PCI DSS FOR LARGE ORGANIZATIONS

10 TIPS

1

LOCATE CARDHOLDER DATA

Large organizations should locate all payment card functions and cardholder data processed across different channels or geographical locations.

IDENTIFY ROLES AND RESPONSIBILITIES

Determining roles, responsibility, and ownership within multiple business units is a vital step in the effective management of PCI DSS controls.

2

3

RECORD DATA LOCATION AND RESPONSIBILITY

Documenting all ownership across business units is critical for large organizations to maintain an accurate view of the tasks individuals and teams have been assigned.

RECORD PAYMENT CHANNELS

Large organizations often have multiple payment channels—for example, card-present channels, ecommerce websites, and call centers.

4

5

COLLABORATE

In the case of mergers and acquisitions within a large organization, collaboration is key when it comes to completing assessments and intertwining PCI compliance activities.

INFORM STAKEHOLDERS

Many stakeholders outside IT organizations can have difficulty understanding and retaining the PCI DSS knowledge relevant for their role.

6

7

MAINTAIN COMPLIANCE

Large organizations should treat PCI compliance as a year-round process, which includes consistently performing regular assessments and tests, as well as keeping up to date with PCI DSS releases.

TRAIN RELEVANT STAFF

Organizations with diverse functions and skill levels across its staff may need to create multiple versions of PCI DSS training that are tailored to each skill level and function.

8

9

LIMIT ACCESS

Maintaining effective access control practices and ensuring that only authorized individuals can access sensitive data is crucial for the security of the business.

CONSIDER REGULATION

Larger organizations are likely to be subject to several regulations, such as the General Data Protection Regulation (GDPR), or local privacy laws such as the California Consumer Privacy Act (CCPA).

10