Businesses face a legal minefield when it comes to information technology, with legislation covering issues as diverse as data protection, IT procurement contracts, outsourcing, escrow and joint ventures. This comprehensive, plain-English guide covers the IT-related legal issues faced by businesses and their staff on a daily basis.

The book provides the non-specialist with the tools to work out what needs to be done, who to get advice from and how to deal with IT and legal experts.

- Prior knowledge of the law is not required
- Covers data protection, procurement contracts, how to avoid employment problems and intellectual property law
- Dedicated chapters on cloud computing, open source software and freedom of information
- Explains WEEE (Waste Electrical and Electronic Equipment) regulations
- Includes examples from actual case law to illustrate common issues

About the editors
Jeremy Holt is the Head of the Computer Law Group of Clark Holt Commercial Solicitors.
Jeremy Newton is a Director at Technology Law Alliance in London, a law firm specialising in IT, outsourcing and e-commerce law.

You might also be interested in:
Data Protection and Compliance in Context
Stewart Room

Written in plain English, it provides practical advice...A valuable addition to my bookshelf.
British Journal of Healthcare Computing and Information Management

A small but perfectly-formed legal guide to spotting potential IT problems…With this book you'll stay on the right side of a very complex subject.
Internet Works (Reviews of previous edition)
Our mission as BCS, The Chartered Institute for IT, is to enable the information society. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

Our vision is to be a world-class organisation for IT. Our 70,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised qualifications.

Further Information
BCS The Chartered Institute for IT, First Floor, Block D, North Star House, North Star Avenue, Swindon, SN2 1FA, United Kingdom.
T +44 (0) 1793 417 424
F +44 (0) 1793 417 444
www.bcs.org/contactus
A MANAGER’S GUIDE TO IT LAW
Second Edition

Jeremy Holt and Jeremy Newton (Editors)
## CONTENTS

Contributors ix  
Acknowledgements xi  
Abbreviations xii  
Glossary xv  
Useful websites xix  
Preface to second edition xxi

### 1  IT CONTRACTS – Jeremy Holt

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Parts of a contract</td>
<td>1</td>
</tr>
<tr>
<td>Who are you going to call?</td>
<td>2</td>
</tr>
<tr>
<td>Checking out the supplier</td>
<td>3</td>
</tr>
<tr>
<td>Letter of intent</td>
<td>3</td>
</tr>
<tr>
<td>The supplier’s terms</td>
<td>3</td>
</tr>
<tr>
<td>What contracts are there likely to be?</td>
<td>4</td>
</tr>
<tr>
<td>Appendix: Main points of an IT contract</td>
<td>11</td>
</tr>
</tbody>
</table>

### 2  SYSTEMS PROCUREMENT CONTRACTS – Jeremy Newton

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The negotiation process</td>
<td>13</td>
</tr>
<tr>
<td>Beware the standard contract</td>
<td>15</td>
</tr>
<tr>
<td>Contract mechanics</td>
<td>15</td>
</tr>
<tr>
<td>Commercial highlights</td>
<td>18</td>
</tr>
<tr>
<td>Problem management</td>
<td>20</td>
</tr>
<tr>
<td>Enforceability of exclusion clauses</td>
<td>23</td>
</tr>
<tr>
<td>Conclusion</td>
<td>25</td>
</tr>
<tr>
<td>Appendix: The ’reasonableness’ test in practice</td>
<td>26</td>
</tr>
</tbody>
</table>

### 3  AVOIDING EMPLOYMENT PROBLEMS – Jeremy Holt

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>28</td>
</tr>
<tr>
<td>Computer and email usage policies</td>
<td>28</td>
</tr>
<tr>
<td>Avoiding health and safety claims</td>
<td>33</td>
</tr>
<tr>
<td>Appendix: Specimen policy for computer and email use</td>
<td>35</td>
</tr>
</tbody>
</table>

### 4  INTELLECTUAL PROPERTY LAW FOR COMPUTER USERS – Jennifer Pierce

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>40</td>
</tr>
<tr>
<td>Hardware and intellectual property rights</td>
<td>41</td>
</tr>
<tr>
<td>Software and intellectual property rights</td>
<td>42</td>
</tr>
<tr>
<td>Databases and intellectual property rights</td>
<td>44</td>
</tr>
</tbody>
</table>
## SOURCES

<table>
<thead>
<tr>
<th>Source</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Websites and intellectual property rights</td>
<td>45</td>
</tr>
<tr>
<td>Domain names and intellectual property rights</td>
<td>46</td>
</tr>
<tr>
<td>The internet and trade marks</td>
<td>47</td>
</tr>
<tr>
<td>The internet and copyright and database right</td>
<td>49</td>
</tr>
<tr>
<td>Appendix: A basic guide to intellectual property and related rights</td>
<td>49</td>
</tr>
</tbody>
</table>

## 5 SOURCE CODE ESCROW – Jon Leigh and Graham Wood

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>55</td>
</tr>
<tr>
<td>The importance of escrow for software users</td>
<td>55</td>
</tr>
<tr>
<td>When do you need escrow?</td>
<td>56</td>
</tr>
<tr>
<td>Technical considerations</td>
<td>59</td>
</tr>
<tr>
<td>Verification</td>
<td>59</td>
</tr>
<tr>
<td>What should be lodged?</td>
<td>60</td>
</tr>
<tr>
<td>The agreements</td>
<td>61</td>
</tr>
<tr>
<td>User’s duties</td>
<td>62</td>
</tr>
<tr>
<td>Choosing an escrow agent</td>
<td>62</td>
</tr>
<tr>
<td>Advantages of escrow for software owners</td>
<td>62</td>
</tr>
<tr>
<td>Conclusion</td>
<td>63</td>
</tr>
</tbody>
</table>

## 6 OUTSOURCING – Jeremy Newton

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>65</td>
</tr>
<tr>
<td>Defining the services</td>
<td>66</td>
</tr>
<tr>
<td>Design risk</td>
<td>67</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>67</td>
</tr>
<tr>
<td>Pricing and payment mechanisms</td>
<td>69</td>
</tr>
<tr>
<td>The outsourcing life cycle</td>
<td>70</td>
</tr>
<tr>
<td>Other relevant issues</td>
<td>73</td>
</tr>
</tbody>
</table>

## 7 DATA PROTECTION – Andrew Katz

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>74</td>
</tr>
<tr>
<td>What data are covered</td>
<td>75</td>
</tr>
<tr>
<td>Sensitive personal data</td>
<td>76</td>
</tr>
<tr>
<td>Who needs to notify?</td>
<td>76</td>
</tr>
<tr>
<td>How to notify</td>
<td>77</td>
</tr>
<tr>
<td>Data protection principles</td>
<td>80</td>
</tr>
<tr>
<td>Rights of data subjects</td>
<td>88</td>
</tr>
<tr>
<td>Exemptions</td>
<td>89</td>
</tr>
<tr>
<td>Penalties and enforcement</td>
<td>90</td>
</tr>
<tr>
<td>References</td>
<td>91</td>
</tr>
</tbody>
</table>

## 8 DOING BUSINESS ONLINE – Jeremy Newton

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>92</td>
</tr>
<tr>
<td>Information to be provided to clients</td>
<td>93</td>
</tr>
<tr>
<td>Forming contracts electronically</td>
<td>95</td>
</tr>
<tr>
<td>Performance and cancellation</td>
<td>97</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>98</td>
</tr>
<tr>
<td>Marketing communications</td>
<td>99</td>
</tr>
<tr>
<td>Consequences of non-compliance</td>
<td>100</td>
</tr>
<tr>
<td>Other considerations</td>
<td>101</td>
</tr>
<tr>
<td>Appendix: Consolidated information requirements</td>
<td>102</td>
</tr>
</tbody>
</table>
CONTENTS

9 SETTING UP JOINT VENTURES – Andrew Katz 103
  Introduction 103
  Joint ventures and IT projects 103
  Establishing a joint venture 104
  Structure of a joint venture 107
  The operating agreement 112
  Competition law 114
  Appendix: Checklists for a joint venture operating agreement 115

10 CLOUD COMPUTING – Stuart Smith 117
  What is cloud computing? 117
  The services in the cloud 118
  The evolution of cloud computing 118
  Cloud formations 119
  Silver linings and thunder clouds 119
  Data protection and security 122
  Important clauses in a cloud computing contract for services 123
  Conclusion 125

11 OPEN SOURCE SOFTWARE – Andrew Katz 126
  Introduction 126
  What is open source? 126
  The public domain 130
  Open source and communities 130
  Open source software businesses 132
  Running open source in your business 133
  Open source and licensing 134
  Software development in context 137
  Contracting open source projects 137
  Open source software and due diligence 140
  Open source policies and procedures 141
  Open source software: employees and contractors 141
  Open source software and patents 142
  Associated licences 143
  Further information 143

12 WEEE REGULATIONS – Andy Lucas 144
  Introduction 144
  The players 144
  What is WEEE and what do the regulations cover? 146
  Key obligations on IT businesses 149
  Key commercial issues 151
  Further information 152

13 FREEDOM OF INFORMATION – Victoria Hordern 153
  Introduction 153
  Transparency Agenda 154
  Public authorities 154
  A public authority’s obligations 154
  Providing information to the public authority 155
Sara Ellacott is the Senior Legal Director, EMEA Litigation, at Oracle Corporation. Sara advises on issues arising out of IT projects. She has experience of a wide range of dispute resolution procedures, including negotiated settlements, High Court litigation, arbitration and mediation. Sara speaks regularly on issues related to risk and dispute management.

Jeremy Holt is the head of the Computer Law Group of Clark Holt Commercial Solicitors (www.clarkholt.com). He has specialised in IT and ecommerce law for over 20 years. In 2003, Jeremy helped set up, in Swindon, the first museum in the country dedicated to the history of computing. He was for 11 years the Secretary of the Law Specialist Group of the British Computer Society. Jeremy writes and lectures extensively on IT law and contracts.

Victoria Hordern is a senior associate in Field Fisher Waterhouse LLP’s Privacy and Information Law Group (www.ffw.com). She advises the public sector, charities and private companies on compliance with privacy and information law, has provided tailored training on handling exemptions and exceptions under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 respectively, as well as training more broadly on data protection and privacy matters. She has assisted with responses to information access requests (both for those organisations responding to a request and for those affected by the potential disclosure) and is particularly interested in the tension between the privacy and information access regimes.

Andrew Katz is a partner at Moorcrofts Corporate Law, a niche corporate and commercial legal practice based in Marlow, Buckinghamshire, and specialises in technology, media and telecoms work. He trained in London and moved to a large Midlands firm where he became their youngest-ever partner. Andrew was previously a computer consultant and was one of the first people to advise public bodies on data storage and retrieval using optical (CD-ROM) technology, and he became an accredited developer for Steve Jobs’s NEXT computer system. He is currently interested in the legal challenges of open source software and peer-to-peer networking. He has been a member of the board and council of the Telecommunications Industry Association.

Jon Leigh has been Director of Escrow Solutions at NCC Group plc since 2003 where he is responsible for the product development and sales strategies of the Group’s Escrow Solutions division. Jon has been with the NCC Group for more than 20 years having joined the escrow division in 1997 as head of testing.
Previously he was project manager of several European consortium projects to establish internationally recognised conformance testing services. Jon previously worked for Ferranti Computer Systems having graduated from Hull University with a Joint Honours degree in Chemistry and Computing.

**Andy Lucas** is a partner in the Technology Law Group of Field Fisher Waterhouse LLP. He specialises in all aspects of non-contentious computer law. He has acted for both suppliers and customers in numerous large-scale software procurements and is currently an adviser to many government departments on some of their most high profile technology implementations. This advice includes not only the drafting and negotiation of agreements and schedules, but also expert advice on the implementation of the public procurement regulations.

