



CASE STUDY

PCI DSS Programs for Small Merchants: Making PCI DSS “Business As Usual” in large, multinational, distributed environments

THE MERCHANT



Accor is the largest hotel operator with a network of 5,000 hotels in 110 countries distributed through a hotel portfolio of 39 hospitality brands from luxury to economy.

Accor also has new businesses in private rental, co-working, concierge services, dining & events and digital solutions, with 300,000 employees whose commitment and passion is helping Accor reinvent hospitality.

For more information visit:
<http://www.group.accor.com>

THE SOLUTION



Vigistrust is an award-winning provider of SaaS Governance Risk Compliance (GRC) solutions with users in over 120 countries. Vigistrust 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 education, compliance validation and compliance management solutions.

For more information visit:
<http://Vigistrust.com>

How Accor and Vigistrust 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?

Accor: Accor comprises more than 39 brands of hotels of all types and sizes in over 110 countries. The group includes owned and managed hotels and franchisees. At the Accor 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?

Accor: Facing the challenges Accor 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. Secure payments throughout the merchant organization is the end game – for hotels this includes reception, restaurants, bars, gyms, spas, shops. It was also important for us to use the PCI DSS compliance program as a foundation for other compliance and risk assessment programs to maximize on successes achieved through the original program.

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

Vigistrust: The real value added for merchants is access to plain-English business-driven security advice so they can easily implement and maintain good security practices. This is done through Vigistrust, an award winning Integrated Risk Management (IRM) SaaS solution. Providing education through eLearning and access to user friendly, procedures helps merchants understand why payment security is important and what's involved. Additionally, easy access to all PCI DSS SAQs, policies & procedures and training is provided on Vigistrust.

Why did Accor choose Vigistrust?

Accor: Working with the right partner is essential to the success of our PCI DSS program.

The relationship with Vigistrust spans nearly a decade. We first met Vigistrust 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. Their PCI Compliance program tailored for the hospitality industry, now available on Vigistrust, has been evolving with ours over the years. We first engaged Vigistrust in 2012 for PCI DSS eLearning for 15,000 users. We further customized this for our hospitality needs over the years, leading up to a full, two-part customized program released in 2013 and incorporated PCI Risk assessment and Vendor Risk Management questionnaires into the platform.

From the outset, we found Vigistrust to be a flexible partner that could adapt to our needs and work with us to develop tailor-made PCI DSS training solution by Accor hotels.

What makes a good future safe and scalable PCI DSS portal?

VigiTrust: A PCI DSS portal must make it straightforward for merchants to prepare for, validate and maintain their compliance levels. From an enterprise perspective, portals are mission critical tools allowing them to report not only on completion, but also on exceptions allowing PCI program managers to help merchants struggling to understand and implement good security required to achieve compliance. Additionally, portals must provide dynamic reports on compliance status across the whole portfolio as well as allow for the production of reports required by acquiring banks and card schemes.

What about continuous compliance and BAU?

Accor: Making PCI DSS compliance Business as usual is a must. From a compliance management perspective, organizations need access to real time PCI compliance status and have the ability to dynamically monitor their small merchant's portfolio compliance levels. Of course, regular static pre-defined reporting also helps but the real value is the ability to have access to compliance snapshots on demand. Accor uses a mix of pre-defined reports including an overall "Meteo/Weather" report as well as the ability to use VigiOne to zoom in on selected merchants as required and on demand.

What Key Performance Indicators (KPIs) have Accor implemented through VigiOne to monitor PCI DSS compliance across its portfolio of merchants?

Accor: Accor really wanted to promote objectives and KPIs related to PCI DSS compliance throughout the organization. This includes monitoring progress against PCI DSS program steps, identify top performers, follow new hotel onboarding, identify non-compliant properties, manage renewal dates.

What collaboration features do organizations need in a good PCI DSS portal to manage large portfolio of merchants?

VigiTrust: Accor really benefits from the fact VigiOne allows for the reproduction of the Accor worldwide organization (per hubs, brands, management type) such that the overall PCI DSS team can collaboratively help small merchants. VigiTrust for its part is also working with Accor on the platform to provide support whilst multiple



QSAs working with Accor in various hubs are connected to VigiOne to do preparation work, assist with compliance work, document site visits to conduct gap analysis, manage evidence collection and remediation work and conduct full QSA Assessments

Can you explain the concept behind One Portal - Multiple Regulations and why it matters to small merchants & PCI DSS compliance?

VigiTrust: Small merchants need to comply with PCI DSS but they also need to comply with local and international data security mandates, for instance GDPR. Accor is building on the PCI program it built and extended its VigiOne implementation to cover GDPR, Risk Assessments and VRM (Vendor Risk Management). On their portal Accor and their QSAs have access to all merchants SAQs (multilingual), SAQ D Service Provider and ROCs. In terms of GDPR, users can do processing mapping, PIAs (Privacy Impact Assessments), Data Subject Access Request and Data Breach Response Plan. Additionally, Accor and VigiTrust released risk assessments & readiness questionnaires and GDPR and VRM readiness questionnaire on the same platform: one platform, multiple regulations.

PCI DSS - SECURITY POLICIES FOR HOTEL FRONT DESK / RECEPTION



Data Retention & Cleansing	<ul style="list-style-type: none"> 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 	Visitors Log	<ul style="list-style-type: none"> 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
CVV (Credit Card Verification code)	<ul style="list-style-type: none"> 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 	EPT (Electronic Payment Terminal)	<ul style="list-style-type: none"> 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
SecurePAYbyLink	<ul style="list-style-type: none"> I use SecurePAYbyLink for all TARS*-non-supported booking requests (*TARS=The Accor Reservation System) I never ask for a copy/scan of a payment card to guarantee a reservation 	IRP & SIR (Incident Response Plan & Security Incident Response)	<ul style="list-style-type: none"> 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
Email & Fax	<ul style="list-style-type: none"> I deal with fax right upon receipt and shred immediately Alternatively, I lock faxes into the Reservations cabinet 	Shredder	<ul style="list-style-type: none"> I destroy cardholder data using a shredder to make it unrecoverable when it is no longer needed for business or legal reasons
ID & Passwords	<ul style="list-style-type: none"> I do not share my ID and passwords for critical systems I only use "strong" passwords I never write down passwords on paper 	Security Policy	<ul style="list-style-type: none"> I am aware about our company security policy and best practices and comply with them at all times
USB Keys	<ul style="list-style-type: none"> I never connect visitors USB keys to devices on the hotel network Instead, I direct visitors to the Business Center/ WebCorner 	Security Awareness Training	<ul style="list-style-type: none"> I validate my annual certification assessment annually
		Merchant Tickets/ Receipts	<ul style="list-style-type: none"> I store merchant tickets/receipts in a locked cabinet/ drawer