

# PAYMENT CARD INDUSTRY SOFTWARE SECURITY FRAMEWORK

## PCI SECURE SOFTWARE LIFECYCLE STANDARD

### CORE REQUIREMENTS & OBJECTIVES

Defines the requirements over traditional software development lifecycle by introducing security concepts and activities throughout the design, development, deployment, and maintenance phases of a software lifecycle to be taken care of by the **Vendor**.

#### Secure Objective 1 :

##### Software Security Governance

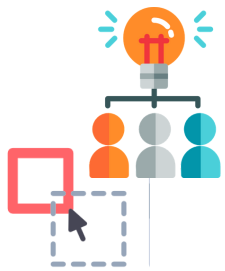
#### Security Responsibility and Resources

- Establish formal responsibility and authority for the security of the vendor's products and services.
- Allocates resources to execute the strategy and ensure skillful personnel employment.



#### Software Security Policy and Strategy

- Define, maintain, and communicate software security policy.
- Strategies for ensuring the secure design, development, and management of its products and services.
- Monitor and track performance against the software security strategy.

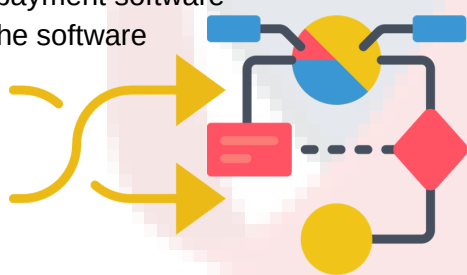


#### Secure Objective 3 :

##### Secure Software and Data Management

#### Change Management

- Identify and manage payment software changes throughout the software lifecycle.



#### Software Integrity Protection

- Protect the integrity of the payment software throughout the software lifecycle.



#### Sensitive Data Protection

- Confidentiality of customers' sensitive production data on vendor systems is maintained.



#### Secure Objective 2 :

##### Secure Software Engineering

#### Threat Identification and Mitigation

- Continuously identify, assess, and manage risk to payment software and services



#### Vulnerability Detection and Mitigation

- Detect and mitigate vulnerabilities in the software and its components.
- This ensures payment software remains resistant to attacks throughout its entire lifetime.



#### Secure Objective 4:

##### Security Communications

#### Vendor Security Guidance

- Provide stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of its payment software applications.



#### Stakeholder Communications

- Maintain communication channels with stakeholders regarding potential security issues and mitigation options.



#### Software Update Information

- Provide stakeholders with detailed explanations of all software changes.