**Jeremy Newton** is a Director of Technology Law Alliance, a specialist IT/outsourcing law firm. He has over 20 years’ experience of IT and outsourcing contracts, both in practice and in-house with Sun Microsystems and on secondment to HM Treasury. Apart from contributing to this book, he is a contributor to *Computer Law* (Oxford University Press), and writes and lectures widely on the subject. Jeremy is also the Secretary of the Financial Services Specialist Group of the BCS, and an active member of the international Technology Law Association (iTechLaw).

**Jennifer Pierce**, a partner in the law firm Charles Russell (www.crlaw.co.uk), advises both customers and suppliers in the UK and overseas in respect of legal issues relating to software, equipment, peripherals and other associated technology as well as internet and data usage. Her clients range from household names to private individuals. Jennifer writes and lectures widely on intellectual property and information technology. She is the joint editor and a major contributor to *Working with Technology: Law and Practice*, published by Sweet & Maxwell, a visiting lecturer of the Queen Mary Intellectual Property Research Institute, and has appeared as an expert on BBC current affairs programmes.

**Stuart Smith** was a solicitor in the Computer Law Group of Clark Holt Commercial Solicitors for three years before joining the Information Technology Team of Bond Pearce in 2011. He advises a range of customers and suppliers of hardware, software and IT services.

**Graham Wood** is a consultant with Curule Consultants Ltd providing specialist advice on intellectual property and information technology law. He spent four years with the National Computing Centre in Manchester where he was a lawyer in the Escrow department. Graham is currently project manager for the introduction of data protection legislation in Bermuda. He speaks regularly and writes for international business publications.
ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions made by the following:

Martin Bazem
Richard Folsom
Peter James
Charlotte Hanham
Dawn Holt
Daniel Hopkin
David Hudson
Nathan Hudson
Nia Hudson
Annette Leigh
Isabelle Katz
Lucy Katz
Oscar Katz
Miranda Mowbray
Antonia Newell
Melanie Newton
Adrian Phillips
Tina Pullen
Sian Rudgard
Christopher Smith
Sally Smith
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AATF</td>
<td>Approved Authorised Treatment Facility</td>
</tr>
<tr>
<td>ADR</td>
<td>Alternative Dispute Resolution</td>
</tr>
<tr>
<td>AE</td>
<td>Approved Exporter</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider/Provision</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BIS</td>
<td>The Department for Business Innovation and Skills</td>
</tr>
<tr>
<td>BPO</td>
<td>Business Process Outsourcing</td>
</tr>
<tr>
<td>BSD</td>
<td>Berkeley Software Distribution</td>
</tr>
<tr>
<td>CAP</td>
<td>Code of Advertising Practice</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CPR</td>
<td>Civil Procedural Rules</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>DCF</td>
<td>Designated Collection Facility</td>
</tr>
<tr>
<td>DMA</td>
<td>Direct Marketing Association</td>
</tr>
<tr>
<td>DR</td>
<td>Dispute Resolution</td>
</tr>
<tr>
<td>DSE</td>
<td>Display Screen Equipment</td>
</tr>
<tr>
<td>DTI</td>
<td>Department of Trade and Industry</td>
</tr>
<tr>
<td>DTS</td>
<td>Distributor Take-back Scheme</td>
</tr>
<tr>
<td>EA</td>
<td>Environment Agency</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EC2</td>
<td>Elastic Compute Cloud</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EEE</td>
<td>Electrical and Electronic Equipment</td>
</tr>
<tr>
<td>EEIG</td>
<td>European Economic Interest Grouping</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>EMAS</td>
<td>Employment Medical Advisory Service</td>
</tr>
<tr>
<td>EMU</td>
<td>Economic and Monetary Union</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FLOSS</td>
<td>Free, Libre and Open Source Software</td>
</tr>
<tr>
<td>FM</td>
<td>Facilities Management</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FOSS</td>
<td>Free and Open Source Software</td>
</tr>
<tr>
<td>FSF</td>
<td>Free Software Foundation</td>
</tr>
<tr>
<td>GPL</td>
<td>General Public License</td>
</tr>
<tr>
<td>HMRC</td>
<td>Her Majesty’s Revenue and Customs</td>
</tr>
<tr>
<td>HSE</td>
<td>Health and Safety Executive</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Right</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>JV</td>
<td>Joint Venture</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LLC</td>
<td>Limited Liability Corporation</td>
</tr>
<tr>
<td>LLP</td>
<td>Limited Liability Partnership</td>
</tr>
<tr>
<td>MIT</td>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>NIEA</td>
<td>Northern Ireland Environment Agency</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OFT</td>
<td>Office of Fair Trading</td>
</tr>
<tr>
<td>OGC</td>
<td>Office of Government Commerce</td>
</tr>
<tr>
<td>OIN</td>
<td>Open Invention Network</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Source Initiative</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PCS</td>
<td>Producer Compliance Scheme</td>
</tr>
<tr>
<td>PFI</td>
<td>Private Finance Initiative</td>
</tr>
<tr>
<td>PI</td>
<td>Performance Indicator</td>
</tr>
<tr>
<td>POBA</td>
<td>Project Open Book Accounting</td>
</tr>
<tr>
<td>PPP</td>
<td>Public Private Partnership</td>
</tr>
<tr>
<td>RSI</td>
<td>Repetitive Strain Injury</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SEPA</td>
<td>Scottish Environment Protection Agency</td>
</tr>
<tr>
<td>SI</td>
<td>Systems Integration</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SSADM</td>
<td>Structured Systems Analysis and Design Method</td>
</tr>
<tr>
<td>TCC</td>
<td>Technology and Construction Court</td>
</tr>
<tr>
<td>TUPE</td>
<td>Transfer of Undertakings (Protection of Employment) Regulations</td>
</tr>
<tr>
<td>UCTA</td>
<td>Unfair Contract Terms Act 1977</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VAT</td>
<td>Value Added Tax</td>
</tr>
<tr>
<td>VCA</td>
<td>Vehicle Certification Agency</td>
</tr>
<tr>
<td>VDU</td>
<td>Visual Display Unit</td>
</tr>
<tr>
<td>WEEE</td>
<td>Waste Electrical and Electronic Equipment</td>
</tr>
</tbody>
</table>
Acceptance Testing  The running of a set of programs, under designated conditions, on a computer before the acceptance of the system by the customer.

Alternative Dispute Resolution (ADR)  A method of settling disputes without resorting to the legal courts. Examples include mediation and expert determination.

Application Service Provider (ASP)  A business that rents out the use of software running on its own servers to remote customers using a web-based connection to access the service.

Business Process Outsourcing (BPO)  The subcontracting by a business of some or all non-core business activities allowing it to concentrate on its principal activities.

Change Control  The process for changing customer requirements during a project.

Civil Procedure Rules (CPR)  The rules of practice and procedure that apply to the conduct of civil litigation in England and Wales.

Claimant  The person who brings a legal action before the courts in England and Wales (formerly called the plaintiff).

Competition Law  The law relating to the abuse of market power by buyers or sellers such as price fixing, cartel and the abuse of monopolies (also called anti-trust law).

Cookie  A tag sent by a server to an internet user that is sent back to the server each time the internet user accesses that server.

Copyright  A right for the creator of an original literary, dramatic or musical work to prevent the copying of such work. The right lasts for the life of the creator plus 70 years. No registration is required in the United Kingdom.

Customer Relationship Management (CRM)  An integrated information system that is used to run the pre-sales and post-sales activities of a business.
**Database Right**  A right under European law for the creator of a database to prevent the copying of such a database for 15 years. No registration is required.

**Data Controller**  A person who holds information about a living individual either on a computer or in structured manual records.

**Data Subject**  A living individual about whom another holds information on a computer or in structured manual records.

**Decompiler**  A program that generates high-level source code from machine code.

**Design Right**  A right to prevent the copying of the external appearance of a manufactured article. Such protection can last for 25 years from the time of registration.

**Display Screen Equipment (DSE)**  Computer monitors and any other screens that display text, numbers or graphics.

**Dispute Resolution (DR)**  The settling of an argument between two parties.

**Distance Selling**  A sale where the buyer and seller do not meet face to face, for example sales via the internet, sales catalogue, fax or telephone.

**Domain Name**  The address of an internet site, including a host name, subdomain and domain, separated by dots (e.g. www.bcs.org.uk).

**Due Diligence**  The process of investigation into a business or intellectual property rights before their purchase or entry into a contract relating to them.

**Economic and Monetary Union (EMU)**  The consolidation of European currencies into the monetary unit of the euro that began in 1999.

**Enterprise Resource Planning (ERP)**  A software system designed to support and automate the business processes of medium and large businesses.

**Escrow**  The process of an independent third party holding something in readiness for a possible event. One example is an escrow agent holding the source code of software that would be released to a customer if the supplier became insolvent.

**European Economic Area (EEA)**  The countries of the member states of the European Union, plus Iceland, Liechtenstein and Norway.

**Facilities Management**  The management of a user’s computer installation by an outside organisation.

**Force Majeure**  A supervening event, such as a general strike or outbreak of war, that a contract provides will validly prevent one party to the contract from carrying out its obligations to the other party.

**Framing**  A method of including one page from the web within what appears to be another page.
**Information Commissioner**  A government official in the United Kingdom who holds a register of data controllers and enforces data protection legislation (formerly known as the Data Protection Registrar).

**Information Technology (IT)**  The application to information processing of current technologies from computing, telecommunications and microelectronics.

**Intellectual Property Right (IPR)**  Legal rights for the owners of inventions, designs and other materials to control their publication or use. Examples include patents, trade marks and copyright.

**Interface**  Software that enables a program to work with the user, with another program or with the computer’s hardware.

**Joint Venture (JV)**  An arrangement between two (or more) businesses under which they work jointly for a common purpose.

**Linking**  In a web page, the process of using a hypertext connection or highlighted piece of text to move the reader to another page.

**Metatag**  A tag that identifies the contents of a web page (such as a keyword for search engines).

**Moral Right**  The right of the author of a copyright literary work to be identified as its author and for the work not to be subjected to derogatory treatment.

**Non-Disclosure Agreement (NDA)**  A contract between two parties under which one (or both) will keep various matters confidential.

**Object Code**  The list of machine code instructions produced by passing the source code of a computer program through a compiler or an assembler.

**Original Equipment Manufacturer (OEM)**  A misleading term for a business that repackages material made by other businesses. Unlike a value-added reseller, an OEM does not necessarily add anything except their name to a product.

**Outsourcing**  The assignment of tasks, such as payroll and data entry, to independent contractors outside the business.

**Passing Off**  The action of a business giving the impression that it is (or is linked to) another business. This may be by the use of a similar name or other marketing get-up or the appearance of a product.

**Patent**  A right granted by the state to an inventor of a new invention that, in return for a full public disclosure of the invention, the inventor will have a monopoly over the exploitation of the invention for up to 20 years.

**Personal Data**  Information about a living individual.

**Repetitive Strain Injury (RSI)**  Damage to the hands, arms, neck, back or eyes due to computer use.
**Respondent**  The person against whom a legal action is brought in the courts in England and Wales (formally called the defendant).

**Sensitive Personal Data**  Information about a living individual that relates to their race, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life or criminal record.

**Service Level Agreement (SLA)**  A contract between two organisations about the quality of service to be provided by one to the other.

**Source Code**  A textual description of a computer program, written in a programming language.

**Spam**  Email that is not requested by the recipient (the word is believed to have been taken from a repetitive Monty Python song).

