Significant Change Requirements and Definition

PCI version 3.0 requires that external and internal penetration testing is conducted on an environment when a **significant change** has been implemented into the environment. PCI provides guidance for evaluating what constitutes a significant change but leaves the ultimate evaluation to the organization. This document provides guidelines for the evaluation; however, since each environment is different each change should be evaluated in context. Since the implementation of a significant change could potentially require the engagement of significant outside resources to perform the penetration testing, it is advisable, when possible, to group significant changes together so as not to incur additional unnecessary expenses. If a significant change is planned it should be logged in the RFC system and identified as such. Each merchant group bears responsibility for adequately planning and coordinating the activities necessary to maintain PCI compliance; however, if the PCI coordination team is engaged at the start of this planning process they can assist you with aligning the resources to perform the necessary post implementation activities.

From PCI Guidance: The determination of what constitutes a significant upgrade or modification is **highly dependent on the configuration of a given environment**. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant.

#	Requirement Description
11.03.01	Perform **external** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
11.03.02	Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Guidelines for Determining a Significant Change

Category	Type	Category	Comments
Servers			
	Add server	Major	
	Remove server	Standard	

Category	Type	Category	Comments
Network Devices			
	Add network device	Major	
	Remove network device	Required Judgment	Most device removals should occur in conjunction with adding a device.
Workstations			
	Add workstation	Major	
	Remove workstation	Standard	
Interfaces			
	Add interface/service/protocol	Major	
	Remove interface/service/protocol	Standard	
Software			
	Major upgrades	Major	
	Planned vendor released minor upgrade or patch	Standard	
	Emergency security patches	Requires Judgment	
	Configuration change	Requires Judgment	
	New Software	Major	
Hardware			
	Network cards	Standard	
	Hard drives	Major	
	Processors	Standard	
	Peripherals	Standard	
User accounts			
	Add/Remove User Account	Standard	
	Add/Remove Process account	Standard	
	Add/Remove Administrative account	Standard	
Firewall rules			
	Add firewall rule	Requires Judgment	Should be in conjunction with a new/changed server, workstation, interface, or software component

Category	**Type**	**Category**	**Comments**
	Remove firewall rule	Requires Judgment	Should be in conjunction with a new/changed server, workstation, interface, or software component