Institute of IT Professionals
NEW ZEALAND

Information Technology
Code of Practice

Guidelines of good and acceptable practice for IT professionals and organisations operating in New Zealand.

June 2015

About IITP

The Institute of IT Professionals (IITP), formerly known as the NZ Computer Society, is the professional body of the IT sector in New Zealand.

IITP has a proud history spanning over 50 years and has been a part of the computing and IT sector in New Zealand since formation in 1960.

IITP Vision

IITP is the authoritative voice of the IT profession that leads professional development and good practice in IT.

Table of Contents

1: Introduction

1.1 Purpose

1.1.1   The purpose of the *IITP Code of Practice* is to assist members in applying the Tenets of the *Code of Ethics*, which have been written in broad terms, to a Code of Practice. Whilst not specifically part of the Code of Ethics, the Code of Practice should be read in conjunction with the Code of Ethics and members will be expected to have considered the content of the Code of Ethics, this and any other supplements in any matter of professional conduct.

1.1.2   The Code of Practice and Code of Ethics are not prescriptive but form the basis, in conjunction with the Constitution and Bylaws, of the Institute's concept of Professional Conduct and Practice.

1.1.3   The Code of Practice describes suggested standards of recommended practice relating to information technology (IT) or information and communications technology (ICT). Its intent is to provide a framework of guidance.

1.1.4   This code should be read in conjunction with the *Code of Ethics*.

1.2 Context

1.2.1   This code is intended for IITP members but is made freely available for the guidance of non-members within the industry. No additions, modifications or deletions are permitted other than by express permission of the National Board of the Institute of IT Professionals NZ. No warranty or obligation is given or implied.

1.2.2   The Code of Practice cannot and does not purport to cover all activities of each or any individual member.

1.3 Using the Code

1.3.1   The IITP *Discipline and Professional Conduct Board* recommends that you read and use the Code particularly where it might help and assist you in daily work. It describes:
- 1.3.1.1 Common practices of relevance to all IT professionals
- 1.3.1.2 Key practices specific to particular IT skills
- 1.3.1.3 Practices specific to particular business or education streams

1.3.2   You are advised to follow all the common practices but, in general, you need only select those practices relevant to your needs.

1.3.3   The Code will be posted on the Institute website as a downloadable document.

1.4 Disclaimer

1.4.1   The IITP accepts no responsibility for any errors and omissions in this Code of Practice. Furthermore, reference to another organisation's web site does not constitute a recommendation, or endorsement, of that organisation, site, or its content, by the IITP.

1.4.2   In the event of an apparent conflict in responsibilities, obligations or prescribed practice, please consult the Institute's *Discipline and Professional Conduct Board* at the earliest opportunity.

1.5 Terminology

1)   **Client:** Any person, organisation or department for whom the member undertakes to provide IT services, in any way; this includes other departments within the member's organisation.

2)   **Organisation:** Any company, government department or other body for which the member as an individual undertakes professional practice. The member may be an employee, contractor, consultant, student or volunteer.

3)   **User:** Any person, department, company or other body served by IT.

4)   **System:** A group of electronic equipment and software which together provide a particular service. *System* may be interpreted as encompassing non-computer procedures such as clerical, manual, communication and electromechanical processes.

5)   **Information Technology** (IT): IT is to be taken to include IS (Information Systems) and ICT (Information Communication Technology) where relevant.

1.6 Acknowledgements

1.6.1   The Institute acknowledges the existence of many other Codes of Practice, applicable within the IT profession and other industries. Specifically, it acknowledges and thanks the *British Computer Society* for permission to utilise and base much of the IITP Code of Practice on the BCS Code of Good Practice. Other Codes have materially assisted in the development of the IITP Code as to concepts and practices and it is hoped that the authors of these documents draw some satisfaction when seeing familiar ideas. Those of particular relevance are listed in Appendix A.

1.6.2   The Institute acknowledges the contributions made to this document by a number of members of the Institute.

1.7 Future Editions of the Code

1.7.1   Members who wish to recommend or have considered good practices in those above or for areas not yet covered are encouraged to provide contributions to the IITP Discipline and Professional Conduct Board (details in 1.8).

1.8 Responsibility for the Development and Maintenance of the Code

1.8.1   The operational responsibility for the Code of Practice lies with the IITP CEO.

1.8.2   The development and maintenance of the Code of Practice are the responsibility of the Discipline and Professional Conduct Board.

1.8.3   This Code of Practice is not an immutable document. In the rapidly changing IT world, it is expected to change to reflect new or revised practices. Members are encouraged to submit recommended changes to:

Discipline and Professional Conduct Board
Institute of IT Professionals NZ
P O Box 10044
Wellington   6143
pcb@IITP.org.nz

1.9 Other Contact Details

1.9.1   **President of the Institute**

The President
Institute of IT Professionals NZ
P O Box 10044
Wellington   6143
president@IITP.org.nz

1.9.2   **Chief Executive of the Institute**

The Chief Executive Officer
Institute of IT Professionals NZ
P O Box 10044
Wellington   6143
ceo@IITP.org.nz

1.9.3   **IITP General Details**

Institute of IT Professionals NZ
P O Box 10044
Wellington   6143
info@IITP.org.nz

Phone: +64 (4) 473 1043
Toll Free: 0800 252 255
Fax: +64 (4) 473 1025

2: Practices Common to all Disciplines

2.1 Conflict of Interest

❑ Identify and avoid or mitigate any conflict of interest before entering employment or beginning a project or other job.

❑ Be prepared to disclose any real, potential or perceived conflict of interest to affected parties. Note that a perceived conflict may not be initially identifiable.

❑ Be aware that a perceived conflict of interest, though possibly not actual, can still affect relationships and interactions and so must be afforded as much attention as any other conflict.

❑ Actively seek to remedy any discovered conflict of interest identified at any stage in a job or project life cycle. Remedies include: removing the cause of the conflict (which may include removing yourself from the conflict), not taking part in any decision-making which is affected by the conflict, involving someone else on your behalf who is not compromised and so on.

❑ Report any real, potential or perceived conflict of interest to your superiors, management, board, committee or any appropriate entity or entities.

❑ Be prepared to work with those who are or might be affected by any real, potential or perceived conflict of interest at any time.

2.2 Maintain Your Competence

❑ Seek to improve your IT skills by attending relevant internal courses, external courses, using computer-based training or reading technical publications.

❑ While striving to put newly learned skills into practice, be cautious of attempting anything which you are not qualified to do; inform your management if so requested and only proceed if your management accepts the consequences.

❑ Keep up to date with technological advances, through training, technical publications and specialist groups within professional bodies; recognise that information gained from the Internet may not be validated.

❑ Attain appropriate qualifications.