**Specification**  In relation to software, a description of the operating environment and proposed features and functionality of a new program; in relation to computer hardware, information about its capabilities and features.

**Structured Systems Analysis and Design Method (SSADM)**  A technology that is widely used for the analysis and design of IT systems.

**Subject Access Request**  The right under data protection legislation in the United Kingdom for an individual to ask a data controller what information it holds about that individual.

**Systems Integration (SI)**  The combining of different programs or components into a functional system.

**Systems Procurement**  The choice and purchase of a new computer system.

**Technology and Construction Court (TCC)**  A division of the High Court of England and Wales that deals with technically complex legal claims.

**Trade Mark**  A graphic sign that is capable of distinguishing the goods or services of one organisation from another. A trade mark can last indefinitely (including where it has been registered).

**Transfer of Undertaking (Protection of Employment) Regulations (TUPE)**  Legislation in the United Kingdom that preserves the employment rights of individuals upon the sale of the business in which they work.

**Value Added Tax**  A sales tax applied in the United Kingdom.

**Verification**  The process of confirming that a result is correct or that a procedure has been performed.
USEFUL WEBSITES

www.bcs.org/content/conWebDoc/1562  BCS Professional advice register
www.worklink.org.uk  Worklink service
www.bsi.org.uk  British Standards Institution
www.cedr.com  Centre for Effective Dispute Resolution
www.dma.org.uk  Direct Marketing Association
www.fpsonline.org.uk  Fax Preference Service
www.hse.gov.uk  Health and Safety Executive, Information line: 08701 545500, Publications: 01787 881165
www.informationcommissioner.gov.uk  Information Commissioner, Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Telephone: 01625 545700, Email: mail@notification.demon.co.uk
www.iso.org  International Organization for Standardization
www.itechlaw.org  International Technology Law Association
www.mpsonline.org.uk  Mailing Preference Service
www.mca.org.uk  Management Consultancies Association
www.the-stationery-office.co.uk  Stationery Office Ltd
www.tpsonline.org.uk  Telephone Preference Service
This book is a practical guide for managers dealing with computer-related issues. The authors felt the law in England in this area should be summarised in a way that is easy to understand. Things have changed so much and so quickly since the first edition that it was felt that the book should be updated to reflect these changes.

The book is not designed to be read from cover to cover. Readers can dip into the various self-contained chapters to find the answers that they seek. It provides practical advice on the appropriate steps that should be taken.

We hope that it will be a valuable guide to managers as well as being of interest to IT professionals, legal practitioners and students.

Jeremy Holt and Jeremy Newton
This chapter outlines the contents of a contract and lists the matters that should be covered by different types of contract. If you do not have time to read all of the chapter, the appendix to this chapter lists the main points that you should consider.

INTRODUCTION

Pity the unfortunate manager. It has been bad enough trying to get the computer project organised. Now, possibly at the last moment, the contracts have arrived, some with print small enough to make the reader go blind. The manager suspects (rightly) that these contracts are one-sided in favour of the supplier, but knows that the project will only proceed if those contracts (or something similar) are signed. How does the manager work out what needs to be done and from whom advice can be obtained? This chapter provides a practical framework of help in this situation. If you are looking for an academic guide to computer contracts, you must look elsewhere.

PARTS OF A CONTRACT

The first point to consider is the form that contracts normally take. At its simplest a contract consists of:

- the date on which the contract was entered into;
- the names and addresses of those entering into the contract;
- a short description of what the contract is about (generally entitled ‘Background’, ‘Recitals’ or even, regrettably, ‘Whereas’);
- definitions of terms used in the contract;
- what the supplier is going to do for you;
- what you must do for the supplier;
- what you must pay the supplier.
Do not forget we are engaged in contract first aid here. If all else fails, concentrate on what the supplier is going to do for you and what you are expected to pay. Standard terms that are not specific to this individual contract (what lawyers call 'boilerplate') are generally grouped together at the end of the contract. A list of the more important boilerplate clauses is shown in the box.

### IMPORTANT BOILERPLATE TERMS

**Force Majeure** – this says that neither party shall be liable for any failure to perform the contract because of circumstances beyond its control such as an Act of God, fire, flood etc. This is likely to be invoked by the supplier more than the client. This clause effectively absolves the supplier from responsibility, so the circumstances in which it can be invoked should be checked carefully to ensure that they are no wider than is reasonable.

**Entire Agreement** – this says that the entire agreement between the parties is set out in the written contract and so no other previous representations by the supplier may be relied upon by the client. This is a reasonable principle, but the client must make sure that the contract deals with all the important points.

**Governing law and jurisdiction** – ideally this should be English law enforced in the English courts. An alternative is to agree arbitration, and as this happens behind closed doors then the supplier may worry less about bad publicity.

It is sensible to agree an alternative dispute resolution procedure (such as mediation), which must be carried out before any dispute is referred to the courts or to arbitration.

### WHO ARE YOU GOING TO CALL?

You are not going to be able to do all this on your own. You are going to need professional advice. Computer law is a specialist area, and a rapidly changing one (it did not even exist as a field of legal practice 25 years ago). The correct advice from a lawyer experienced in this field can save a great deal of trouble later. The function of a good lawyer is to assess risk, help the client to understand the level of risk and then reduce it.

There are two directories of lawyers that you might like to consult: Chambers’ Guide to the Legal Profession and The Legal 500. New versions are published each year and each has sections on lawyers who specialise in computer law (sometimes called ‘information technology law’). These two books can generally be found in the reference section of a public library, and can also be searched without charge on the web. Alternatively, you can ring the Law Society or the Society for Computers and Law for suggestions of lawyers who work in this field and who could help you.
CHECKING OUT THE SUPPLIER

It may seem like an obvious point but make sure that you know who you are dealing with. This will mean, at least, doing a company search. A credit check would do no harm. As the Army maxim has it ‘time spent on reconnaissance is seldom wasted’. If you discover that the supplier company was set up last year and has an issued capital of £1 you may like to consider asking for a guarantee of the contract from a more substantial body. Business is not all about making a rational decision on paper. Do you get good vibes from the supplier? On small things, do they do what they say that they will do? If, for whatever reason, you do not trust them, do not go ahead with the contract under any circumstances because this will only lead to worry and tears later.

LETTER OF INTENT

The supplier may ask for a letter of intent from you because it may need to start work on your project before contracts are signed, and because the negotiation and agreement of the contract terms may take a little while. Alternatively, you may like to suggest one so that you are not pressurised into signing the contracts before you have gone through them properly. A letter of intent is no more than written confirmation from you of your intention to enter into a contract with the supplier. What is critical, however, is that the letter of intent from you to the supplier must contain a statement that the letter is not intended to be contractually binding, otherwise you may unwittingly enter into a contract earlier than you intended. Where there is a non-binding letter of intent and the supplier, at your request and to save time, starts work on the project, it is reasonable for the supplier to ask to be paid for this initial work carried out regardless of whether the project proceeds or not. There are two important matters to agree. The first is the rate for the job (e.g. a daily rate – work normally starts under a letter of intent on a time and materials basis; the definitive contract may include a fixed price for a specified deliverable). The other is an overall cap on your liability to the supplier for this work. This obligation to pay the supplier should be contractually binding (unlike the rest of the letter of intent).

THE SUPPLIER’S TERMS

There is, of course, no obligation on you to accept that you will purchase a new computer system on the basis of the supplier’s terms.

You could propose your own terms entirely – this is certainly an approach taken by large organisations with extensive experience of computer contracts. However, it is generally better to use the supplier’s contract terms (unless they are completely unreasonable) as a start and amend them to your satisfaction. It is a good idea to ask for the supplier’s proposed terms at as early a stage as possible. Do not wait until you have told them that they have been awarded the contract.
WHAT CONTRACTS ARE THERE LIKELY TO BE?

Any computer system will require the purchase of hardware (e.g. servers, PCs, printers etc.), software (the application software and the operating system software) and services (such as support and maintenance). When computers first started to be widely and routinely used in business life about 30 years ago the emphasis was very much on the hardware, which was comparatively unreliable. Nowadays the emphasis is much more on the software and services. It is normal to decide upon the software first and then to choose the appropriate hardware. If the contract relates to the procurement of a new system, the reader is referred to Chapter 2. The rest of this chapter deals with the purchase or licence of individual services or components.

Contracts for consultancy services
Long before the order for a new system is placed, the client may enter into a consultancy contract, perhaps relating to a feasibility study, analysing requirements, recommending a system to meet those requirements, helping select the appropriate suppliers, or assisting with preparation of an invitation to tender. A large part of the work carried out in the computer industry is under consultancy contracts. The client may need help on a one-off basis or require skills that do not exist within the client’s workforce, so there is a need for an outside consultant to carry out the work. Sometimes the consultancy arrangement is dealt with by means of an exchange of letters; a formal consultancy agreement, however, is a better option for both parties.

- **Defining the deliverables** One of the most important issues that must be dealt with in such a contract is a detailed description of what the consultant is expected to do. If the description is loose or inexact, this can give rise to differences between what the client is expecting to receive and what the consultant is expecting to deliver. This can, predictably, lead to disputes. So defining the nature and quality of the deliverable is particularly important.

- **Payment arrangements** The payment to the consultant by the client may be on a time and materials, fixed price or estimated maximum price basis. It is an aspect of consultancy that the amount of work required will be uncertain. The disadvantage of a fixed price payment mechanism (as with any other contract) is that the consultant will inevitably include a contingency element in the price quoted. If the consultancy can be broken down into a series of stages, payment against milestones will allow each party to gauge how the work is going.

- **Copyright and confidentiality** Copyright will almost always be an issue. Broadly speaking, there is a simple choice as to how the parties deal with ownership of copyright in the consultant’s work. Either the consultant can assign to the client all intellectual property rights in whatever is produced (provided that the consultant has been fully paid) or the consultant can grant a perpetual licence to the client to use such intellectual property rights for the purposes of the client’s business (see Chapter 4 for more details). It goes almost without saying that the consultant should be obliged to keep confidential any information given by the client about its business. It is important to note that if there is no agreement with a consultant about copyright the
client does not automatically get ownership of such copyright. It stays with the consultant (although there may also be an implied licence for use of the copyright by the client).

The problem is that once a consultant has carried out an assignment for one client in an industry, the consultant may be ideally placed to carry out assignments for other clients within that same industry. Sometimes, therefore, clients go further and stipulate in the contract that not only must their own information be kept confidential, but also that the consultant must agree not to carry out projects for the client’s competitors for a period (perhaps a year) after the work is completed.

- **Insurance** In order to provide peace of mind to the client, the client may require the consultant to take out professional indemnity insurance. This is still relatively inexpensive because, in practice, it is rare for claims to be made under such policies.

- **Key personnel** The client will want to know the identity of the staff who the consultant will be using to carry out the work. It is normal for the client to be able to veto any staff members of whom they disapprove for whatever reason.

The client will want to retain the right to terminate the consultancy contract if the consultant is guilty of serious misconduct or any other conduct likely to bring the client into disrepute.

**Contracts for hardware purchase**

Computer hardware is much more reliable than it used to be, so contracts for the supply of hardware are not generally contentious. A hardware purchase contract requires the following details:

- A detailed description of the hardware (this is likely to be in a schedule).
- A warranty about the quality of hardware (normally this warranty applies for a year after acceptance of the hardware by the client).
- Delivery dates.
- Price.
- Acceptance testing.
- Future maintenance.
- Training.

