

Turning PCI compliance into a business asset

“Our customers are retail merchants, so payment card data security is paramount to them. That's why we set out to build our entire IT ecosystem, from the ground up, to be PCI DSS compliant.

Our goal was to ensure that data security would never be an issue for customers or potential customers. And the fact that our IT systems were designed from the start with compliance in mind is a definite competitive advantage for us.”



Jeff T. Liesendahl - CEO, Accertify

Turning PCI compliance into a business asset

challenge

Customer requirements and best-business practices dictated that Accertify should build its IT systems to comply with the PCI DSS standard from the very beginning.

Executive management was looking for this adherence to industry standards to become a tangible business asset.

With a goal of being compliant and validated to the PCI Data Security Standard in a short timeframe, Accertify chose HALOCK Security Labs as its partner.



Accertify is in a unique position. It processes no credit card transactions, but works with customers whose livelihoods depends on credit card transactions.

These customers look to Accertify to monitor and protect their companies from fraud. Because of this, Accertify is held to the highest level of data security standard by some of the largest credit card processing companies in the world.

Special Customers

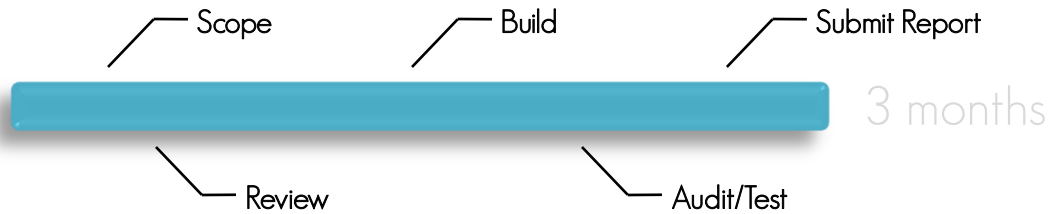
solution

With guidance and expertise from HALOCK, Accertify was able to implement an IT security program that fully adhered to the PCI DSS guidelines within just three months.

Bringing to bear capabilities ranging from governance through network architecture, systems hardening and secure application development, HALOCK acted as Accertify's trusted information security partner.

Turning PCI compliance into a business asset

the project



Scope

The first effort undertaken on the path to bring full PCI compliance to Accertify's systems was to identify and scope the elements and systems that would need to adhere to the DSS standard. For this step HALOCK assigned a team of PCI Qualified Security Assessors to work with the Accertify team to better understand the intent of each PCI requirement.

It was determined that any system or process that was associated with credit card data needed to continue through the remaining steps in the PCI compliance project.

By working with HALOCK and their Qualified Security Assessors early in the process, Accertify was able to avoid false starts and failed Reports on Compliance.

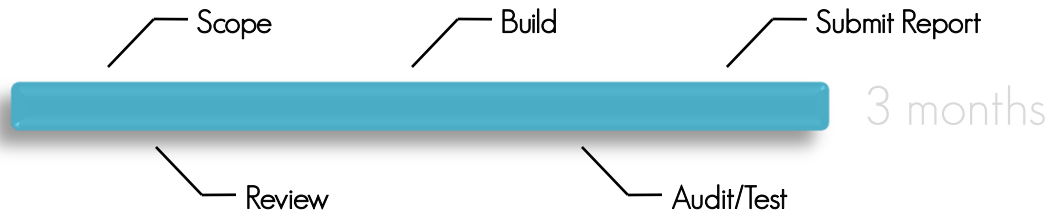
Review

Once the systems targeted for PCI compliance were identified, HALOCK began a review of the architecture of Accertify's application development and networking infrastructure.

HALOCK's Secure Application Services group worked closely with Accertify's development team to craft the SDLC documentation, ensuring that Accertify's custom code was being built to PCI standards.

Turning PCI compliance into a business asset

the project



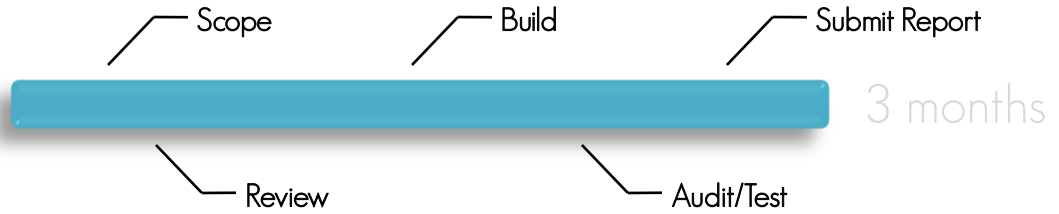
Build

With the architecture and design elements in place, it was time to bring to bear all of HALOCK's varied, security-focused capabilities. Network architects expanded and implemented a secure networking environment with the help of HALOCK partners RSA and Qualys. Secure software developers worked with Accertify technicians to write bullet-proof code using the previously defined SDLC documentation.

