

Inhaltsverzeichnis

Vorwort	V
1 Information – Treibstoff für Produktion und Dienstleistung	1
1.1 Anforderungen an das Information Lifecycle Management (ILM)	1
1.2 Information Lifecycle und Information Lifecycle Management . . .	3
1.2.1 Zugriff, Verfügbarkeit und Schutz	5
1.2.2 Reduktion der Risiken der Non-Compliance	7
1.2.3 Fähigkeit, Informationsmanagement anhand des Informationswertes zu priorisieren	8
1.3 Der Informationslebenszyklus	10
1.3.1 Kosten im Informationslebenszyklus	12
1.4 Der Informationslebenszyklus-Strategien-Mix	15
1.5 Die Informationswert-Aufbewahrungszeit-Matrix	32
2 Information Lifecycle Management (ILM-) Modelle	37
2.1 Herausforderung: Strategisches Handeln	38
2.2 Zusammenspiel zwischen Geschäftsprozess, Information Lifecycle und Data Lifecycle	41
2.3 Die Ziele der strategischen IT-Planung	44
2.4 Entwicklungstrends Speichernetzwerke	50
2.5 Strategische Einführungskonzepte für ILM	54
2.5.1 Phase 1	56
2.5.2 Phase 2	56
2.5.3 Phase 3	56
2.5.4 Phase 4	57
2.5.5 Phase 5	57
2.6 Strategische ILM-Prozessmodelle	57
2.6.1 ILM als Prozessmodell	58
2.6.2 ILM als Modell mit dem Fokus Adaptive Enterprise . . .	58
2.7 Schlüsselfaktor Klassifizierungskonzepte	60
2.8 Schlüsselfaktor IT-Sicherheit	62
2.9 Schlüsselfaktor Qualitätssicherung	65
2.10 Schlüsselfaktor Risikomanagement	66

2.11	ILM-Projektmanagement: Anforderungen an die Projektorganisation und -Struktur	67
3	Information Lifecycle Management – Projektorganisation und -struktur	69
3.1	Projektkurzbeschreibung	69
3.2	Anforderungen an das Projektmanagement	71
3.2.1	Allgemeine Anforderungen an das Projektmanagement	71
3.2.2	Anforderungen an ein V-Modell und V-Modell-XT basiertes Projektmanagement	72
3.2.3	Anforderungen an ein von der Gesellschaft für Projektmanagement (GPM) konformes Projektmanagement-Modell	73
3.2.4	Anforderungen an das Projektmanagement basierend auf “Henley Projectmanagement Course“	74
3.2.5	Anforderungen an das Projektmanagement basierend auf “PRINCE2“	74
3.2.6	Anforderungen an das Projektmanagement hinsichtlich des IT-Grundschutzes	75
3.2.7	Anforderung an das Projektmanagement hinsichtlich ISO 20000 konformer Optimierung der Service-Geschäftsprozesse	76
3.2.8	Weitere Projektmanagement-Dienstleistungen	77
3.2.8.1	CMM und CISA	77
3.2.8.2	Projekt-Exit-Management	78
3.3	Anwendung des Projektmanagements in den beteiligten Unternehmungen	78
3.4	Aktivitäten der Startphase	81
3.4.1	Erstellung des Projektleitfadens/ Projektmanagementplans	81
3.4.1.1	Zielsetzung	81
3.4.1.2	Geltungsbereich	81
3.4.1.3	Projektgremien	81
3.4.1.4	Besprechungen	82
3.4.1.5	Eskalationsbehandlung	83
3.4.1.6	Gesamtprojektplan	83
3.4.1.7	Berichtswesen	84
3.4.1.8	Änderungsmanagement	85
3.4.1.9	Definition der Projektziele	86
3.4.2	Die Projektfeldanalyse	90
3.5	Aktivitäten über die komplette Projektlaufzeit	93
3.5.1	Die Risikoanalyse	93
3.5.2	Projektstrukturierung	100
3.5.3	Projektorganisation KONCOM/IT	101
3.5.4	Phasenmodell und Meilensteine	103

