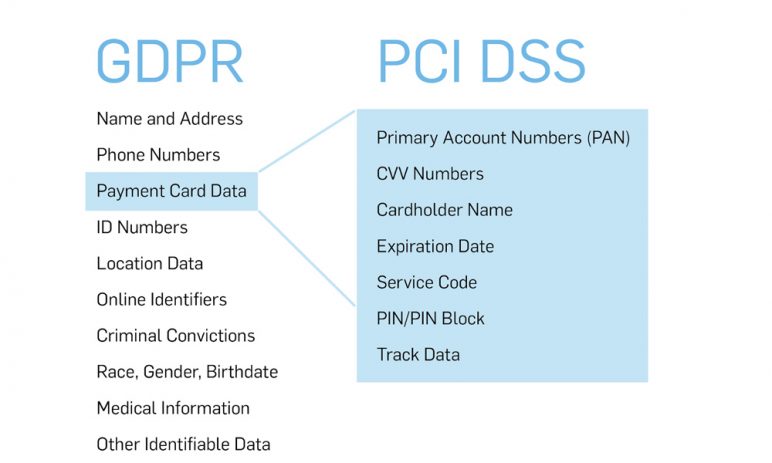
**PCI DSS LÀ GÌ?**

PCI DSS viết tắt cho Payment Card Industry Data Security Standard là một tiêu chuẩn an ninh thông tin bắt buộc dành cho các doanh nghiệp lưu trữ, truyền tải và xử lý thẻ thanh toán quản lý bởi 05 tổ chức thanh toán quốc tế như Visa, MasterCard, American Express, Discover và JCB. PCI DSS là một tiêu chuẩn được các tổ chức thanh toán quốc tế nêu trên ủy quyền quản lý cho Hội đồng Bảo mật dữ liệu thẻ thanh toán PCI SSC (Payment Card Industry Security Standard Council).

Tiêu chuẩn này được phát triển nhằm mục đích gia tăng kiểm soát đối với dữ liệu chủ thẻ và hạn chế sự gian lận, trộm cắp dữ liệu thẻ thanh toán. Chứng chỉ sẽ có hiệu lực trong một năm, và các doanh nghiệp phải thực hiện tái đánh giá định kỳ. Các doanh nghiệp xử lý số lượng giao dịch lớn sẽ lựa chọn hình thức thuê chuyên gia đánh giá (Qualified Security Assessor – QSA) bên ngoài thực hiện thẩm định và xuất bản báo cáo tuân thủ (Report on Compliance – RoC) trong khi các doanh nghiệp xử lý số lượng giao dịch nhỏ hơn sẽ phải hoàn tất bảng câu hỏi tự đánh giá (Self-Assessment Questionaire – SAQ).

## MỤC TIÊU GIÁM SÁT CỦA PCI DSS LÀ GÌ?

PCI DSS bao gồm 06 mục tiêu giám sát lớn như sau:



## ****Các mục tiêu giám sát PCI DSS****

## ****12 YÊU CẦU CỦA CHUẨN BẢO MẬT AN NINH DỮ LIỆU THẺ THANH TOÁN (Payment Card Industry Data Security Standard – PCI DSS)****

Hội đồng Tiêu chuẩn bảo mật an ninh dữ liệu thẻ thanh toán (Payment Card Industry Data Security Council – PCI DSC) được thành lập bởi năm tổ chức cung cấp thẻ thanh toán quốc tế phổ biến như: Visa Inc, MasterCard Worldwide, American Express, Discover Financial Services, JCB International, nhằm mục tiêu bảo vệ an ninh dữ liệu thẻ thanh toán trên toàn Thế giới.

Từ đó, tiêu chuẩn bảo mật an ninh dữ liệu thẻ thanh toán PCI DSS được phát triển nhằm hỗ trợ các tổ chức thanh toán thẻ bảo vệ dữ liệu của khách hàng, chống lại việc xâm nhập và sử dụng dữ liệu khi chưa được phép. PCI DSS sẽ giúp cho các Doanh nghiệp hạn chế các lỗ hổng bảo mật và rủi ro bị đánh cắp thông tin; đồng thời tăng cường bảo vệ dữ liệu lưu trên thẻ.

Tiêu chuẩn này được áp dụng cho tất cả các tổ chức có lưu trữ, xử lý hoặc truyền tải dữ liệu lưu trữ trên thẻ và các tổ chức này bắt buộc phải bảo vệ dữ liệu lưu trên thẻ khi họ thực hiện giao dịch. Các thông tin dữ liệu thẻ thanh toán bao gồm: Số tài khoản (PAN), tên chủ tài khoản, ngày hết hạn và mã xác thực.

Một loại dữ liệu khác, thường được gọi là dữ liệu xác thực nhạy cảm (SAD), cũng buộc phải tuân thủ tiêu chuẩn PCI DSS, nhưng thông thường việc lưu trữ thông tin SAD bị cấm. Tuân thủ PCI DSS là điều bắt buộc, không phụ thuộc vào tổ chức của công ty hoặc số lượng thẻ giao dịch xử lý mỗi năm. Các công ty outsource các tổ chức bên ngoài xử lý thẻ thanh toán cũng phải tuân thủ PCI DSS.

### **Tiêu chuẩn này bao gồm 12 yêu cầu về bảo mật thông tin như sau:**

1. Xây dựng và duy trì hệ thống tường lửa nhằm bảo vệ dữ liệu thẻ thanh toán.
2. Không dùng các tham số hoặc mật khẩu được thiết lập sẵn từ các nhà cung cấp hệ thống (thiết bị mạng, đường truyền Internet…)
3. Bảo vệ dữ liệu thẻ thanh toán khi lưu trữ trên hệ thống
4. Mã hóa thông tin thẻ trên đường truyền trong quá trình giao dịch
5. Sử dụng và cập nhật thường xuyên phần mềm phòng chống virus
6. Xây dựng – duy trì hệ thống và các ứng dụng đảm bảo an ninh mạng
7. Hạn chế việc tiếp cận với dữ liệu thẻ thanh toán
8. Cấp phát và theo dõi các tài khoản truy nhập hệ thống
9. Giới hạn các phương pháp tiếp cận vật lý với dữ liệu thẻ
10. Kiểm tra và lưu trữ tất cả các truy nhập vào hệ thống và dữ liệu thẻ
11. Thường xuyên đánh giá và thử nghiệm lại quy trình an ninh hệ thống
12. Xây dựng chính sách bảo vệ thông tin tại doanh nghiệp.

### **12 yêu cầu này có thể được tóm tắt thành 06 lĩnh vực chính như sau:**

1. Xây dựng và duy trì một hệ thống mạng lưới an ninh
2. Bảo vệ dữ liệu thẻ thanh toán
3. Duy trì chương trình quản lý lỗ hổng an ninh
4. Thực hiện các biện pháp giám sát truy cập chắc chắn
5. Thường xuyên theo dõi và kiểm tra hệ thống mạng
6. Duy trì chính sách an ninh thông tin