

# **A Conceptual Model for Compliant Management Systems**

by

**Leigh Howard de la Motte,  
B.Comp. (Hons.), Grad. Cert. Commercialisation**

A dissertation submitted in fulfilment  
of the requirements of the Degree of

**Doctor of Philosophy**

**University of Tasmania**

**November 2012**

## Declaration

---

I, Leigh de la Motte, declare that this dissertation contains no material which has been accepted for the award of any other degree or diploma in any tertiary institution. To my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the text of the dissertation.

This dissertation may be made available for loan and limited copying and communication in accordance with the Copyright Act 1968.

Signed,

Leigh de la Motte

Date:

## Abstract

---

The dissertation specifies a Set of Concepts and a Conceptual Model for Compliant Management Systems (CMSs). The Set of Concepts is drawn from existing methodologies and the CMS Model, which is based on the Concepts, is evaluated against a compiled Set of Standard Requirements. The dissertation is analytical, conceptual and argumentative in nature.

The Model is designed to enable the future development of compliant, efficient and globally functional organisational Information Technology (IT) Systems. The *Three Central Requirements* of the Model – *Compliance* (essentially a Legal requirement), *Efficiency* (essentially a Business Management requirement) and *Global Functionality* (essentially an IT requirement) – necessitated a multi-disciplinary investigation in the Legal, Business Management and IT areas.

Compliance was the focus of the research as initial investigations showed no significant solutions existed that provided specific guidelines for the design of inherently compliant IT systems. As compliance relates to meeting regulatory requirements on a local or jurisdictional basis, whereas efficiency and global functionality favour global standards for IT systems (that enable system interoperability), the means for delivering “globally compliant” IT systems is problematic. The research therefore took the approach of “thinking globally and acting locally” by designing a Model appropriate for individual local organisations that can be used, in association with the development of appropriate regulation, as a template for globally compliant IT systems.

It was found that the issues of *Privacy*, *Consent*, and *Accountability* were at the core of compliance requirements and that Digital Service Contracts with systematic Authorisation mechanisms for contract parties (represented as IT System “Groups”) provided the means for assuring compliance. The Model proposes software based on *Service*, *Group* and *Service Contract* components – the Service Contract components fulfilling Legal requirements, the Service components fulfilling Business Management requirements and the Group components fulfilling IT requirements.

The Model description in the dissertation focuses on the IT System design. Technical (software design) issues are not explored in detail, making the dissertation readable to persons with minimal IT background. The aim was to draw together existing knowledge in the Legal, Business Management and IT disciplines and to explore relationships between the fields at a high level rather than to delve in detail into any of the three disciplines. The research spans many fields within the three research disciplines, including Contract Law, Privacy Law, Company Law, Legal Consent, Franchising Systems, Business Process Management, Service Oriented Architectures, Cloud Computing, Access Control, Authorisation, Operating Systems, Data Management and Object Oriented Programming.

## Acknowledgements

---

The initial part of the research (about 75%) was supervised by the School of Computing and Information Systems. The remainder was supervised by the School of Law.

Special thanks go to my Supervisors – Jacky Hartnett, for her patience, time and advice on security and IT concepts, Prof Gino Dal Pont for his guidance in producing this dissertation and his advice on legal matters and Prof Young J. Choi for his oversight.

I would also like to thank all the health practitioners and administrators that have contributed ideas. Special thanks go to my wife, Heather, for her insights into hospital practices.

Christian McGee and Andrew Spilling were very helpful in assisting me with IT issues. My thanks also go to Daniel de la Motte for proof reading this document.

Finally, thank you to all my PhD colleagues, who have always made themselves available to assist when asked. Particular thanks go to Barry Pearn and Dean Steer for their help.

