



ISO 27001 and Compliance Survey Results

Survey conducted during March and April 2007

Which single regulation area do you expect to spend the most money on in 2007 and 2008?	Percentage
Sarbanes Oxley	42%
Payment Card Industry (PCI) Data Security Standard	12%
Various Data Breach Notification Laws	31%
Gramm Leach Bliley (GLBA)	4%
Other	12%
Total	100%

How many individual regulations related to information security would you estimate that your organization needs to comply with?	Percentage
0-2	23%
3-5	27%
6-10	19%
More than 10	31%
Total	100%

To what extent is ISO standard 17799 used in your information security management program?	Percentage
Not at all	15%
We use some of the ISO 17799 best practices	35%
We use most of the ISO 17799 best practices	15%
Align ISMS with ISO 17799 as the foundation	35%
Total	100%

ISO 27001 is a standard allowing for certification of an information security management system in accordance with ISO 17799. How would you assess your familiarity with 27001?	Percentage
Know virtually nothing about 27001	23%
I have a basic understanding of 27001	42%
I have researched the applicability of 27001 to my organization	15%
I have have a strong understanding of the 27001 standard	19%
Total	100%

Global adoption of 27001 is aggressive in Asia, with approximately 2,000 certifications awarded in Japan while there are currently 49 certified companies in the U.S. How would you assess your ISO 27001 certification plans over the next two years?	Percentage
No chance	19%
We may have a business unit(s) pursue certification	50%
Full organizational certification	4%
Unknown at this time	27%
Total	100%

What do you see as the main drivers for an organization to seek 27001 compliance? (More than one answer possible)	Percentage
To assert security to business partners	35%
As a proxy for compliance with security regulations	35%
As a best practices defense against security incident-related litigation	27%
To create a baseline for continuous improvement in our ISMS	31%
Total	127%