❑ Actively participate in specialist bodies such as the IITP Specialist Groups.

❑ Commit to a continuing professional development (CPD) programme and seek further contemporary education and training on IT and related matters.

2.3 Adhere to Regulations

❑ Follow the standards relevant to the client organisation's business, technology and development methods; encouraging new standards, where appropriate standards do not exist.

❑ Use standards in an intelligent and effective manner to achieve well-engineered results.

❑ Keep up to date with new standards and promote their adoption by the organisation when they are sufficiently mature and can offer real benefit to the organisation. Keep up to date with internal and external regulations and promote their adoption by the organisation if of benefit to the organisation or if necessary to sustain the public good.

❑ Ensure that you are up to date with the substance and content of the legal and regulatory frameworks (including but not restricted to data protection, health and safety, copyright geographical and industrial) as well as Codes and Standards that apply to your work; act at all times in a manner that gives full effect to your obligations under such legal and regulatory frameworks and encourage your colleagues to do likewise.

❑ Seek professional advice at an early stage if you have any doubts about the appropriate application of the law or regulations.

- ❑ Concern yourself with the needs of people with, for example, visual impairments, dyslexia or physical disabilities; as a minimum, comply with the New Zealand Human Rights Act 1993 and current Standards.
- ❑ Comply with non-discriminatory legislation in the areas of race, colour, ethnic origin, sexual orientation, disability or age in all aspects of your work.

2.4 Act Professionally as a Specialist

- ❑ Maintain your knowledge of your specialism at the highest level by, for example, reading relevant literature, attending conferences and seminars, meeting and maintaining contact with other leading practitioners and through taking an active part in appropriate learned, professional and trade bodies.
- ❑ Evaluate new products, assess their potential benefit and recommend their use where appropriate.
- ❑ Keep in close touch with and contribute to current developments in the specialism, particularly within the organisation and your own industry.
- ❑ When competent, offer expert advice, both reactively and pro-actively, to those engaged in activities where the specialism is applicable; this includes budgetary and financial planning, litigation, legislation and health and safety.
- ❑ Understand the boundaries of your specialist knowledge; admit when you may be required to cross this boundary and seek advice from colleagues with the necessary expertise; do not make misleading claims about your expertise.
- ❑ Exercise a sense of social responsibility for the implications of your work.
- ❑ Consider ways to inform colleagues of advances in technology, circulating documents, setting up libraries and arranging discussion groups where appropriate.
- ❑ Be aware that people within the organisation may not share your expertise; avoid technical jargon and express yourself clearly in terms they understand.
- ❑ Be aware of the risks and liabilities resulting from giving incorrect advice; consider taking out professional indemnity insurance.

2.5 Use Appropriate Methods and Tools

- ❑ Keep up to date with new methods and the tools to support these methods
- ❑ Promote the effective use of methods and tools within the organisation.
- ❑ Recommend the adoption of new methods only when they have been demonstrated to be effective for the organisation and are, preferably, supported by suitable tools.
- ❑ Explain to non-IT staff the purpose of any methods that have impact on their duties, so that they can understand the outputs and appreciate the benefits.
- ❑ Recognise the scope and applicability of methods and resist any pressure to use inappropriate methods.

2.6 Manage Your Workload Efficiently

- ❑ Report any overruns to budget or timescales as they become apparent; do not assume that you will be able to recover them later.
- ❑ Where applicable, such as working for a client, ensure that your work is covered by Terms of Reference and be wary of exceeding them.
- ❑ Do not undertake, or commit to, more assignments than you can reasonably expect to meet in a given time.
- ❑ Ensure that you have the necessary resources to complete assignments within agreed time scales.

2.7 Participate Maturely

- ❑ Provide constructive criticism of colleagues' work, aiming to improve the quality of the work without belittling your colleagues.
- ❑ Accept constructive criticism of your work, appreciating that your colleagues may have better solutions.
- ❑ Maintain good working relationships with colleagues, clients and users, even if you may strongly disagree with them; however, ensure that such disagreements are recorded.
- ❑ Ensure that the views of all participants are taken into the account and are fairly represented in the resulting list of actions.
- ❑ Follow up all actions placed on yourself, even in cases where you do not entirely agree with them.
- ❑ Utilise technical reviews as an aid to your professional judgement, seeking specialist advice where appropriate.

2.8 Respect the Interests of your Clients

- ❑ Declare any personal gains, financial or otherwise, that you may make from any proposed work; do not falsify or conceal information for your own benefit.
- ❑ Accept only those assignments which you are qualified and competent to undertake; you have a particular responsibility when you consider an assignment to be of questionable value to your client.
- ❑ Safeguard the confidentiality of all information concerning your clients.
- ❑ Refrain from acting for several clients with competing or conflicting interests without prior agreement from all parties.
- ❑ Utilise professional judgement and act with professional objectivity and independence at all times; in this respect "independence" is taken to mean "independence of relationships which might be taken to impair objectivity".
- ❑ Inform clients immediately of any interests or change of circumstances, which might prejudice the objectivity of the advice given.
- ❑ Disclose any interests in products which you may recommend to your client.
- ❑ Do not disclose to any third party any confidential information about your clients or its competitors.

2.9 Promote Good Practices within the Organisation

- ❑ Document all work to a level of detail that others could take over your work if need be.
- ❑ Identify opportunities for increasing the awareness of IT throughout the organisation.
- ❑ Be aware of the interaction of your work with that of others involved in the same activity.
- ❑ Seek to identify potential hazards, failures and risks associated with your work or work place, and seek to ensure that they are appropriately addressed.
- ❑ Ensure that those working under your supervision or direction are competent, that they are made aware of their responsibilities and they accept personal responsibility for the work delegated to them.
- ❑ Help to promote a culture within the organisation which strives for continuous improvement; seek involvement and participation in best practices at all levels.
- ❑ When problems arise, take responsible corrective actions, even when such actions are beyond your responsibility.
- ❑ Take every opportunity to contribute to formal quality management systems within the organisation and fully understand quality and commercial practices.
- ❑ Contribute positively to the fulfilment of the overall QA function of the organisation where the function exists.
- ❑ Consider the introduction and promotion of QA functions where they do not exist, are relevant and are within your competence.
- ❑ Otherwise, consider the promotion of QA functions by competent third parties where the functions do not exist and are relevant.
- ❑ Ensure the organisation's practices on the collection and use of personal data comply with applicable national, regional and international laws and (self) regulatory schemes.
- ❑ Accept the blame for your own faults, rather than transferring the blame onto items for which you are not responsible.