# Table of Contents

---

## Chapter 1

<b>Introduction .....</b>	<b>1</b>
1.1 Research Goals and Central Requirements .....	1
1.1.1 Limits of the Research.....	2
1.1.2 Ultimate Control and Compliance.....	3
1.2 The Research Disciplines .....	4
1.2.1 Disciplinary Dissertation Approaches.....	5
1.2.2 Use of Terminology.....	6
1.3 Background .....	7
1.3.1 Regulatory (Legal) Background.....	8
1.3.2 IT Background.....	9
1.3.3 Business Management Background .....	11
1.3.4 Existing Research Methodologies .....	12
1.4 CMS Definitions.....	15
1.4.1 Major CMS Terms.....	16
1.4.2 Definitions of Major CMS Terms .....	16
1.4.3 Organisational CMS Terms.....	18
1.4.4 Introducing the Seven General Concepts .....	19
1.5 Services .....	23
1.5.1 All-Encompassing Services.....	23
1.5.2 Standardized Service Parties .....	24
1.5.3 Standardized Service Processes.....	25
1.5.4 Commercial Service Aspects.....	26
1.5.5 Compliant Management System .....	27
1.5.6 Enabling Service Automation and Reuse.....	28
1.6 Groups .....	30
1.6.1 Groups used to Define and Manage Resources.....	30
1.6.2 Hierarchical Groups .....	32
1.6.3 Globally Addressable Groups .....	33

1.6.4	Group Templates .....	34
1.6.5	Group Types and Sub-Types .....	34
1.6.6	Groups Associated with Services .....	35
1.7	Service Contracts .....	35
1.7.1	Organisation Based Contracts .....	36
1.7.2	Single-Service Contracts .....	36
1.7.3	Sub-Service Contracts .....	37
1.7.4	Generic Service Contracts .....	37
1.7.5	Digitally Managed Contracts.....	38
1.7.6	Digital Service Contracts Enabling Compliance.....	39
1.8	Compliance Concepts .....	40
1.8.1	Privacy .....	40
1.8.2	Consent .....	41
1.8.3	Accountability .....	42
1.8.4	Authorisation .....	43
1.9	Dissertation Structure .....	47

## Chapter 2

<b>Methodology .....</b>	<b>49</b>	
2.1	Introduction .....	49
2.1.1	Initial Aim of the Research .....	49
2.1.2	Background .....	50
2.1.3	The Aim of Developing a Comprehensive and Practical Model..	50
2.1.4	A Research Voyage .....	51
2.2	Research Methodology .....	51
2.2.1	Examining Research Fields .....	53
2.2.2	Extracting Design Requirements .....	54
2.2.3	Finding Model Concepts .....	54
2.2.4	Developing the Model .....	55
2.2.5	The Validation Approach .....	56
2.3	Linking the General Concepts .....	58
2.3.1	Using Groups to Manage Authorisation and Consent.....	59
2.3.2	From Authorisation and Consent to Privacy .....	59

2.3.3	Linking Accountability and Privacy.....	60
2.3.4	Using Services to Manage Business Processes .....	60
2.3.5	Unifying the General Concepts with Service Contracts.....	61
2.4	Research Philosophy .....	61
2.4.1	Use Inductive Reasoning.....	61
2.4.2	Develop a Simple General Purpose Solution .....	62
2.4.3	Use Best Practice from Existing Solutions.....	63
2.4.4	Achieve Efficiency through Standardization .....	64
2.4.5	Incorporate Change Management .....	64
2.4.6	Adopt User-friendly Components .....	65
2.4.7	Automate Administration .....	66
2.5	Conclusion.....	67

## Chapter 3

<b>Literature Review .....</b>	<b>68</b>	
3.1	Introduction .....	68
3.2	Computer Security.....	69
3.2.1	Information Security Issues.....	69
3.2.2	Data Security Qualities.....	70
3.2.3	Information Ownership and Control .....	70
3.2.4	Authentication and Authorisation .....	72
3.2.5	Access Control Basics .....	73
3.2.6	The Principle of Least Privilege.....	74
3.2.7	Granularity.....	75
3.2.8	Computer Security Conclusion .....	75
3.3	Role-Based Access Control.....	75
3.3.1	Group Concept .....	77
3.3.2	Context Concept.....	78
3.3.3	Multiple Contexts .....	79
3.3.4	Constraint Concept.....	80
3.3.5	RBAC Conclusion.....	81
3.4	Set Theory .....	82
3.4.1	Set Based Access.....	82



