# The Business Value of ISO27K - a Case Study


## Summary

This case study concerns an IT services company that implemented ISO/IEC 27002:2013, the Code of Practice for Information Security Management, and was certified against ISO/IEC 27001:2013, the Specification for an Information Security Management System, gaining significant business advantages as a result. The case reveals some surprising linkages between information security management and general business management, and several indirect business benefits that are seldom mentioned.


## Introduction

### *This case study*

This case is derived from a presentation by the Managing Director of "ServiceCo" [not its real name], an IT services company, to an audience of information security and IT audit specialists. The MD was a stand-in speaker – his CIO was scheduled to speak but had to pull out at the last minute. The MD explained that he was happy to speak on this topic given his passion for information security and the business benefits it has his generated for his company.

### *ServiceCo's business situation*

ServiceCo supplies IT services, hardware and software to corporate clients. Having gained its ISO 9002 certificate nearly a decade earlier, employees were used to working in a consistent manner using documented quality procedures and guidelines. A couple of years ago, however, the atmosphere within the company had turned sour. Management decisions were mostly being made instinctively on gut-feel with little real analysis. With staff turnover increasing, senior management recognized the need to change and took a long hard look at the organization's strengths and weaknesses.

ServiceCo management decided to implement ISO27K (meaning both ISO/IEC 27001 and 27002). According to a ServiceCo director, "Implementing ISO27K made business sense. Securing ServiceCo's internal information would reduce the risk and hence the cost of serious breaches. ISO27K is a known security framework originally developed by some of the world's leading companies (BT, HSBC, Shell International and Unilever, amongst others), so it gave us the means to implement best practice security controls."

# Business benefits of ISO27K

The MD said “ISO27K is not just about information security or IT – it actually helps the organization save and make money.” He identified the following direct and indirect business benefits of ISO27K for ServiceCo.

## *Direct benefits*

**Increased reliability and security of systems**: “Like all businesses ServiceCo is reliant upon information systems. ISO27K has ensured that we now have controls in place that maintain system availability and reduce the risk of vulnerabilities being exploited. Post-certification ‘surveillance visits’ and re-certification audits against ISO/IEC 27001 ensure the business keeps up-to-date with the latest vulnerabilities and best practices.”

**Increased profits**: “Sales and margins are up, and clients’ perceptions of our business have improved. Our ISO/IEC 27001 certificate demonstrates that we can be trusted to secure our customers’ data, as well as our own. Our customers not only understand that our investment in ISO27K has given them benefits, but they are prepared to spend a little more for a secure IT infrastructure. Since gaining ISO/IEC 27001, we have already seen a marked increase in our bottom-line profit and some new customers are telling us they prefer to trade with companies who have a recognized security certification. Additionally, we are now seeing more Invitations to Tender from business that list ISO/IEC 27001-compliance as a pre-requisite. And, by the way, our employees are wasting less time surfing the Internet for sites not related to work!”

**Cost-effective and consistent information security**: “We have implemented cost-effective security matched to our business needs. ServiceCo had many technical safeguards throughout the organization, but the risk assessment highlighted that some of our safeguards offered little or no business benefit and would provide a better return off investment if they were reconfigured to protect assets that required a higher level of protection. All divisions and departments within ServiceCo had previously developed their own security guidelines. ISO27K helped us develop a consistent approach to security by creating uniform policies incorporating industry best practice. Where necessary, employee compliance with the policies is supported by an enforceable disciplinary process.”

**Systems rationalization**: “Analyzing our information and information security requirements properly means we spend our money wisely. We were able to cut about 50% of our systems and data when we realized they were not worth keeping, and we actually relaxed controls on some low-risk systems.”

**Compliance with legislation**: “Implementing ISO27K forced us to comply with UK legislation in areas such as data protection and software copyright.”

## *Indirect benefits*

**Improved management control**: “Managers have more control over the organization, and better-quality information with which to manage it - management effort is therefore reduced.”

**Better human relations**: “Clear policies, procedures and guidelines make things easier for our staff – the atmosphere has improved and staff turnover has reduced. ISO27K has made ServiceCo different from our competitors and provided the company with a unique selling point, leading to a better working environment for all of our staff. Employees now recognize that their earning potential is dependent on how customers perceive the company brand and that any negative publicity could affect them. Professionalism has improved throughout the company. Given that so much of security relies on internal controls, we needed to look more carefully at who we were employing. Through ISO27K we introduced more through recruitment processes that reduce the risk of employing people unsuitable to the position or who could potentially put our business at risk. We now know who is working for us!”

**Improved risk management and contingency planning**: “Through the ISO/IEC 27001 certification process, ServiceCo identified its vulnerabilities, threats and potential impacts to the business. As a result of this and implementing controls from ISO/IEC 27002, ServiceCo now has a more structured approach to risk management. For example, we now have a rational process to decide which risks to transfer to our insurers. We also now have a business continuity plan that suits the business, not just the IT department. The risk assessment identified information assets that are critical to the success of the business. This enabled us to produce a business continuity plan that prioritized these assets and reduces our potential exposure to financial loss or negative publicity.”

**Enhanced customer and trading partner confidence**: “With the heightened sensitivity to security breaches, trading partners, customers and vendors were looking evidence of security. ISO/IEC 27001 certification has provided this assurance. In any industry you have to stand out from your competitors. Being the first IT Value Added Reseller in the world to obtain ISO/IEC 27001 is a bold statement that will always be unique to ServiceCo. Having the ISO/IEC 27001 logos on our company literature is a continual reminder to potential and existing customers that we are a professionally-run organization who take the confidentially, integrity and availability of their and our information seriously.”

# ISO27K costs

“Despite what people say, the costs of implementing ISO27K are very modest. The main cost element was the pain of cultural change (we had to ‘let a couple of our people go’ for not complying with our policies and procedures). The regular compliance reviews to maintain our certification only costs us about £3k [US$5k] a year so ISO27K is very cost-effective. We are now talking to our assessors about combining the ISO/IEC 27001 and ISO 9002 audits to save time and money.”