2.10 Represent the Profession to the Public

- ❑ Contribute to the education of the public whenever you have the opportunity, so that they can be aware of and form an objective and informed view on IT issues.
- ❑ Ensure that all complaints from members of the public are dealt with properly through to resolution; such complaints include, but are not restricted, to accessibility, data protection and data security issues.
- ❑ Encourage user and consumer trust in reputable and proven global networks and electronic commerce or their descendant, relevant technologies.

3: Key IT Practices

3.1 Programme/Project Management

3.1.1 When Managing a Programme of Work

❑ Make a clear distinction between projects that result in contract deliverables and programmes that provide your client with process improvements and benefits.

❑ Advise your client if, in your opinion, any stage in the programme will not deliver the anticipated benefits.

❑ Work with your client and supplier(s) to reach a common understanding of the programme structure in terms of projects, deliverables, costs, inter-project dependencies, external assumptions and responsibilities for each element of work.

❑ Adopt transparent reporting based on quantitative, objective measures that are shared by your client and supplier(s) to ensure a common understanding of the status of the programme, the risks and any variances from plan.

❑ Review and agree with your client any key external pressures and influences for business improvement, plans for organisational change, parallel programmes (with potential mutual dependencies) and the effect these may have on the programme.

3.1.2 When Defining a New Project (especially large-scale)

❑ Encourage your client to:
  • Explain fully the corporate objectives that underpin the requirement, the scope, issues, constraints and risks to be addressed.
  • Articulate clearly the desired business benefits and how they will be measured.
  • Explain fully the project deliverables.
  • Define the information and services that your client will provide.

❑ Offer constructive challenge to your client if:
  • The requirement is unrealistic
  • Any of your client's expectations are unreasonable
  • There is a better way of meeting the requirement
  • A relatively minor change to the requirement might significantly reduce the cost, risk or timescale.

❑ Select and list appropriate quality standards and procedures.

❑ Devise an acceptance strategy that will fairly demonstrate that the requirements of the project have been met.

❑ List your assumptions, especially those that relate to goods or services provided by your client, and gain your client's approval of their validity.

❑ Define the escalation/exception procedures to be followed in the event of deviation from the plan.

3.1.3 When Planning

❑ Ensure that the scope, deliverables, timescales, costs and responsibilities are agreed in advance.

❑ Seek out similar projects and benefit from the lessons learned.

❑ Make realistic estimates of the costs, timescales and resource requirements, wherever possible basing your estimates on recognised methods and/or experience of delivering similar solutions.

❑ Seek to determine client or project expectations with respect to both functional and non-functional aspects.

❑ Resist the pressure to accept estimates produced in earlier stages.

- ❑ Be aware of the pitfalls associated with estimating tools; use other methods to double-check the feasibility of the results.
- ❑ Assure yourself that you have the resources required to complete the work within the agreed costs and timescales.
- ❑ Do not depend on later contract changes to recover overspend.
- ❑ Determine processes for revisiting and revising any aspects of the plan.

3.1.4 When Managing Project Risks

- ❑ Seek out the real risks to the client, the organisation and any suppliers.
- ❑ Resist the temptation to identify only the manageable risks.
- ❑ Openly and frankly discuss with your client the options for allocating, managing, mitigating and insuring against the risks.
- ❑ Avoid accepting responsibility for a risk that would be better owned by your client.
- ❑ Where risk is created by virtue of the scale or novelty of a solution for which there is no reliable benchmark for estimation, consider a modular or incremental approach to reduce risk.
- ❑ Devise mitigation actions that will reduce the chances of the most serious risks happening.
- ❑ Regularly review the risks and revise the mitigating actions.
- ❑ Make yourself aware of the differences between civil and criminal law in the treatment of risk

3.1.5 When Managing and Deploying the Project Team (especially large-scale)

- ❑ Ensure that all team members are given written instructions on each task to be performed, with target completion dates.
- ❑ Monitor the deployment of individuals objectively to ensure that they are contributing effectively whilst developing skills and experience.
- ❑ Deal sensitively with team members who are not performing well; investigate the root causes and take effective measures.

3.1.6 When Tracking Progress

- ❑ Maintain metrics on all project activities so that effective monitoring is enabled and so that later projects can benefit.
- ❑ Accurately record the effort spent on each task; do not hide overruns by booking to other tasks.
- ❑ Provide early warning of any possible overrun to budget or timeline, so that appropriate actions can be taken. This may require review of earlier estimates.
- ❑ Do not assume that any overruns can be recovered later in the project; in particular do not cut back on later activities such as testing.

3.1.7 When Closing a Project

- ❑ Honestly summarise the mistakes made, good fortune encountered and lessons learned.
- ❑ Recommend changes that will be of benefit to later projects.

3.2 Relationship Management

3.2.1 When Seeking New Customers

- ❑ Seek to ensure that a common understanding exists throughout the organisation of its corporate objectives, market position, product lines and development plans and that these form the basis of marketing strategy.

3.2.2 When Selling to Prospective Customers

- ❑ Do not overstate the capabilities, performance and benefits of the proposed products or services.
- ❑ Ensure the organisation has the necessary resources available to deliver on schedule.
- ❑ Make your prospective client aware of any risks in your proposed solution.
- ❑ Assure yourself that your prospective client will have or have access to the necessary skills, equipment and organisation to make effective use of your proposed solution.
- ❑ Identify to your prospective client any additional costs or changes necessary to make effective use of the proposed products and services.
- ❑ Within the limits of the law, strive to understand what your competitors offer, make every effort to provide a superior solution, but resist the temptation to belittle the offerings of your competitors.
- ❑ Maintain contact with your prospective client after conclusion of the sales activity; elicit any shortcomings in the sales activity and initiate remedial actions.

3.2.3 When Negotiating Contracts and Service Levels

- ❑ Avoid later disappointment by negotiating achievable service levels at realistic prices.
- ❑ Avoid situations that could be interpreted as corrupt (accepting or giving lavish gifts, entertainment, etc).
- ❑ Whilst aiming for a successful relationship, ensure the agreement of dispute resolution terms and processes that the organisation can afford if need be.

3.2.4 When Managing Customer Relationships

- ❑ Instil in your client a well-founded confidence in the products and services to be delivered, and your commitment to performance, risk, timescales and delivery.
- ❑ Set targets and monitor performance against these targets, aiming to exceed the contractual targets.
- ❑ Resist the temptation to hide overruns; do not assume that you will recover any lost time in later stages of the project.
- ❑ Keep your client informed of any problems that might impact on the quality of the deliverables.
- ❑ Ensure that any strategic problems are identified at the earliest opportunity and that solutions are identified and implemented.
- ❑ Do not sub-contract out any of your responsibilities without prior agreement by your client; if you do sub-contract, fulfil your responsibilities for the performance of the work.
- ❑ Actively represent your team, ensuring that effective relationships are built and maintained with your client, suppliers and other departments in the organisation.
- ❑ Respond promptly to your client's queries and complaints and ensure that all necessary actions are taken.
- ❑ Encourage your client to participate in reviews to facilitate process improvement.
- ❑ Be sensitive to and consider encouraging changes to your client's processes which will increase the benefits of your products and services.