Problems can arise if the hardware is not large enough for anticipated demand, and with the integration of hardware (such as servers and printers), which may have been supplied by different suppliers. In many cases the cost of the hardware is not a large percentage of the total system cost. Profit margins on hardware are relatively low, so the software supplier may be relaxed about whether the client obtains the hardware from the software supplier or from a third-party supplier. It is always worth asking the software supplier to quote for supplying the hardware because they may have better bargaining power than you would have on your own. At the end of the day, the two most important matters in a contract
for hardware are to check that there is an exact description of what you are buying and that there is an obligation on the supplier to repair or replace it if it does not work properly.

Contracts for hardware maintenance
Hardware maintenance is more of a commodity than software maintenance and there are likely to be more alternative suppliers for the maintenance of hardware (and so prices are keener). There are two different types of hardware maintenance: preventive maintenance and corrective maintenance. Preventive maintenance covers the regular testing of the hardware (e.g. once every six months) before any problem is reported. Corrective maintenance deals with faults as and when they arise, normally in response to a service call from the client. With corrective maintenance the key element is the response time: how quickly will the supplier start to respond to the problem once it is reported? This is generally within a fixed number of working hours. For example, an engineer may have to arrive at the site no more than eight working hours after the problem has been reported by the client. This does not mean that the engineer will solve the problem within eight hours, merely that a start will be made to try to solve it. Sometimes online diagnosis is used: the client’s hardware is linked by telecommunications to the supplier who can solve the fault at a distance. (The impetus for online diagnosis came from the USA where the distances were so great it was often not practicable to send an engineer in person.) Payment for hardware maintenance is generally made in advance on a monthly or quarterly basis. The annual amount varies but can often be between 10 per cent and 15 per cent of the list price of the hardware. Other points that will normally be covered in a hardware maintenance contract include a right for the supplier to:

- make an additional charge for frivolous or unnecessary call outs;
- increase the charges from time to time, perhaps in accordance with a recognised index (such as the Consumer Price Index); and
- refuse to cover equipment that is more than five years old or which is past its reasonable working life.

The client will be under an obligation to:

- pay for corrections that are not caused by the equipment itself (e.g. faults arising from electrical fluctuations);
- notify the supplier of problems promptly after they arise (so that time does not make them worse); and
- allow the supplier reasonable access to the equipment.

Contracts for software licences
At its simplest, any contract for software should allow you to use the software in the way that you envisaged without the risk that anyone can come along later and say either that you can not use it any more or that you have got to pay more money. It follows, therefore, that one of the first checks that you should do is to confirm that the software supplier either owns the copyright in the software or has the right to license it to you. It is a feature of the computer industry that
software is often licensed to end-users by organisations other than the actual owner (for example it may be sub-licensed by a distributor or channel partner). You should not put up with oblique answers to your demand for evidence that the supplier can license the software to you. They should be able to produce it immediately.

At this point you may wonder why a licence agreement is necessary at all. Why can the supplier not simply sell you the software? The supplier is not actually selling you ownership of the software (because they would like to continue to license it to other people). The licence is only a permit for you to use the software for your own purposes. This leads onto the next important point. You must check in the licence agreement to whom the software is licensed and for what purpose. Is the software to be licensed to your particular company or can it be used by the whole of your group (in which case the software supplier will want more money)? Alternatively, is the software to be restricted to a limited number of users and, if more than that number use it, then do you have to pay an additional licence fee? This is one of the oldest tricks in the software supplier’s book. They allow the client to sign up for a very limited number of users and then the supplier makes a considerable profit from the additional users who will almost inevitably be required by the client later. The supplier, of course, responds that this simply reflects the extra use (and, as a result, commercial benefit) that the client is making of the software.

It is also possible that at some time in the future the client may want to outsource its computer operations (see Chapter 6). Consequently, provision for the transfer of the licence from the client to an outsourcing company should be made in the original software licence agreement.

**Contracts for software maintenance**

No software of any complexity is ever free from errors. The older the system the more likely that it will need maintenance. Furthermore, if a system is installed in a rush (e.g. to meet a particular deadline), then it is likely not to have been tested properly and so require more attention after it has been installed. In some ways, future charges for maintenance are the icing on the cake for software developers. If they can generate sufficiently wide sales of the software, then support fees can be guaranteed for years to come. It is important for managers to be aware of this as three-quarters of a budget for software may be for future software maintenance. The client is well advised to check how wide the maintenance supplier’s client base is (the wider the better) and to look at the offices from which the supplier will be providing the support (and how many people will be providing such support). The maintenance contract will almost certainly be prepared by the supplier. Some of the most common provisions are discussed below.

- **Charging arrangements** – Sometimes the cost of the software licence is bundled with the first year’s maintenance charges. One interesting point is from when the support charges should run. Some clients argue that they should start from the end of the warranty period for the software. However, it is now generally accepted that they should begin from acceptance of the system because warranty and support are separate matters.
• Scope of maintenance services – Maintenance or support will normally cover the investigation by the supplier of errors in the system reported by the client as well as updated documentation and telephone or, more frequently nowadays, online advice. It will, in most cases, cover updates to the software (but not necessarily new versions of the software). The client may want to categorise different kinds of problems into those that could be critical for its business and those that are no more than an irritation and could be dealt with next time a new version of the software comes out. The supplier’s response time will be different depending on the severity of the problem. The supplier will not normally commit to a fix within a particular period, only that they will start to fix it within a particular time.

• Exclusions from scope – The maintenance supplier will also be keen to list in the contract what maintenance does not cover. Most of these exceptions are reasonable. They generally include problems arising from changes to the software made by people other than the supplier, incorrect use of the software by the client or events beyond the control of the maintenance supplier such as hardware failure, fluctuation of electrical supplies or accidents. Normally, the maintenance supplier will still seek to help the client where the exceptions apply (indeed there should be a contractual obligation to do so). However, the supplier may want to make an additional charge for such work and will not guarantee any particular recovery time. From the supplier’s point of view it becomes difficult to manage support if the client base is using a number of different versions of the software. Consequently, the supplier normally restricts support to the latest two versions of the software and will refuse to support earlier versions.

• Charge increases – The client will want to ensure that the maintenance charges will not rocket up. One means of doing this is to tie the maintenance charges to a percentage of the list price of the software (e.g. 10–15 per cent), but of course the supplier has control over the list price. Alternatively, any increase in maintenance charges can be tied to a recognised index. Clients sometimes suggest the Consumer Price Index. However, suppliers (who know that increases in salaries are generally greater than increases in retail prices) prefer to tie them to an earnings index. There is some logic in this because the bulk of the supplier’s expenses are salaries.

• Payment arrangements – Payment is almost invariably made in advance. In the past, it was for a year, but now it is more commonly paid three months or a month in advance. This is so that if the supplier goes into liquidation the client will not have overpaid very much and the client can also swiftly withhold the payment of maintenance charges if there is a problem with the service provided.

• Termination – It is important for the client to look at the termination clauses of the contract offered by the supplier. The client will want to know how much notice they have to give to end the maintenance contract. This is often three or six months. It is a good idea for the client to ask the supplier to commit on its part to supply maintenance (if the client wants it) for the potential life of the software (e.g. five years).
Contracts for software development

Software will often need to be customised for the client by the supplier. However, this is really only a tinkering with the main programs. In certain circumstances, it may be necessary for the client to commission new software because there is no existing software that meets the client’s needs. Contracts for software development are complex and it is wise for the client to seek professional advice both about the specification for the software and the contract under which the software will be written. This is all the more important because software development projects have a reputation for taking longer, and for costing more, than originally forecast. Consequently background research by the client into the proposed supplier is particularly worthwhile. Pricing for the project will be either fixed price or time and materials. Payments will normally be made conditional upon project milestones being reached. The client will seek to ensure the quality of the software product delivered by the supplier by requiring acceptance tests of the software and a warranty from the supplier that the product will be in accordance with the agreed specification. A thorny question is whether the client should own the copyright in the software program produced. At first glance, it might be thought that this should obviously belong to the client who has paid for it. However, all the client needs is to use the software; the client needs neither to own it nor to develop it further. There is a benefit to the client in the supplier having an incentive to carry out further development of the software program and license it to other clients. The original client does not then pay the total cost of all the subsequent fixes and has the benefit of the faults reported by other users. If the supplier becomes insolvent, then the client needs access to the source code of the software in order to maintain it. For this reason the client should require the supplier to put a copy of such source code in escrow with an independent third party so that it is available if required (see Chapter 5). The supplier will normally provide a warranty that defects in the software reported within a particular length of time after the start of its use will be rectified. This is frequently 90 days after acceptance of the software by the client.

Service level agreements

Service level agreements (SLAs) are critical to the computer industry, but they are rarely fully understood. Under an SLA, a supplier undertakes to supply a service to a client at a particular level.

Perhaps because so few lawyers have a reasonable working knowledge of the computer industry, SLAs are often drawn up by the participants without legal advice.

A service level agreement should cover the following:

- The service required (i.e. what the client wants and what the supplier is prepared to commit to supply).
- Quality standards (i.e. the standards or levels the supplier must achieve), such as host/terminal response times, batch processing times, ‘uptime’ or processor availability, by specifying what? when? how? and by whom?
- Deliverables (e.g. regular reports).
• The consequences of failing to meet service procedures or standards (e.g. compensation in the form of service credits).
• Procedures for the client to monitor performance of obligations by the supplier.
• Procedures for change control (i.e. changing part of the service that is being provided by the supplier under the agreement).
• Terms dealing with access to, and security of, the client’s site and data.
• A procedure for disaster recovery (either upon a system failure or a catastrophe).
• The agreed frequency of meetings between the client and the supplier to review the supplier’s performance of the agreement, properly minuted with subsequent action plans and awards of priority.

Ideally, an SLA should be a self-enforcing agreement within a continuing relationship. There should be no need for either side to litigate and changes required should be dealt with through a change control procedure. In some ways, the process of creating the SLA is as valuable as the agreement itself. SLAs can be between different businesses or between different parts of the same organisation (such as the IT department and its users). Facilities Management Agreements, Software Maintenance Agreements and Managed Data Network Agreements are all examples of SLAs. Alternatively, the SLA may be one aspect of a larger agreement for services, that is it may be the schedule that stipulates how well the services have to be provided and what happens if the supplier does not provide this.

What form should a service level agreement take?
At its weakest, an SLA may be a simple oral understanding, documented by an exchange of letters. The best form is a formal legal agreement with the technical procedures and specifications annexed as separate schedules.

What happens if the terms of a service level agreement are broken?
If the breach is fundamental, the party not in breach will be entitled to terminate the agreement and sue for the loss suffered as a result of the breach. In other circumstances there will be a system for measuring breach and apportioning cost. These systems range from an event-based system (i.e. if... then...) to a more sophisticated system of ‘failure points’ (i.e. if there are more than five examples of... then...). The functions of such compensation systems vary from simply drawing attention to a problem to compensation for loss. Compensation for loss is difficult to quantify and, if it is excessive, will be unenforceable by a court. In practice, the right to withhold payment is a valuable weapon. The end (or slowing down) of payments by the client into the supplier’s accounts department is likely to put pressure on the supplier. Escalation clauses are undervalued and should be more widely used. These provide for a problem to be escalated up the various tiers of management on both sides if it cannot initially be resolved. Even the best SLA does not last for ever and there must be a procedure for orderly termination and (if necessary) migration from the supplier’s system to another system.
The failure to include such clauses was a frequent weakness of early SLAs. Migration is critically important in relation to facilities management contracts and, as a rule of thumb, a year is generally allowed for this. The supplier should also be required to provide all reasonable assistance to the client with the migration to another system.

**Contracts relating to cloud computing**

Cloud computing is sometimes called software as a service. It appears set to revolutionise the computer industry over the next few years. See Chapter 10 for a description of what cloud computing is and the contracts that you are likely to need.