Firewall and authentication management configuration was completed by HALOCK as well as server hardening and continued guidance on developing operational security procedures and processes. Event logging and IDS event policy development were handled as a team effort with HALOCK providing PCI compliance guidance and the Accertify team configuring their custom analysis engine for generating alerts.

Turning PCI compliance into a business asset

the project



Audit/Test

Once Accertify's systems and code base were hardened and backed by proper policies, aggressive testing was required to prepare for the final audit. HALOCK ethical hackers performed vulnerability scanning and penetration testing against the new systems using the tools and techniques employed by actual hackers.

Any vulnerabilities were rectified and affected policies were modified to position Accertify to submit a Report on Compliance that would easily pass muster.

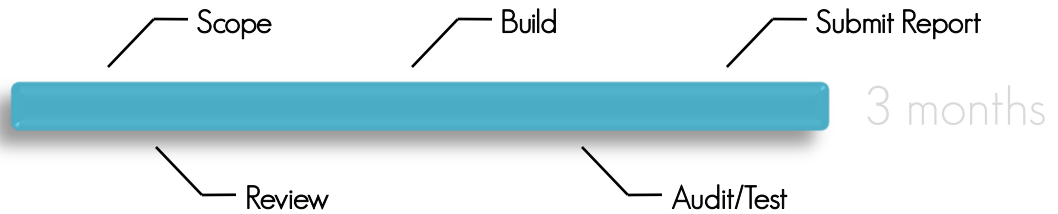
Payment Card Industry Data Security Standard was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, cracking and various other security vulnerabilities and threats.

A company processing, storing, or transmitting payment card data must be PCI DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined. Merchants and payment card service providers must validate their compliance periodically.

What is PCI?

Turning PCI compliance
into a business asset

the project



Submit Report

Classified as a Level 2 Service Provider, Accertify is required to submit an annual Report on Compliance with credit card companies.

The creation of this report was simplified by HALOCK thoroughly documenting evidence of Accertify's technical, operational and software development security controls.

“Because HALOCK’s assessment and compliance services are separate from our networking and application services groups, we are able to provide appropriate checks and balances and move our clients quickly into compliance with the PCI Data Security Standard.”

Terry Kurzynski - CEO, HALOCK Security Labs



summary

Having built its security program from the ground up to be PCI DSS compliant, Accertify looks to not only leverage their PCI compliance toward full ISO 27001 registration in the future but also to reduce security maintenance costs. Not having to implement compensating controls in order to comply with PCI is a cost advantage for Accertify.

As part of its security program, Accertify has contracted with HALOCK to provide on-going services including monthly vulnerability scanning, quarterly penetration testing and other services. Because HALOCK's services are also structured after the ISO 27001 guidelines, they fit precisely into their customer's security programs.

The primary question pondered about any business investment is 'does this investment contribute to my company's bottom line'? For Accertify, the answer is yes. E-commerce customers are more comfortable doing business with a company whose security program is mature and aligns with all applicable industry standards.

The ISO 27001 standard is a model for establishing, implementing, reviewing, maintaining, and improving an Information Security Management System (ISMS); often referred to as a Security Program.

Smart companies follow the ISO 27001 standard to unify their security requirements under one framework.

ISO 27001

Turning PCI compliance into a business asset

who is Accertify?

Accertify™ provides leading-edge fraud prevention solutions to merchants who accept transactions when a credit card is not present. Accertify's experienced fraud prevention experts have developed Interceptas™, the only integrated, end-to-end solution which applies state-of-the-art automation to every step in the merchant's process of managing fraud exposure. Interceptas™ helps merchants maximize revenues and reduce their total cost of fraud through improved detection rates, reduced false positives, fewer chargebacks and increased productivity. It ensures that all of a merchant's fraud prevention tools, data and processes work together for maximum efficiency and effectiveness. Accertify is a full-service provider of consulting, outsourcing and hosting services.



“We look forward to a long-term partnership with HALOCK to ensure the security of our client’s data and to continue to comply with the PCI DSS standard.”

Andrew Lauter - CIO, Accertify



who is HALOCK?

HALOCK's mission is to protect their clients and their digital assets.

HALOCK, through their directive of Purpose Driven Security, provides solutions globally that protect their clients and their digital assets by anticipating, interpreting and delivering changes in the information security landscape.

HALOCK consultants are guided by The Code (HALOCK's Code of Ethics) and armed with Purpose Driven Security to be their client's security partner.

Purpose Driven Security increases shareholder value and guards against the temptation of the 'blinking lights' by driving clients to understand:

"Why"

Why this policy? Why this standard?
Why this control? Why this response?
Why this expense?

Purpose Driven Security