- ❑ Resist the temptation to blame your client for all misunderstandings.
- ❑ Ensure that the necessary processes and procedures are in place to maintain or recover the delivery of systems and services in the event of any physical, technical or environmental disaster or major outage, providing continuity of service to your client.

3.2.5 When Managing Supplier Relationships

- ❑ Act impartially when selecting new suppliers; establish evaluation criteria that are not biased towards a particular solution and apply the criteria rigorously to all proposals.
- ❑ Encourage resolution of any shortcomings in the service, through proper communication between all parties, rather than resorting to penalty clauses.
- ❑ Whilst representing the interests of your own organisation, act impartially in any dispute between the supplier and the users.
- ❑ Provide regular feedback to the supplier, so that any improvements can be made before any problems become serious.

3.3 Security

3.3.1 In General

- ❑ Demonstrate a high level of professional competence, such as prescribed in AS/NZS ISO/IEC 27000 series comprising Information Security standards.
- ❑ Maintain a thorough understanding of relevant regulations and guidelines.
- ❑ Keep up to date with the threats, vulnerabilities to those threats and the range of countermeasures available to avoid, reduce or transfer risk.

3.3.2 When Assessing Risks

- ❑ Consider the use of specialist tools.
- ❑ Resist any pressure to oversimplify the risk analysis; involve personnel at all levels within the organisation to elicit the threats and the vulnerabilities to those threats.
- ❑ Ensure that the decision-makers are fully aware of all the relevant facts and the possible consequences of their decisions.

3.3.3 When Implementing Countermeasures

- ❑ Recommend a balanced and cost-effective mix of countermeasures that offer the required levels of confidentiality, integrity and availability.
- ❑ Promote a culture within the organisation where everyone recognises the importance of security and is aware of their responsibilities for security; encourage incident reporting to identify potential breaches of security.
- ❑ Whilst dealing sensitively with people, be aware that breaches of security are more likely from within the organisation.

3.4 Safety Engineering

3.4.1   In General

- ❑   At all times, take all reasonable care to ensure that your work and the consequences of your work cause no unacceptable risk to safety.
- ❑   Take all reasonable steps to make your management, and those to whom they have a duty of care, aware of the risks you identify; make anyone overruling or neglecting your professional advice formally aware of the consequent risks.

3.4.2   When Building a System

- ❑   Examine the proposed use of proprietary digital communication systems and seek out common-cause failures between control and protection functions.
- ❑   Beware of novel approaches to specification, design and implementation of knowledge-based computing and control systems; be attentive to their attendant problems of verification, validation and the effect on safety- related operation.
- ❑   Be aware that, whilst distributed systems involving communications systems are relatively easy to assemble from standard commercial components, it is difficult to predict their overall operational behaviour and there may well be hidden complexities.
- ❑   Determine the adequacy of the protection and control systems for remote plant; enumerate the hazards to which the plant may be subjected and relate each to the proposed protection and control systems.
- ❑   Be aware of the intended operational environment of integrated modular systems.
- ❑   Establish that the proposed integration of the mechanical structures (moving parts) with micro-electromechanical (MEMS) components is based on components intended for mechanical operation based on computer control.
- ❑   Treat any proposed integration of a new system with an existing system to a thorough examination.
- ❑   Be aware that the overall behaviour of systems based on software components of unknown or uncertain pedigree (SOUP) and commercial off-the-shelf products (COTS) will be affected by software components not specifically designed for safety purposes.

3.4.3   When Assessing Complexity

- ❑   Only use evaluated and validated software languages or accredited components for control systems.
- ❑   Establish/determine and use practicable software development methods and validation tools for embedded software, particularly in small systems.
- ❑   Ensure that the sensing devices and software within programmable electronic systems (PES) are compatible with the human form.
- ❑   Apply 'proven in use' analysis to achieve the appropriate level of safety integrity for opto-electronic components/techniques used for the sensing of personnel presence.
- ❑   Be aware that increased complexity of smart sensors increases the possibility of systematic failure; that there is a need for software and firmware version control; that, operationally, there is a dependence on configuration management by the user.

3.5 Change Management

3.5.1   When Advising on Business Change

❑   Appreciate the implications of new processes on both people and the organisation; seek consultative strategies to ensure a smooth transition to new processes.

❑   Strive to understand the underlying resistance to change and, if unfounded, seek consultative re-assuring strategies to promote understanding of the benefits.

❑   Challenge any apparent malpractices and investigate the root causes.

❑   Appreciate that not all improvements need technological solutions; significant benefits can often be achieved through procedural or organisational changes.

❑   Identify, understand and show the drawbacks as well as the benefits of proposed changes.

❑   Modify your approach and style to obtain co-operation and commitment and resolve potential conflict.

❑   Show sensitivity to political and cultural issues as well as technical and business effectiveness targets.

❑   Monitor the progress of the changes, learning from any mistakes made and, where possible, resolving any problems encountered.

3.5.2   When Controlling Changes

❑   Promote the importance of a structured change management process, where all changes are prioritised, assessed and tracked.

❑   Ensure that the appropriate impact analysis is conducted before any change is authorised.

❑   Seek out and resolve any conflicts between changes and ensure that the totality of the changes is in keeping with the organisation's goals.

❑   Ideally, and especially in large-scale situations, check each change provides a cost-effective solution to a technical and/or business need, and is prioritised accordingly.

❑   Keep to a minimum the number of changes to be made at a given time.

3.6 Quality Management

3.6.1   When Establishing a Quality System

- ❑ Express the organisation's commitment to quality through a clear and concisely written quality policy.
- ❑ Make all members of the organisation aware of the quality policy.
- ❑ Provide a means for all members of the organisation to find standards and procedures applicable to their work.
- ❑ Make a clear distinction between mandatory, optional and advisory standards.

3.6.2   When Constructing New Quality Standards

- ❑ Involve those who will follow the new standards in the writing and reviewing.
- ❑ Keep the language simple; avoid jargon wherever possible.

3.6.3   When Managing a Quality System

- ❑ Appropriately recognise individual achievements in attaining quality targets.
- ❑ Regularly review the standards and strive for continuous improvement.

