**What are Compensating Controls**

Compliance to PCI Data Security Standards can be a challenge for any organization. However, it becomes more challenging when an organization is unable to meet any of the written requirements of the standard. The PCI Security Standards Council, however, has provided a way to deal with this; the documentation of the compensating controls. A compensating control helps organization minimize the risk by identifying how the requirements affect its framework.

**What is a compensating control?**

After an organization has adopted all important measures to achieve PCI DSS compliance, there may be some areas that it has failed to address because of some technical or business constraints. The organization then needs to develop, document and maintain compensating controls for these unaddressed areas as per the requirements of PCI DSS.

Let us suppose a scenario in which a system can only be accessed with a shared login and the password complexity requirements do not apply to that system. Here, there is increased risk of misuse of information or a possible interception. In order to cater to this risk, we need to document and identify controls to meet the criteria of the PCI DSS Assessment Procedures.

Some of the compensating controls associated with reduction in risk according to the requirements could include the following:

* Change the passwords frequently
* Apply a maximum limit to the shared account usage and keep monitoring the system for any possible use beyond the limit
* Restrict shared account to generic and non-administrative tasks
* Disable the shared account so that it cannot log in to the system

Any area that is not addressed during early compliance should be accurately identified and presented to the Qualified Security Assessor for review purposes. The assessor then decides whether these controls actually are adequate enough to address the risks or not.

**Criteria for Compensating Controls**

According to the PCI SSC, the compensating controls must meet the following criteria. The four functions every compensating control must undergo are:

* meet the intent and rigor of the original PCI DSS requirement
* provide a similar level of defense as the original PCI DSS requirement
* be “above and beyond” other PCI DSS requirements
* be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement3

Every assessor is required to validate the compensating control for the risk the requirement is supposed to cater to. After an assessment is complete, all processes must stay in control to ensure that PCI compliance is maintained.

**Rules for Documenting a Compensating Control**

Documenting a compensating control may not be an easy task, as it requires a lot of effort and turns out to be costly in the long run. However, organizations that fail to meet all requirements of PCI DSS are adopting the use of compensating controls.

Basic Seven rules must be followed before documenting a compensating control:

1. Identify which requirement of the PCI DSS will be addressed by the compensating control.
2. Identify the reason why the PCI DSS requirement cannot be met by the organization in the process of PCI compliance.
3. Define the objectives of the PCI DSS requirement and that of the compensating control.
4. Identify any other risk the organization may face as a result of implementing that compensating control.
5. Identify and define all the compensating controls.
6. Identify what procedure would be followed to validate the compensating controls.
7. Identify what procedure would be followed to maintain the compensating controls.

Now to explain these rules one by one, the first rule indicates that only one requirement of the PCI DSS should be addressed by a compensating control at one time. But in real practice, a number of compensating controls can be written for a whole group of PCI requirements which fall under a single requirement. It mostly depends upon your QSA to determine whether every requirement should have a separate compensating control or not.

When identifying a business constraint, many companies put forward the reason that it is simply unable to meet the requirement; hence the use of compensating control. This reason is not enough to justify a compensating control. The organization must identify and document a solid reason or reasons to prove the need of a compensating control.

The biggest confusion arises when documenting the section 4,5, and 6 of the compensating control. In section 4 the organization is supposed to document the compensating controls for not being able to implement the particular requirements. In section 5 the organization validates the compensating controls mentioned in section 4. In section 6 the organization documents the maintenance process of the compensating controls. The rule that must be followed here is that after documenting particular compensating controls in section 4, they need to be further carried on to section 5 and 6 where their validation and maintenance needs to be documented as well. But mostly organizations fail to discuss the validation and maintenance of the compensating controls mentioned in the section 4. It is important here to make a list of all compensating controls in section 4 and then document them further in section 5 and 6 in the same order as in section 4.

**Compensating Controls are not Shortcuts**

At first, compensating controls may seem like a short cut to achieving compliance. However, they are not. In reality they might cost more in terms of finances, rather than addressing the vulnerability itself to achieve compliance. Neither are they a permanent solution. Although they can be documented for almost every requirement of the PCI DSS, (with the exception of requirement 3.4), it is still better to solve the main issue itself and minimize the business constraints.

In every yearly assessment, it is a must for the assessor to review that the compensating controls follow the 4 points of criteria as laid down by the PCI Security Standards Council. The assessor also needs to check that the business constraints for which the compensating controls were developed are still there and that the controls are still serving the very same purpose.