3.5.5	Ablauf- und Terminplanung	105
3.5.6	Einsatzmittelplanung	106
3.5.7	Kostenplanung/Finanzmittelplanung	107
3.5.8	Berichtswesen, Statusgespräche, Projektinformationswesen	108
3.5.9	Projektsteuerung (Arbeitsweise und Hilfsmittel zur Termin-, Leistungs- und Kostensteuerung)	112
3.5.10	Projektkultur, Teambildung und Teamarbeit	112
4	Information Lifecycle Management Projekt	119
4.1	Der Projektplan	119
4.2	Die erarbeiteten Grundlagen	140
4.2.1	Generelle Migrationsverfahren	140
4.2.2	Generelle Migrationsverfahren	141
4.3	Vorbereitung und Durchführung der Ausschreibung	150
4.3.1	Speicherkonzept und Technologieauswahl	150
4.3.1.1	Anbindung von Plattenkapazitäten über Network Attached Storage (NAS)	150
4.3.1.2	Anbindung von Speichersystemen über Storage Area Networks (SAN)	154
4.3.1.3	Archivierung	156
4.3.1.4	Schlussfolgerungen für EurAmFi AG und KONCOM/IT	159
4.3.1.5	Storagefunktionalität	159
4.3.1.6	Technische Anforderung Speichersysteme, Switche und Direktoren	161
4.3.1.7	„Pre Site“-Anforderungen und Standort	162
4.3.1.8	Definition der Speicher-Schutzklassen	163
4.3.1.9	LUN-Größen	164
4.3.1.10	Anzahl der Host Bus Adapter (HBA)	165
4.3.1.11	Anzahl Switch Ports	165
4.3.1.12	Hochverfügbare Services und Schutzklassen	169
4.3.1.13	Failover-Konzept	172
4.3.1.14	Backup-Konzept	179
4.3.1.15	IT-Sicherheits-Konzept	181
4.3.1.16	Wartungsverträge für Einzelkomponenten	182
4.3.1.17	Abhängigkeiten zu anderen Entwicklungsvorhaben	183
4.3.2	Die Ausschreibungsunterlagen und Informationen zur Anfrage	184
4.3.2.1	Die Anfrage und die beteiligten Unternehmen	184
4.3.2.2	Erwartungen an das Angebot	185
4.3.2.3	Vorgehen zur Bieterauswahl und Beauftragung	186
4.3.2.4	Angebot als „Try- and Buy-Lösung“	186
4.3.2.5	Angebotsfristen	186
4.3.2.6	Fragen zur Ausschreibung	187
4.3.2.7	Ansprechpartner	187

4.3.2.8	Datenschutz- und Geheimhaltungserklärung	187
4.3.2.9	Ist-Situation	187
4.3.3	Zielumgebung	196
4.3.4	Anforderungskatalog und Leistungsverzeichnis	197
4.3.5	Migrationsverfahren und Test der Migration	198
4.3.5.1	Migration der Daten	199
4.3.5.2	Die Entscheidungstabelle zur Anbieterauswahl	201
5	Testkonzept zur Qualitätssicherung	209
5.1	Generalisierter Testplan	210
5.1.1	Revision	210
5.1.2	Allgemeiner Überblick – generalisierter Testplan	211
5.1.3	Ausfall eines HBAs	211
5.1.4	Ausfall eines primären Servers	212
5.1.5	Ausfall eines Primärspeichersystems	212
5.1.6	Ausfall des Primärstandortes	213
5.1.7	Wiederherstellung eines primären Servers	213
5.1.8	Wiederherstellung des Primärstandortes	214
5.1.9	Backup eines Produktionssystems	215
5.1.10	SNAP von Primärsystem und Mapping an Backup-Server	216
5.1.11	Restore eines Primärsystems aus einem SNAP	218
5.1.12	SNAP der Spiegelgeräte und Mapping der SNAP-Geräte an Backup-Server	219
5.1.13	Restore eines Systems aus dem SNAP-Spiegel	220
5.2	Testplan Windows-Cluster	221
5.2.1	Revision	221
5.2.2	Konfigurationsorientierte Tests	222
5.2.3	Namensauflösung	222
5.2.4	Servicerelevante Tests	223
5.2.4.1	Online-Austausch HBA	223
5.2.4.2	Failover-Tests Clustermember 1	223
5.2.4.3	Failover-Tests Clustermember 2	227
5.2.4.4	Skalierungsmöglichkeiten	230
5.3	Backup und Restore	231
5.3.1	Erstellen eines Snapshots	231
5.3.2	Backup und Restore einzelner Dateien und Verzeichnisse mit Snapshots	231
5.3.3	Backup und Restore kompletter Datenträger mit Snapshots	232
5.4	Ermittlung der SAP-Datenbanklast für einen Testvergleich bei Inbetriebnahme des SAN	232
5.5	Test der Datentypisierung und Archivierung	233

