Appendix 6: Mitigation and control of risks in computer projects

For large computer projects the following suggestions are offered for risk mitigation:

- establish the objectives and the business case very clearly and comprehensively at the outset;
- identify the lead sponsor, if more than one sponsor is involved, and set up a clear machinery for decision-making by the sponsors;
- consider running a pilot project;
- subdivide the project into semi-independent modules;
- use established software which is already working, as far as possible (even if there is some loss of functionality), reserving any brand-new software to a relatively small part of the whole;
- avoid as far as possible any technologies which have not previously been tested thoroughly in practice;
- draw up a clear specification;
- check carefully that the project, if delivered according to specification, will fully achieve the objectives;
- ensure there is clear ownership of the project at an appropriately senior level;
- employ consultants to ensure that there is a good blend of IT expertise and business expertise and a genuine partnership between the experts on each side;
- revisit the project specification to see if further modifications can be made to reduce the risks which have been identified;
- define clearly which risks will be borne by the contractor and which by the sponsor(s), and write the contract accordingly with an appropriately structured payment mechanism;
- take up references regarding contractors' performance on previous projects;
- choose a contractor with a record for reliable delivery, even if not lowest cost;
- give appropriate financial incentives (or penalties) to the contractor to ensure maximum effort on his part to control risks;
- set up well-defined mechanisms to control specification changes, with appropriate levels of authorisation;
- use a flexible design that can readily be adapted to cope with legislative changes, and establish an early warning system that flags adverse consequences of legislative changes in time;
- address the toughest design issues first;
- pay particular attention to the user-friendliness of any component of the system which will use the Internet;
- ensure that the development team has sufficiently high-quality 'back up cover' in case some members fall sick or leave;
- consider whether insurance could play a part (e.g. key-man insurance);
- establish contingency plans to extend the life of the current system should there be a time over-run on the new project;
- set up a system for testing in modules the parts of the system which involve new software or new technology, with contingency plans for dealing with the situation should they not work;

- establish contingency plans in case the contractor goes out of business while the project is being developed or under warranty;
- plan in detail the transition from the old system to the new.

Once the project is authorised, it is vital that proper machinery should be put in place to control the residual risks, including:

- appointment of a fully competent project manager with a clear remit and defined authority;
- preparation of containment and contingency plans;
- appointment of risk custodians;
- appropriate budgetary controls, including contingency allowances for minor variations;
- strict controls on even minor specification changes;
- controls to make sure that all the intended risk mitigation actions are in fact taken;
- a crisis management committee that can be called at short notice;
- establishment of project 'landmarks' at the outset, with dates attached to them – some of these landmarks will be followed by additional gateways requiring reaffirmation of project continuance;
- a detailed procedure for monitoring and analysing trends;
- full communication to all concerned;
- regular risk reviews, including reviews of whether the project (when completed) will still meet customers' needs if these have changed;
- a project steering group, meeting monthly, to consider emerging issues of policy, timing or resource constraints, on which all interested parties should be represented, at a sufficiently senior level, and the project manager should attend.

Note: Large IT projects are often actually IT-enabled business change projects, and hence great attention needs to be paid to the robustness of the case for the business change, and the risks involved in that business change, as well as the IT-specific risks set out above. Experience has shown that, where such projects have failed, this is often due to a failure of the business change rather than a failure of the IT component.