

Evolution of the Payment Card Industry Data Security Standard - PCI DSS

João Ambra CISSP, MCSO, 27001 Lead Auditor - December 13, 2006

Around the year 2000, due to the large increase in the amount of frauds using credit card numbers, credit card companies started to individually define security requirements. In order to make this task easier, the companies got together in 2004 and created a single standard called Payment Card Industry Data Security Standard - PCI DSS. The idea was to reduce the efforts made by commercial businesses, which sometimes had to comply with several different standards, as well as those made by credit card companies, which have since then been able to share control and training efforts. All companies that operate, transmit, or store credit card information are subject to this standard, which provides several different degrees of requirements based on the size of the commercial entity.

The new version 1.1 was launched in September 2006. It is effective as of 2007 in the United States, and is now managed by a council dedicated to maintaining the standard, the PCI Security Standards Council (<https://www.pcisecuritystandards.org/>).

Unlike other regulations, PCI provides detailed descriptions of the security controls that are to be implemented. This difference was reinforced in version 1.1, which also presents a better definition of compensating controls. These controls can be used to mitigate the absence of a required control under special conditions, such as budget limitations.

Online sales have been growing throughout the past few years. This can be demonstrated by recent facts such as the 42% increase in online sales on the last Black Friday (Nov. 24, the day after Thanksgiving): more than 600 million dollars in a single day (data from comScore). However, the growth in online sales also triggers growth in other areas. In 2005, losses resulting from Internet frauds were for the first time higher than those caused by "real world" crime and reached 3 billion dollars, according to an FBI report.

According to Gartner, only 17% of the 280 companies in the sales industry are compliant, although such a detailed standard as the PCI is now available. This shows that companies find it difficult to implement proper security controls to protect their businesses, which is one of the reasons why companies should use risk management tools, such as Risk Manager, to help them in the painstaking task of implementing controls and tests. The tool is extremely useful, especially after the implementation of the necessary controls, when all of them have to be regularly monitored and tested.