The following recommendations are compiled from the experience of Fortrex and Thales eSecurity to help you avoid common compliance pitfalls. Reaching and maintaining PCI DSS compliance can be a big undertaking for any organization, whatever its size. However, knowing and preparing for these challenges in advance will save you time and money.

**IMPROVE YOUR STRATEGIC PLANNING**

1. **RELY ON AUTHORITATIVE SOURCES BEFORE MAKING DECISIONS TO ENSURE SOUND REASONING**
   Using anecdotal evidence and skewed polling as the basis for your decision-making is a recipe for disaster. A better approach to support your strategic planning includes careful review of Security Standards Council (SSC) guidance and knowledgebase articles as well as consultation with a Qualified Security Assessor (QSA).

2. **SEGMENT YOUR ENVIRONMENT TO HELP REDUCE SCOPE**
   Given the depth of the PCI DSS cybersecurity control requirements, compliance is more easily achieved when leveraging network segmentation to effectively isolate your cardholder data environment (CDE). The presence of cardholder data in multiple diverse locations within your organization makes your compliance task much more difficult. Therefore, focus on reducing CDE scale and complexity, keeping in mind that technology solutions including point-to-point encryption (P2PE) and tokenization are well proven and trusted methods of removing clear-text cardholder data from merchant systems and reducing scope.

3. **DESIGN A COHESIVE SECURITY ARCHITECTURE TO ADDRESS EVOLVING THREATS**
   One of the prevalent themes within the PCI DSS is attention to risk management processes. Security architecture planning efforts should consider all applicable requirements as well as changes to its threat environment including those which impact third-party risk and operational resourcing constraints. It is all too easy to end up with a fragmented approach to security based on multiple proprietary vendor solutions and inadequate technologies that are expensive and complex to operate. Instead, seek comprehensive, easy-to-integrate solutions from fewer vendors that cover all your needs and can be extended when needed.

4. **WRITE DETAILED DOCUMENTATION TO SUPPORT COMPLIANCE**
   Policy and procedure establishes those requirements which guide your day-to-day operations. Lack of explicit documentation to support the adoption of PCI DSS requirements hinders your ability to define CDE cybersecurity principles and associated operational requirements. Be sure to include sufficient detail to ensure that there is common understanding and consistently effective prioritization.

**IMPLEMENT EFFECTIVE DATA PROTECTION**

5. **CENTRALIZE KEY MANAGEMENT TO REDUCE COMPLEXITY**
   Trying to manage a diverse range of systems all with their own independent key management processes will make your compliance task extremely difficult. Therefore, focus on how you can achieve your key management goals from a centralized tool, which will result in a more streamlined approach and give you more flexibility, especially when new databases or locations need to be secured.
Utilizing hardware security modules (HSMs) or FIPS 140-2 certified enterprise key management solutions will support delivering clear separation of duties between key custodians and storage administrators in addition to assuring cryptographic key security and availability.

6. ACHIEVE DATA AVAILABILITY WHILE RETAINING CONFIDENTIALITY TO MAXIMIZE PRODUCTIVITY

PCI DSS requires that all retained cardholder data be rendered unreadable, but supporting processes which also periodically cause the data to be unavailable can easily prove disruptive. For example, selected cryptographic key solutions which require your system to be offline while the key rotation and data transformation processes are being performed, can leave you without access to your data for hours or days at a time. However, technology is now available that provides ongoing access to your data as the transformation from encryption under the old key to encryption under the new key is being applied. You get the best of both worlds – full compliance and 24x7 access to your data.

7. LIMIT DATA RETENTION TO SIMPLIFY EFFORT

Unnecessary data retention may result in legal and compliance risk, violate applicable contractual or regulatory requirements, increase the effort needed to manage archived cryptographic keys, and, ultimately, contribute to the realized impact of a data breach. It is much more efficient to delete data on a scheduled basis and in accordance with PCI DSS, local, and industry regulations.

ENSURE ONLY AUTHORIZED DATA ACCESS

8. RESTRICT ACCESS TO WHAT IS NECESSARY TO PERFORM JOB RESPONSIBILITIES

Data access control methods often lack the ability to prevent administrators and privileged users from viewing cardholder data, especially when relying solely on basic operating system or database controls. Further, centralized audit logging of all administrative actions with sufficient granularity is a fundamental PCI DSS requirement. By deploying data security software agents to supplement native operating system access controls, you can prevent unauthorized data access and generate actionable intelligence while still allowing normal administrative duties to be carried out.

9. CONTROL PRIVILEGED CREDENTIALS TO PREVENT ABUSE

The PCI DSS, as well as cybersecurity industry best practices, do not permit the use of generic or shared accounts, including for administrative use such as interactive logon and non-console access. Without careful planning, your application or service account’s default credentials and shared knowledge of their passwords will lead to non-compliance. To address this, deploy a privileged account management solution that provides you with the greater security and flexibility needed, while eliminating insecure practices such as the programming of clear-text security credentials in source code.

10. IMPLEMENT STRONG ACCESS CONTROLS TO MITIGATE BOTH INSIDE AND OUTSIDE THREATS

Your principle threat of cybersecurity attack is not necessarily going to originate from outside connections. Failure to restrict outbound and intra-LAN communication controls makes the job of an attacker easier and the probability of a pivot attack much more likely. The implementation of strong access controls to complement your encryption strategy enables you to manage exactly who can access your systems and data, ensuring only necessary communications and access are permitted.

This is only one example of the practical advice available to help simplify your PCI DSS compliance. For more detailed information please request a copy of our latest book, PCI Compliance & Data Protection for Dummies.