3.6.4   When Performing a Quality Assurance Function

- ❑ Ensure that every project or product has a quality plan:
  - • Check that quality plans call up applicable standards, not just the list of mandatory standards.
  - • Encourage the collection, use and analysis of metrics so that improvements can be demonstrated quantitatively.
  - • Ensure that all sub-contractors follow the quality plan if they do not have a suitable quality system.
  - • Ensure that there are procedures for the acceptance, storage and maintenance of all externally-supplied materials.
- ❑ Act as the Quality Champion in reviews and testing:
  - • Demonstrate a pragmatic approach towards attaining quality
  - • Do not be distracted by details of no consequence

3.6.5   When Conducting Quality Audits

- ❑ Create a programme of audits to demonstrate that the organisation's Quality System is operating effectively and providing management with sufficient control and visibility
- ❑ Understand that the audit process is or can be made to be constructive and, to facilitate that, welcome external auditors into the organisation so as to benefit from their experience rather than just hide shortcomings from them to pass the audit.
- ❑ Remind those being audited that the audit is there to help them do their jobs better, rather than pick fault with their work.
- ❑ Encourage those being audited to prepare well for the audit; let their preparation become part of the improvement process, not just a mechanism to get through the audit.
- ❑ Use your experience of problem areas and the history of previous audits to select areas to audit and constructively seek to avoid real, potential or perceived bias.
- ❑ Follow up the audits and make sure actions are being taken to make real improvements.

4: Practices Specific to Education and Research Functions

4.1 Education

4.1.1   When Preparing Courses

- ❑　Ensure the curriculum is founded upon your research, practice and/or scholarship.
- ❑　In designing curricula, ensure that learning outcomes take into account external benchmarks and expectations.
- ❑　Ensure students are equipped with the necessary underpinning to comprehend future developments.
- ❑　Expose students within the curriculum to legal, social, cultural and ethical issues.

4.1.2   When Delivering Courses

- ❑　Develop in each student an independence of thought and learning ability and thus prepare students for career progression and ongoing CPD beyond the confines of this educational experience.
- ❑　Make explicit to all stakeholders the outcomes to be expected from engaging in the course.
- ❑　 Develop yourself as a reflective and reflexive educational practitioner, building on student feedback as appropriate.

4.1.3   When Assessing Student Ability

- ❑　Ensure that assessment is fair in its discriminatory function.
- ❑　Ensure feedback to each student is sufficient to identify strengths and enable weaknesses to be addressed.

4.1.4   When Tutoring Students

- ❑　Encourage students to join a professional body, either now or later, as part of their career plan.
- ❑　Ensure that students are made aware of codes of conduct and practice and emphasise the importance of adhering to them, whether or not they join a professional body.
- ❑　Ensure that students are made aware that their courses cannot cover all the details of specific topics in computing and that their knowledge will need to be constantly refreshed through CPD as a result of ongoing developments in the subject.
- ❑　Ensure that students are made aware that different organisations have different organisational and computing cultures and conventions, and that they will need to adapt to their environment.
- ❑　Ensure students recognise the nature and unacceptability of plagiarism.

4.2 Research

4.2.1   When Performing Research

- ❑　Be aware that perceived research goals are expected to offer benefits to the organisation or its clients but not to the detriment of society or the public.
- ❑　Recognise the potential use or misuse of the outcomes of your research and only proceed with the research if you can justify to yourself the consequences.
- ❑　Avoid providing IT support of research on human subjects and animals, where such research is not legal, not consensual or (in humans) not authorised by the subject or, where relevant, by Ethics Committees or Authorities.
- ❑　Strive to safeguard the confidentiality and anonymity of private data used in research.
- ❑　Investigate the analysis and research by other people and organisations into related topics and acknowledge their contribution to your research.
- ❑　Where allowed by the organisation, share the results of your work with other researchers, through papers issued through research publications and presented to conferences.

5: Practices Specific to Business Functions

5.1 Requirements Analysis and Specification

5.1.1   When Conducting Systems and Business Analysis

- ❑ Assure yourself of the soundness of your analysis methods; that they will deliver an accurate and complete representation of the requirement, enable a seamless transition into design and provide a sound basis for testing and acceptance.
- ❑ Strive to understand the organisation's business and search for changes that will bring tangible benefits.
- ❑ Involve and consult representatives of all stakeholder groups.
- ❑ Be aware of technical constraints and assure yourself that solutions are technically feasible.
- ❑ Be aware of the impact of new or changed business solutions on people's working lives and deal sensitively with them.
- ❑ Consider the impact of new systems on the public and avoid solutions that impose unacceptable levels of risk on their mental or physical well-being.
- ❑ When analysing current practices, show respect for people at all levels in the organisation and assure them that their views will at least be considered and if rejected, reasons can be given.
- ❑ Demonstrate an understanding of the business issues; be persuasive and explain to users and management, in language they understand, the benefits of the changes being introduced, as well as identifying any drawbacks and trade-offs.
- ❑ Document the results of your analysis in a style that can be understood by the users and the developers.
- ❑ Explain your analysis methods to the users and encourage them to understand the results and verify their correctness.

5.2 Software Development

5.2.1   When Designing New Systems

- ❑ Recommend the organisation to adopt new technology, but only when it is sufficiently well proven for the organisation, offers a cost-effective solution and is compatible with the organisation's IT strategy.
- ❑ Where appropriate, strive to understand the corporate needs of the organisation and aim to design systems that benefit those needs.
- ❑ Consider the needs for scalability, connectivity, capacity, performance, resilience, recovery, access, security and create cost-effective solutions that meet those needs.
- ❑ Produce design specifications that clearly state the objectives, scope, features, facilities, reliability, resilience, constraints, environment, system functions, information flows and traffic volumes as well as identifying requirements not met and scope for improvement.
- ❑ Resist the pressure to build in-house when there may be more cost- effective solutions available externally and vice versa. That is, choose, justify and be prepared to defend a sensible solution strategy

5.2.2   When Designing Software

- ❑ Strive to achieve well-engineered products that demonstrate desirable attributes at the level required including fitness for purpose, reliability, efficiency, security, safety, maintainability and cost effectiveness
- ❑ Take responsibility for ensuring the design balances requirements for functionality, service quality and systems management.

- ❑ Encourage re-usability; consider the broader applications of your designs and, likewise, before designing from new seek out any existing designs that could be re-used.
- ❑ Ensure your designs facilitate later stages in the development lifecycle, particularly testing.
- ❑ Check that the products of your designs meet anticipated needs such as that they can be used by both experienced and inexperienced users and are suitable for use for training purposes (e.g., on-line help, training databases).

5.2.3 When Creating Web Sites

- ❑ Seek to ensure the organisation's practices on the collection and use of personal data comply with applicable national, regional and international laws and (self) regulatory schemes where such interaction is relevant.
- ❑ Construct a privacy statement that protects the rights of consumers and make this statement visible at the web site; consider using a privacy policy statement generator, such as the one provided by the Organisation for Economic Co-operation and Development (OECD).
- ❑ Increase awareness of privacy practices to visitors to your web sites; consider creating a link between your homepage and your privacy statement, or between pages where you collect personal data and your privacy statement.
- ❑ Ensure the web site conforms to the Human Rights Act 1998 and other published and endorsed usability standards.

