Hospitality Structures:
Locating Accountability for PCI DSS Compliance

Hotel organizations are complicated. They can include brands, franchisors, franchisees, management groups, and individual properties – and often a mix of each. As a result, the question is often asked: "Who is responsible for ensuring PCI DSS compliance?".

The Golden Rule: Every Entity is Obligated to Ensure Security

PCI requirements apply to merchants or service providers who handle, process, or store cardholder data. Every hotel meets this definition and is required to assess its environment to meet PCI DSS standards.

Responsibilities include:

- Safely handling of cardholder data on hotel property and systems
- Training every employee for data protection and management
- Ensuring all cardholder data environment (CDE) systems are patched and protected from vulnerabilities and malware.
- Maintaining secure systems (including updates) at front desk systems, systems connected to PMS, POS systems, payment gateways, payment devices, and all other systems on the same network segments

Management Groups should:

- Ensure that properties maintain and adhere to a written Information Security Policy
- Implement security awareness training to ensure data protection
- Be aware of data flow and on what systems transactions are processed
- Be aware of how to respond to cardholder data breaches, exercise this plan, and adjust it based on updated threats.
- Monitor compliance of service providers with which entities share cardholder information

How Structure May Impact PCI Procedure

Organizational structure impacts some aspects of PCI compliance procedure

Be on the lookout for:

- **PCI DSS Levels** – PCI DSS contains four compliance levels that correspond to transaction volume. Typically, each property's volume is calculated independently of the hotel brand, but situations may vary
- **Updates –** brands may handle their proprietary systems (PMS, POS), but owners bear the costs of upgrading to current PCI DSS compliant versions of those systems

Debunking Myths

MYTH **"Brands and franchises handle compliance."**

REALITY All hospitality enterprises must be certified independent of brand requirements. PCI DSS compliance is not guaranteed by the brand or handled by the franchisor. It is the responsibility of each owner to ensure that all properties are compliant. All entities within the card payment environment are required to be compliant.

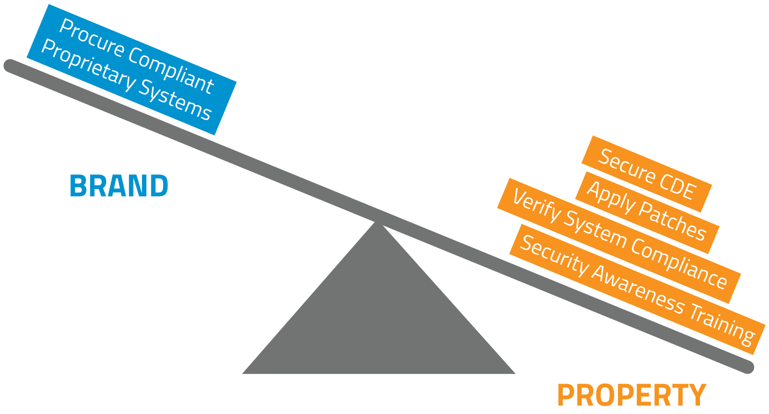
MYTH **"Software providers of PMS or POS systems ensure their products are compliance – so it doesn't need to be verified."**

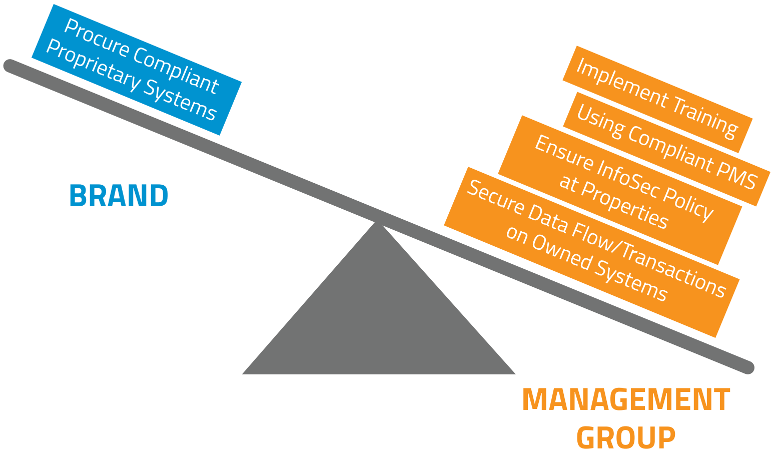
REALITY Compliance is the responsibility of the merchant, not the software vendor. You must ensure software systems meet the Payment Application Data Security Standard. You must know whether a PMS vendor has had a Qualified Payment Assessor validate the software as compliant. PMS and POS systems must be installed and maintained in a compliant manner.

MYTH **"Franchisors and brands have no responsibilities for PCI DSS compliance – it's all at the property-level"**

REALITY Responsibility is shared in perception and reality. First, reputations are interlinked – a breach at any level of an organization or brand will impact all others. Second, tasks undertaken by the brand (such as procurement and provisioning of the PMS) must be also compliant.

The primary responsibility for PCI DSS compliance lies at the property level.


Procure Compliant Proprietary Systems
BRAND
Secure CDE
Apply Patches
Verify System Compliance
Security Awareness Training
PROPERTY


Procure Compliant Proprietary Systems
BRAND
Implement Training
Using Compliant PMS
Ensure InfoSec Policy at Properties
Secure Data Flow/Transactions on Owned Systems
MANAGEMENT GROUP