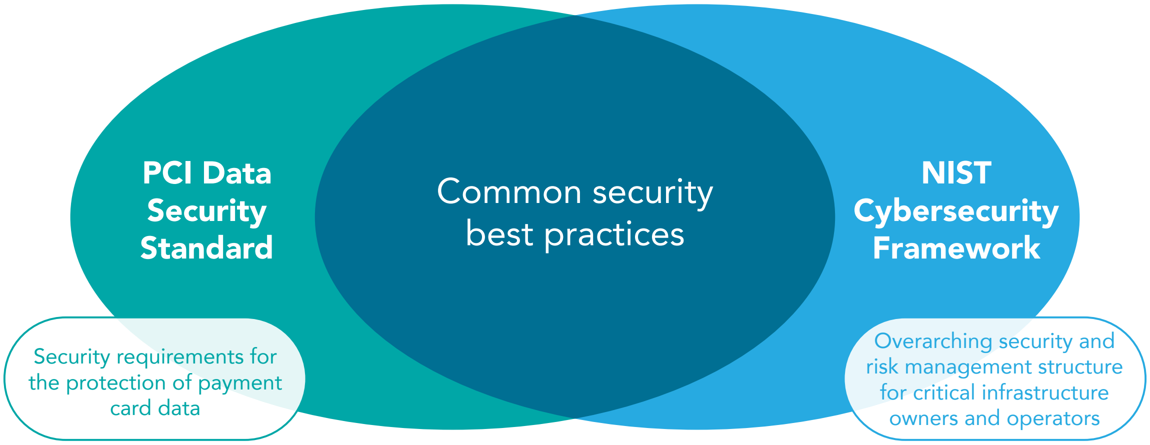
Mapping PCI DSS to the NIST Cybersecurity Framework

How meeting PCI DSS requirements can help toward achieving NIST Framework outcomes for payment environments

The PCI Data Security Standard (PCI DSS) and the NIST Cybersecurity Framework share the common goal of enhancing data security. The Mapping of PCI DSS to the NIST Cybersecurity Framework provides a resource for stakeholders to use in understanding how to align security efforts to meet objectives in both PCI DSS and the NIST Framework.



PCI Data Security Standard

Security requirements for the protection of payment card data

Common security best practices

NIST Cybersecurity Framework

Overarching security and risk management structure for critical infrastructure owners and operators

PCI DSS provides specific security requirements for payment card data

PCI DSS defines security requirements for the protection of payment card data, as well as validation procedures and guidance to help organizations understand the intent of the requirements. Rapid changes in threats require more detailed standards for payment security. PCI DSS is focused on the unique threats and risks present in the payments industry. It is intended for all entities involved in storing, processing, or transmitting payment card data, and provides foundational security requirements across twelve main security objectives to protect payment environments.

NIST Cybersecurity Framework provides broad security and risk management objectives

The NIST Framework provides an overarching security and risk-management structure for voluntary use by U.S. critical infrastructure owners and operators. The NIST Framework Core component consists security Functions, Categories of security activity, and Subcategories of actions. These Subcategories reference globally recognized standards for cybersecurity. As the NIST Framework is broadly focused on organizational risk management, achieving NIST Framework outcomes does not provide assurance that payment data is also protected.

Both PCI DSS and the NIST Framework are solid security approaches that address common security goals and principles as relevant to specific risks

While the NIST Framework identifies general security outcomes and activities, PCI DSS provides specific direction and guidance on how to meet security outcomes for payment environments. Because they are intended for different audiences and uses, they are not interchangeable, and neither one is a replacement for the other.

Mapping PCI DSS to the NIST Framework

The mapping covers all NIST Framework Functions and Categories, with PCI DSS requirements directly mapping to 96 of the 108 Subcategories. The mapping illustrates how meeting PCI DSS requirements can help toward achieving NIST Framework outcomes for payment environments.

How to use the Mapping

Stakeholders can use this mapping to identify opportunities for control efficiencies and greater alignment between organizational security objectives. For example, the mapping can help identify where the implementation of a particular security control can support both a PCI DSS requirement and a NIST Framework outcome. Additionally, an entity's internal evaluations to determine the effectiveness of implemented controls may help the entity prepare for either a PCI DSS or NIST Framework assessment, or both.

The mapping is not a tool for demonstrating compliance to either PCI DSS or the NIST Framework, nor does meeting either a PCI DSS requirement or its corresponding NIST Framework outcome result in the other being met.

Download the Mapping of PCI DSS to the NIST Cybersecurity Framework

pcisecuritystandards.org

Learn more about PCI DSS

https://www.pcisecuritystandards.org/pci_security

Learn more about NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

PCI DSS brings engagement of entire payment community

PCI SSC works with merchants, service providers, financial institutions, and others in the payments industry, as well as our assessor and forensic investigator communities. This keeps all stakeholders aware of current risks to payment data and ensures that PCI Standards continue to address those risks.