New ISO 27004: Indicators for Security

Measuring progress enhances recognition of information security within the organization

(January 2010) - Indicators are to make information security measurable and thus calculable for management. This is the goal of the new "ISO/IEC 27004 – Measurement", a supplementary standard of the well-known Standard for Information Security ISO 27001. Thus the ISO Bodies give strong signals towards a culture of indicators. For up to now, measuring techniques were not really in the centre of interest. "The topic of security, which is nebulous for non-experts, is made tangible by indicators and will be allowed to play a more important role in future." This is what Erich Scheiber, Managing Director of the Certification Body CIS, forecasts. For if progress is measured, this will also make it visible to other Departments to what high extent information security penetrates all the business areas – from purchasing via marketing to HR management.

Methods, formulas, analyses, …
The supplementary standard, which has been published recently, provides companies with a detailed guide for quantitative progress control and reports in information security (IS). This is to help to make process improvement according to "Plan-Do-Check-Act" even more effective and focused. The standard offers measuring techniques, mathematical formula, definitions of basic dimensions and derived dimensions, analyzing techniques as well as decisional criteria for expressive IS indicators.

… combined with gut feeling
"On the whole, ISO 27004, which is very methodological, is not conceived to be implemented one by one. Organizations will profit if they selectively use contents and start with chosen indicators," explains CIS Auditor Herfried Geyer. Partly the contents follow the American counterpart NIST SP 800-55, which, however, leaves more room for qualitative assessments. "NIST SP 800-55 can be combined with ISO 27004 well and can nonchalantly be called a practicable functionalization of gut feeling," says Herfried Geyer.

Examples of acquisitions
Important requirements the umbrella standard ISO 27001 places on security, such as monitoring of security controls, documentation of measuring techniques or evaluation of trainings made, are optimally met by using ISO 27004. In this respect, it is left to the user to decide what types of indicators are useful. Depending on the policies and situation, the examples are as follows:

- integrity of customer data: complaints in per cent, hard bounces relating to newsletters in per cent
- success of training: share of employees participating in awareness programmes, understanding of the imparted contents in per cent (multiple choice via intranet)
- third-party agreements: share of suppliers with IS relevant delivery contracts, fulfilment / non-fulfilment, problem rate
- account control: failure rate at user accounts
- security incidents: number/reduction a year (classification of the cases acc. to ISO 27001)

More recognition
"In future, measuring progress by using indicators will lead to an increasing recognition of security concerns and IS Representatives within the company," Herfried Geyer expects. Thanks to this, information security, which focuses on IT too much, can become a holistic concern, which will significantly contribute to increasing business success, even in the employees' eyes.

Info box:
ISO 27004 includes the contents:

- Management responsibilities
- Measures and measurement development
- Measurement operation
- Data analysis and measurement results reporting
- Measurement Program evaluation and improvement
- Annexes A-B, which furnish a metric structure and examples