6	Datenklassifizierung	235
6.1	Speicherklassifizierungskonzepte	235
6.2	Generische Klassifizierungsansätze	239
6.2.1	Statische Klassifizierungsmodelle	240
6.2.1.1	Modell: Anwendungsklassifizierung	240
6.2.1.2	Modell: Archivierungsbasierte Klassifizierung	240
6.2.1.3	Modell: Auskunftsklassifizierung	241
6.2.1.4	Modell: Business-Transaction-basierte Klassifizierung	242
6.2.1.5	Modell: Data-Protection-Initiative-Klassifizierung	244
6.2.1.6	Modell: Datenverwaltungs-Dienstleistungen-Klassifizierung	244
6.2.1.7	Modell: Datumsklassifizierung	245
6.2.1.8	Modell: Dienstleistungsklassifizierung	245
6.2.1.9	Modell: Disaster-Recovery-Klassifizierung	245
6.2.1.10	Modell: Geschäftsfeldklassifizierung	246
6.2.1.11	Modell: Informationsmanagement-Dienstleistungen-Klassifizierung	246
6.2.1.12	Modell: Metadatenbasierte Klassifizierung	247
6.2.1.13	Modell: Security-based-Klassifizierung	247
6.2.1.14	Modell: Standardbasierte Klassifizierung	248
6.2.1.15	Modell: Value-driven-Klassifizierung	248
6.2.1.16	Modell: XAM-Klassifizierung	249
6.2.2	Dynamische Klassifizierungskonzepte	251
6.3	Tiered Storage als Lösungsinstrument bei der operativen Umsetzung der Klassifizierung	252
6.4	Projektbezogene Umsetzung	253
6.4.1	Betriebsstandards der EurAmFi AG	254
6.4.1.1	Infrastrukturstandards	254
6.4.1.2	Speichersysteme	255
6.4.1.3	Netzwerk	255
6.4.2	Standards für Sekundärinfrastruktur	256
6.4.2.1	Stromversorgung	256
6.4.2.2	Klimatisierung	256
6.4.2.3	Verschiedene Standorte	256
6.4.3	Klassifizierung nach Server und Anwendungen	257
6.4.4	Abgrenzung zwischen Klassifizierung nach Verfügbarkeit, Verfügbarkeitsklasse und SLA	259
6.4.4.1	Attribute von Verfügbarkeitsklassen	259
6.4.4.2	Maximale Hardwareausfallzeit (physikalische Wiederherstellzeit)	261
6.4.4.3	Maximale logische Wiederherstellzeit	261
6.4.4.4	Notwendigkeit eines Service-Desk	262
6.4.4.5	Notwendigkeit einer Betriebsbereitschaft	263
6.4.4.6	Reaktionszeiten	264
6.4.4.7	Betriebszeiten	265