3.5	Clark-Wilson Model.....	83
3.5.1	Well Formed Transactions .....	83
3.5.2	The Clark-Wilson Model.....	84
3.6	Health Informatics .....	86
3.6.1	Cooperative Practices .....	86
3.6.2	Multiple Authorisations.....	87
3.6.3	Guaranteed Access .....	87
3.7	Professional Access Control.....	88
3.7.1	Professional Management .....	88
3.7.2	Service Teams .....	89
3.7.3	Restricted Access .....	89
3.7.4	Authorisation Timing .....	90
3.7.5	Authorisation Ordering.....	92
3.8	Purpose Based Access Control.....	92
3.8.1	Purpose Concept.....	92
3.9	Service Oriented Architecture .....	93
3.10	Cloud Computing .....	95
3.10.1	Inter-Domain Access.....	95
3.10.2	Inter-Domain Roles .....	96
3.10.3	Inter-Domain Rule Processing .....	97
3.11	Generic Programming .....	98
3.11.1	The Generic Nature of Services and Groups.....	98
3.11.2	User Perceptions of Service and Group Concepts.....	99
3.11.3	Generic Services and Groups .....	100
3.12	Business Process Management.....	101
3.12.1	Workflow Processes .....	101
3.12.2	Organisational Systems .....	102
3.12.3	Business Constraints and Workflow Management .....	103
3.12.4	Task Based Authorisation .....	104
3.12.5	Task Based Access .....	104
3.12.6	Standard Business Processes .....	105
3.13	Legal Compliance.....	106
3.13.1	Organisational Compliance .....	106

3.13.2 Privacy Requirements.....	107
3.13.3 Client Consent .....	108
3.13.4 Legal Accountability .....	109
3.13.5 Service Contracts.....	111
3.14 Design Requirements Table .....	113
3.15 Conclusion.....	115

## Chapter 4

<b>Model Concepts .....</b>	<b>116</b>
4.1 Introduction .....	116
4.2 Model Concepts Relationship Diagram .....	116
4.3 Services .....	118
4.3.1 C#1: Global Services.....	118
4.3.2 C#2: Service Based Organisation.....	119
4.3.3 C#3: Serviceflow Dependencies .....	119
4.3.4 C#4: Service Cells .....	120
4.3.5 C#5: Client-Services.....	121
4.3.6 C#6: Service Profiles.....	121
4.3.7 C#7: Service Based Information .....	122
4.3.8 C#8: Client-Service Management .....	122
4.3.9 C#9: Service Based Security .....	122
4.4 Groups .....	123
4.4.1 C#10: Service Teams.....	123
4.4.2 C#11: Contextual Groups .....	124
4.4.3 C#12: Group Based Organisation.....	125
4.4.4 C#13: Group Based Access .....	126
4.4.5 C#14: Global Groups.....	127
4.4.6 C#15: Global Group Addressing .....	128
4.4.7 C#16: Group Based Services.....	128
4.4.8 C#17: Group Based Information Storage .....	129
4.4.9 C#18: Set Based Groups.....	130
4.4.10 C#19: Partial Permissions .....	131
4.4.11 C#20: Group Based Management .....	132

