



# Survey Results

- Up
- How 27000 Works
- History of 27000
- The Future of 27000
- The ISMS Journal
- FAQs
- Is 27001 for you?
- Survey Results**

- Home
- About Gamma
- Tour our Web Site
- Events
- White Papers
- Services
- Visitors' Book
- How to contact us
- Internal Control
- ISMS
- Smart Cards
- Common Criteria

Over the past seven years, people have been kind enough to complete our [ISO/IEC 27001 questionnaire](#). If you were one of those people - thank you. If not, then still please read on and perhaps try the questionnaire yourself and see how your needs compare with others. On this page, we summarise our findings since 1st January 1998 'till **7 March 2006**. Over these 8 years the results have been quite uniform.

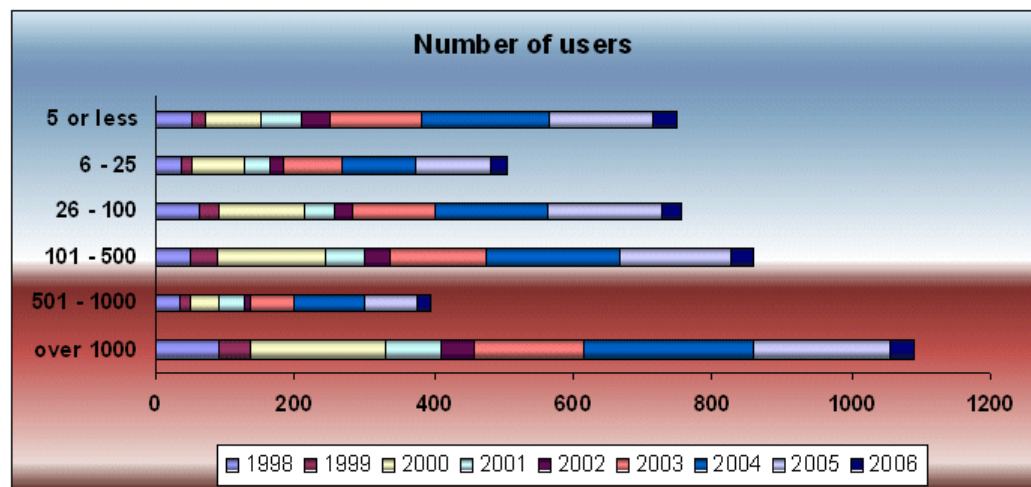
The questionnaire assists you to conduct a high level risk assessment of your information systems. It takes account of your operational needs concerning the confidentiality, integrity and availability of your information, from *your* perspective and that of *other* stakeholders (e.g. your shareholders) as perceived by you. It adjusts the risk in accordance with the size of network that you have, number of users and external connectivity. The result is expressed in terms of whether ISO/IEC 27001 is appropriate for you now, sometime in the near future, or not at all. The result is also expressed in terms of the scope of certification, in the sense that your operational concerns are general or are biased towards confidentiality, *or* integrity and availability. [Click here](#) to jump forward to the answers.

R  
L  
E  
A  
S  
T  
U  
E  
L  
S  
T  
S



We have analysed 4363 responses in total. There were 332 in 1998, 165 in 1999, 663 in 2000, 308 in 2001, 183 in 2002, 696 in 2003, 989 in 2004, 852 in 2005 and 175 so far this year. Duplicates have been removed from the analysis.

In terms of network size, number of users etc., there was a reasonable spread (the x-axis indicates the number of respondents that answered the question in the same way).

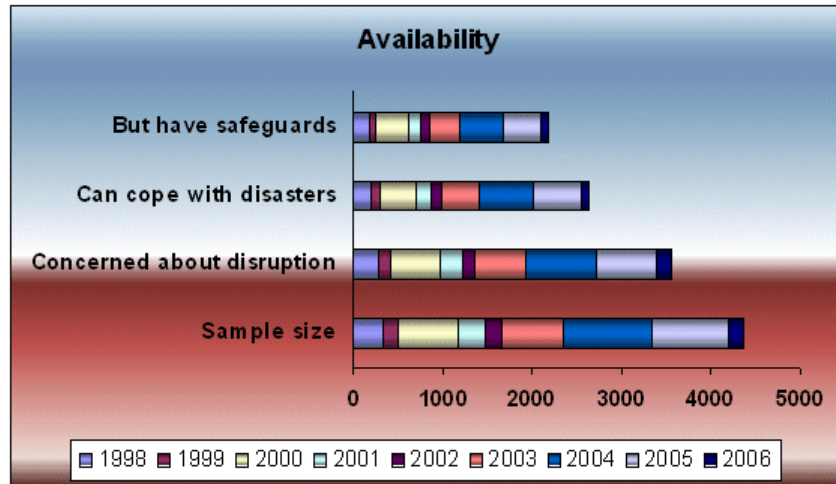


Out of the 4363 respondents, 13% claimed not to have a network, 84% claimed they had Internet or other forms of remote access and 76% said that they were very dependent upon their computer network.