**APPENDIX: MAIN POINTS OF AN IT CONTRACT**

Read this on its own if you have not got enough time to read the rest of this chapter. But read it carefully.

- Make sure that you know exactly what you want and what is achievable because if you do not know, then you are not going to get the contract right. (Among the most common causes of computer project failure are unclear client requirements and unrealistic client expectations.)

- Make sure that all the prospective suppliers sign a confidentiality agreement with you. If you are going to give them a detailed functional specification of what you want and information about your business you do not want there to be any question of that confidential information being obtained by your competitors.

- Beware of falling into the trap of entering into a contract before you intend to. There are no legal formalities in this country about entering into a computer contract, so make sure that all pre-contract correspondence is headed ‘subject to contract’. If you leave discussions about a written contract incomplete (e.g. lots of draft contracts sent between you and the supplier but nothing ever signed), then a court is likely to take the last undisputed draft as being the basis of the contract between you and the supplier.

- If a particular point is important to you make sure that you get it in writing from the supplier. It may well be that an aspect that is critical to you is not dealt with in the supplier’s draft contract at all. If so, you must, for evidence’s sake, get it in writing from the supplier. An ordinary letter from the supplier is sufficient provided that it is either referred to in the main contract or, possibly, included as a schedule or as an attachment. If the supplier drags its heels and, despite repeated requests from you, refuses to confirm a point in writing, you should write to the supplier saying that you are only entering into the main contract on the basis that this point is agreed. If the matter ever goes to court the production of your letter will be of great assistance to your case.

- Make sure that you get the supplier to agree to supply support and maintenance for the products purchased for a decent length of time (e.g. five years). You do not want the supplier cancelling support after a couple of years just when your new system is working well. Note that you do not have to commit
to take the support and maintenance for five years: ideally your commitment should be on a year by year basis. It is just that the supplier agrees to make the support available to you for at least five years if you want it.

• Make sure that you order enough training. One of the most common reasons for the failure of a computer project is inadequate training. It is sadly all too common that, if there is an overspend in other areas, the amount budgeted for training is cut. As a rule of thumb, roughly 20 per cent of a project's cost should be spent on training. If it is substantially less than that you should ask why.

• Make sure that the procedure for acceptance testing is known and agreed. If this has not been sorted out in the contract, how are you going to stop a bad system from being installed? In the past, the test data were generally supplied by the client; nowadays it is more acceptable for it to be provided by the supplier.

• Make sure that you can get access to the source code of the software programs supplied if the supplier either goes into liquidation or stops supporting the software. Ideally, this source code should be deposited with an independent third party (see Chapter 5) and kept updated by the supplier as each new version comes out.

• Finally, never forget that the contract is a delivery mechanism for ensuring that a project is completed in the right way at the right time by the right person and for the right price. No more, no less.
Terms like ‘computer contract’ or ‘system procurement contract’ cover a broad range of commercial transactions, from the purchase of a single CD-ROM from a high street retailer through to multimillion pound agreements for consultancy or outsourcing services. This chapter outlines the legal issues that need to be addressed in any contract of this type, using examples from actual case law to illustrate the kinds of dispute that commonly arise in relation to systems procurement, and discusses how the process of drafting and negotiating the agreement can be used to prevent some of the most common problems.

**THE NEGOTIATION PROCESS**

The function of a written contract is to record the terms governing the supply of goods and services. In the absence of a clear, express understanding between the parties, certain terms may be implied into the contract as a matter of law, for example, that products will be delivered within a ‘reasonable’ time and that they will be of ‘satisfactory’ quality. The main terms that can be implied into a contract as a matter of law are summarised in the box.

**TERMS IMPLIED BY LAW**

Certain terms may be implied into a contract as a matter of law: this means that the contract will include these provisions automatically, unless the parties expressly agree to exclude them. The main implied terms are summarised below.

**Title** – All contracts of sale include an implied term that the seller has the right to sell the goods in question [Sale of Goods Act 1979 s.12(1)]. If the seller fails to transfer ownership (e.g. because the goods are subject to the rights of some third party, such as a bank), then it will be in breach of this term and the buyer may reject the goods and recover the price, plus damages.

**Quiet possession** – This right is, in effect, a promise by the seller that no person will in the future acquire rights over the goods and enforce them against the buyer [Sale of Goods Act 1979 s.12(2)]. If this should happen (e.g. because the use of the product turns out to infringe some third-party intellectual property right), then the buyer will be entitled to claim damages. In the worst case, where the third party exercises its rights in such a way as to prevent the buyer using the goods at all, the
buyer’s damages will be assessed as the cost of buying a replacement, in effect returning the original purchase price.

**Correspondence with description** – Goods must correspond with the description given by the seller (Sale of Goods Act 1979 s.13). This description can take many forms: a standard printed specification, an agreed user requirements specification, and even claims made by the sales force or set out in the manufacturer’s publicity material.

**Quality and fitness for purpose** – Goods must be of satisfactory quality and reasonably fit for their purpose (Sale of Goods Act 1979 s.14). ‘Satisfactory quality’ means that the goods meet the standard that a reasonable person would regard as satisfactory, taking account of any description of the goods, the price (if relevant) and all the other relevant circumstances.

**Reasonable care and skill** – The law also implies a term into contracts for services (such as consultancy, development or support), to the effect that the services will be provided with reasonable care and skill (Supply of Goods and Services Act 1982 s.13).

Apart from the above terms, which are implied as a matter of statute law, terms may also be implied from the facts and circumstances of the particular contract, if they are necessary to give ‘business efficacy’ to the contract.

However, given the vagueness of the implied terms and the unpredictability of their legal interpretation, any prudent buyer or seller of IT systems will prefer to ensure that the parties’ intentions are recorded as clearly and unambiguously as possible.

The negotiation process that leads to the written contract should help ensure that the parties understand each other’s expectations and commitments.

Many IT projects fail precisely because the parties do not exercise sufficient care to ensure that their expectations match, and often because of an uncritical acceptance by the customer of the supplier’s standard terms of business (or indeed, by the supplier of the customer’s standard procurement contract).

Any well-drawn contract will have provisions relating to three broad categories of expectation. The aim of the negotiation process is to ensure that no essential terms are missing from the final agreement, and this chapter will address each of the categories in turn:

- **Contract mechanics** – who delivers what, and when?
- **Commercial highlights** – what is the price, who owns the resulting intellectual property rights, and what warranties are given in respect of the system?
- **Problem management** – what happens if the project goes wrong and what remedies are available?
BEWARE THE STANDARD CONTRACT

The dangers of agreeing unquestioningly to the standard supply terms (or, for that matter, to a client’s standard terms of procurement) are illustrated by the case of Mackenzie Patten v. British Olivetti.

A law firm bought an Olivetti computer system to run their accounts. They discussed their needs with the salesperson and signed up to Olivetti’s standard terms. These dealt only with the system’s technical performance: they did not address certain other important issues that had been discussed between the parties.

In the event, the system proved unsuitable for the firm’s purposes: it was slow, difficult to use, and could not expand to cope with new business, but none of these matters was dealt with in the written contract. Even though a court found that Olivetti was bound by its salesperson’s claims that the system would be suitable for the law firm’s needs, the firm had by that stage expended significant time and money in the litigation and still had to find a replacement system.

Put another way, ‘standard’ forms are only suitable for entirely ‘standard’ transactions, and will often fail to address some essential point that the parties had in mind for their particular deal.

CONTRACT MECHANICS

Principal obligations
An IT contract need not be a complex document. It does not even need to be in writing, though a written document is clearly desirable to record fully each party’s commitments to the other. In the simplest case, however, a written contract need say no more than this: that the supplier will provide a system X computer to the client; and that the client will pay £Y to the supplier.

That is the essence of the commercial relationship and there is nothing else (from the strict legal point of view) that requires to be said. However, if the aim of the contract process is to ensure that the project goes ahead smoothly and with the minimum scope for disagreement between the two sides, the contract should be considerably more specific in terms of what is being delivered, when and how.

Specification
A clear specification is the foundation stone of a successful systems supply contract. Although the law implies a term into a contract that the system will conform to its description and be of satisfactory quality, this is no substitute for ensuring that the supplier and the client agree (and document, in as detailed a manner as possible) exactly what is to be provided and the performance and quality standards to be achieved.
Every system supply contract should, accordingly, include a detailed specification setting out:

- the required functionality (what the system is required to do);
- performance targets (how well it is supposed to do it);
- compatibility requirements for interfaces with other systems.

The need for a formal system specification

The legal implications of not developing a proper specification are illustrated by the case of Micron Computer Systems Ltd v. Wang (UK) Ltd.

One of Micron’s complaints against its supplier was that the Wang system did not provide ‘transaction logging’. The judge observed that ‘the acknowledged absence of a transaction logging facility is not in reality a fault in the system that was sold. Micron can only complain about its absence if Micron can establish a contractual term … to the effect that the system included such a facility. In order to make good its case in transaction logging, Micron must therefore establish that they made known to Wang that they required such a facility’.

The judge found that Micron had not made its requirement for transaction logging clear to Wang and accordingly that part of Micron's case failed.

Timetable

The process of preparing the specification should enable the parties to assess the likely timescale for the project and to prepare a project plan setting out key deliverables (or ‘milestones’) and their expected dates. In almost all major systems implementations, staged payments will be triggered by the achievement of individual milestones. It is, accordingly, essential that these are identified with as much precision as possible and generally reflect the terminology of the contract.

The buyer will usually have in mind a timescale within which the system should be provided, although the sophistication of the timetable will vary according to the complexity of the project and how closely the payment arrangements are tied into the achievement of specific milestones.

Delivery

Although the law provides for an implied term that goods will be delivered ‘within a reasonable time’, delivery arrangements should always be dealt with expressly. From the point of view of contractual certainty, the ideal approach is for the contract to set out specific delivery dates, but it should also go on to deal with the ‘mechanics’ of delivery and installation. The contract should address:

- the date on which delivery is to be made;
- whether all the elements of the system are to be delivered at one time or whether it is to arrive in instalments;
- who has responsibility for installation and testing;
- the implications of late delivery or non-delivery (e.g. an express provision permitting cancellation of the contract, with or without compensation to the buyer, if the goods are not delivered by some cut-off date or if some other key milestone is not achieved by the required date).

**Acceptance testing**

Formal acceptance testing arrangements are a crucial aspect of any successful procurement. The system is required to meet the functions and performance targets set out in the specification, but until it is tested the parties can not determine whether those requirements have been met.

The nature of acceptance tests varies widely between projects. Where a major piece of development work is involved, the parties may negotiate and document detailed testing arrangements as part of the contract. At the other extreme, the acceptance procedure may simply be that if the buyer uses the system ‘live’ for, say, 30 days without rejecting it, then it is deemed to have been accepted.

From the point of view of creating contractual certainty, then, the acceptance procedure should:

- provide for an objective and measurable ‘yardstick’ as to the standards of performance and functionality to be demonstrated;
- address all those elements that are necessary to demonstrate, to the buyer’s satisfaction, that the system meets its requirements; and
- be clear as to the consequences of both the passing and failing of the acceptance test.

Acceptance will generally trigger payment of the whole or the final instalment of any lump sum charges, or the start of periodic charges, and following acceptance the buyer’s remedies will be limited to a claim under the warranty provision.

In the event of failure of the acceptance tests, the contract will typically provide for a period during which the supplier may rectify problems and then retest; but further failure will signal the premature end of the contract, with the buyer able to return the hardware and software in exchange for a refund of any money paid.

