



# randtronics

**We understand how technology and compliance fit together.**

## **PCI DSS Remediation Services**

### **Introduction**

Randtronics offers a range of professional services designed to help organisations overcome the challenges to achieving PCI DSS compliance:

- We can assist your organisation with the selection, design and deployment of encryption solutions to meet the requirements to protect cardholder data at rest and in motion.
- We can help your organisation get its PCI DSS compliance program on track, through identification of scope, compliance gap analysis, and remediation consulting.

### **PCI DSS Compliance and Encryption**

PCI DSS Requirement 3 states that cardholder data needs to be rendered unreadable anywhere it is stored, and Requirement 4 states that cardholder data needs to be encrypted wherever it is transmitted over open, public networks. Protection methods such as encryption, hashing, truncation, and masking are critical components of cardholder data protection.

For many organisations becoming compliant with these requirements is an enormous task. The related sections of the standard contain many concepts which are unfamiliar to most people. Implementing an encryption solution requires an understanding of key management considerations (key storage, key distribution, key rotation), implementation aspects, performance impacts and recovery capabilities.

Many organisations make the wrong choices when selecting technologies to meet regulatory compliance. In today's competitive market, it can be quite difficult to identify which solutions exist that meet your needs and which one is right for your organisation. Randtronics offers a vendor-independent view of what technologies will suit your environment. We equip you with the right knowledge and skills to ensure that you become compliant with ease and efficiency.

Our consultants can assist your organisation with the selection, design and deployment of solutions for the protection of cardholder data at rest and in motion. We have experience with a wide range of encryption technologies including database encryption, file encryption, network encryption, encryption of mobile devices, email encryption. We can design solutions for all popular computing platforms and databases.

We can also assist you with the implementation of tokenisation solutions, which can be useful for reducing the scope of PCI DSS in your environment or which may provide a compensating control in cases where encryption may not be feasible on certain legacy platforms. Furthermore, we provide solutions for the masking of payment card data displayed to employees or other parties.

Encrypting data can seem like a problematic task and some companies will go to great lengths to avoid doing so. However with the right choices and knowledge, complying with these requirements can be simple and cost-effective.

*securing your business*

## PCI DSS Compliance Program

Randtronics security consultants have expertise and experience across all twelve requirements of the PCI DSS. With our consulting services we can help your organisation get its compliance program on track. The PCI DSS Remediation services that Randtronics can provide to your organisation include:

- Data flow analysis and scope identification: Randtronics consultants will help to identify the systems within your environment that store, process or transmit cardholder data. We survey and consult the key people within your organisation to determine where (and why) cardholder data is being stored and develop an overall view of your in-scope environment.
- Compliance gap analysis and remediation advice: We will perform a compliance assessment of your in-scope environment. The assessment report examines key areas with compliance gaps and related remediation strategies. We provide estimations for costs, resources and effort involved in becoming compliant.
- Preparation of the Self Assessment Questionnaire (SAQ).
- Act as the point of contact for your organisation to liaise with your QSA.

Additionally, we provide a number of security services that can assist your organisation in meeting PCI DSS requirements, including:

- Penetration testing, web application security assessments, and application source code reviews (Requirements 6 and 11). Please refer to our Penetration Testing Services Brochure for more details.
- System hardening (Requirement 2): Our consultants will assess the security of system components in the cardholder data environment against industry accepted hardening standards such as those developed by the National Institute for Standards and Technology (NIST) and the Centre for Internet Security (CIS). We can perform system hardening and develop system configuration standards.
- Security policy development (Requirement 12): Our consultants will assist you with the development of a security policy framework that is tailored to your organisation and meets all PCI DSS requirements.

---

## Contact Us

For more information about Randtronics PCI DSS Compliance Services feel free to Contact Us.

**Phone:** (612) 8873 1999

**Fax:** (612) 9870 8560

**E-mail contact:** [sales.team@randtronics.com](mailto:sales.team@randtronics.com)

**Website :** [www.randtronics.com](http://www.randtronics.com)



*securing your business*