



How to get ISO9000/TickIT certification right first time

S.R. Hill

*DNV Quality Assurance Ltd, Palace House, 3
Cathedral Street, London, SE1 9DE, UK*

ABSTRACT

A substantial number of IT organisations do not get ISO9000/TickIT certification on the first audit. The problems encountered are discussed and advice given. Statistics on common causes of failure by ISO9001 clause are given.

INTRODUCTION

TickIT is the UK Government's Department of Trade and Industry originated scheme for the ISO9000 certification of information technology organisations. TickIT arose from needs identified by the IT industry. Its use for UK accredited certification is mandatory and it is rapidly spreading to other countries.

ISO9001, EN29001, BS5750 Part 1 are equivalent International, European and British standards for quality management systems (QMS). There are many other equivalent national standards. ISO9002, EN29002, BS5750 Part 2 are the equivalent standards for organisations which do not design products or services to order. This paper uses "ISO9000" for ease of reading.

ISO9000 accredited certification has increasingly become a requirement for suppliers to large organisations and a sign of an organisation's commitment and systematic approach to quality. Many companies need ISO9000 to stay in business.

The market need for ISO9000 certification has been met by independent consultants who advise their clients on how to set up a QMS and how to get certification; and by accredited certification bodies who assess organisations



140 Software Quality Management

against ISO9000 and "award" the certificate if successful.

"Accredited" essentially means government approved. TickIT certification bodies must be accredited. DNV Quality Assurance was the first certification body to be accredited followed by BSI Quality Assurance (a separate organisation from BSI Standards), LRQA, BVQI and SGS Yarsley. Other certification bodies may have been accredited by the date of publication of this paper.

QUALITY MANAGEMENT SYSTEMS

A QMS is a management system for ensuring that customers receive the products or services as promised. For ISO9000 it needs to be formal i.e. thought out, documented, and evidenced i.e. records need to be kept to show that key management controls have been applied.

Here lie two of the problems for an organisation going for ISO9000: how much to document and what records to keep?

PROBLEMS ENCOUNTERED

The main problems encountered by an IT organisation going for ISO9000 certification are:

- 1 Deciding whether TickIT applies
- 2 Choosing a consultant
- 3 Winning over independently minded technical staff
- 4 How much to document
- 5 What records to keep
- 6 How to make sure that key activities have been properly included
- 7 How to choose a certification body

These problems are addressed in the following sections.

DOES TICKIT APPLY?

The main guidance document, ISO9000-3, covers only the software development aspects of TickIT. Clarification on the wider aspects of IT has been helped by the publication of a concise definition of TickIT (Disc TickIT Office [1]). At the time of writing this lists the following areas:

- 1 Software development where software forms all or part of the organisations product or service.
- 2 Internal software development where it is not part of the product but can

significantly affect the organisation's product or service.

- 3 Non trivial software replication.
- 4 IT facilities management.
- 5 Computer operations involving software development or maintenance.
- 6 Non trivial systems integration services.
- 7 Services where software evaluation or selection takes place.
- 8 Non trivial software archiving and storage services.
- 9 Prime contractors who sub-contract software development.

Not covered are:

- 1 Software stockholding (warehousing).
- 2 Software sales (over the counter, mail-order).

This still leaves "grey" areas e.g. how does one know when the systems integration or software evaluation cases apply? The author has a simple test for "grey" areas: if the skills of a TickIT auditor are needed for a proper audit, then it comes under the TickIT scheme.

Those organisations who are in a "grey" area may ask the advice of certification bodies. A non-TickIT certification body will err on the side of "not applicable". A TickIT certification body will be able to advise from a point of knowledge and experience.

At the end of the day the need is to have a credible certification that is recognised by ones business partners and customers. TickIT will impose no extra requirements on an organisation. It merely gives guidance for IT organisations and ensures properly qualified auditors are used. You don't want your QMS audited by someone who requires you to "calibrate your floppy disks" do you!

WHICH CONSULTANT?

Some organisations choose a consultant to help them set up their QMS on the basis that he is known by a friend of the Managing Director. Others will pick one from a business directory. There are many "quality consultants" around but not many who know how to apply ISO9000 to IT organisations. Here are some simple tests to help you select a consultant:

- 1 Are they a registered TickIT auditor? Ask to see their card. If they are then they will know about IT organisations and what auditors look for.
- 2 If they are not a TickIT auditor then you should:
 - (a) Test their knowledge and experience of setting up a QMS

142 Software Quality Management

- have they actually done it themselves?
- (b) Test their knowledge of IT
 - do they know what configuration management is and how it applies to you?
 - what experience do they have of different development lifecycles?
 - what would they expect coding standards to cover?
- 3 Do not employ a consultant if:
 - they offer you an "off the peg" QMS (they rarely fit and will not stand up to an assessment)
 - they offer to write a large part of your QMS for you (they are only interested in your money and will pad the job out by creating mountains of paper and bureaucracy)
 - they try to baffle you with science and jargon (certification is a simple process; anyone who cannot explain it in simple terms is incapable, just wants your money, or both)

WINNING OVER THE STAFF

IT people are highly intelligent, creative and independently minded. Their initial reaction to the proposition to put in place an audited QMS is that it will stifle their work and turn them into mindless form fillers. This of course is rubbish.

