ACHIEVING ISO 27001 SENDS MORE THAN JUST A COMPLIANCE MESSAGE

Ralf Gladis,
CEO,
Computop

The protection of sensitive customer data is a topic of key concern to all banks and financial services companies and is integral to their digital transformation projects. Despite this, however, ISO 27001, the auditable international standard relating to information risks, represents unchartered territory for many financial organisations, not least payment processing providers.

ISO 27001 defines the requirements of an information security management system (ISMS), incorporating policies, procedures, processes and systems that help to oversee risks relating to information assets such as cyber-attacks, hacking attempts and data theft. While some organisations adopt the standard as a framework for best practice without choosing to be certified, others put in place and document those processes and policies that contribute to information security so that they can be certified. It is a considerable undertaking, but it is also vitally important.

Last year we elected to be certified according to ISO 27001- one of very few payment service providers in Europe to achieve this – because we felt that it fully addresses one of the most important aspects of financial transactions – secure data exchange.

Sensitive data under threat

The global pandemic has accelerated the already severe threat to data security, and it is the financial sector that has borne the brunt of the attacks. According to a report published last September, the banking industry experienced a 1,318% year-on-year increase in ransomware demands in the first half of 2021, and was the industry most affected by this form of attack. Given that figures suggest the average cost of a data breach in the financial sector in 2021 was $5.72 million, it is imperative for organisations to do everything they can to protect sensitive data.

This was topmost in our minds when we started the process of certification. It is incumbent on any payment processing provider to operate at the highest possible security level, but by achieving ISO 27001, we would also be demonstrating our commitment to quality as a service provider to our many banking partners.

The 114 standards that need to be adhered to as part of gaining certification might look, at first glance, like a high mountain to climb. However, if an organisation is already working towards the delivery of secure protocols for financial transactions, or if they adhere to PCI-DSS regulations for processing credit cards, they are already on the road to ISO 27001 compliance.

The benefits of certification

Implementing the measures within the scope of ISO 27001 certification automatically increases data security, but there is also the added benefit of reducing the effort required during security audits. During a tendering process, for example, questions relating to hardware and software processes are becoming more and more frequent, and the emphasis on data security is increasingly intense, but this is relieved if a company already has ISO 27001 certification. The most common standards required during tenders are proven during the testing process for the certificate and are considerably more stringent than the annual PCI-DSS audit that credit card companies require of their data processors.

For payment service providers there is also another layer that can be satisfied through ISO 27001 certification. If the PSP is a white-label provider, or essential outsource, for a financial services company, they will be required by MA Risk and EBA guidelines, to prove the PSPs compliance with common standards. With ISO 27001 in place, this is considerably easier to achieve than the alternative of an in-house audit.

What's it all about?

At its core, ISO 27001 addresses each of the three pillars of information security: people, processes and technology. It requires organisations to identify the information security risks inherent in their business operation and put in place appropriate controls to tackle those risks.

In our case, based on the 114 standards of the certificate, we implemented a range of measures that included management, employees, data centres and external service providers. For other PSPs or for banks, the measures may be different depending on their priorities and areas of risk. Other examples that might need to be considered include human resource security, asset management, physical and environmental security, and system acquisition, development and maintenance. There is no requirement for organisations to implement all 114 of the standard's controls.

A mark of achievement

In today's ultra-competitive world, anything that marks an organisation out for quality will increase its standing with customers. In our case retail companies across Europe can now be confident that their faith in our seamless IT security and secure administrative processes has been further bolstered by positive assessments under ISO 27001 and will be stringently audited on a regular basis. From the confidentiality classification of documents to data protection training for new employees, our processes have been examined and optimised as part of the certification process, with our team investing around 300 man-days in ensuring that we met the criteria for success.

However, regardless of whether the organisation is a PSP, a bank or an insurance company, working towards such certification is not a one-off task that can be ticked off when the certificate is obtained. A key component of the ISO 27001 regulations is the willingness of the company and its core team to engage in a continuous improvement process. This ensures that it is not only protected against current cyber security threats, but also has the necessary processes and tools in place to identify new threat scenarios at an early stage and respond in a timely manner.

It is an effort worth making. In a world threatened constantly by new and insidious forms of cyber-attack, and our reliance on digital technology growing greater by the day, compliance and regulation are essential. While ISO 27001 is not a security solution in itself, it encourages companies to adopt stringent behaviours and processes that reduce the risk of attack. It also demonstrates the effort that a company will go to in order to ensure it takes the security of its own and its customers' data seriously, and this is a crucial message to send to the outside world.