5.2.4 When Programming

- ❑ Strive to produce well-structured code that facilitates testing and maintenance.
- ❑ Follow programming guidelines appropriate to the language and encourage your colleagues to do likewise.
- ❑ Produce code that other programmers should be able to maintain; use meaningful naming conventions and avoid overly complex programming techniques, where these are not strictly necessary.
- ❑ Make yourself aware of the limitations of the platform (operating system and hardware) and avoid programming techniques that will make inefficient use of the platform.
- ❑ Wherever possible, avoid platform-specific techniques that will limit the opportunities for subsequent upgrades or portability of the code.
- ❑ Check that the code is in accordance with the design specification and resolve any differences.

5.2.5 When Testing

- ❑ Plan the tests to cover as many paths through the software as possible, within the constraints of time and effort.
- ❑ Assure yourself that the coverage of the testing is sufficient; take appropriate actions to resolve any shortcomings in the tests planned by yourself or by your colleagues.
- ❑ Promote the use of test tools that will maximise the effectiveness of the testing.
- ❑ Create a test environment whereby tests can be re-run and the results are predictable.
- ❑ Do not rely solely on the direct outputs of tests, but check values are as expected.
- ❑ Recommend improvements to the effectiveness of the software under test.
- ❑ Maintain a detailed testing log.
- ❑ Accurately document all anomalies arising during the testing and make sure they are investigated and resolved but remain impartial.
- ❑ Design regression testing to identify any undesirable side effects of a software change.
- ❑ Resist any pressure to curtail testing; make anyone overruling or neglecting your professional advice formally aware of the consequent risks.

5.2.6   When Porting Software

- ❑   Investigate the differences between the current and the new platform and identify changes to be made to ensure the software functions correctly.
- ❑   Make intelligent use of tools to convert the software, identify their limitations and take actions accordingly.

5.2.7   When Integrating Software

- ❑   Check that all software components meet the defined criteria for test.
- ❑   Devise integration tests that build upon component tests already performed and demonstrate that the components interface correctly with each other.
- ❑   Check the documentation of the components and assure yourself that they are compatible with each other and with the target platform.
- ❑   Maintain a configuration management system that records the status of each component.
- ❑   Devise workarounds that will enable the software to be used correctly despite known shortcomings.
- ❑   Release builds for operational use only when all known shortcomings have been resolved or workarounds devised; resist the temptation to meet timescales by overlooking shortcomings.

5.2.8   When Writing Technical Documentation

- ❑   Set a high standard of documentation and encourage your colleagues to do likewise.
- ❑   Follow the appropriate documentation standards: the organisation's house style and specific standards for the type of document.
- ❑   Identify omissions or shortcomings in the organisation's documentation standards and actively seek out ways to improve them.
- ❑   Strive to keep documentation and design models up to date.
- ❑   Ensure documentation is sufficient to enable effective ongoing maintenance.

5.2.9   When Writing User Documentation

- ❑   Investigate the subject of the documentation, through hands-on use, talking to experts and reading related documents; do not assume it works in a particular way.
- ❑   Assure yourself that you understand the real purpose of the document and structure the document accordingly.
- ❑   Strive to understand the potential readership, their expectations and abilities; be aware that some readers may have difficulties with reading, language or comprehension.
- ❑   Write the document in a straightforward style appropriate to the readership; avoid jargon.
- ❑   Make intelligent use of diagrams that complement the text and aid overall understanding.
- ❑   Check with experts that the document is correct and with potential readers that it meets their expectations.

5.3 System Installation

5.3.1 When Scheduling Installation Work

- ❑ Ensure that the Installation Procedures identify all relevant safety and security procedures.
- ❑ Ensure that appropriate licences exist for all software to be installed.
- ❑ Avoid unnecessary installation work, by recommending only those upgrades that will bring genuine benefits, not just extra revenue to the suppliers.

5.3.2 When Installing Hardware or Software

- ❑ Reduce the risk of installing faulty items, by checking that all necessary pre-installation tests have been performed on all items to be installed.
- ❑ Reduce the risk of installing any viruses by ensuring up-to-date virus checking is in place.
- ❑ Investigate any previous installations, particularly any that have failed, and avoid repeating the same mistakes.
- ❑ Follow all applicable safety procedures and encourage other to do likewise, even if they are not under your direct control.
- ❑ As an ideal, aim to involve the future users of the system, so that they understand its architecture and characteristics and will be able to perform well-defined maintenance work on their own.

5.3.3 When converting data

- ❑ Identify data that must be converted before or as part of the installation process.
- ❑ Work with the client so that all parties understand what data are to be converted and what the expected outcomes are.
- ❑ Identify relevant priorities for the activity.
- ❑ Use appropriate tools in the conversion process such that they produce a robust outcome as, for example, opposed to just a rapid outcome..
- ❑ Develop / use appropriate strategies to ensure data integrity throughout the process, ideally that give assurance to the client at all stages.
- ❑ Work with the client to prove the resultant data and its acceptability within the expected outcomes.

5.3.4 When Testing Installations

- ❑ Do not ignore seemingly trivial faults in order to meet installation deadlines.
- ❑ Record all exceptional events and ensure actions are taken to investigate and resolve them.

5.3.5 When Handing over the Completed Installation

- ❑ Provide documentation of all outstanding problems.
- ❑ Ensure that the receiving entity is capable of taking over the installation, identifying any additional training that may be necessary.
- ❑ Provide contact details so that you can resolve any problems that may arise following hand-over.
- ❑ Return any items removed to the owner or dispose of according to agreed procedures.
- ❑ Identify business continuity planning requirements and ensure the client agrees to develop a disaster recovery plan, which will maintain the continuity of the system to an appropriate level.

5.4 Training

5.4.1   When Determining Training Needs

- ❑ Create an environment where staff at all levels and abilities are encouraged to further their careers through training.
- ❑ Review business plans, identify skills shortages that could, with additional training, be filled by existing staff and publicise these opportunities.
- ❑ Review recruitment plans and identify the training necessary for new recruits to become fully productive and understand the organisation's culture.

5.4.2   When Producing Training Plans

- ❑ Seek out areas where the organisation could improve through increased training and pursue the necessary budgeting.
- ❑ Evaluate external training organisations and recommend using their services if they offer improvements in quality and costs.
- ❑ Consider identifying the career paths within the organisation; encourage equal opportunities for full and part-time workers, and define the training required to progress from one step to the next where appropriate for the client.
- ❑ Identify training which can be provided by experts in that particular area, nominate individuals with that expertise and the attitude to make good trainers, and arrange any necessary instructor training.
- ❑ Arrange for suitably equipped training facilities in an environment conducive to training.