## Availability

These claims on network dependency ought to be reflected in terms of our respondents regard for

*Availability of Information*, i.e. that information can be accessed by a user when he/she needs it:

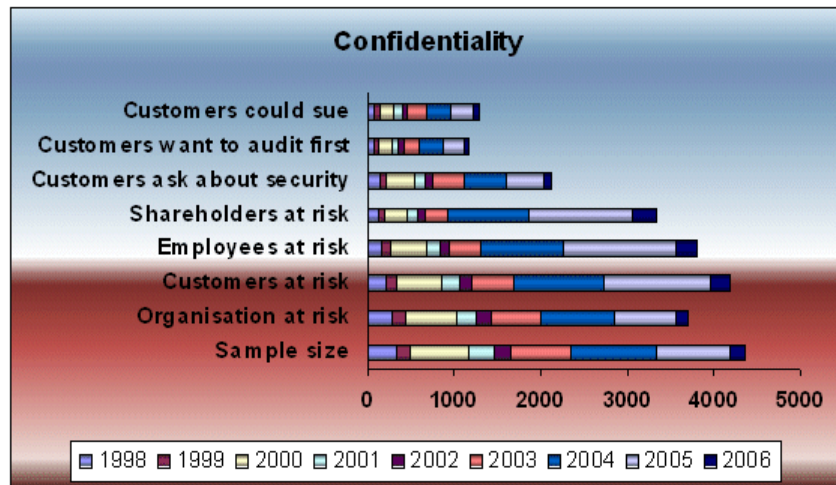


Indeed it is, with the vast majority of respondents having appropriate safeguards in place. For the remainder, it would be unfair to say that they have yet to address their concerns; it could be outside the scope of their ISMS! For example, if you lease a database from a supplier, loss of that database may not be as important to you as if you had created the database yourself, since the supplier could always give you another copy.

## Confidentiality

There used to be a generally held belief that the commercial world is not concerned with confidentiality. Not so, and this bears out our "Insurefast" study.

78% of respondents directly expressed concern about the leakage of sensitive information to outsiders:



The Insurefast example concerns a Marine Cargo Insurance Service. At the time of our study, one of the shareholders, a bank, conducted a security review. Unfortunately, they had conducted it on the premise that the Insurefast system was a "payment" system, for which confidentiality is *not* high on the agenda. One of the factors that convinced us that confidentiality *must be top* of the agenda was responses to our questions concerning whether customers want to "check out your security" before they will buy your service, and whether "customers would sue you" if you got it wrong. 29% say their customers would sue, 27% say that their customers want to audit first and 48% say that their customers ask them about security.

## Integrity

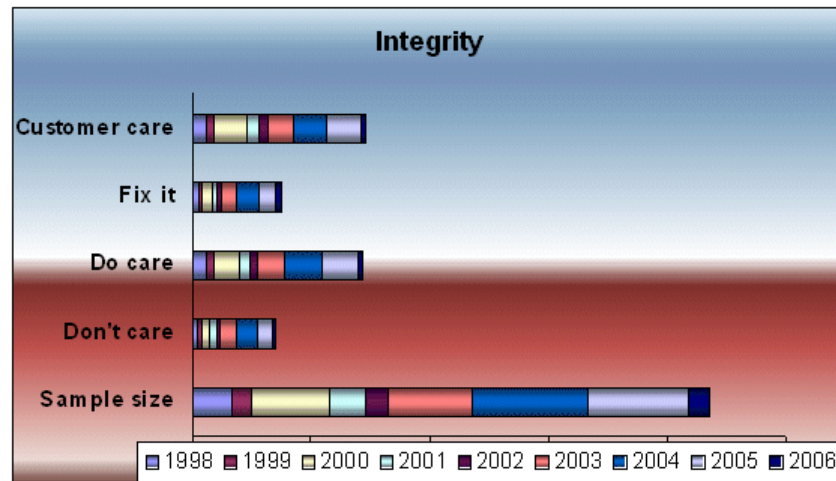
The traditional IT definition of integrity asserts that the information contained within a computer system is what you put in. There is also a business-orientated definition that asserts the information is "fit-for-purpose", and in particular that "management" can make informed decisions, based upon such information. This doesn't mean that the information is correct or that it reflects reality. It merely means that the user can readily determine the reliability of that information and base his/her decisions accordingly. Barings will continue to be the canonical example of the failure to apply this business-orientated definition of information integrity.