**Client obligations**

The successful implementation of a complex IT system normally requires the performance of obligations not just by the supplier, but also by the client. Although primary responsibility for providing a system rests with the supplier, the client may well have obligations in relation to providing information about its business, testing the software, providing employees to be trained and so on.

These obligations need to be spelled out in the contract every bit as clearly as the supplier’s commitments.

**Change control**

Client requirements may change frequently over the lifetime of a project. The parties need to agree a procedure for specifying and agreeing changes to the scope
of work. The proper management and documentation of these changes will help to avoid disputes about what each party's obligations actually were.

The contract should include a formal ‘change control’ clause, setting out a mechanism whereby the client can request (and the supplier can recommend) changes to the specification, the project plan, or any other aspect of the deal. Any such change needs to be considered from the point of view of:

- technical feasibility;
- impact on the respective obligations of the supplier and client;
- cost implications;
- impact on the timetable.

As a general rule, no change should take effect unless it has been formally agreed and documented by both parties.

**Termination**

Provision has to be made for termination of the contract, setting out the circumstances in which the contract may be brought to an end and the consequences of that action. These provisions will vary according to the nature of the contract and the deliverables.

Apart from a general right to terminate the contract in the event of material breach or the insolvency of the other party, the following points should be considered:

- The client may wish to reserve a right to cancel or terminate the contract for convenience (say, because its business requirements change). In that event, the parties will need to discuss what compensation (if any) should be payable to the supplier.

- Contracts for development services are typically terminable by the client if specific time-critical milestones are significantly overdue. Provision should be made for treatment of the developed software on termination, including delivery of all copies (and source code) and certification that no copies have been retained.

- Contracts for continuing services (consultancy, support and maintenance services, bureau services) should be terminable on notice. The length of the notice and the earliest dates on which it may be effective are matters of negotiation in each case.

**COMMERCIAL HIGHLIGHTS**

**Pricing and payment**

There are as many pricing and payment structures as there are types of IT deal, and there is little to be gained from making generalisations about pricing and payment terms. The one point worth making is that, where payments are
tied into specific targets (such as system acceptance or other milestones), the terminology and structure of the payment schedule should accurately reflect that of the timetable.

There are several payment-related mechanisms that are commonly used to ensure that both parties have incentives to perform their obligations:

• The client may wish to provide for payment by instalments as the various parts of the system are delivered, retaining a proportion of the price until the complete system has been tested. The retention of a significant proportion of the charges will give the buyer some assurance that the supplier will finish the job.

• In respect of periodic fees, specifically, the buyer will be concerned about the supplier’s rights to increase the fee and may seek to limit rises by agreeing to, for example, only one increase a year or by tying increases to an appropriate index.

• It is common for hardware suppliers to retain title in the goods they supply as security for payment. This means that although the buyer gets possession of the goods, ownership remains with the seller until certain conditions (normally payment in full) are met. If the buyer fails to comply with the conditions, the seller can repossess the goods and sell them to recoup its losses.

**Intellectual property rights (IPRs)**

System supply contracts generally entail the transfer of technology and information from one party to another, for example, specifications, software, data and confidential business information. The lawful use of technology and information depends on compliance with the laws relating to copyright, confidentiality, database rights and other forms of intellectual property (see Chapter 4), so system supply contracts must deal comprehensively with IPR issues. There are two key IPR aspects to consider: ownership, and warranties and indemnities in respect of third-party IPRs.

In relation to ownership, the contract should specify what IPRs are to be created or used, and precisely who owns them (including identifying the owners of any third-party IPRs that are to be used or licensed). Copyright law contains a common trap for the unwary in relation to contracts for software development or consultancy work. The IPR in work undertaken by a contractor (as opposed to an employee) will normally vest in the supplier rather than the client. This means that an express, written assignment of copyright is needed if the aim is for the client to own these IPRs outright.

In relation to warranties, most system supply contracts will contain an assurance that the client’s use of the system will not infringe third-party rights and an indemnity in respect of any claims that may arise against the client. The contract should set out any express warranties required by the client as to the supplier’s ownership or entitlement in respect of the IPRs comprised in the system, together with a process for addressing any breach of those warranties.
In relation to the possible infringement of third-party IPRs, the client will typically impose a formal obligation for the supplier to deal with any such allegations, especially if the system is a critical part of the client’s business and merely rejecting it and claiming back the purchase price would be insufficient. A typical IPR indemnity clause will provide:

- a right for the supplier to take over, litigate and/or settle any such action;
- a right for the supplier to modify the system so that it does not infringe the alleged right, provided that it still conforms with the specification; and
- an indemnity given by the supplier against the client’s losses in the event of a successful third-party claim.

Supplier warranties
The client will normally require the supplier to give certain other express assurances in respect of the system to be delivered. Ideally, the client will want to obtain a warranty that the system will comply with its specification and/or meet specified performance criteria.

Such warranties are often subject to time limits or other restrictions. It is not unusual for the supplier to seek to limit the warranty to, say, six months from acceptance: after that point, any defects are rectified under maintenance and support arrangements (paid for by the client) rather than under warranty.

PROBLEM MANAGEMENT

Contractual remedies
The parties must consider at the negotiation stage what happens if a contract does not go according to plan, for example if the supplier fails to deliver a working system within the contracted time frames. Although damages and other remedies may be available as a matter of general law, it is preferable to spell out expressly the remedies that each party may have in particular situations.

One common mechanism for managing such disputes is to provide for payment of ‘liquidated’ damages for certain breaches. This involves setting out in advance the precise sum to be paid as compensation for certain breaches (e.g. late delivery at £X per day). Provided that the sum is a genuine estimate of the likely losses and not a penalty to force the other party to perform, the clause will be enforceable.

If the breach in question persists for a specified time or reaches a specified level of severity, the innocent party may also want a right to terminate the contract outright.

Limitations and exclusions of liability
IT suppliers generally seek to restrict their potential exposure to actions resulting from breach of contract or defects in the system. This is treated by some as purely a ‘legal’ issue, but in fact is a major question of commercial risk assessment and allocation, and these provisions can be amongst the most hard-fought in any contract negotiation.
A typical standard exclusion clause may take the following form:

- The supplier does not exclude liability for death or personal injury caused by negligence.
- The supplier seeks to exclude liability altogether for certain kinds of loss, often termed ‘special’, ‘indirect’ or ‘consequential’.
- The supplier accepts a limited degree of liability for certain other classes of loss.

From the legal point of view, exclusion clauses need to be considered from two broad angles. First, suppliers will often argue that they should have no liability for ‘consequential loss’, on the basis that the nature of IT products means that their uses (and so the potential losses resulting from failure) are not easily foreseeable at the time the contract is made and the potential exposure is in any case disproportionate to the contract value. Whether this is an acceptable commercial stance depends on the nature of the system and the extent of the client’s dependence on it. However, the courts have exercised considerable ingenuity in manipulating and interpreting expressions like ‘consequential loss’ in ways that the parties may not originally have intended.

**CONSEQUENTIAL LOSS: THE SEMANTIC LABYRINTH**

Although they are commonly used in all sorts of commercial agreements, the meaning of the expressions ‘special’, ‘indirect’ and ‘consequential’ in the context of contractual claims is open to interpretation by the courts, and there is often a resulting lack of certainty as to the precise effect of an intended exclusion.

The usual starting point for any discussion of consequential loss is the case of *Hadley v. Baxendale*. In that case, the court distinguished two classes of loss that could be recovered for breach of contract. These are:

- Such losses as may fairly and reasonably be considered either as arising naturally, that is according to the usual course of things ... or such as may reasonably be supposed to have been in the contemplation of both parties at the time they made the contract as the probable result of the breach of it.
- If the parties were aware of special circumstances at the time the contract was made, the losses which they would reasonably contemplate would be the amount of injury which would ordinarily flow from a breach under these special circumstances.

That basic distinction has been reworked several times over the years, but the terminology that is widely used in IT contracts does not fit neatly into the *Hadley v. Baxendale* rules and in fact means different things to different people. Indeed, the courts are repeatedly restating the meaning of these expressions in an effort to bring clarity to the concepts, but two cases will illustrate the kind of semantic problems that can arise.
In the 1999 case of British Sugar Plc v. NEI Power Projects Ltd, NEI had supplied some defective power equipment, with a headline value of about £100,000, to British Sugar. The sale contract expressly limited the seller’s liability for ‘consequential loss’.

As a result of breakdowns, increased production costs and resulting loss of profits, British Sugar put in a claim of over £5 million. British Sugar argued for the narrowest construction of the term ‘consequential loss’, interpreting it to mean ‘loss not resulting directly and naturally from breach of contract’; whereas NEI argued that the term meant ‘all loss other than the normal loss which might be suffered as a result of the breach of contract, negligence or other breach of duty’. The court found for the claimant and approved earlier authorities that ‘consequential damages’ means the damages recoverable under the second limb of Hadley v. Baxendale.

By this analysis, where loss of profits or loss of business (commonly regarded as typical examples of ‘consequential loss’) arise naturally from the breach of contract, they should be recoverable by the user: a result that may surprise many IT suppliers.

More recently, in 2009, British Gas brought a claim against Accenture in relation to a failed project to design and build of a new billing system (GB Gas Holdings Ltd v. Accenture (UK) Ltd). The new system was supposed to replace the utility company’s existing Customer Relationship Management (CRM) and billing systems for residential customers, and was accordingly critical to its business. The contract stated that neither party would be liable for ‘loss of profits or of contracts arising directly or indirectly; loss of business or of revenues arising directly or indirectly; [or] any losses, damages, costs or expenses whatsoever to the extent that these are indirect or consequential or punitive’. The High Court found that this exclusion did not prevent British Gas from recovering losses like overpaid gas distribution charges (which resulted from its own suppliers being given incorrect information about gas usage) and additional borrowing charges (resulting from the late billing or non-billing of customers). The court found that all these losses were foreseeable as ‘the very likely consequence’ of the breach; and that they were accordingly ‘direct’ losses and should be recoverable.

Similar confusion applies in relation to other commonly used terms. The term ‘consequential’ has at one point been defined simply to mean ‘not direct’; but there is also judicial authority to suggest that ‘direct loss’ could include ‘consequential loss’ in certain circumstances. Likewise, the term ‘special damages’ has no fewer than four possible meanings, including past (pecuniary) loss calculable as at the trial date (as opposed to all other items of unliquidated ‘general damages’); and losses falling under the second rule in Hadley v. Baxendale (as opposed to ‘general damages’ being losses recoverable under the first rule).

Secondly, there is an extensive body of law relating to the enforceability of exclusion clauses generally: if the exclusion clause is found to be unreasonable or defective in some other way, then the party seeking to rely on the exclusion may nevertheless be exposed to a greater degree of legal and financial risk than it originally envisaged.
The combined effect of the enforceability rules and the uncertainty about the meaning of commonly used language is that clarity is of the utmost importance in the wording of exclusion clauses: it is not in anybody’s interest for the effect of the exclusion to be uncertain and indeed it is surprising that businesses should continue routinely to use some of the terminology that regularly crops up.

Instead of debating abstract concepts like ‘consequential loss’, suppliers and clients alike should focus on the specific risks associated with the particular system. The client will generally accept that the supplier has a legitimate concern about exposure to unspecified types of liability, but the kinds of loss that will flow from a breach of an IT supply contract can be classified, at least in general terms:

- Loss of cost or salary savings, or other expected benefits.
- Costs of repairing or replacing the defective system.
- Costs of additional IT staff and consultants required to make the system work.
- Loss of profits resulting from non-performance.
- Costs of wasted management time.

These categories of loss are not intended to be definitive: there is no ‘definitive list’ as such, and each client and supplier will have its own specific concerns.