5.4.3   When Designing Training Courses

- ❑ Taking into account the abilities of the trainees, structure the content and duration of training courses to avoid overload through variety and breaks.
- ❑ Identify the trainee skill pre-requisites, so that any necessary pre-training can be undertaken before the course and training of unprepared trainees avoided.

5.4.4   When Producing Training Course Material

- ❑ Strive for consistency across all course material; follow any appropriate guidelines and encourage the production of any that are missing.
- ❑ Write training manuals that complement existing documentation (e.g., user manuals), reflect the structure of the training courses and provide a useful form of reference following the training courses.
- ❑ Construct examples, both compatible with the training manuals and relevant to the business, so that trainees can apply the training to normal working situations.
- ❑ Design exercises that both stretch the trainees and enable the trainer to evaluate the trainees' performance.
- ❑ Design tests that will enable the trainer to assess trainee abilities objectively.
- ❑ Verify the accuracy and appropriateness of the training material with technical and business experts before starting any training.
- ❑ Review the training material with the trainers and improve the training material following any wide ranging and detailed questioning.

5.4.5 When Preparing Training Facilities

❑ Check the layout of the training room provides trainees with visibility of the trainer and visual aids, unobstructed by equipment and other trainees.

❑ Ensure that all computerised equipment for use by the trainer or trainees provides access to the correct versions of the software.

❑ Ensure that any electronic training data has been correctly initialised and is isolated from all operational data.

❑ Provide a training environment free from non-essential interruptions (particularly important for on-the-job training).

5.4.6 When Delivering a Training Course

❑ Encourage an atmosphere where trainees feel comfortable about asking questions, either during or at the end of training, as appropriate.

❑ Respond to questions from all trainees, avoiding any favouritism.

❑ Record any discrepancies with or between the training material or computer systems used in the training and initiate corrective action.

❑ Monitor the performance of trainees, through questions and exercises, identify where trainees are advancing at different paces and resolve any great discrepancies (e.g., separate into groups).

❑ When an individual trainee is clearly not keeping up with the rest of the class, avoid personal criticism and discourage ridicule by other trainees; if appropriate removing the trainee from the course.

5.4.7 When Assessing Trainee Ability

❑ Assess objectively, against pre-set criteria, the mastery of skills by trainees and, in accordance with the organisation's policy.

❑ Recognise trainees' achievements by issuing competence certificates to those who have reached the required mastery of skills or attendance certificates to those who have attended the complete course, but have not reached the required mastery of skills.

❑ Where trainees have not reached the required mastery of skills, agree with the individual's manager what additional training or other actions should be taken.

❑ Ensure that all records of assessments are stored securely and are only accessible by authorised individuals.

❑ Refrain from citing examples of the performance of particular trainees during future training courses.

5.4.8 When Assessing the Success of a Training Course

❑ Encourage trainees to complete course completion forms while everything is still fresh in their minds, honestly recording possible improvements in the course.

❑ Review course assessment forms and identify areas where training could be improved.

❑ Ensure the confidentiality of course completion forms if necessary.

5.4.9 When Evaluating the Benefits of Training

❑ Record in the course completion form possible improvements to the course and additional training requirements for the trainees

❑ Review course completion forms completed by trainers and identify where additional pre- or post-training could make training more successful.

❑ Monitor metrics produced by the organisation (production rates, failure rates) and demonstrate where training has improved, or additional training could improve these metrics.

❑ Periodically review the training plan and implement improvements.

5.5 System Operations

5.5.1   When Managing Systems Operations

❑ Ensure that you are up to date with and abide by all applicable legislation and regulations including health and safety regulations.

❑ Continually review the effectiveness of the current IT strategies in supporting the organisation's objectives; promote new strategies where these may benefit the information and communications needs.

❑ Maintain your awareness of other options for providing IT, such as outsourcing, new approaches to recruitment and retention, and global supply contracts.

❑ Participate fairly in the evaluation of these options, even if they may result in uncertainty about your career.

❑ Regularly review new developments and price changes (network tariffs, licence fees), recommending changes to the organisation when they offer both cost- savings and acceptable service levels, availability, response times, security and repair times.

❑ Use appropriate capacity management tools to monitor the hardware, software and networks to provide early warning or prediction of capacity problems; initiate actions (such as procurement of additional equipment) to prevent over capacity.

❑ Establish a configuration management system that tracks the delivery and formal testing of configuration items, the content of each build and the status of all defects.

5.5.2   When Assuring Business Continuity

❑ Use business impact analysis methods, tools and techniques as appropriate to identify business processes critical to the continuity of the organisation.

❑ Define criticality criteria and the quantifiable and qualitative impacts on the organisation arising from the loss of systems' availability, integrity or confidentiality.

❑ Use security risk analysis methods, tools and techniques as appropriate to identify potential exposures to application systems critical to the continuity of the organisation's business e.g. single points of failure, lack of effective countermeasures or lack of tested, up-to-date recovery plans.

❑ Define and prioritise actions to address the potential exposures, to a level appropriate to the organisation.

❑ Define contingency planning and disaster recovery procedures to standards that will maintain the continuity of application systems critical to the organisation's existence to a level agreed by the organisation; regularly test and maintain these procedures and ensure appropriate actions are taken to deal with new or changed risks.

5.5.3   When Providing System Administration and Operations

❑ Adopt a policy that minimises the replenishment of consumables (in particular paper, printer cartridges) and enables recycling of those consumed.

❑ Proactively seek to improve the performance of the system (in particular databases, networks) by regularly monitoring responsiveness and tuning performance parameters accordingly.

❑ Continue to check back-up and recovery procedures really work before any recovery is necessary.

❑ Regularly monitor resource usage and failure rates and keep management informed of any trends.

❑ Be cautious when rectifying operational exceptions and error conditions, calling for expert help if there is any concern that the operational data may be compromised.

❑ When any error condition necessitates the restriction or removal of system resources, be aware of the users needs, wherever possible informing them in advance of any limitations and keeping them informed of progress.

5.5.4 When Performing Database Administration

❑ Be aware of the sensitivity of the organisation's data, taking measures to prevent unauthorised access, without preventing access by legitimate users.
❑ Refrain from accessing data which you have no need to see.
❑ Enforce strict partitioning between operational data and data used for training or test purposes; ensure that support staff are unable to carry out any testing on the operational data.
❑ Make yourself aware of the database licensing conditions and prevent situations where they could be breached.

