



Revisorns syn på ISO 27000- serien och SAS 70

Rätt Säkerhet 2009
Andreas Halvarsson

25 maj, 2009

 **ERNST & YOUNG**
Quality In Everything We Do

What is SAS 70

AICPA STANDARDS

- ▶ The AICPA's Statement on Auditing Standards No. 70 "Service Organizations" (SAS 70) provides your customers and their auditors information to assist them in evaluating the system of internal control related the services you provide. The AICPA standards provide for the issuance of two types of reports:
- ▶ **Type I** - A report on controls placed in operation as of a point in time
- ▶ **Type II** - A report on controls placed in operation and tests of operating effectiveness covering a period of time

TYPE I REPORTS

- ▶ Type I reports are designed to provide information regarding:
 - ▶ the services that the Company provides to its customers
 - ▶ controls over relevant processes and supporting technology
 - ▶ whether such controls were suitably designed and had been placed in operation
 - ▶ Testing of controls is not performed for a Type I report, and therefore, provides limited value to users and their auditors.

TYPE II REPORTS

- ▶ In a Type II engagement, the procedures for a Type I engagement are performed as well as tests of specific controls to evaluate their operating effectiveness in achieving the specified control objectives.
- ▶ To be useful to user auditors, the report should cover a minimum reporting period of six months.

Why do customers require SAS70 and/or ISO 27001 statements/certificates

- ▶ Customers have outsourced significant parts of their revenue streams to service organizations. The customer's shareholders require reliable internal controls in place for management of the service organizations customers financial data.
- ▶ The customers place SAS70 requests to the service organization to be able to rely on the service organizations internal control of customers revenue streams without performing further audits.
- ▶ A common misunderstanding is that when a service organization is SOX (US SOX, J-SOX, Bolagsstyrningskoden) compliant, a service organizations systems are all SOX compliant. This is not the case. A service organizations own financial systems are SOX compliant.

Significant increase during 2008-2009

Objectives with SAS70 and ISO 27001 initiative

- ▶ The overall objective is to manage the customer's demands via a global cost efficient solution. This will benefit both the service organization and the customers.

- ▶ A global approach to SAS70 and ISO 27001 will reduce current costs through the following means
 - ▶ Reaching economies of scale; knowledge and experiences will be reused
 - ▶ Leveraging on common areas in the SAS70 reviews among the contracts
 - ▶ Establishing consistent standards among the contracts
 - ▶ Clarifying roles, responsibilities and controls
 - ▶ Enhancing the service organizations position in the sales process and in negotiations with customers

What is the difference between SAS 70 and ISO 27001

- ▶ ISO 27001 contains around 130 controls.
- ▶ SAS 70 within a typical service organization contains around 35-40 controls.
- ▶ The SAS 70 controls are based on ISO 27001 so both a SAS 70 and a ISO 27001 equals around 130 controls.
- ▶ ISO 27000 for a service organization only is sometimes insufficient. A ISO certificate issuer can not issue a SAS 70. A audit firm can issue both a SAS 70 and an ISO 27000 certificate. Due to customer demands audit firms have started to move into the ISO market.
- ▶ A service organization can obtain a ISO certificate if they in a plan can show remediation. SAS 70 is *not forgiving* and a service organization will not receive a complete SAS 70 if there are any remarks.
- ▶ An IT-auditor can trust a SAS 70 but never a ISO certificate regarding financial statements.

Why organizations succeed in ISO and SAS 70 – observations

- ▶ Implement controls the current processes! No one will read your MS Word documents
- ▶ Do not mix legal (law), legal (contract) demands with business (for example KPI) demands
- ▶ Always assess the price for a control
- ▶ Always demand the right to audit in contracts but do not use it to over audit your supplier (the service organization)
- ▶ Withdraw all company directives(!), look at the demands (ISO and SAS 70) and then rewrite the directives (and save some pain within your organization)
- ▶ Do not attempt to do everything by your self (Directives, Controls, Implementation, pre-assessment, audit)

And finally – vad vill vi säga till IT Sverige idag?

The screenshot shows the Computer Sweden website interface. At the top, there's a navigation bar with 'SAJTER', 'COMMUNITY', 'KARRIER', and 'EVENT'. Below that is a search bar and user login information. A large banner for Audi Approved :plus is visible, featuring a silver Audi car and a '10 dagar' badge. The main content area is divided into several sections: a search bar for blogs, a 'Nytt inlägg' button, and a featured article titled 'Jäv i IT-branschen' by Andreas Halvarsson. To the right, there are sections for 'CS KOMPENDIUM OM KRAVHANTERING' and 'CS WEBINAR: Virtuella möten och videokonferenser'. The bottom of the page shows a list of 'MEST LÄST' (Most Read) articles.

Computer Sweden - Sveriges IT-tidning - dagliga nyheter om it-branschen, telekom mm - Del av IDG - Microsoft Internet Explorer p

File Edit View Favorites Tools Help

Back Search Favorites

Address <http://csblogg.idg.se/bloggar/it-risker/>

En sajt i IDG-nätverket | söndag 24 maj 2009

Översikt Prenumeration Kundenservice Annonsera Om IDG

SAJTER COMMUNITY KARRIER EVENT Sök i IDG-nätverket SÖK Inloggad som Andreas Halva... Mitt IDG Logga ut

Nyligen inkörd.

Audi Approved :plus

- Extra omfattande checklista
- Kraftigt utökad garanti
- Attraktivt finanserbjudande
- Heltäckande försäkringsmöjlighet
- Förlängd bytesrätt

10 dagar

Bloggar CS Karriärnätverk Itivarden.se CS Jobb CS Utbildning CS Seminarier Kompendier Nyhetsbrev Ordlistan

Sök i bloggar: Ange sökord Sök

CS bloggar **It-risker**

CS BLOGGAR » IT-RISKER

Nytt inlägg

It-risker

Här bloggar Andreas Halvarsson, it-rådgivare och it-revisor på Ernst & Young, om aktuella händelser inom it och deras konsekvenser.

Jäv i IT-branschen

Domaren i Pirat Bay-målet anses jävig av många och så kanske det är. Är så fallet, kommer han avsättas från sitt uppdrag. Men innan vi pekar finger på svenskt rättväsende, som har en lång tradition av att faktiskt pröva jäv, kanske vi ska fundera på hur det ser ut i IT-branschen? Om jäv skulle prövas här hur många skulle då "avsättas"?

Hämta pdf!

VIRTUELLA MÖTEN

ANNONS

CS WEBINAR:
Virtuella möten och videokonferenser

MEST LÄST

- Äventyrliga prylar
- Hemserver med Atomkraft
- En tekniskt fullpackad Arena
- "Öppen kod sex"

<http://csblogg.idg.se/bloggar/it-risker>



Andreas Halvarsson
+46 8 520 594 55
andreas.halvarsson@se.ey.com
www.ey.com/se

The information contained within this document and any related oral presentation conducted by Ernst & Young AB (EY) contains proprietary information and may not be disclosed, used or duplicated - in whole or in part - for any purpose without the express written consent of EY.

