

# PCI DSS Compliance Maturity Model



## Continuous Compliance

Organizations are able to continually improve operational procedures through automation and technology improvements. Organization is continuously compliant and compliance is maintained as part of the overall security strategy. Achieving the report on compliance is accomplished effectively and efficiently.



### Level 4

#### Quantitatively Managed

Understanding of critical controls, their frequencies and impact on other controls using statistical analysis. Organization is in a proactive compliance posture. Organization is monitoring security controls and gaps are detected and responded to in a timely manner. Organization has time to optimize their compliance frameworks to achieve Continuous Compliance.



### Level 3

#### Defined

Operational procedures are documented, in-use, and known to all affected parties. Organization is becoming proactive and better positioned to respond to changes in the PCI DSS or the security landscape overall. Organization has moved from a project based compliance posture to a more formal sustainability program.



### Level 2

#### Repeatable

Processes, policies, and standards are documented, planned, performed, monitored, and controlled. Organization is often reactive leading to long tail remediation efforts and delays in achieving a report on compliance. Organization is unable to sustain compliance.



### Level 1

#### Initial

Processes are newly defined, untested, unmonitored. Compliance posture is reactive, time consuming, and costly. Organizations may receive a report on compliance using costly compensating controls and unsustainable processes.