CASE STUDY
PCI DSS Programs for Small Merchants: Making PCI DSS "Business As Usual" in large, multinational, distributed environments

THE MERCHANT

ACCOR HOTELS
Feel Welcome

AccorHotels is the largest hotel operator with a network of 4,300 hotels in 100 countries distributed through a hotel portfolio of 25 hospitality brands from luxury to economy.

AccorHotels also has new businesses in private rental, co-working, concierge services, dinning & events and digital solutions, with 25,000 employees whose commitment and passion is helping Accor reinvent hospitality.

For more information visit:
http://www.accorhotels.com

THE SOLUTION

VIGITRUST

VigiTrust is an award-winning provider of SaaS Governance Risk Compliance (GRC) solutions with users in over 120 countries. VigiTrust enables large organizations, their subsidiaries, franchise operations and wider enterprise networks, to achieve and maintain compliance with legal and industry security frameworks including PCI DSS, GDPR and HIPAA. This is done through the provision of an education, compliance validation and compliance management solution.

For more information visit:
http://VigiTrust.com

How AccorHotels and VigiTrust help thousands of hotels achieve and maintain compliance with PCI DSS

Let's hear from the merchant and the partner provider.

What PCI DSS program management challenges do you face?

AccorHotels: AccorHotels comprises more than 25 brands of hotels of all types and sizes in over 100 countries. The group includes owned and managed hotels and franchisees. At the AccorHotels Group, compliance efforts are spread across different teams and business units including security/compliance, country offices, local management and other lines of business. Coordinating these efforts is challenging, and central to this is the need to educate merchants, get them onboard with the PCI Data Security Standard (PCI DSS) and simplify their compliance efforts as much as possible.

What kind of PCI DSS compliance program was needed?

AccorHotels: Facing the challenges AccorHotels had with PCI DSS compliance on scale, we knew we needed a comprehensive multinational, multidimensional, and multicultural PCI DSS program to support our network of hotels. We needed a program that would have value-add to help our merchants achieve and maintain compliance.

What does 'value-add' mean when it comes to a PCI DSS compliance program?

VigiTrust: The real value add for merchants is access to plain-English business-driven security advice so they can easily implement and maintain good security practices. Secure payments throughout the merchant organization is the end game – for hotels this includes at reception, restaurants, bars, gyms, spas, shops. Providing education through eLearning and access to user-friendly procedures helps merchants understand why payment security is important and what's involved. Additionally, to help merchant demonstrate they are PCI DSS compliant, we provide SAQs (Self-Assessment Questionnaires) and AOCs (Attestations of Compliance) through our SAQ engine.

Why did AccorHotels choose VigiTrust?

AccorHotels: Working with the right partner is essential to the success of our PCI DSS program. We first met VigiTrust at their PCI European Roadshow in June 2011. They impressed us by highlighting the need to demystify PCI DSS for target audiences, prompting us to think about how we could customize a PCI DSS program for the hospitality industry. Up to that point, all the programs we had found were very generic. To be successful, we felt the program needed to be aimed at specific PCI DSS issues facing the hospitality industry.

We first engaged VigiTrust in 2012 for PCI DSS eLearning for 15,000 users. We further customized this for our hospitality needs in the next two years, leading up to a full, two-part customized program released in 2013. From the outset, we found VigiTrust to be a flexible partner that could adapt to our needs and work with us to develop a tailor-made PCI DSS training solution for AccorHotels.

What makes a good PCI DSS compliance portal?

VigiTrust: A good portal benefits those that work with merchants (such as acquirers, franchises, service providers, etc.) by providing all parties full visibility on the effectiveness of PCI DSS programs. By reporting not only on program completion but also on exceptions, program managers can help those merchants struggling to understand and implement good security practices, and that need help moving toward compliance.

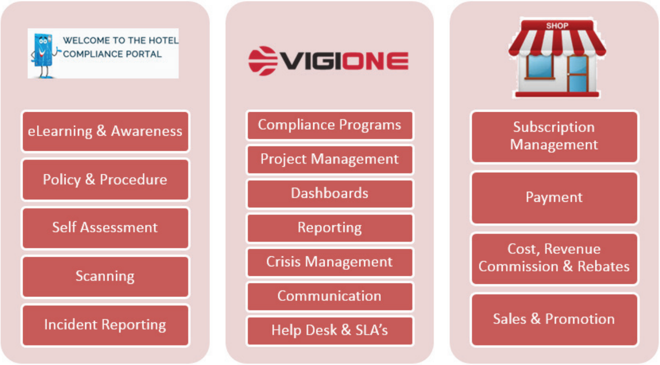
A good portal also needs to facilitate a 'Business as Usual' approach to PCI DSS. Entities need to implement "always present" security - not just strive to be compliant at the time of an annual assessment . Security is a journey, not a destination. Supporting an organization's continuous PCI DSS compliance must therefore be the primary objective of the portal.

