

Contents

Preface	ix
Who should read this book	ix
Purpose of this book	x
1 Introducing Utility Computing	1
1.1 Real problems and real solutions	5
1.1.1 Real issues identified – regulation, legislation and the law	5
1.1.2 More regulation, legislation and the law	6
1.1.3 Current storage growth	8
1.2 New storage management	9
1.2.1 What are the things organisations need to consider?	11
1.2.2 What does data lifecycle management mean?	13
1.2.3 Why is IT lifecycle management important?	15
1.2.4 Goals of data lifecycle management	16
2 The Changing IT Imperative	19
2.1 Introduction to utility computing	22
2.2 General market highlights	25
2.2.1 Current storage growth	26
2.2.2 Enterprises for which DLM is critical	30
2.3 Real challenges and opportunities	36
2.3.1 Real issues identified	36
2.3.2 Data compliance	37
2.3.3 Case study in ineffective storage reporting	39
2.4 Summary	40
3 Being Compliant	43
3.1 So what are the regulations?	46
3.2 Financial services companies	49
3.2.1 Crime in the finance sector	52

3.3	Telecommunications companies	54
3.4	Utilities companies	58
3.5	Public authorities and government	59
3.6	Managing data for compliance is just a specialised form of data management	61
3.7	Just plain junk data!	63
3.8	The bottom line – what is mandated?	64
3.8.1	Record retention and retrieval	65
3.8.2	Auditable process	68
3.8.3	Reporting in real time	69
3.8.4	Integrating data management from desktop to data centre to offsite vault	72
3.8.5	Challenge – the data dilemma	72
4	Data Taxonomy	75
4.1	A new data management consciousness level	77
4.1.1	De-mystifying data classification	79
4.1.2	Defining data classification	81
4.1.3	Classification objectives	81
4.1.4	Various approaches to data classification	82
4.2	Data personification	83
4.2.1	Business infrastructure mapping analysis	84
4.3	Classification model and framework	87
4.4	Customer reporting	97
4.4.1	Summary reports	98
4.4.2	Detailed reports	100
4.4.3	Summary graphs	104
4.5	Summary	105
5	Email Retention	107
5.1	Email management to achieve compliance	108
5.2	What is archiving?	109
5.2.1	Email archiving requirements	110
5.3	How should organisations manage their email records?	111
5.4	Email retention policies are for life – not just for Christmas	113
5.5	How companies can gain competitive advantage using compliance	114
5.5.1	Compliance makes good business sense	115
5.6	What laws govern email retention?	117
5.6.1	How long do we have to keep email records?	118
5.7	Write once, secure against tampering	119
5.8	Storage recommendations for email	121
5.9	Conclusion	124
6	Security	125
6.1	Alerting organisations to threats	125
6.1.1	Vulnerability identified and early warnings	129
6.1.2	Early awareness of vulnerabilities and threats in the wild	130
6.1.3	Listening posts	132

6.2 Protecting data and IT systems	133
6.2.1 Threats blocked using vulnerability signatures to prevent propagation	134
6.2.2 Preventing and detecting attacks	135
6.2.3 Managing security in a data centre	136
6.2.4 Monitoring and identification of systems versus vulnerabilities and policies	137
6.2.5 Responding to threats and replicating across the infrastructure	138
6.2.6 Patches and updates implemented across infrastructure	139
6.2.7 Keeping information secure and available	140
6.3 Conclusions	140
Reference	143
7 Data Lifecycles and Tiered Storage Architectures	145
7.1 Tiered storage defined	145
7.1.1 Serial ATA background	147
7.1.2 Serial ATA overview	148
7.1.3 Serial ATA reliability	150
7.1.4 Bit error rate (BER)	151
7.1.5 Mean time before failure (MTBF)	152
7.1.6 Failure rate breakdown	154
7.1.7 No free lunch	155
7.2 RAID review	156
7.2.1 RAID 5 review	156
7.2.2 RAID 6 overview	158
7.3 Tape-based solutions	159
7.3.1 Virtual tape library primer	160
7.4 Recoverability of data: you get what you pay for	163
7.5 Conclusion	166
Bibliography	167
8 Continuous Data Protection (CDP)	169
8.1 Introduction	169
8.2 CDP data-taps	171
8.2.1 Application data-tap	172
8.2.2 File system data-tap	172
8.2.3 Volume data-tap	172
8.3 CDP operations	175
8.3.1 CDP store	177
8.3.2 CDP stakeholders	180
8.4 Conclusion	182
9 What is the Cost of an IT Outage?	185
9.1 Failure is not an option	185
9.1.1 Tangible costs	187
9.1.2 Intangible costs	189
9.2 Finding the elusive ROI	191

9.3	Building a robust and resilient infrastructure	192
9.3.1	Five interrelated steps to building a resilient infrastructure	194
9.3.2	Disaster recovery concepts and technologies	194
9.3.3	Disaster tolerance	196
9.4	Conclusion – Analysing business impact	198
9.4.1	Identifying critical functions	199
10	Business Impact	201
10.1	Business impact	201
10.1.1	Business impact analysis	202
10.1.2	Cost versus adoption	207
10.1.3	Service level agreements and quality of storage service	211
10.2	The paradigm shift in the way IT does business	212
10.2.1	Aligning business with IT	212
10.2.2	Software consistency and agnostic support	214
10.3	The Holy Grail: standard software platform	214
10.3.1	Business technology reporting and billing	215
10.3.2	Smart storage resource management	216
10.3.3	Data forecasting and trending	217
10.3.4	Policy-based Administration	219
10.4	Summary	219
	Bibliography	220
11	Integration	221
11.1	Understanding compliance requirements	221
11.1.1	Automating data lifecycle management	226
11.1.2	Content searching	229
11.2	Understanding hardware and its constructions	233
11.2.1	Current storage technologies	234
11.2.2	Disk-based storage strategies	234
11.3	Understanding user expectations	237
11.3.1	Organising data	238
11.4	Knowing the capabilities of your data management tools	240
11.4.1	Virtualisation of storage, servers and applications	241
11.4.2	Product technology and business management functionality	243
11.5	Solution integration – business data and workflow applications	243
11.5.1	Standard management and reporting platform	245
11.5.2	Meeting business objectives and operational information (Figure 11.7)	246
11.6	A ten-point plan to successful DLM, ILM and TLM strategy	247
11.7	Conclusion	248
	References	248
	Index	251