Using ISO/IEC 27001 certification to increase resilience, reassure clients and gain a competitive edge

"Without robust systems in place, we could lose business. That's why we went down the standards route. We wanted to achieve best practice and demonstrate it to both commercial and government clients, who are insisting on it."

Bill Millar,
Head of Security,
Infrastructure Outsourcing Services,
Capgemini UK

Customer objectives

- Improved security, protecting clients' assets, resources and people
- Gain a competitive edge
- Assurance of the confidentiality, integrity and availability of information

Customer benefits

- Improved security for Capgemini UK and its clients
- 'Badge on the wall' proof of best practice to potential and existing clients
- Increased security awareness and buy-in among management and staff
- Enhanced security documentation and reporting

Customer background

Capgemini is Europe's largest IT services company and a global leader in consulting, technology, outsourcing and local professional services.

Headquartered in Paris, it has a 45-year history as an independent company and now operates in over 40 countries and 100 languages. In 2012 it reported annual revenues of €10.3bn.

Why certification?

Security is a key building block upon which the entire Capgemini group depends; protecting its assets, resources and people – and those of its clients – and ultimately providing it with a competitive edge.

Key security drivers include traditional threats such as accidents, natural disasters and attacks by computer system hackers, but also new 'threats' such as increased government regulation and tougher requirements from the PIN card industry.

Bill Millar, Head of Security for Capgemini's infrastructure outsourcing services business in the UK, explains "If we fail to comply with regulations we risk heavy fines and severe damage to our reputation. Security has also become a major concern for clients. Without robust systems in place, we could lose business. That's why we went down the standards route. We wanted to achieve best practice and be able to prove that to ourselves, but we also wanted to demonstrate it to both commercial and government clients, who are insisting on it."

Millar identified a range of measures required by Capgemini UK to ensure the confidentiality, integrity and availability of information it needs to hold to carry out its business effectively. He was determined that these measures should be pragmatic, business-focused, risk-based, holistic, systematic, cost-effective and directed by the client's or Capgemini's own standards. With this in mind, the company sought certification to the information security standard ISO/IEC 27001, which offers a comprehensive approach to information security.

Benefits

Capgemini UK lists a host of benefits from ISO/IEC 27001 certification, including improved security for the company and its clients, assurance of best practice to new and current clients, enhanced security awareness and enthusiasm among staff, and improved security documentation and reporting.

Security is now highly valued at board level in the company, creating operational buy-in and financial backing, and making the issue an integral part of Capgemini UK's outsourcing business. Above all, says Millar, "It's not just about looking after data; it's about looking after people and physical security too – it's not just for techies."

He continues, "We are really pleased with the benefits that certification has brought us. Our customers like it as they don't have to get and pay for external auditors – they use our reports from BSI to assure themselves of the quality of our security."

Implementation

Capgemini's Dutch and Indian operations had been the first to adopt the information security standard ISO/IEC 27001 and "they were clearly getting benefit from it," says Millar. For example, in putting together bids and tenders, he says the UK business was "producing reams of paper on each occasion, spending huge amounts of time and money proving our infosec credentials. Our overseas colleagues simply provided their ISO/IEC 27001 certificate number. We thought, 'let's just get certification' and release staff to do other jobs."

By early 2008, Millar had created a business case to justify the required investment and by February of that year he had won the approval of his board, both financially and in terms of 'buy-in'. "It wasn't difficult. In fact, the board asked 'why aren't we doing this already?" he says. He used Capgemini's own UK Security Forum as the control structure for the project, sponsored by the company's Chief Financial Officer, and recruited a dedicated two-person team.

First, the company's risk approach was clarified and then it started to communicate with staff and gain buy-in from account leads. Next, it brought its security documentation up-to-date, adding new areas such as mobile security. Finally it began a cycle of security audits, systematically covering the areas initially scoped.

BSI's role

Capgemini identified BSI as its preferred external auditor. "BSI proved extremely helpful right from the start by advising on the scope of the project and suggesting that we reduce our scope and approach the task in 'bite-sized chunks', which made it much more manageable," says Millar. "Having selected BSI as our auditor, we found the process actually very straightforward, but it required a lot of work."

He continues, "The external audit by BSI went very smoothly because we had done the work. It took place in a measured fashion, with our principal task being to ensure that the right people, from senior managers to technicians, were lined up to see the auditors."

Just 10 months from the start of the project, in November 2008, Capgemini's UK outsourcing business achieved its goal of having an information security management system certified to ISO/IEC 27001. The company has since planned and prepared for 6-monthly surveillance audits by BSI, and has gone on to recertify itself in 2011, with 10 of its 14 UK sites now covered by the standard.

As for the future, further recertification is due every three years, while fresh goals include certifying the final four UK sites, as well as 'spreading the word' about the benefits of ISO/IEC 27001 to other parts of the group outside the UK, including Poland and Germany.

bsi.

+44 845 080 9000
certification.sales@bsigroup.com
bsigroup.com

bsi. ISO/IEC 27001 Information Security Management