International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 13, Issue 2, Jul–Dec 2024; 893–922
© IASET

International Academy of Science, Engineering and Technology
IASET
Connecting Researchers; Nurturing Innovations

ISO 27001 AND PCI DSS: ALIGNING COMPLIANCE FOR ENHANCED SECURITY

***Venkata Reddy Thummala*[1] *& Prof.(Dr.) Vishwadeepak Singh Baghela*[2]**

[1]*Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India*

[2]*School of Computer Science and engineering at Galgotia's University, Greater Noida, India*

ABSTRACT

In today's digital landscape, organizations face increasing pressure to safeguard sensitive data and maintain regulatory compliance. ISO 27001 and PCI DSS represent two prominent frameworks aimed at bolstering information security and protecting payment card data, respectively. While ISO 27001 provides a comprehensive framework for establishing, implementing, and continuously improving an Information Security Management System (ISMS), PCI DSS focuses specifically on securing cardholder data in payment processing environments. Aligning these standards can significantly enhance an organization's overall security posture and streamline compliance efforts. This paper explores the synergies between ISO 27001 and PCI DSS, highlighting their overlapping principles, such as risk management, access control, and incident response. By integrating these frameworks, organizations can reduce duplication of efforts, optimize resource allocation, and address broader security objectives while meeting specific regulatory requirements. The discussion delves into practical strategies for alignment, including leveraging the ISO 27001 risk assessment methodology to address PCI DSS requirements and utilizing shared controls for efficient compliance management. The challenges of dual compliance, such as resource constraints and varying audit processes, are also examined. Ultimately, aligning ISO 27001 and PCI DSS not only supports regulatory compliance but also fosters a culture of security awareness and resilience. By adopting a unified approach, organizations can ensure robust protection of sensitive data, build stakeholder trust, and adapt to evolving security threats in a dynamic regulatory environment. This paper underscores the importance of strategic alignment for achieving enhanced security and long-term operational excellence.

KEYWORDS: *ISO 27001, PCI DSS, Information Security, Compliance Alignment, Risk Management, Data Protection, Cardholder Security, Regulatory Requirements, Security Framework, Organizational Resilience*

Article History

***Received:* 04 Nov 2024 | *Revised:* 18 Nov 2024 | *Accepted:* 29 Nov 2024**