Do not try to impose a QMS. It will not work. You will fail the assessment because your staff will not be willing to work to the QMS.

Staff can be won over by:

- 1 Giving awareness talks on what it will really be like - preferably from someone who has experienced what it is like. This will not convince them but it should open their minds.
- 2 "Seeding" the organisation with staff who have been on an Internal IT Auditor Course. This will turn most sceptics into converts. Their colleagues will then start to accept that perhaps it will be okay.

HOW MUCH TO DOCUMENT?

ISO9000 certification requires a written system. In practice this means a Quality Manual and procedures. It is a mistake to document too much.

Only document enough to:

- 1 Impose standard practice where it is desirable e.g. how to record the result of a design review or what to put in a code header.
- 2 Meet the standard e.g. there must be a procedure for "contract review".
- 3 Give instructions for unusual or infrequent actions e.g. disaster recovery or complaints.

A Quality Manual of 20 to 40 pages will be quite sufficient. It should say what your organisation does to ensure quality. It can be written against ISO9001 or ISO9000-3 clauses if desired but does not have to be.

WHAT RECORDS TO KEEP?

"Quality Records" are records kept to:

- 1 Demonstrate that a key control action has taken place e.g. a contract review or
- 2 Record an item of information that may be needed if there is a subsequent quality problem e.g. a modification to code took place.

Only keep what is essential. Develop simple forms and standard formats to make it easy, reliable and foolproof.

KEY ACTIVITIES TO PAY ATTENTION TO

Figures 1 and 2 show statistics on "non-conformities" found in ISO9000/TickIT main audits. "Category 1" non-conformities are serious deficiencies which prevent certification taking place until fully corrected. "Category 2" Non-conformities are one-off lapses but enough of them can add up to a Category 1 and so prevent certification.

The lesson is quite clear. The key areas which cause organisations not to get certification right first time are:

- 1 Design Control
 - no project plans
 - plans not up-dated
 - no progress control
 - rules, practices, methods not complied with
 - phase inputs and/or outputs not defined
 - no design verification
 - design change not controlled



144 Software Quality Management

2 Contract Review

- contracts not being adequately reviewed

3 Quality System

- absence of key procedure(s)

4 Document Control

- inadequate system for control of documents or
- widespread inadequate control of procedures/project documentation

Special attention to these areas will increase your chances of getting ISO9000/TickIT certification at the first attempt.

WHICH CERTIFICATION BODY?

The five TickIT accredited bodies have been listed earlier in this paper. Some organisations make the mistake of approaching just the one that gives the "kite mark". They think that this will be more credible. A look at the IT client lists of some of the others will show this to be untrue.

But aren't they all the same when it comes to how certification is done? No! Examples of differences are:

- some abandon audits if a category 1 non-conformity is found
- some do planning visits to ensure audits run smoothly

Remember, you have a choice!

CONCLUSIONS AND RECOMMENDATIONS

The probability of getting ISO9000/TickIT certification on the first audit will be greatly increased if:

- 1 You treat certification as a project and appoint a project manager
- 2 You choose the right consultant
- 3 You win over your staff
- 4 You document your systems to the right extent
- 5 You keep adequate and appropriate records
- 6 You ensure key activities are covered
- 7 You ensure everything is in order by performing at least two thorough internal quality audits prior to the certification visit.

REFERENCES

- 1 Disc TickIT Office, Application of the TickIT Scheme, A Concise Definition. Issue 1.0, August 1993.