Our questions were phrased to determine how respondents "squared-up" to this business-orientated definition. We feel that there four stages:

- That the concept is irrelevant to the organisation, or that it *genuinely doesn't care*
- That the concept is relevant and understood, but that the organisation is not yet in control (*does care*)
- The organisation is in control, sufficient to spot errors, e.g. in invoices, and *fix them* before a customer, or external party spots it.
- The organisation is so much in control that as part of a *customer care* programme it is proud to publicise its ability to spot errors and correct them.

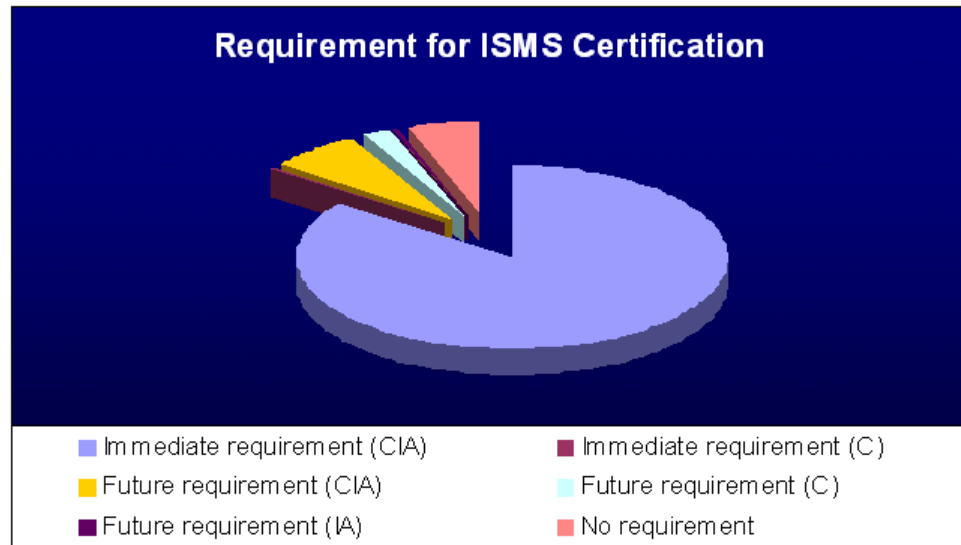
The ability to spot errors and fix them quickly is dependent on the time to detect and the time to fix. Take a look at our paper on "[measuring the effectiveness of an internal control system](#)" for a presentation of the underlying theory.

Our results:



## So, who needs ISMS certification?

It would appear that 3709 out of 4363 respondents do (that's 85%), they need it now and their scope should encompass confidentiality, integrity and availability. Surprisingly, only six who desire immediate certification have a bias towards confidentiality or integrity and availability, and that is a bias towards confidentiality:



228 (5%) respondents do not appear to have a need for ISMS certification: 420 (10%) do at some future time of which 80 appear to have a bias towards confidentiality and 30 towards integrity and availability.

Out of the 3709 respondents who appear to have an immediate need for ISMS certification only 1639 (38%) claim to have an ISMS in place. *To those of you who do not, the message is still the same:*

**Better get cracking. Having an effective ISMS is what ISMS is all about!**

And for those of you who discovered some time ago that you needed ISMS certification, what are you doing about it? [Click here](#) to see how many organisations world wide have been successfully certified, but it is still a lot smaller than our overall sample size.

---

Gamma is an ISO/IEC 27001:2005 and BS EN ISO 9001: 2000 registered company, certified for the provision of information security consultancy. BSI certificate numbers IS 85916 and FS 30710. Please send comments to [webmaster@gammasl.co.uk](mailto:webmaster@gammasl.co.uk) or complete our [Visitors' Book](#). Gamma Secure Systems, Diamond House, Frimley Road, Camberley, Surrey, GU15 2PS, UK Tel: +44 1276 702500 - Fax: +44 1276 692903. Copyright © Gamma Secure Systems Limited 1998-2006

Page last updated: 8 March, 2006