Architectural Design Document (ADD)
Enterprise Cybersecurity Design Strategy

Enterprise-Scale Cybersecurity Compliance Pattern

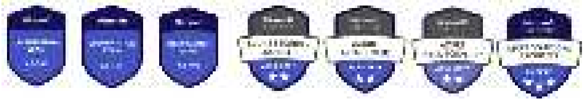
living document (ld)

Prepared for

VBIC

Prepared by

Dr. Olaf Cames, DBA, MSc(Dist)
MSc in IT with Distinction (Information Cybersecurity)
Doctor of Business Administration



legal@action-science.org
Polycloud Cybersecurity Architect

copyright VBIC 2022

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
Dec 2022	Dr. Olaf Cames, DBA, MSc(Dist)	2.01 draft	Commercial marketplace consulting service offer

copyright VBIC 2022

Revision/Sign off sheet

Name	Version approved	Position	Date

copyright VBIC 2022

Contents

Enterprise-Scale Cybersecurity Compliance Pattern 1
Change Record 2
Executive Summary 9
Adaptation of Enterprise Cybersecurity Design Strategy 9
Chosen pattern: 9
1. Background 10
1.1. Enterprise Cybersecurity Design Strategy 10
1.1.1. Part I: Achievement of goals with limited resources: Automate the build, compliance checking, and remediation for Azure 10
1.2.1. Process Overview 10
1.2.1.1. Cybersecurity (PC) Template Process Flow (PCTPF) 10
1.2.1.2. Business Enablement Process 12
2. High-level Functional Use Cases 12
3. Business Objectives (Goal) and Critical Success Factors 13
3.1. Micro-Approval request 13
3.1.1. Micro-Approval request for Use Case 5 14
4. Business Process Context, Scope 17
4.1. Actors 17
4.1.1. Use Case 5: Micro-Approval request (sample/template) 17
4.2. Actors 18
4.2.1. Use Case 1 18
4.2.2. Use Case 2 18
4.2.3. Use Case 3 18
4.2.4. Use Case 4 18
5. Software-Defined Cloud Interconnects Architecture Pattern (SDCIA) 19
5.1 Cybersecurity SDCI Architecture Pattern (PSDCI) 19
5.2 Cybersecurity SDCI Zone Pattern (PSDCI-Z) 20
5.3 Cybersecurity Branch Connectivity Automation Pattern (PBCA) 21
6. Software-Defined Cloud Interconnects Landing Zone Pattern (SDCIZ) 22
6.1. Cybersecurity Policies Pattern (PPP) 22
6.2. Cybersecurity Automated Routing Pattern (PARP) 23
6.3. Cybersecurity Automated Routing Pattern (PARP) 24
6.4. Cybersecurity Enterprise-Scale Landing Zone Architecture Pattern (PLAAP) 25

copyright VBIC 2022

6.5. Combination of PCTPC and PLAAP Pattern 26
6.5.1. Micro approval embedded in target Architecture (sample/template) 26
6.6. Cybersecurity Kubernetes Pattern (PKP) 27
6.6.1. Resources and Workload Protection Pattern (PKP-RWPP) 27
27
6.6.2. Cybersecurity Kubernetes multi-tenancy and deployment dependency management pattern (PKP-MTDM) 28
7. Part III: Cybersecurity Cyber Threat Intelligence Pattern (PCTIP) 31
7.1. Analysis 31
7.1.1. Activity documentation, synthesis, and correlation 31
References 32
Glossary 33
Appendix A 36
Subject: 36
Status: 36
- Overview 36
- Scope of this review 36
In-Scope 36
Out-of-Scope 36
- Cloud Governance 38
Platform Maturity Remaining Risk Statement 38
- Architecture Diagram 148
- Technical Details 149
- Business/Flow Details 149
- Authentication 149
- Authorization 149
- Audit and Logging 149
- Input Validation / Output Encoding 149
- Session Management 149
- Data Cybersecurity 149
- Firewall Rules 149
- Potential Exceptions to Proposed Design 149
- QuickStart 149
RACI matrix 149
- Glossary 150
- References 150
Appendix B 153

copyright VBIC 2022

Subject: 153
Status: 153
- Overview 153
- Scope of this review 153
In-Scope 153
Out-of-Scope 153
- Cloud Governance 155
Platform Maturity Remaining Risk Statement 155
Platform Automation Remaining Risk Statement 158
Platform Assurance Controls Remaining Risk Statement 163
- Architecture Diagram 183
- Technical Details 185
- Business/Flow Details 185
- Authentication 185
- Authorization 185
- Audit and Logging 185
- Input Validation / Output Encoding 185
- Session Management 185
- Data Cybersecurity 185
- Firewall Rules 185
- Potential Exceptions to Proposed Design 185
- QuickStart 185
RACI matrix 185
ARM template 186
Template Deployment 190
- Glossary 190
- References 190
Appendix C 191
Decision record template for Cybersecurity pattern (draft) 191
1. Prologue (Summary) 191
2. Discussion (Context) 191
3. Solution (Decision) 191
4. Consequences (Results) 191
1. Prologue (Summary) 191
2. Discussion (Context) 191
3. Solution (Decision) 191
4. Consequences (Results) 191

copyright VBIC 2022

Appendix D 192

Lower-level augmentation indicator in the level 300 design strategy 192

Appendix E 193

Lower-level architectural design modification proposal 193

Appendix F 195

Cybersecurity Cryptographically Isolating Single Tenant Instances Pattern (PCITP) 195

Appendix G 196

Variational Quantum Eigensolver (VQE) 196

Stricter Cybersecurity requirements beyond semantic Cybersecurity: addressing remaining attack surfaces in homomorphic encryption 196

copyright VBIC 2022

Dr. Olaf Cames

Digitally signed by Dr. Olaf Cames
Date: 2022.12.27 15:25:25 -05'00'

Figures

Figure 1 The Cybersecurity (PC) Template Process Flow (PCTPC) 10
Figure 2 The Cybersecurity (PC) Template Process Flow (PCTPC) deliverables 11
Figure 3 Figure 3 Cybersecurity Cybersecurity Architecture Risks - 2 dimensional statistics 11
Figure 4 The Cybersecurity (PC) Template Process Flow (PCTPC)- Business Enablement Process (BEP) 12
Figure 5 Adaptation of Cybersecurity SDCI architecture via PSDCI pattern 19
Figure 6 Adaptation of Cybersecurity SDCI zone architecture via PSDCI-Z pattern........ 20
Figure 9 Cybersecurity Branch Connectivity Automation Pattern (PBCA) 21
Figure 10 Cybersecurity Policies Pattern (PPP) 22
Figure 11 Cybersecurity Automated Routing Pattern (PARP) 23
Figure 12 Cybersecurity NoOps Automation via PARP Pattern 24
Figure 13 Adaptation of enterprise-scale landing zone architecture via PLAAP Pattern 25
Figure 14 Use Case 5: Micro-Approval request embedded in target Architecture via PCTPC and PLAAP Pattern 26
Figure 15 Cybersecurity Kubernetes Resources & Workloads Protection 27
Figure 16 Cybersecurity Kubernetes multi-tenancy and deployment dependency management pattern (PKP-MTDM)........ 28
Figure 17 Excerpt from RACI Chart - Best Practice - ID AARACI104 v1.04 155
Figure 18 Cybersecurity scaling solution cryptographically isolating single tenant instances available for AES 128-bit, 256-bit symmetric, and homomorphic keys........ 195
Figure 19 Variational Quantum Eigensolver (VQE) 196
Figure 20 Quantum Homomorphic Encryption with a Classical Client 196

copyright VBIC 2022