

## AI298 - Approaches to restoring stability and integrity

This note outlines a series of methods of improving the stability of the product. A three pronged approach is recommended:

1. **Fix the individual problems which are currently affecting the live environment.** Measure through reduction in incidents and need for offices to reboot, etc. This is underpinned by the monitoring activity being run jointly by Pathway and POCL. Target needs to be agreed, likely to be based on:
  - reduction in overall number of system stability incidents
  - reduction in maximum number of incidents per office
  - reduction in number of “authorised reboots” overall and maximum per office
  - reduction in number of “unauthorised reboots” (as indication of user perceived instability/lock up)
2. **Re-visit the existing product to ensure we have a stable base from which to go forward.** This acknowledges that stability related problems can remain hidden in software in the early stages of use, only to be revealed either as volumes increase, as filestores age, as new releases of software or data make new demands on resources, etc.

A programme of activities should be put in place, to run in parallel with early live usage, to ensure the stability and integrity of the base product. This programme would potentially include:

- reterospective design reviews, including “targetted” reviews of specific risk areas (eg failures, double activities, across paradigm boundaries etc). Preferably involve an independent viewpoint outwith Pathway; POCL may also add value.
  - review end to end design approach to ensure common assumptions (eg across paradigm boundary - who is validating what?)
  - introduction of defensive measures at key risk areas
  - ensure similar errors to those fixed at (1) have been addressed, even if no “fault” has yet emerged
  - targetted “lab” testing of specific risk areas, eg monitoring of resource usage (eg memory leakage etc)
3. **Re-visit the development approach to ensure that future developments do not introduce similar stability problems into the live estate.** Opportunities may include:
    - increased effort in the design and design review activities - including more independent reviews, peer reviews, and “targetted reviews” considering specific conditions.
    - increased use of code inspections, peer review of code etc
    - increased consideration of exception conditions

- more aggressive “lab” testing by design-aware expert team
- more stress testing
- use of technical tools for memory monitoring etc PRIOR as an assurance rather the debugging activity.
- extended trialling in a ring-fenced subset of offices (this assumes that POCL would accept the “debugging” of software, rather than trialling of the business processes, in a live environment. Expectation management!).