However, the starting point for constructing an effective provision must be to identify the categories of loss that are foreseeable, and to state explicitly how the parties intend to allocate these risks between themselves. Any unspecified types of loss will then fall to be determined by the court according to normal legal principles.

**ENFORCEABILITY OF EXCLUSION CLAUSES**

**The contra proferentem rule**
An exclusion clause will only operate to limit a party’s liability if it covers the breach that has occurred. The rules of interpretation are complicated, but in general the more serious the breach of contract, the more clearly worded the clause must be if it is to exclude liability for that breach: it is interpreted against the person who seeks to rely on it.

One illustration of this rule at work is the case of *Salvage Association v. CAP Financial Services Ltd.* In that case, a contract to supply bespoke software contained a warranty from the supplier under which it promised to remedy certain types of defect, and also provided that a limitation of liability would apply ‘if CAP fails to perform its obligations under [the warranty]’.

The wording of the warranty was sufficiently ambiguous that the court could interpret it as meaning that the warranty did not come into effect until after acceptance of the system by the client. Acceptance had never in fact occurred because the dispute began before the contract’s acceptance procedures were reached, so the court decided that the warranty never came into effect and so
the exclusion of liability never came into effect either. The result was that the supplier’s liability for breach of contract was completely unlimited.

**The ‘reasonableness’ test**

Under Section 3 of the Unfair Contract Terms Act 1977 (UCTA), where the buyer deals either as a consumer or (if the buyer is a business) on the seller’s written standard terms, any exclusion clause favouring the seller must satisfy a test of ‘reasonableness’ in order to be effective.

The measure of ‘reasonableness’ is whether it was fair and reasonable to include the clause at the time the contract was made. The court will take account of matters such as the following:

- The relative bargaining position of the parties.
- Whether the buyer received some benefit (e.g. a lower price) for agreeing to the clause.
- How far the buyer knew or ought to have known of the existence and extent of the clause.
- If the exclusion is contingent on compliance with some condition (e.g. regular maintenance), whether it was reasonable to expect the condition to be complied with.
- Whether the goods were ‘off the shelf’ or were specially made or adapted to the client’s order.

The courts have also held that the question as to which of the parties can most readily insure against the loss is a relevant consideration and that a limitation of liability is more likely to be reasonable than a complete exclusion.

The appendix to this chapter outlines the way in which the courts have applied the UCTA reasonableness test in practice.

**Special considerations in software contracts**

Computer programs are governed mainly by the law of copyright, which requires that the user of a program has a licence from the copyright owner. (Note that the term ‘licence’ is synonymous with ‘permission’ or ‘consent’.)

There are no particular legal formalities with regard to the form of the licence, but it is desirable for the licence to be in writing to ensure that there is complete clarity as to what may and may not be done with the software.

The type of licence depends on the nature of the package:

- Standard software is often supplied by retailers or distributors under a ‘shrink-wrap’ licence: the disk is wrapped in a clear plastic film, through which the terms of the licence granted by the copyright owner are clearly visible, along with an instruction that breaking the seal on the package will amount to acceptance of those terms.
• Contracts for bespoke software tend to be entered into on a more formal basis because of the need to agree a specification and to address other issues arising out of the development process. (It may also be the case that the client wishes to own the program outright rather than use it under licence, in which case see the warning in the section on IPRs as to the need for an express assignment of copyright from the contractor.)

The term of the licence may be perpetual or for a fixed period. Again, it is desirable for the term to be spelled out expressly because, in the absence of any express contractual provision, the normal rule is that an intellectual property licence is terminable by ‘reasonable notice’.

The licence will often impose restrictions on the use that the client may make of the software. Common restrictions include:

• limiting the number or class of users who may access the software;
• restricting use to the ‘internal purposes’ of the client (to prevent the client depriving the supplier of potential licence fees by using the software to provide bureau services to third parties);
• prohibiting the client from transferring the software to any third party, on the basis that the supplier has a right to know precisely who is using its software.

These are all legitimate concerns on the face of it, but the client should check the wording carefully to ensure that the permitted uses reflect all its present and anticipated future requirements. Exceeding the permitted use may leave the client exposed to a claim for copyright infringement or to being charged additional licence fees. At the very least, consider:

• Does this wording prevent the client processing data on behalf of other companies in its group?
• Does the clause operate in such a way as to allow the supplier to impose undefined conditions (such as additional licence fees) in the event of a transfer of the software?
• Might the restriction operate to prevent the client getting a third party to run the system as part of an outsourcing arrangement?

CONCLUSION

The delivery of a working system that meets the client’s needs is a difficult enough task, but it is even more difficult to achieve in a contractual vacuum.

Clearly recording each party’s contractual obligations and setting up appropriate mechanisms for resolving potential disputes will help to ensure the project stays on track. Defining those obligations and mechanisms is the principal purpose of the contract negotiation process.
APPENDIX: THE ‘REASONABLENESS’ TEST IN PRACTICE

St Albans City and District Council v. International Computers Ltd

ICL had developed a complex package (COMCIS) to calculate and administer the community charge (or ‘poll tax’) system of local taxation. St Albans used COMCIS to calculate the number of community charge payers in its area and used that figure to set its community charge rate. The software contained an error, so that although the St Albans database contained all the necessary details, the population figure reported was too high, the per capita charge was therefore set too low and, as a result, St Albans suffered a financial loss.

The contract contained a clause limiting ICL’s liability to the price or charge payable for the item of equipment, program or service in respect of which the liability arose or £100,000 (whichever was the lesser) and completely excluding liability for any indirect or consequential loss or loss of business or profits sustained by the client. Liability turned on whether this clause was reasonable under UCTA.

ICL contested that UCTA applied at all, arguing that the contract had not been on standard terms. However, the judge held that UCTA did apply. Even though many elements of the contract were negotiated at length (e.g. delivery dates and specification), ICL’s standard terms (which contained the limitation and exclusion clauses) ‘remained effectively untouched in the negotiations’, and indeed were referred to by ICL staff as ‘Standard Terms and Conditions’ in witness statements and letters.

The court then went on to consider whether the exclusions were ‘reasonable’ and concluded that they were not. Although St Albans knew of the limitation and had attempted to negotiate it, the following factors operated to render the clause unreasonable:

- ICL had substantially more resources than St Albans.
- ICL held product liability insurance in an aggregate sum of £50 million worldwide.
- ICL called no evidence to show that the limitation to £100,000 was reasonable, either in relation to the potential risk or the actual loss.
- The contract had mistakenly been made on an outmoded version of the General Conditions; in the then current version, the standard limitation had been increased to £125,000.
- Local authorities are not in the same position as private sector businesses: their operations are constrained by statute and financial restraints and they cannot necessarily be expected to insure against commercial risks.
- St Albans received no inducement to agree to the limitation and there was evidence that all ICL’s competitors imposed similar limitations of liability.
- When St Albans tried to negotiate the limitation, albeit at the last moment, ICL in effect said that this was not possible because it would delay the provision of the software to St Albans beyond the date for implementation of the community charge.
The judge accordingly found that ICL had not discharged its burden of proving that the term was fair and reasonable and also that, financially, ICL was better placed to bear a risk of this kind through insurance and to spread it across its client base.

**South West Water Services Ltd v. International Computers Ltd**

SWW and ICL had entered into two contracts (a turnkey agreement and a project management agreement) under which ICL was to deliver a client service system to SWW. After ICL accepted that it would be unable to deliver the system to specification and in accordance with a planned timetable, SWW sued for breach of contract, claiming that ICL had failed to deliver the system as agreed, and for misrepresentation.

Both agreements had contained a clause based on a standard ICL contract and purporting to limit ICL's liability for any claim for loss or damage.

The evidence was that, during the negotiations, SWW had originally submitted its own standard procurement conditions to ICL and that ICL had rejected them.

The question then arose whether, in these circumstances, the ICL limitations could be regarded as ICL's 'standard terms'. The court followed the St Albans decision in finding that, even though SWW originally offered its own terms in negotiations, in the event ICL had dealt on ICL's standard terms that had been only slightly adapted. The fact that one fairly predictable eventuality, that is failure to progress the project to a point where there was a system in place for SWW that was capable of being tested, had not been addressed in the documentation also tended to suggest that the contract should be regarded as 'standard terms'.

The judge went on to note that the extent to which a party has had discussions and has freely entered into a contract on the other party’s standard terms may be relevant as an important circumstance in considering whether those terms are reasonable. ICL argued that its standard limitation clause should be treated as reasonable in this case because its terms had been subject to arm’s length discussion and negotiations, but this was found not be the case on the evidence.

*This contribution is based on the author’s chapter on System Supply Contracts, in the 6th edition of Computer Law (2007), published by Oxford University Press.*
INDEX

academic licences 134
acceptance testing
  definition xv
  procedure 12, 17
software development
  contracts 9
  systems procurement
  contracts 17
access, staff usage policy 36
agency agreements, joint ventures 108
alternative dispute resolution (ADR)
  definition xv
application service provider (ASP) xv, 65, 118
Approved Authorised Treatment Facilities (AATFs) 145
Approved Exporters 145
arbitration
  agreement in contract 2
  as dispute resolution method 172
asset register 71
asset transfer 72
backup of data
  cloud computing 123, 124
  data protection issues 86
  specimen policy 38
benchmarking 70
boilerplate terms 2
business process outsourcing (BPO) xv, 65
business-to-business contracts 99
cancellation rights, under Distance Selling Regulations 97–98
change control
  clause in contract 17–18
  definition xv
Civil Procedure Rules 1998 (CPR)
  definition xv
  dispute resolution 169, 171
  mediation 172
cloud computing
  advantages 119–121
  backup requirements 123, 124
  contract for services 123–125
  customer obligations 123–124
  data protection issues 124–125
  indemnities 125
  limitation of liability 125
service rental 123
  supplier obligations 124
  costs 120
data protection issues 122–123, 124–125
definition 117
disadvantages 121–122
due diligence 121–122, 123
environmental issues 121
evolution 118–119
free trials 121
generally 117
internet reliability and 121
maintenance and support 121
mobility 120
resource access 119
sale of data 125
scalability 120
security 120, 124–125
services 118
storage 120
supplier dependence 121–122
types of cloud 119
Code of Advertising Practice 84
community clouds 119
Community designs 54
Competition Act 1998 114
competition law
  definition xv
  joint ventures and 114–115
Computer Misuse Act 1990 32
costs 120
consumer
  93
consumer contracts 99
Consumer Protection (Distance Selling) Regulations 2000
  cancellation rights 97–98
  information requirements 95
  non-compliance 101
contra proferentem rule 23
costs 120
correspondence 11
consumer
  99
deliverables 5
terminal agreement clause 2
FOIA clause 162
force majeure clause xvi, 2
formation 97
function 13
governing law and jurisdiction
  clause 2
hardware maintenance 6
hardware purchase 6
implied terms 13–14
legal structure 95–96
letters of intent 3
main points 12
open source software 140
pre-contract correspondence 11
selection of lawyer 2
service level agreements (SLAs) 11
software development 11
software licences 7
software maintenance 8
suppliers
  assessing suitability 3
  proposed terms 3, 15
  support requirements 12
  training requirements 12
contributor agreements 142
processed in accordance with data subject's rights 85–86 processing for limited purposes 81 security 87 processing by third parties 87 consent to 82 definition 80 fair and lawful 80–81, 123 in accordance with subjects rights 85–86 limited purposes 81 without consent 81 scope 76 security of personal data 79 International Standard 87 procedures 87 proportionality 87 sensitive personal data consent to processing 82 definition xviii, 76 terminology 74

