

WI Reference: WI3649S
Title: Data corrections
Author: Steve Parker
Created: 08/09/2011
Last update: 12/09/2012
Last updated by: Steve Parker
Version: 2
End date: 06/09/2013

Details:

The DPA requires that access to personal data remains within the European Union and PCI data security standards mandate physical security restrictions must be applied where update access is allowed to user data. Currently the only units which fulfil all these requirements for data access are the SSC and ISD Unix. The responsibility for data correction is vested with the SSC although ISD sometimes act under SSC authorisation.

Corrections to live system data must be authorised and auditable.

Data corrections

Support activities may lead to a data correction. If any correction is required then a clear audit trail must exist in the form of narrative on a Peak incident or an MSC sub task. This should include the reason for the change and technical detail showing how the change is being carried out.

Financial data

Changes to financial data are rarely required. Where a requirement exists such changes must be made via contra journal entries to maintain audit ability. In the very rare cases where this is not possible the change must be made using the two man rule. The "two man rule" (sometimes called the "four eyes rule" in security circles) specifies that there must be two individuals that must act in concert in order to perform some action. Further, each individual should have comparable knowledge and skill in order to detect attempts of subversion initiated by the other.

Within the SSC, one member of the SSC will perform the data correction while a second member of the SSC will witness the change being made. Both names must be recorded on the MSC for audit purposes.

References:

Reference Type Value Description

New Reference:

Reference Type	Value	Description
Peak Incident		<input type="button" value="Add"/>

View WI3649S

Other versions of this WI:

Version 1

[View Changes](#)