COMPENSATING CONTROLS

What's a compensating control?

Per the PCI DSS v4.0:

Compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as stated, due to legitimate and documented technical or business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls. Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.

2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. To understand the intent of a requirement, see the Customized Approach Objective for most PCI DSS requirements. If a requirement is not eligible for the Customized Approach and therefore does not have a Customized Approach Objective, refer to the Purpose in the Guidance column for that requirement.

3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

4. When evaluating "above and beyond" for compensating controls, consider the following:

Note: All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS assessment. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a given compensating control will not be effective in all environments.

COMPENSATING CONTROLS

- Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting cleartext administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of cleartext passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

- Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area but are not required for the item under review.

- Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to address a vulnerability that is exploitable through a network interface because a security update is not yet available from a vendor, a compensating control could consist of controls that include all of the following: 1) internal network segmentation, 2) limiting network access to the vulnerable interface to only required devices (IP address or MAC address filtering), and 3) IDS/IPS monitoring of all traffic destined to the vulnerable interface.

COMPENSATING CONTROLS

5. Address the additional risk imposed by not adhering to the PCI DSS requirement.

6. Address the requirement currently and in the future. A compensating control cannot address a requirement that was missed in the past (for example, where performance of a task was required two quarters ago, but that task was not performed).

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to confirm that each compensating control adequately addresses the risk that the original PCI DSS requirement was designed to address, per items 1-6 above.

To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete. Additionally, compensating control results must be documented in the applicable report for the assessment (for example, a Report on Compliance or a Self-Assessment Questionnaire) in the corresponding PCI DSS requirement section, and included when the applicable report is submitted to the requesting organization.

Reference: PCI DSS v4.0 (March 2022), Appendix B

COMPENSATING CONTROLS

Time, effort, and money go into the creation, implementation, and longevity of compensating controls.

Compensating Controls must have

- Periodic risk assessments
- Periodic process reviews

Compensating Controls are NOT:

- Cost effective
- Sustainable
- The same as using the customized approach to meet a requirement

Compensating Controls will NOT:

- Save time
- Save money
- Save effort

Use the worksheet on the next page for each and every compensating control you have in your Cardholder Data Environment.

Compensating Control(s) Worksheet

COMPLETE THIS WORKSHEET FOR EACH REQUIREMENT THAT'S MET WITH A COMPENSATING CONTROL

PCI Compliance & Sustainability
Payment Card Assessments, LLC

PCI DSS REQUIREMENT NUMBER AND DEFINITION:

	Information Required	Explanation
Constraints	List of constraints precluding compliance with the original requirement.	
Objective	Define the objective of the original control; identify the objectvie met by the compensating control.	
Identified Risk	Identify any additional risk posed by the lack of orginal control	
Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the origianl control and increased risk, if any.	
Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
Maintenance of Compensating Controls	Define processes and controls in place to maintain compensating controls.	