Finally, a good PCI DSS compliance portal is customized to address the nuances of different organizations and industry sectors. It is key that advice provided to merchants be easy to implement, and be given in plain business language that merchants can identify with.

How is the customization of PCI DSS compliance programs achieved?

AccorHotels: Through partnership. AccorHotels provided customization ideas based on our needs and VigiTrust provided the solution. The proof of concept for an AccorHotels Merchant Compliance Portal (MCP) came in 2014. Reflecting the customization we achieved, we renamed it the Hotel Compliance Portal "HCP". Today HCP is a known acronym across all AccorHotels properties, security and compliance teams.

VigiTrust: VigiTrust has very detailed and effective customization process. This includes discovery workshops aimed at mapping out all areas that need to be customized, from eLearning to policies and procedures and SAQ choice wizards. This collaborative process initially requires time from our client organization champion, but the approach not only reduces the amount of time spent with each merchant, it also increases program accuracy and effectiveness. In the end, merchants – in this case hotels – benefit from a platform that is relevant to their environment, explained in terms they understand and branded in a way they recognize and identify with. For AccorHotels properties, HCP has become part of their daily tool set for compliance!



How has the partnering relationship developed?

VigiTrust: Customization is not about a one-time solution. It's about adapting to the needs of our customers as they change.

AccorHotels: Our compliance portal expanded from 100 to over 3,000 locations. Beyond ongoing content customization, this required multi-brand granular dynamic reporting, which VigiTrust deployed for us in 2016. Reporting is now available across all brands, per use type, completion status (completion/exception) and country. The incorporation of new features around policies and procedures and multiple SAQs also took place at this time, and in 2017 VigiTrust integrated other AccorHotels preferred third-party tools into HCP.

What's next?

AccorHotels: We're putting all aspects of our governance, risk and compliance together on a specially designed GRC platform developed by VigiTrust to address multiple regulations on the platform moving forward. For instance, GDPR has several common themes with PCI DSS. Rather than re-inventing the wheel, we can leverage HCP to address some GDPR requirements .

VigiTrust: AccorHotels' next step is to migrate the HCP to VigiOne, VigiTrust's next generation GRC platform. It is a more scalable, robust, faster solution that also provides for interaction with external auditors such as QSAs, who can help manage compliance levels from a single platform. All clients are currently migrating to VigiOne.

PCI DSS - SECURITY POLICIES FOR FRONT OFFICE

ACCORHOTELS
Feel Welcome

Data Retention & Cleansing	• I only keep information required for the operation • I delete sensitive data as soon as I receive authorisation • I only store cardholder data in PCI compliant software or in a locked cabinet and shred it according to our Data Retention Policy
CVV (Credit Card Verification code)	• I do not store CVVs, either on paper or electronically • I never write down CVVs • I remove CVVs from e-mails using the Action => Edit option • I print Adobe Acrobat PDF files and make CVVs unreadable
AccorHotels Payment Autorisation Form	• I only use the AccorHotels PAF for TARS-non-supported booking requests • I never ask for a photocopy of a payment card to guarantee a reservation
Email & Fax	• I deal with fax right upon receipt and shred immediately • Alternatively, I lock faxes into the Reservations cabinet
ID & Passwords	• I do not share my ID and passwords for critical systems • I only use "strong" passwords • I never write down passwords on paper
USB Keys	• I never connect visitors USB keys to devices on the hotel network • Instead, I direct visitors to the Business Center/ WebCorner

Visitors Log	• I register visitors in the appropriate log at the Front Desk • I register myself in the appropriate log when accessing restricted areas such as Computer Room and Archive Room
EPT (Electronic Payment Terminal)	• I inspect my EPTs daily and keep them stored in a safe location • When working on night shift, I inspect all EPTs daily and record the audit into the Zero Pinpoint Inventory tool
IRP & SIR (Incident Response Plan & Security Incident Response)	• I am aware about my responsibility regarding cardholder data and about the importance of confidentiality • I know how to detect a system security incident and I immediately react on it
Shredder	• I destroy cardholder data using a shredder to make it unrecoverable when it is no longer needed for business or legal reasons
Security Policy	• I am aware about our company security policy and best practices and comply with them at all times
Security Awareness Training	• I validate my annual certification assessment annually
Merchant Tickets/ Receipts	• I store merchant tickets/receipts in a locked cabinet/ drawer