

# Recommendation Report: Compliance Tool for PCI DSS

To: Mark Taylor, GRC Team Lead

From: Michael Jordan, GRC Intern

Date: June 18, 2025

Subject: Recommendation Report – Compliance Tool Selection for PCI DSS

## Introduction

As SecureTech continues to expand its client base in the financial industry, maintaining strict compliance with **Payment Card Industry Data Security Standards (PCI DSS)** has become a top priority. Our organization must ensure the protection of cardholder data, implement secure payment processes, and continuously monitor system access and network activity. To support these objectives, I conducted a comparative analysis of two highly regarded compliance tools: **Netwrix Auditor** and **RSA Archer**. This report outlines their key features, benefits, and challenges, followed by my recommendation for the most appropriate solution to meet SecureTech's current and future compliance needs.

## Tool 1: Netwrix Auditor

**Netwrix** is a compliance and audit management solution designed to keep your auditors satisfied. Netwrix claims to reduce audit preparation time by as much as 85% by eliminating the need to sort through spreadsheets, compile reports, and gather logs for both internal and external audits. Beyond compliance, Netwrix offers a comprehensive security solution that helps mitigate the risk of data breaches and safeguards your sensitive information.

### Key Features:

- Change auditing
- Real-time alerts
- Access rights reporting
- Automated compliance reporting

### Benefits:

- Rapid deployment and ease of use
- Real-time access and change monitoring
- Prebuilt PCI DSS compliance reports and audit trails
- Cost-effective and scalable for SecureTech's current size

**Challenges:**

- Limited enterprise-wide risk dashboarding (compared to RSA Archer)
- Requires SQL Server infrastructure for optimal performance

**Tool 2: RSA Archer**

RSA is widely recognized for its comprehensive approach to risk management. It offers a centralized platform that enables organizations to identify, assess, and mitigate risks across various areas, including IT, finance, and operations.

**Key Features:**

- Risk assessments
- Policy management
- Automated compliance workflows

**Benefits:**

- Comprehensive GRC management suite
- Strong policy lifecycle and risk assessment workflows
- Integrates well with other enterprise systems

**Challenges:**

- High cost and resource-intensive implementation
- Complex setup requiring advanced configuration and dedicated staff
- Less effective for real-time system and access monitoring

**Recommendation**

After reviewing the capabilities and limitations of both platforms, I recommend that **SecureTech** adopt **Netwrix Auditor** as its primary compliance tool for PCI DSS. It offers:

- **Purpose-built support for PCI DSS controls**, including access restrictions, change tracking, and audit logs.
- **Fast deployment** with minimal training requirements for the compliance team.
- **Cost-effective licensing** that fits within our current technology budget.
- **Real-time alerting and preconfigured PCI DSS reports**, reducing the time and effort needed for audit readiness.

Netwrix Auditor not only addresses SecureTech's current compliance priorities but also offers a scalable foundation as we expand our infrastructure and client base.

## **Conclusion**

Compliance with PCI DSS is a mission-critical requirement as SecureTech continues to serve clients in the financial sector. While RSA Archer offers a broad, enterprise-grade compliance suite, it exceeds our current operational needs and budget. In contrast, **Netwrix Auditor** aligns directly with our goals of safeguarding cardholder data, detecting unauthorized activity, and simplifying audit preparation. I recommend we move forward with Netwrix Auditor and initiate a phased implementation beginning this quarter.