6.4.4.8	Sonderzeiträume	266
6.4.4.9	Wartungszeiträume	266
6.4.4.10	Maximaler geplanter Datenverlust	266
6.4.4.11	Betriebsumgebung der Anwendung	267
6.4.5	Verfügbarkeitsklassen	267
6.4.6	Verfügbarkeitsklassen und KONCOM/IT-Datenklassen	268
6.4.7	Klassifizierung mit Hilfe von Metadaten	270
6.4.8	Content-basierte Klassifizierung	270
7	Sicherheit	273
7.1	Speichersicherheit	273
7.2	Klassische Sicherheitskonzepte bei zentraler Datenspeicherung	274
7.2.1	Firewall	274
7.2.2	Virtual Private Network	275
7.2.3	Access Control List	276
7.2.4	FC-Verkabelung	277
7.2.5	Kontinuierliche Datensicherung	277
7.3	Klassische Sicherheitskonzepte in einer verteilten Speicherumgebung	278
7.3.1	Ergänzende Maßnahmen	278
7.3.2	Port Based Network Access Control	279
7.3.3	Mandatory Access Control	279
7.3.4	Role Based Access Control	279
7.3.5	Management der Speicherinfrastruktur	280
7.4	Security-Management-Planung im Bereich Speicheradministration	281
7.4.1	Maßnahmenkatalog Infrastruktur (M 1)	281
7.4.2	Maßnahmenkatalog Organisation (M 2)	281
7.5	SAN-Zoning und LUN-Masking	285
7.6	Anforderung an die Organisation und die Betriebsführung	286
7.6.1	Das Sicherheitsmanagement	287
7.6.2	Management des kontinuierlichen Geschäftsbetriebs	288
7.6.2.1	Definition der Sicherheitspolitik	288
7.6.2.2	Definition des Umfangs des ISMS	288
7.6.2.3	Risikoidentifikation und -analyse	288
7.6.2.4	Risikomanagement	289
7.6.2.5	Auswahl von Steuerungszielen und -maßnahmen	289
7.6.2.6	Erklärung der Anwendbarkeit	289
7.6.3	Anforderungen an die Organisation und die Standards	289
7.7	Allgemeine Sicherheitsanforderungen an eine verteilte Infrastruktur	290
7.8	Backup als Bestandteil einer Sicherheitsstrategie	290
7.8.1	SLA als Kernforderung für den Backup- und Wiederherstellprozess	291
7.8.2	Wiederherstellungsprozess	292

7.8.3	Backup Medium Festplatte	293
7.8.4	Backup-Medium Band	294
7.8.5	Verschlüsselung des Backups als Bestandteil einer Sicherheitsstrategie	294
7.8.5.1	Sicheres Verschlüsselungsverfahren	295
7.8.5.2	AES-Algorithmus II	295
7.8.5.3	Verschlüsselung am besten in der Virtual-Tape-Library	295
7.8.5.4	Authentizität der Daten	296
7.8.5.5	Schlüsselverwaltung	296
7.9	Disaster Recovery als Bestandteil einer Sicherheitsstrategie	297
7.10	Archivierung als Bestandteil einer Sicherheitsstrategie	298
7.10.1	Rechtliche Anforderungen an die Archivierung	298
7.10.2	Lotus Notes und E-Mail als rechtsrelevante elektronische Erklärungen	299
7.10.3	Lotus Notes und E-Mail als Beweismittel bei der Dokumentation betriebswichtiger Vorgänge	300
7.10.4	Grenzen der Dokumentation: Lotus Notes und E-Mail versus Mitarbeiterschutz	300
7.10.5	Lotus Notes und E-Mail als Gegenstand der gesetzlich zwingenden Dokumentation von Geschäftsvorfällen	301
7.10.6	Zulässige Archivierungsformen	301
7.10.7	Folgen einer Verletzung der Archivierungspflicht	302
7.10.8	Archivierungsprozess	303
7.10.9	Archivierungsformate und Archivierungsformatanforderungen	304
7.10.10	Langzeitstabile Formate für textbasierte Informationen: SGML, HTML und XML	305
7.10.10.1	SGML	305
7.10.10.2	HTML	306
7.10.10.3	XML	306
7.10.11	Langzeitstabile Formate für Pixelgrafiken: TIFF	307
7.10.12	Langzeitstabile Formate für Pixelgrafiken: PNG	308
7.10.13	Langzeitstabile Formate für Pixelgrafiken: GIF, BMP, JPEG, JPEG 2000	309
7.10.13.1	GIF	309
7.10.13.2	BMP	309
7.10.13.3	JPEG	309
7.10.13.4	JPEG 2000	309
7.10.14	Langzeitstabile Formate für Vektor- und kombinierte Grafiken: EPS	310
7.10.15	Langzeitstabile Formate für Vektorgrafiken: SVG	311
7.10.16	Langzeitstabile Formate für Seitenbeschreibung und beliebige Grafiken: PDF	311
7.10.16.1	PDF als ISO-Norm	312