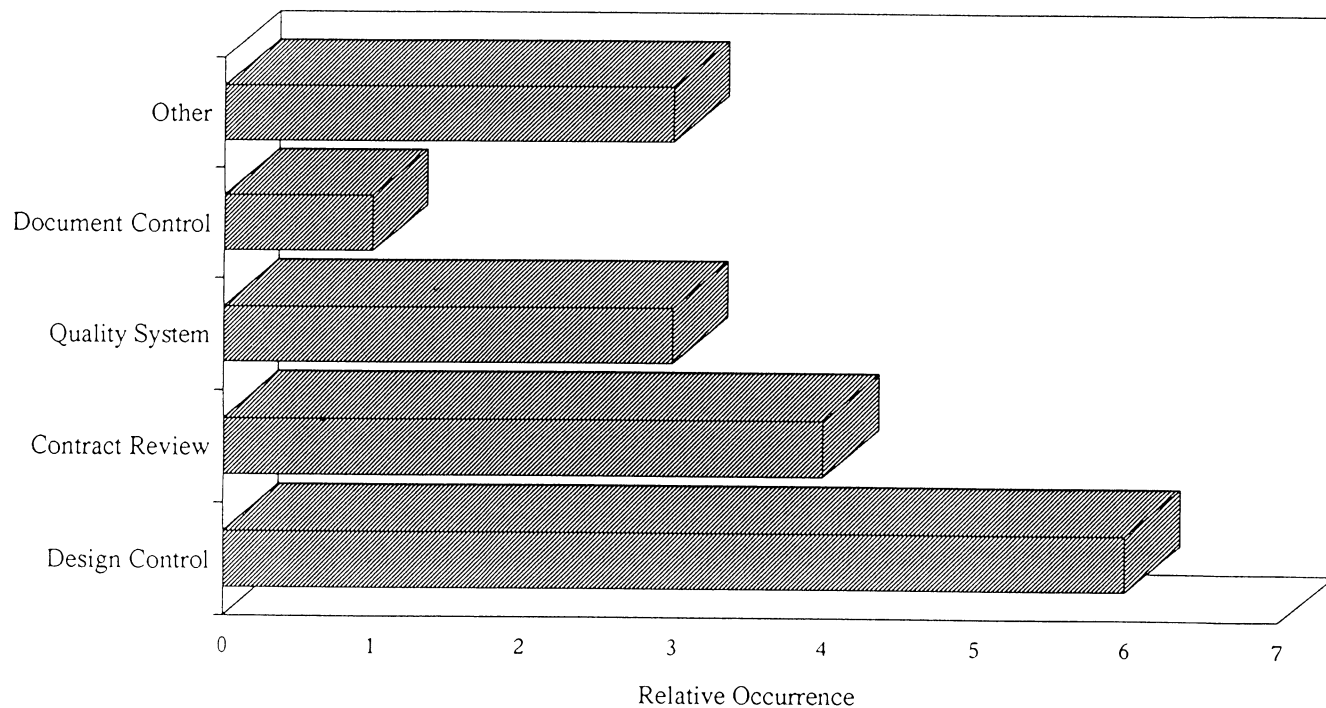


Figure 1 : Category 1 - Non Conformities found on DNVQA Initial Audits

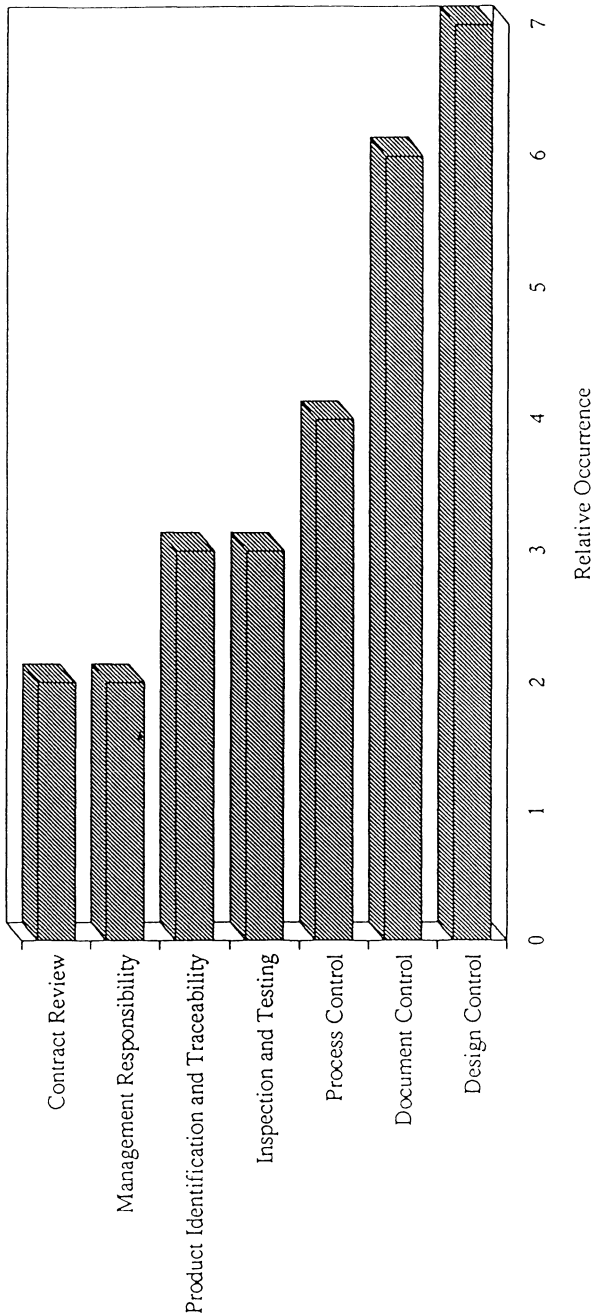


Figure 2 : Category 2 - Non Conformities found on DNVQA Initial Audits