Data Protection Act 1998
criminal offences within 91 Enforcement Notices 90 exemptions notifications 76–77, 90 subject access provisions 90 subject information provisions 90 fines for breach 74, 90 marketing, right to opt out 85 notifications exemption from requirements 77, 90 personal data under 87 procedure 79 principles of data protection 80 scope 76 sensitive personal data under 76, 82 terminology 74
data subjects access requests complying with 89 definition xvi exemptions 90 time limit 89 consent to processing 80 definition xvi information provisions complying with 80 exemptions 90 marketing, opting out 85 provision of details to 80 rights 75, 88 access requests 89 information on processor 88, 90 marketing 85 processing in accordance with 85–86 database right definition xvi, 40 generally 44, 50–51 linking, infringement caused by 49 databases copyright 49–50 intellectual property rights and 45 licences to use 44 protecting own rights 45
declaration of software 43 deliverables, consultancy services contracts 4 Department for Business Innovation and Skills (BIS), non-household equipment 148 description, implied term 13–14 design rights 40 Community designs 54 definition xvi UK design right 53–54 UK registered designs 53 Designated Collection Facilities (DCF) 145 Direct Marketing Association 84 direct marketing, data subjects' right to opt out 85 Disability Discrimination Act 1995 35 disclaimers, on business emails 32–33 disks, staff usage policy 36 display screen equipment (DSE) definition xvi regulations 34 dispute resolution (DR) arbitration 172 choice of method 165 definition escalation to senior management 167 expert determination 167–169 key factors 165 litigation 170 mediation 175 methods 165 negotiation 166 reasons for need 164 distance contracts information requirements 95 legislation 93 distance selling definition xvi regulations see Consumer Protection (Distance Selling) Regulations Distance Selling Directive 1997 93 performance time limits 97 see also Consumer Protection (Distance Selling) Regulations distribution agreements, joint ventures 108 Distributor Take-back Scheme (DTS) 145, 150 domain names avoiding dispute 47 cyber-squatting 46 definition xvi intellectual property rights and 47 problems with 46 registration 47 trade marks and 46, 47 DSE Regulations 34 dual licensing 130, 136–137 due diligence asset transfer 72 cloud computing 121–122, 123 data protection issues 79 definition xvi open source software projects 138, 140–141
ecommerce
cancellation rights 97–98
Consumer Protection (Distance Selling) Regulations 2000 95
customer rights enforcement 101
contract formation 97
country of origin principle 99
Electronic Commerce Directive 2000 93
generally 92
information requirements
checklist 102
Consumer Protection (Distance Selling) Regulations 2000 95
Electronic Commerce (EC Directive) Regulations 2002 93, 97
jurisdiction 99
marketing communications 100
don-compliance with legislation 101
performance time limits 107
resources 101
spam, restrictions on sending 100
Stop New Orders 101
terminology 93
electrical and electronic equipment 146
Electronic Commerce (EC Directive) Regulations 2002
information requirements 94, 97
information society service providers enforcement actions against 101
operating rules for 99
marketing communications 100
non-compliance 101
Electronic Commerce Directive 2000 93
contract formation by electronic means 97
hosting/caching of material 101
information society service providers marketing communications 100
see also Electronic Commerce (EC Directive) Regulations
email
business confidentiality 37
disclaimers 33
specimen policy 37
confidentiality 37
disclaimers, in business 33
employees’ misuse, consequences for employees 28, 29
information disclosure 33
monitoring by employers 30
private 31
specimen restriction 37
problems with 29
storage 29
unsolicited 84
see also spam
usage policies 33
action plan 33
establishing 32
monitoring 30
specimen 37
employees
code ownership 142
customer systems usage
action plan 33
monitoring by employers 30
policy 32
customer systems usage 36
display screen use 34
email
monitoring by employers 30
private 31
hacking 32
internet usage
inappropriate material 37
monitoring by employers 30
policy considerations 32
specimen restriction 37
misuse of computer systems consequences for employers 28–29
specimen policy 38
private email 31
specimen restriction 37
right to eye tests 34
employers
computer usage policies 32
consequences of staff misuse of computers 28–29
monitoring of staff communications 29–30, 38–39
provision of eye tests 34
Enforcement Notices, under Data Protection Act 1998 91
Enterprise Act 2002 114
entire agreement clause 2
Environment Agency (EA) 145, 149
Environmental Information Regulations 2004 153
equipment disposal
collection v. disposal 152
commercial issues 153
financial responsibility 144, 149, 151
household equipment 148
PCS financial responsibility 149
waste handling obligations 151
non-household equipment 148
PCS financial responsibility 149
waste handling obligations 150
see also Waste Electrical and Electronic Equipment (WEEE) Regulations
escalation clauses
as dispute resolution method 167
in service level agreements 10
escrow
definition xv, 55
importance for software users 56
see also source code escrow
European economic interest grouping (EEIG) 111–112
exclusion clauses
contra proferentem rule 23
enforceability 22
forms 21
reasonableness test 24, 27
expert determination, as dispute resolution method 167–169
eye tests for screen users 34
facilities management (FM)
contract xvi, 65
Fax Preference Service 84
First-tier Tribunal (Information Rights), FOIA appeals 157
fitness for purpose, implied term 14
force majeure
as boilerplate term 2
definition xv
framing
definition xvi
in trade mark infringement 48
Free Software Foundation (FSF) 127
freedom of information
contract clauses 162
definition 153
legislation
see Freedom of Information Act (FOIA)
procurement 161–162
public interest test 158
requests for information
appeal to Information Commissioner’s Office 157
appropriate/cost limit 158–159
process 157
public authority actions 157
refusal to respond 158
time limits 155
unclear requests 155
withholding information 158
Transparency Agenda 154
withholding information 158
Freedom of Information Act (FOIA) 2000
appeals
to Information Commissioner’s Office 157
to Information Tribunal 157
dealing with 160–161
exemptions 158–159
absolute 158
commercial prejudice 160
confidential information 160
qualified 159
impact on private companies 159–160
public authorities
obligations 155
provision of information to 156
status under 154
request process 156–157
see also freedom of information
GNU General Public Licence 134, 135–136, 138
hacking, by employees 32
hardware
authorised sales 41
intellectual property rights and 42
maintenance
contracts for 6
types 6
purchase
contracts for 6
retention of title 19
repairs 42
special conditions of sale 42
health and safety
action plan 34–35
advice 33–35
password protection, computer usage policies 38
patents 40
application procedure 51
definition xvii
duration 51
matter patentable 51
open source software and 142
software 51
payment arrangements
cloud computing 120
consultancy services contracts 4
hardware maintenance contracts 6
outsourcing contracts 70
software development contracts 9
software maintenance contracts 8
systems procurement contracts 19
penalties 90–91
performance indicators (PIs) 68
performance points 68
personal data
see data protection
platform as a service (PaaS) 117
see also cloud computing
pre-contract correspondence 11
pricing structures, outsourcing contracts 70
Privacy and Electronic Communications (EC Directive) Regulations 2003
cookies 84–85
unsolicited email 84, 100
unsolicited text messages 84, 100
private clouds 119
private companies
dealing with FOIA 160–161
impact of FOIA 159–160
commercial issues 159–160
privacy 160
reputation 160
public authorities and 164
contractual requirement to locate information 156–156, 161
information subject to disclosure under FOIA 155
see also freedom of information
procurement, FOIA issues 161–162
Producer Compliance Scheme (PCS) compulsory membership 149
definition 146
project open book accounting (POBA) 69–70
proportionality, personal data security 87
public authorities
obligations 155
private companies and 154
contractual requirement to locate information 156–156, 161
information subject to disclosure under FOIA 155
provision of information 156
see also freedom of information requests for information 156
status under FOIA 154
public clouds 119
public domain, software in 130
quality of goods, implied term 14
quiet possession of goods, implied term 14
ratchet mechanism 68
reasonable care and skill, implied term 14
reasonableness test 24, 26–27
record keeping
computer usage policy 37
waste handling 151
repetitive strain injury (RSI) action on plan on reducing 35
definition xvii
level of claims 33
reseller agreements 107
retention of title, hardware supply contracts 19
royalty deals, joint ventures 108
Safe Harbor (2000) 87
Scottish Environmental Protection Agency (SEPA) 145
security
cloud computing 120, 124–125
computer usage policies 37
personal data 78–78, 86–87
service description drafting 66
service level agreements (SLAs) breach 10
contracts for 11
definition xvii
elements 68
escalation clauses 10
form 10
outsourcing 69
termination 10
service provider, definition 93
service recipient, definition 93
software
adapting 42, 43
backup copies 43
copyright in 42, 50, 56
decomposition 43
development
see software development
intellectual property rights and 44
licences
see software licences
maintenance
see software maintenance
patenting of 51
proof of ownership 63
public domain 130
supply contracts, special considerations 25
usage policy 36
software as a service (SaaS) definition 117
emergence 118
see also cloud computing
software development contracts for 9
special considerations 25
copyright in product 9
payment arrangements 9
source code escrow and 9
suppliers’ warranties 9
termination rights 18
software licences
contracts for 7
financial issues 132
non-compliance 44
open source software 127–129, 130, 134–137
academic licences 134–135
compatibility 136
copyleft licences 135–136
dual licensing 130, 136–137
external use 139
internal use 138–139
patent licences 142
permitted uses under 25
restrictions imposed by 25
scope 43
staff usage and 36
term 25
transferring 44
types 25
software maintenance
charging arrangements 7, 8
contracts for 8
exclusions 8
IPR issues 43
payment arrangements 8
scope 8
termination 8, 18
sole traders, disclosure of information on letters 32
source code
compatibility 59
conversion to executable code 56, 126
definition xviii, 56
deposit agreements
see source code escrow
open source software 126, 138
security 56, 126
storage issues 63
source code escrow
advantages for software owners 62–63
agents 62
agreements 61–62
items to be lodged 61
proof of ownership of software 63
providing for in IT contracts 12
release events 61
requirement for 57–58
software development and 9
technical considerations 59
user’s duties 62
verification 60
when needed 56–57
spam
definition xviii
legal restrictions on sending 100
specification xviii
staff transfers, TUPE and 73
standard contracts, dangers of 15
statement of requirements 66
Stop Now Orders 101
suppliers
cloud computing 121–122, 124
suitability 3
terms proposed by 3, 15
warranties given by
cloud computing services contracts 124
software development contracts 9
systems procurement contracts 20
systems procurement contracts
acceptance testing 17
breach 20
Businesses face a legal minefield when it comes to information technology, with legislation covering issues as diverse as data protection, IT procurement contracts, outsourcing, escrow and joint ventures. This comprehensive, plain-English guide covers the IT-related legal issues faced by businesses and their staff on a daily basis.

The book provides the non-specialist with the tools to work out what needs to be done, who to get advice from and how to deal with IT and legal experts.

- Prior knowledge of the law is not required
- Covers data protection, procurement contracts, how to avoid employment problems and intellectual property law
- Dedicated chapters on cloud computing, open source software and freedom of information
- Explains WEEE (Waste Electrical and Electronic Equipment) regulations
- Includes examples from actual case law to illustrate common issues

ABOUT THE EDITORS
Jeremy Holt is the Head of the Computer Law Group of Clark Holt Commercial Solicitors.

Jeremy Newton is a Director at Technology Law Alliance in London, a law firm specialising in IT, outsourcing and e-commerce law.

You might also be interested in:
DATA PROTECTION AND COMPLIANCE IN CONTEXT
Stewart Room

Written in plain English, it provides practical advice... A valuable addition to my bookshelf.

British Journal of Healthcare Computing and Information Management

A small but perfectly-formed legal guide to spotting potential IT problems... With this book you’ll stay on the right side of a very complex subject.

Internet Works
(Reviews of previous edition)