

Banking Industry: New Security standard for Payment Card Industry demands for extended Quality Management

In 2004 the foundation of the PCI SSC (Payment Card Industry Security Standards Council) was founded by the five largest payment card companies, among them Visa, Mastercard and American Express, to define and establish common security standards for the payment card industry. Before the advent of this group, every payment card company had its own security standard and every company working with different card companies had to be in compliance with all of these standards. Since its foundation it has been the goal of PCI SSC¹ to harmonize these requirements into one common standard, the PCI Data Security Standard (DSS), first published in December 2004. Every company that is handling with credit card data has to be compliant with this standard. This is the case for small merchants where customers pay with their credit card just as for the banks handling the financial transactions.



However, the impact is different for the involved parties: For the small merchant it is sufficient to guarantee that all used devices are compliant with PCI-DSS. For the banks this is much more difficult, since they usually operate large IT environments containing a mix of networks, 3rd party systems, COTS software and own developments.

After several high-profile data security incidents caused by exploits in various companies, a new version of the PCI-DSS-Standard has been adopted and is binding since 1.1.2009². The most interesting change is the new focus on Application Security: In contrast to typical network-level penetration tests, which are still a must to be compliant with PCI-DSS and which still need to be applied at the end of the software-development step by an independent partner, there is now a much stronger focus on checking application security using technical requirements in advance of testing. The fundamental new requirements are:

- Application of systematic code-reviews that can be supported by tools. The basic idea of that requirement is that most security vulnerabilities can be identified by a detailed code review.
- Creation of complete and consistent architecture modelling documents of all system components that are somehow connected to components handling the credit card data. This includes the requirement for an architecture evaluation, explaining why specific architecture decisions are being taken. Architectures with such a level of quality help perform efficient impact analyses and identify architectural weak points.
- Establishing an overall change-control-process to enable a full traceability for all artefacts created by activities of the software development and software maintenance processes. Doing so assures that all concepts, documents and components are consistent to each other and are helpful tools to guarantee high security.

SQS is providing a dedicated service portfolio for the payment card industry, supporting customers with fulfilling the requirements for PCI DSS compliance. The basic idea is to apply the well-known 360°-Quality approach to make the different single improvements happen. Doing this PCI-DSS-compliance can be reached "on the fly", because the specific requirements of the new PCI-DSS version are well-known in the context of a holistic quality management system.

¹ <https://www.pcisecuritystandards.org/>

² https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml