Kunden sind nämlich begeistert
- Die Berater

Schritt 3:

Die Berater

- ★ helfen, den Fokus nicht zu verlieren
- ★ steuern Erfahrungen bei aus anderen
- ★ verkürzen das Verfahren
- ★ schreiben die ganze Dokumentation



Schritt 3:

Die Berater

- ★ bieten an, bei der Dokumentation zu helfen
- ★ Das Team wird es fordern: Antwort bleibt nein
- ★ Das Team legt revidierte Meilensteinpläne vor: bleibt nein
- ★ Das Team wirkt verzweifelt: Zu diesem Zeitpunkt nimmt man „Ghostwriter“ ins Team.

Nach drei Monaten: Snapshot

- Das Dokumentenmanagementsystem ist ausgewählt
- Soll/Ist-Zwischenstand wird nicht mehr diskutiert
- Jeder kennt seine Aufgaben
- Die Firmenstruktur ist angepasst
- Die Gremien und die Verantwortlichen kennen ihre Aufgaben und haben die Arbeit aufgenommen.

Nach sechs Monaten

- Wo ist die Zeit geblieben?
- Kommunikation des echten Zieldatums
- Intensivcoaching der Nachzügler
- Ausbügeln kleiner Inkonsistenzen
- Vorteile sind bereits zu bemerken
- Mitarbeiter werden nervös
 - ★ Führerscheinprüfungssyndrom
 - ★ ernst nehmen, Trockentrainings

Nach neun Monaten: Der Auditor kommt

- Drei Tage Interviews
- Top Down: Management first
- Bestanden! (Alternative: Nachbessern)
- Ab jetzt gilt's.
- Fertig!? Nie! Regelmäßiger Revisionsprozeß.
- Aber: Feiern erlaubt.



Wie geht's weiter?

- Prozesse weiter verfeinern: PDCA
- „ISO 27001 leben“
- ITIL???
- Reduktion der Teams (nicht Auflösung!)

A large, faded, and blurred image of a group of people in a meeting or conference setting, serving as the background for the central text.

Danke für Ihre Aufmerksamkeit!