

NICE Compliance Center and PCI DSS

PCI DSS is the Payment Card Industry Data Security Standard, applying to all entities that store, process, and/or transmit cardholder data. Revised to enforce more stringent security requirements, PCI DSS 3.2 came into effect February 1st 2018, but organizations have until June 2018 to be up to date with the TLS protocols to safeguard payment data.



What should I do to comply with PCI DSS 3.2?

PCI DSS prescribes 6 goals with 12 requirements:

1. **Build and Maintain a Secured Network**
 - A. Install and maintain a firewall configuration to protect cardholder data
 - B. Do not use vendor-supplied defaults for system password and other security parameters
2. **Protect Cardholder Data** - Cardholder data should NOT be stored unless it is necessary to meet the needs of the business, in this case Cardholder data should be encrypted. Note that Sensitive Authentication Data (including CVV, data from the magnetic stripe, PINs and PIN blocks), may NOT be stored in a digital format even if encrypted.
 - A. Protect stored cardholder data
 - B. Encrypt transmission of data across open, public network
3. **Maintain a Vulnerability Management Program**
 - A. Use and regularly update anti-virus software or programs
 - B. Develop and maintain secure systems and applications, using strong encryption (e.g. TLS 1.2)
4. **Implement Strong Access Control Measures**
 - A. Restrict access to cardholder data by business need-to-know
 - B. Identify and authenticate access to system components including (e.g. MFA)
 - C. Restrict physical access to cardholder data
5. **Regularly Monitor and Test Networks**
 - A. Track and monitor all access to network resources and cardholder data
 - B. Regularly test security systems and processes
6. **Maintain an Information Security Policy**
 - A. Maintain a policy that addresses information security for employees and contractors



With NICE's Compliance Center, PCI DSS compliance is easy!

The Compliance Center is a unique end-to-end compliance solution that assures interactions are recorded, stored and accessible in adherence with specific regulatory requirements and according to the best practices and policies defined by each organization. The solution offers dedicated mechanisms to power better compliance processes:

- Agents can receive real-time notifications on their recording on demand system, or pause & resume activities, to ensure they don't record sensitive information inadvertently
- The IT team can promptly monitor their system's behavior focusing on sensitive data, encryption, and access
- Compliance officers benefit from mission critical mechanisms for policy definition, management and approval



Smarter PCI Compliance Processes

Thanks to its “Assurance Dashboards” application, the PCI DSS Compliance Center solution offers actionable insights on stored and encrypted cardholder data, enabling detection of any interaction in violation with the standard. The Assurance Dashboard offers an overview of the mechanisms in place to detect any vulnerability by leveraging analytics. With the PCI DSS Compliance Center solution, encryption can also be performed retroactively, on past interactions, in order to ensure that historical data is compliant.

Each dashboard is customizable and only displays KPIs and thresholds relevant for each organization. As such, users are notified according to pre-defined criteria that are in full alignment with their organization’s best practices and the sensitivity of the data gathered by each department. Overall, with these dashboards, users can promptly monitor their system, automatically spot any deviations, rapidly carry out investigations and take corrective actions.

The “Policy Manager”, the second pillar of the Compliance Center, is a mission-critical application enabling users to define policies for extraction in case of audits, as well as other common policies such as playback lock, litigation hold, or deletion. The policies can be applied on a large amount of interactions or on very specific ones to accommodate any use case. With dedicated workflows for approval processes and predefined wizards for policy definition and interactions retrieval, all compliance policies can be managed from a centralized hub.

Using DIY mechanisms to complete all actions in a short timeframe, the PCI DSS Compliance Center offering addresses the needs of contact center stakeholders for solutions that empower them to monitor their activities and act upon the insights they gather rapidly, without being dependent on services or third parties.



Advanced Security & PCI Certification

The PCI DSS Compliance Center offering builds on the advanced security measures available with the market leading Engage recording platform. Certified for PCI DSS 3.2, by Trustwave, Engage offers TLS 1.2 protocols, multi-factor authentication and end-to-end encryption to ensure the data is safely stored. NICE’s commitment to the highest security standards also shows through periodic penetration testing and hardening kits, that constantly seek to provide the most secured solution possible.

The PCI DSS Compliance Center solution is part of a wider offering that includes dedicated compliance mechanisms for evidence keeping, GDPR, HIPAA, and consumer protection regulations. Whether organizations need to verify that the interactions they store are adequately encrypted, recorded and are discoverable, or track the quantity and the quality of the data stored, the Compliance Center offers a single answer to the multi-faceted regulatory challenges in place in the contact center.



[Contact us](#) today to know more or to [schedule](#) a demo.

About NICE

NICE (Nasdaq: NICE) is the worldwide leading provider of both cloud and on-premise enterprise software solutions that empower organizations to make smarter decisions based on advanced analytics of structured and unstructured data. NICE helps organizations of all sizes deliver better customer service, ensure compliance, combat fraud and safeguard citizens.

Over 22,000 organizations in more than 150 countries, including over 80 of the Fortune 100 companies, are using NICE solutions.