4.5	Service Contracts.....	133
4.5.1	C#21: Compulsory Compliance .....	133
4.5.2	C#22: Compliant System.....	133
4.5.3	C#23: Worker-Service Contracts .....	134
4.5.4	C#24: Client-Service Contracts.....	135
4.5.5	C#25: Contract Based Services .....	135
4.5.6	C#26: Validation by Authorisation .....	136
4.6	Privacy.....	137
4.6.1	C#27: The “5 Ws” of Access Control .....	137
4.6.2	C#28: Service Based Purpose.....	137
4.6.3	C#29: Service Based Access Principle.....	138
4.6.4	C#30: Service Based Privacy .....	138
4.6.5	C#31: Access by Authorisation.....	139
4.7	Consent.....	140
4.7.1	C#32: Consent Type Specification.....	140
4.7.2	C#33: Service Based Consent .....	141
4.7.3	C#34: Bundled Client Consent.....	141
4.7.4	C#35: Implied Permissions .....	141
4.7.5	C#36: Consent by Authorisation .....	142
4.7.6	C#37: Service Based Information Provision .....	142
4.8	Accountability .....	143
4.8.1	C#38: Service Based Accountability.....	143
4.8.2	C#39: Client-Service Accounting .....	144
4.8.3	C#40: Required Auditing .....	144
4.8.4	C#41: Client-Service Records .....	144
4.8.5	C#42: Service Based Auditing .....	145
4.9	Authorisation .....	145
4.9.1	C#43: Mandatory Authorisation.....	145
4.9.2	C#44: Authorisation Type Specification.....	146
4.9.3	C#45: Managerial Authorisation.....	146
4.9.4	C#46: Client-Service Allocation .....	147
4.9.5	C#47: Worker Acceptance .....	148
4.9.6	C#48: Worker Authorisation.....	148

4.9.7	C#49: Client Authorisation .....	150
4.9.8	C#50: Service Based Authorisation .....	151
4.9.9	C#51: Sub-Service Authorisation.....	151
4.9.10	C#52: Authorisation Management .....	152
4.10	Model Concepts Table.....	152
4.11	Conclusion.....	154

## Chapter 5

<b>Model Description.....</b>	<b>155</b>	
5.1	Introduction .....	155
5.2	Incorporating Model Concepts .....	155
5.2.1	Foundational Model Concepts.....	156
5.2.2	Model Design Concepts .....	157
5.3	Model Components .....	158
5.3.1	Component Relationships.....	158
5.3.2	Organisation Composition.....	159
5.3.3	Component Origin.....	160
5.3.4	Component Instances .....	162
5.4	The Compliant Management System .....	163
5.4.1	CMS Programs and Data.....	165
5.4.2	Global Data Storage .....	169
5.4.3	A Global Access System example.....	170
5.4.4	Managing Components.....	172
5.5	Service Management .....	173
5.5.1	The Service Management Process.....	175
5.5.2	High Level Service Management .....	176
5.5.3	Management of Personal Work.....	177
5.6	Group Management .....	178
5.6.1	Group Management Services .....	179
5.7	Contract Management .....	180
5.7.1	Service Authorisations .....	181
5.7.2	Contract Management Services.....	182
5.8	Client-Service Example.....	183

5.9	Table of Model Concept Mechanisms.....	186
5.10	Conclusion.....	189

## Chapter 6

<b>Analytical Evaluation .....</b>	<b>190</b>	
6.1	Introduction .....	190
6.1.1	The Standard Requirement Set.....	190
6.1.2	Model Evaluation .....	190
6.2	Purpose Related Standards .....	192
6.2.1	SR#1: Purpose & Correctness .....	192
6.2.2	SR#2: Need to Know Access .....	192
6.2.3	SR#3: Intellectual Property .....	193
6.3	Service/Task Related Standards .....	193
6.3.1	SR#4: Critical Protection.....	193
6.3.2	SR#5: Security Integration .....	193
6.3.3	SR#6: Service Based Access .....	194
6.4	Consent Practice Standards .....	194
6.4.1	SR#7: Data Collection.....	194
6.4.2	SR#8: Consent for Purpose .....	195
6.4.3	SR#9: Consent Judgment .....	195
6.4.4	SR#10: Consent Collection .....	196
6.5	Client Rights Standards .....	196
6.5.1	SR#11: Client Access .....	196
6.5.2	SR#12: Accessor Information .....	197
6.5.3	SR#13: Disclosure Account .....	197
6.5.4	SR#14: Restriction .....	197
6.5.5	SR#15: Complaint & Appeal .....	198
6.5.6	SR#16: Information Provision Process .....	198
6.6	Organisation Rights Standards .....	199
6.6.1	SR#17: Directory Data .....	199
6.6.2	SR#18: De-Identified Data.....	199
6.6.3	SR#19: Restriction Refusal .....	200
6.6.4	SR#20: Access Refusal .....	200