7.10.16.2	PDF als Web-Format	312
7.10.16.3	PDF-Features	312
7.10.16.4	PDF-Probleme	313
7.10.16.5	PDF/X	313
7.10.16.6	PDF/A	314
8	ILM aus der Sicht der Anbieter	315
8.1	ILM und die Vollsortimenter	315
8.1.1	EMC ²	315
8.1.2	Hewlett-Packard inklusive TSG ⁹	316
8.1.3	IBM	317
8.1.4	Fujitsu Siemens Computers (FSC)	318
8.1.5	Network Appliances (NetApp)	318
8.1.6	SUN Microsystems mit der ILM-Lösung IM3 ¹⁰	318
8.1.7	Hitachi Data Systems: Der gewachsene Vollsortimenter	320
8.1.8	LSI Logic: Innovation mit Silicon-to-Systems	326
8.1.8.1	IBM	333
8.1.8.2	SUN/StorageTek	334
8.1.8.3	CRAY	335
8.1.8.4	TERADATA (NCR)	336
8.1.8.5	Silicon Graphics (SGI)	336
8.1.8.6	Verari Systems	336
8.1.8.7	Linux Networks	336
8.1.8.8	MaXXan	337
8.1.8.9	SEPATON	337
8.2	Interessante Spezialisten	343
8.2.1	Softwarelösungen	343
8.2.1.1	ECM-Lösungen	343
8.2.1.2	Tool zur Unterstützung der Klassifizierung	346
8.2.1.3	Symantec – der Vollsortimenter im Softwarebereich	347
8.2.2	Brocade – dateibasiertes Information Lifecycle Management (ILM) auf Basis des File Area Networking (FAN)	347
8.2.2.1	File Lifecycle Management	347
8.2.2.2	FAN ist die Basis für ILM	348
8.2.2.3	Einfache, regelbasierte Datenhaltung in Prozessen	350
8.2.2.4	Global Namespace und File Lifecycle Management	350
8.2.2.5	ILM – Komplexität der Umsetzung	351
8.2.3	DELL	352
8.3	ILM-Ansätze der Dienstleister	355
8.3.1	Accenture	355
8.3.2	BCG – Boston Consulting Group	355
8.3.3	Computacenter Compunet	355
8.3.4	CSC Ploenzke	356
8.3.5	EDS	356

8.3.6	Ernst & Young	356
8.3.7	Kienbaum	357
8.3.8	Logica CMG	357
8.3.9	Materna GmbH	357
8.3.10	McKinsey & Company	357
8.3.11	PriceWaterhouseCoopers (PWC)	358
8.3.12	Roland Berger Strategy Consultants	358
8.3.13	Siemens (hier SBS)	358
8.3.14	Deutsche Telekom AG (hier T-Systems)	358
9	Zusammenfassung und Fazit	361
	Literaturverzeichnis	363
	Sachwortverzeichnis	375