

Contents

1	Introduction	1
1.1	Motivation	2
1.2	Risks in Adopting Cloud Computing	7
1.3	Factors Influencing Compliance-based Risks	8
1.3.1	Transparency Risk	9
1.3.2	Process Automation Risk	12
1.3.3	Repudiation Risk	12
1.4	Research Objective	14
1.5	Research Description	15
1.5.1	Main Research Question	15
1.5.2	Research Questions One and Two (Environment)	17
1.5.3	Research Questions Three and Four (Knowledge Base)	17
1.5.4	Research Questions Five and Six (Implementation)	19
1.5.5	Research Question Seven (Evaluation)	20
1.6	Structure of the Dissertation	20
2	Methodology	21
2.1	Information Systems Research Framework	22
2.1.1	Focus Group Discussions Based on Krueger	25
2.1.2	The STIRL Process Based on Buchkremer et al.	26
2.1.3	Systematic Literature Review Based on Vom Brocke et al.	28
2.1.4	Rapid Application Development Based on Martin	31
2.1.5	ALMA Based on Bengtsson et al.	33

2.1.5.1	Case Study Based on Yin	34
2.1.5.2	Semi-Structured Expert Interviews Based on W.C. Adams	34
2.1.5.3	Qualitative Content Analysis Based on Mayring	35
2.2	Guidelines for Design Science in is Research	37
2.3	Discussion	39
3	Theoretical Framework	41
3.1	Definitions and Foundations	41
3.1.1	Cloud Computing Fundamentals	41
3.1.2	The Reference Architecture of Cloud Computing	45
3.1.3	The Meaning of Trust in Multiple Disciplines	46
3.1.4	Risk and Risk Assessment	47
3.1.5	The Relation Between Trust and Risk	49
3.1.6	Cloud Adoption Risks	51
3.1.7	The Elliptic Curve Digital Signing Schema	52
3.1.7.1	Generator Algorithm G	54
3.1.7.2	Signing Algorithm S	55
3.1.7.3	Verification Algorithm V	55
3.1.8	Diffie Hellman Key Exchange	56
3.1.9	Trusted Third Parties	58
3.1.10	Blockchain	59
3.1.11	Smart Contracts	65
3.1.12	Discussion	67
3.2	Environment and Scope of the Dissertation	67
3.2.1	Conducting the Focus Group Discussion	68
3.2.1.1	Planning	68
3.2.1.2	Description of the Categorization	70
3.2.1.3	Questions	70
3.2.1.4	Recruiting	71
3.2.1.5	Moderating	72
3.2.2	Qualitative Content Analysis	72
3.2.3	Categorization and Coding of the Focus Group Discussion	73
3.2.4	Meta-Analysis of the Results	74
3.2.5	Analysis of the Results	76
3.2.5.1	Cloud Computing	76
3.2.5.2	Cloud Computing Advantages	76

3.2.5.3	Cloud Computing Challenges	77
3.2.5.4	Trust Environment	78
3.2.5.5	Compliance and Configuration Environment	79
3.2.5.6	Risk and Trust Management Technologies	80
3.2.5.7	Enhancing Technologies	80
3.2.5.8	Blockchain	81
3.2.6	Discussion	81
3.3	Systematic Literature Review	83
3.3.1	STIRL-based Literature Grouping	84
3.3.2	Definition of Review Scope	89
3.3.3	Conceptualization of Topic	90
3.3.4	Literature Search	90
3.3.5	Literature Analysis and Synthesis	93
3.3.6	Research Agenda	93
3.3.7	Systematic Literature Research Result	93
3.3.7.1	Time Analysis	94
3.3.7.2	Concept Analysis	95
3.3.8	Discussion	105
3.4	Related Work	106
3.4.1	Literature Overview	107
3.4.2	Importance of Blockchain in Compliance Management	109
3.4.3	Sharing Cloud Configurations	110
3.4.4	Ensuring Confidentiality in Cloud Configurations	112
3.4.5	Architecture Design	113
3.4.6	Discussion	114
4	Implementation	117
4.1	Cloud Application Configurations	117
4.1.1	Formal Definition of Streams	120
4.1.2	Formal Definition of Configurations	121
4.1.3	Discussion	122
4.2	Artifact Development	123
4.2.1	Requirements Planning Phase	123
4.2.2	User Design Phase	128
4.2.2.1	Management Smart Contract (Smart Contract)	130

4.2.2.2	Cloud Management Script (Cloud-Side Application)	133
4.2.2.3	Consumer Management Script (Client-Side Application)	138
4.2.2.4	The Business Process in a Nutshell	142
4.2.3	Construction Phase	147
4.2.3.1	Management Smart Contract Implementation	149
4.2.3.2	Cloud Management Script Implementation	151
4.2.3.3	Consumer Management Script Implementation	153
4.2.4	Cutover Phase	158
4.2.4.1	Background on Intrusion Detection Systems	158
4.2.4.2	Deployment	159
4.2.4.3	Cloud Application Configuration	161
4.3	Discussion	164
5	Evaluation	167
5.1	Step One: Set the Goal of the Evaluation	169
5.2	Step Two: Describe Software Architecture	170
5.3	Step Three: Elicit Scenarios	170
5.3.1	Scenario a: Medium-Sized Company Wants to Adopt a Cloud Application from an ISO 27001-Certified Company	171
5.3.2	Scenario B: Large-Sized Company Wants to Adopt a Cloud Application from a Low-Cost Supplier	172
5.3.3	Scenario C: Regional Group Wants to Run a Website from the Existing Software Provider	172
5.4	Step Four: Evaluate Scenarios	173
5.4.1	Selecting and Recruiting the Respondents	174
5.4.2	Drafting the Questions and Interview Guide	175
5.4.3	Polishing Interview Techniques	179
5.4.4	Conducting the Data Collection	179
5.5	Step Five: Interpret the Results	180
5.5.1	Qualitative Content Analysis	180
5.5.2	Categorization and Coding of the Interview Results	181
5.5.3	Describing and Evaluating the Results	181

5.5.3.1	Background and Knowledge	181
5.5.3.2	Case Study	185
5.5.3.3	Risk Management	185
5.5.3.4	Trust Management	185
5.5.3.5	Architecture Notes	186
5.5.3.6	Blockchain	187
5.5.3.7	Wishes or Requests	187
5.6	Answering RQ 7	188
5.6.1	Transparency Risk	190
5.6.2	Process Automation Risk	192
5.6.3	Repudiation Risk	195
5.7	Discussion	197
6	Conclusion and Outlook	201
6.1	Discussion	201
6.2	Conclusion	203
6.3	Limitations and Outlook	207
	Bibliography	211