6.7	Access Rules Standards .....	200
6.7.1	SR#21: Sensitive Information .....	200
6.7.2	SR#22: Relevant Disclosures .....	201
6.7.3	SR#23: Basic Disclosures .....	201
6.7.4	SR#24: Emergency Access .....	202
6.7.5	SR#25: Event Based Disclosure .....	202
6.7.6	SR#26: Victim Disclosure .....	202
6.7.7	SR#27: Regulated Disclosure .....	203
6.8	Authorisation Standards .....	204
6.8.1	SR#28: Authorisation .....	204
6.8.2	SR#29: Role Based .....	204
6.8.3	SR#30: Validation .....	205
6.8.4	SR#31: Written Authorisation .....	205
6.8.5	SR#32: Information Flow .....	206
6.8.6	SR#33: Transaction .....	206
6.8.7	SR#34: Inter-Domain Authorisation .....	207
6.9	Compliance Practices Standards .....	207
6.9.1	SR#35: Openness & Accountability .....	207
6.9.2	SR#36: Compliance .....	208
6.9.3	SR#37: Risk Management .....	208
6.9.4	SR#38: Security Responsibility .....	209
6.9.5	SR#39: Skills & Qualifications .....	209
6.9.6	SR#40: User Account .....	210
6.9.7	SR#41: Privacy Personnel .....	210
6.9.8	SR#42: Data Correction .....	210
6.10	Information Provision Standards .....	211
6.10.1	SR#43: Information Provision .....	211
6.10.2	SR#44: Disclosure Account Data .....	211
6.10.3	SR#45: Staff Reminder .....	212
6.11	Monitoring/Auditing/Reporting Standards .....	212
6.11.1	SR#46: Activity Monitoring .....	212
6.11.2	SR#47: Security Auditing .....	213
6.11.3	SR#48: Management Auditing .....	213

6.11.4 SR#49: Incident Management .....	213
6.11.5 SR#50: Required Documentation.....	214
6.12 Model Rating Table .....	214
6.13 Conclusion.....	216

## Chapter 7

### **Results and Discussion .....218**

7.1 Introduction .....	218
7.1.1 Incorporating the Old and the New .....	219
7.1.2 Tradition and Future Possibilities.....	220
7.1.3 Towards Automated Business Management .....	221
7.1.4 Results and Discussion Topics .....	222
7.2 Contributions of the Research .....	222
7.2.1 Model Concept Set and New Concepts .....	222
7.2.2 The Model .....	230
7.2.3 The Standard Requirements .....	231
7.3 Analysis of the Model .....	231
7.3.1 Model Validation.....	231
7.3.2 Comparison with Current Methodologies .....	232
7.3.3 Limitations of the Model.....	239
7.4 Application of the Model .....	241
7.4.1 Regulatory Compliance .....	241
7.4.2 Business Efficiency .....	250
7.4.3 Global Functionality.....	255
7.5 Future Work .....	259
7.5.1 Compliant Management System .....	259
7.5.2 Service Based Regulation.....	260
7.5.3 Privacy of Personal Records.....	260
7.5.4 Business Web .....	260
7.5.5 Web of Identities .....	260
7.5.6 Supply Chain Management .....	261
7.5.7 Component Repositories .....	261
7.6 Conclusion.....	262

<b>References .....</b>	<b>264</b>
<b>Glossary .....</b>	<b>268</b>