

MOBIUS APPROACH TO PCI-DSS COMPLIANCE

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard aimed at the protection of credit and debit card data. The data stored on credit and debit cards, commonly referred to as cardholder data, can be used to perform fraudulent card transactions in the event it is disclosed to cybercriminals. The standard was developed by the Payment Card Industry Security Standards Council in order to reduce the risks of disclosure by improving information security controls for the protection of cardholder data during handling, storage, processing and transmittal. The standard has been made mandatory by the major card brands (Visa, MasterCard, American Express, Discover, and JCB) for all organisations that handle cardholder data.

The advantages of compliance to PCI-DSS include:

- Increase in consumer confidence by improving security of personal cardholder data
- Competitive advantage through improved image and reputation with partner organisations
- Reduction in risks of cardholder data breaches that lead to fraud
- Reduction in risks of penalties due to non-compliance
- Reduction in risks of financial costs of compensation, recovery, investigations and brand damage

Ultimately PCI-DSS is not just about compliance to a standard, it is about increasing awareness of the importance of protecting cardholder data, the general improvement of information security controls, and adoption of the standard into existing information security programmes.

Some of the activities required to initially achieve compliance include:

- Understanding of PCI-DSS and the detailed requirements of the standard
- Understanding the costs of becoming compliant
- Developing an implementation plan based on priorities and quick wins
- Creating or aligning policies, standards and processes to the standard
- Understanding the investment and implement of new security technologies
- Implementing an awareness campaign and development of awareness content
- Developing process for ongoing compliance to the standard.

The Mobius Consulting approach to PCI-DSS Compliance is focused on helping clients understand how to become compliant, preparing for compliance, understanding changes required, understanding the costs involved and implementing sustainable solutions for ongoing compliance. Our approach follows phases of Plan, Build and Run with outputs of each phase forming the building blocks to achieving and maintaining PCI-DSS compliance.



The Mobius Consulting services and approach to PCI-DSS compliance are ideally suited to organisations embarking on the PCI-DSS journey. Our approach includes deliverables at each phase designed to ensure the success of subsequent phases. We provided compliance initiative sponsors with a roadmap designed specifically to suite the organisation. We develop compliance plans that take into consideration the costs, effort, impact and changes required for compliance to the standard.