

Safe & Sound

Barclaycard's guide to bad compensating controls

I can't do it...

It's true, you can't always meet a PCI DSS requirement to the letter. There is no shame in that and we understand it can be daunting to follow the definition of "meeting the intent and rigour", "providing a similar level of defence", "going above and beyond" and be "commensurate with the level of risk".

At Barclaycard, we review a lot of compensating controls and any exhibiting one or more of the characteristics below is bad:

1. **Doesn't explain why the original control can't be met.**
Sometimes, we just get "we're doing xyz1 to meet the requirement", without "because implementing the original control would mean xyz2 to our organisation".
2. **Doesn't quantify the residual risk** of implementing the compensating control in terms of
 - **volume of cards:** the risk profile will be very different if 50 cards are potentially at risk at anyone time, compared to 10,000 cards.
 - **potential vulnerability window:** the risk profile will be very different if the vulnerability window is 3 hours compared to 30 days.
 - **likely frequency of attack:** the potential exposure could be once every month or for a couple of hours every day. This combined with the above points can have devastating effects (or not...).
3. **Doesn't explain how historical data is being dealt with:**
 - **retention policy:** do you really need to retain the data for that long? In our experience, a review of the retention periods very often leads to risk reduction...
 - **destruction policy:** whilst trying to address a PCI DSS requirement, let's not forget that historical data does not disappear on its own... Make sure that any historical data consistently reduces over the duration of the compensating control.
4. **Doesn't show a timeline of risk reduction** for the duration of the compensating control. With all above, you should be able to quantify the risk reduction overtime.
5. **Is not time bound** (i.e. no end date). Need we say more?
6. **The risk category** (high, medium, low) **is not confirmed by the QSA:** if your QSA is not prepared to confirm in writing the level of risk associated with the compensating control, you should think twice!...

In our experience, it is beneficial for merchants to involve their acquiring bank early when thinking about compensating controls, instead of just presenting them as part of a Report on Compliance (RoC).

The official definition... *Appendix B PCI DSS v2.0*

Compensating controls may be considered for most* PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented 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 rigour** of the original PCI DSS requirement.
2. **Provide a similar level of defence** 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.
3. **Be "above and beyond"** other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. **Be commensurate** with the additional risk imposed by not adhering to the PCI DSS requirement.

All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review.

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.

Companies should be aware that a particular compensating control will not be effective in all environments.

* Please note that compensating controls are not acceptable for the storage of sensitive authentication data post-authorisation.

This information is available in large print, Braille or audio format by calling 0844 811 6666*

*Calls may be monitored and/or recorded to maintain high levels of security and quality of service. For BT business customers, calls will cost no more than 5.5p per minute, minimum call charge 6p (current at March 2011). The price on non-BT phone lines may be different. Calls may be monitored and/or recorded.

Barclaycard is a trading name of Barclays Bank PLC. Barclays Bank PLC is authorised and regulated by the Financial Services Authority and subscribes to the Lending Code which is monitored and enforced by the Lending Standards board. Registered in England. Registered No. 1026167. Registered Office: 1 Churchill Place, London E14 5HP.