5.5.5 When Managing IT Assets

❑ Establish a management policy that states the organisation's commitment to safeguarding its IT assets and promote awareness of this policy within the organisation and to your clients and suppliers.
❑ Assign responsibilities for the purchasing, receipt, installation, movement and ultimate disposal of all IT assets; ensure that records are kept at each step.
❑ Adopt an ethical destruction policy, maximising the re-use of materials and minimising pollution caused by materials not recycled.
❑ Establish mechanisms to protect the organisation's IT assets from external violation; use a combination of software controls (firewalls, virus protection, passwords) and physical controls.
❑ Protect the integrity of the organisation's systems and data by restricting or preventing the (down)loading of unlicensed software onto the organisation's IT equipment; including but is not limited to, freeware, shareware, trial software, screen savers, games and obscene material.
❑ When it is necessary to (down)load software, do so only with the authority of the owner.
❑ Promote awareness of the Privacy Act 1993, in particular the responsibilities of management to inform staff of their obligations under this Act.
❑ Establish regular and random auditing of the organisation's IT assets; use appropriate tools to help automate this.
❑ Encourage your colleagues to appreciate that auditing IT equipment under their control is to help protect them from prosecution, not just to snoop on them.
❑ Resolve anomalies identified by audits; seek agreements with suppliers to resolve any under-licensing issues.
❑ Seek recognition of your achievements through membership of organisations such as FAST (Federation Against Software Theft).
❑ Promote awareness of the ethical and legal issues involved in having obscene material on an IT system.

5.6 Support and Maintenance

5.6.1 When Establishing a Support Service

- ❑ Establish the level of support which may realistically be expected and provide the tools, documentation and suitably trained staff to meet this expectation.
- ❑ Avoid providing a solution that will make it impossible for the client to transfer the service to another supplier.
- ❑ Promote a mechanism to change the levels of service without the client incurring excessive costs.
- ❑ Avoid placing dependencies on the client for tasks that should be included in the service.
- ❑ Ensure that documentation of the supported systems and software is available and in an appropriate form for those receiving the call for support.
- ❑ Provide a means for people to benefit from earlier support; maintain a log of support requests and solutions, maintain a list of frequently asked questions.

5.6.2 When Managing a Support Service

- ❑ Identify to the client any changes to relevant procedures that will improve the efficiency of the service provided, even if this will result in reduced revenues to the organisation.
- ❑ Avoid passing on unnecessary costs to the client, even if they are covered by a service level agreement.
- ❑ Reassure the client that any complaints about the quality of service are being taken seriously and keep him/her informed of improvements.
- ❑ Provide the client with as much notice as possible of any changes in the service levels which may cause costing thresholds to be exceeded.
- ❑ Keep the client informed of any situations that may result in a deterioration in the quality of service and the steps being taken to resolve the situation.
- ❑ Gather records of the services provided and take all the necessary actions to achieve target service levels.
- ❑ Honestly maintain metrics on the services provided, resisting the temptation to hide shortcomings to make the metrics look better, and take positive measures to improve the service.
- ❑ Keep all parties informed of the progress in dealing with support requests, especially when delays are expected.

5.6.3 When Receiving Requests for Support

- ❑ Show respect to all people requesting support, irrespective of business and technical knowledge.
- ❑ Even if a problem seems trivial, give assurance that it will be investigated and a response will be given.
- ❑ Deal appropriately with competing demands for support.
- ❑ Appreciate the consequences of giving incorrect advice.
- ❑ Recognise that some problems that appear trivial from a technical viewpoint may have major impact on the business.

5.6.4 When Investigating Problems

- ❑ Avoid unnecessary work by researching previous problems and looking for common solutions.
- ❑ Where similar problems re-occur, investigate ways of eliminating them, through system/operational changes or additional training.
- ❑ Study the outcome of transient faults and actively monitor for possible symptoms.
- ❑ Be aware of the sensitivity of operational data; keep control of copies of such data and ensure destruction when the investigation is complete.
- ❑ Avoid making investigations on an operational system; if there is no choice, be aware of the consequences.
- ❑ Appreciate the consequences of making changes to operational systems: resist the temptation to make ad hoc fixes unless you are certain they will work.
- ❑ Bring to the attention of your next level of management any problem that you are unable to resolve within the target timescales.
- ❑ Be aware of the costs of investigation, especially when using remote communications links.

5.6.5 When Liaising with Development Staff (Internal or Third Party Suppliers)

- ❑ Do not hand over commercially sensitive information without ensuring that procedures (including, but not limited to, confidentiality agreements, client organisation rules and legal requirements) for the handling, processing, storing and destruction of the information are in place.
- ❑ Ensure all parties appreciate the seriousness of problems and their impact on the operation.
- ❑ Do not allow technical jargon to cloud the issue and prevent understanding of the real problem.
- ❑ Ensure that you are included in any direct communication between the users and development staff.

Appendix A: Bibliography

A.1 IITP Documents and Electronic Material

- IITP Code of Practice Handbook No 6 *circa* 1984
- IITP Code of Good Practice *circa* 1972
- Skills Framework for the Information Age (www.sfia.org.uk)
- SFIAplus
- www.IITP.org.nz/activities/certification

A.2 Relevant Standards and Procedures

- AS/NZS ISO/IEC 27000 series – Information security standards.

A.3 Relevant Codes of Practice and Guidance of Other Professional Bodies

- British Computer Society Code of Conduct. Version 2.0. Issued 5 September 2001
- British Computer Society Code of Good Practice – Version 1 September 2004
- Australian Computer Society – ACS Code of Ethics and Professional Practice
- Canadian Information Processing Society – Ethical Principles
- Canadian Information Processing Society –Code of Ethics and Professional Conduct
- Computer Society of South Africa – Code of Conduct
- Computer Society of South Africa – Code of Practice
- New Zealand Institute of Chartered Accountants – Code of Ethics 2003

A.4 Relevant NZ Legislation

- Bill of Rights Act 1990
- Unsolicited Electronic Messages Act 2007
- Health and Safety in Employment Act 1992
- Copyright Act 1994
- Electronic Transactions Act 2002
- Privacy Act 1993

Appendix B: Glossary of Abbreviations

COTS   Commercial-Off-The-Shelf products
CPD   Continuing Professional Development
ICT   Information Communication Technology
IITP   Institute of IT Professionals New Zealand
ISM   Industry Structure Model
IS   Information Systems
IT   Information Technology
ITCP   Information Technology Certified Professional
MEMS   Micro-ElectroMechanical Systems
NZCS   New Zealand Computer Society (previous name for IITP)
PCB   Discipline and Professional Conduct Board
PES   Programmable Electronic Systems
NZQA   New Zealand Qualifications Authority
SFIA   Skills Framework for the Information Age
SOUP   Software components Of Unknown or uncertain Pedigree