IT Symposium 2007

2K05 ISO 27001 Zertifizierung - Erfahrungen

Rainer Jordan, Atos Origin GmbH

Nürnberg, 18.04.2007

ISO 27001 Zertifizierung – Erfahrungen …

1. Einleitung
2. … vor
3. … während
4. … danach
5. Zusammenfassung

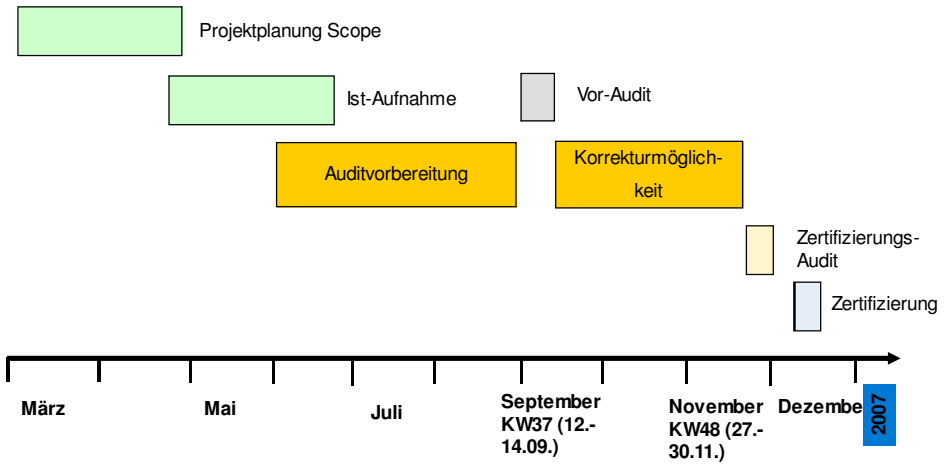
Einleitung

Was möchte ich hier vermitteln:

- Unseren Angang zur Erreichung der Zertifizierung
- Nicht: wie führe ich ein ISMS ein
- Fakt: jeder kümmert sich um Security, hat mehr oder weniger Information Security eingeführt.
- Frage bleibt: reicht das für ein Zertifikat, tue ich das Richtige?

...vor

Projektablauf



...vor

Projektplanung

- Management
  - IT Sicherheit ist Chefsache (Welche Gründe, auch immer: Business Anforderungen, rechtliche, gesetzliche Gründe)
  - Management permanent gegenwärtig
- Scope festlegen – Einheiten identifizieren
- Mit dem Zertifizierer zusammensetzen
- Externe Begleitung (in Kenntnis der Norm und des Zertifizierers) – Prophet im eigenen Haus.

5 2K05 ISO 27001 Zertifizierung - Erfahrungen

...vor

IST-Aufnahme / Gap-Analyse

IST-Stand erfassen / GAPs identifizieren durch interne Assessments

- Zentrales Information Security Management
  - Policy
  - Management
  - Risiko Management / Business Continuity Management/ Schutzbedarfsanalyse
  - Ressourcen
  - Kommunikation
  - Security Organisation
  - Security Incident Management
  - Security Awareness

6 2K05 ISO 27001 Zertifizierung - Erfahrungen

...vor

IST-Aufnahme / Gap-Analyse

- In den Einheiten (betroffen ca 1000 Mitarbeiter)
  - Server Management
    - Systemtechnik
    - ERP/SAP
  - Operations
    - Systemsicherheit
    - RZ-Services
  - Mainframe
    - Systemtechnik MF
    - DB/DC
    - Operations
    - Systemsicherheit
  - Netzwerk Management
    - Netzwerkbetrieb
    - Netzwerksecurity
  - UserHelpDesk
  - Human Resource Management

...vor

IST-Aufnahme / Gap-Analyse

- Während der Assessements
  - **Schulungen/Präsentationen zum ISM**
  - Die Einheiten müssen verstehen was die Norm von ihnen fordert
    - Dokumentation
    - Nachweise
    - Kennzahlen
  - Identifizierte Maßnahmen in eine zentrale Liste aufnehmen

und

  - Die Prozesse, bzw Änderungen und Anpassungen einführen

Auditvorbereitung

...vor

Vor-Audit

- Ein reales Audit mit den Auditoren
  - Gibt Auskunft über den Stand (Zertiizierungsfähigkeit)
  - Auditbericht: Abweichungen – Empfehlungen - Hinweise

  → gehen in die weiteren Aktivitäten ein

Korrekturmöglich-keit

...während

Tag / Woche der Wahrheit

- Wenig Steuermöglichkeiten
- Offen und Aufgeschlossen sein
- Management mit einbeziehen

…danach

- Aufwand im Zertifizierungsprojekt: 300 MT
- Das Management im Projekt visible
- Zeitdauer: neun Monate
- Die Zertifizierung ist ein Projekt - Sicherheit ist kein Projekt
- Nach dem Audit ist vor dem Audit – >
- Sicherheitsprozesse leben
  - …
  - Pläne in einem Security Council regelmäßig auf Umsetzung verfolgen
  - Interne Audits
  - …

Zusammenfassung

1. Management aktiv einbeziehen
2. Awareness schaffen – ein „zuviel“ ist nicht möglich
3. GAP – Analyse nicht unterschätzen
4. Durchführung als Projekt
5. Den Mitarbeitern den Auditstress nicht nehmen
6. Gute Erfahrung mit einem Vor-Audit
7. Offen und ehrlich hilft Ihnen weiter
8. Sie haben nie 100% - aber einen Plan!

For more information please contact:

Rainer Jordan

rainer.jordan@atosorigin.com

Atos Origin
www.atosorigin.com