

# Contents

|          |                                                                                 |           |
|----------|---------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction .....</b>                                                       | <b>9</b>  |
| 1.1      | What is Access Control? .....                                                   | 9         |
| 1.1.1    | Risk Analysis and Remediation (RAR) .....                                       | 10        |
| 1.1.2    | Protect Information and Prevent Fraud .....                                     | 12        |
| 1.2      | Architecture of Access Control .....                                            | 13        |
| 1.3      | Necessity of SOX .....                                                          | 15        |
| 1.4      | Overview of Cross-Enterprise for Access Control .....                           | 18        |
| 1.5      | Summary .....                                                                   | 19        |
| <b>2</b> | <b>SAP GRC Access Control Rule Architect .....</b>                              | <b>21</b> |
| 2.1      | Overview of the Rule Architect .....                                            | 21        |
| 2.1.1    | Rule Files .....                                                                | 23        |
| 2.1.2    | How to Create Rules in an Application .....                                     | 35        |
| 2.1.3    | Active Rules .....                                                              | 37        |
| 2.1.4    | Rule Architect Dashboard .....                                                  | 41        |
| 2.2      | Building Cross-Enterprise Rules .....                                           | 43        |
| 2.2.1    | Example .....                                                                   | 44        |
| 2.3      | Summary .....                                                                   | 45        |
| <b>3</b> | <b>Managing Access Risk .....</b>                                               | <b>47</b> |
| 3.1      | Central Rule Library: The Global Rule Set .....                                 | 47        |
| 3.1.1    | Risk Recognition .....                                                          | 48        |
| 3.1.2    | Risk Identification .....                                                       | 48        |
| 3.2      | Rule Migration in the System Landscape and During the RAR Upgrade Process ..... | 48        |
| 3.3      | Import/Export Utility .....                                                     | 50        |
| 3.3.1    | Configuration .....                                                             | 50        |
| 3.3.2    | Features .....                                                                  | 51        |
| 3.4      | Summary .....                                                                   | 55        |

|          |                                                                                        |           |
|----------|----------------------------------------------------------------------------------------|-----------|
| <b>4</b> | <b>Cross-Enterprise Matrix for SAP GRC AC .....</b>                                    | <b>57</b> |
| 4.1      | Available Real Time Agent (RTA) for SAP .....                                          | 57        |
| 4.2      | RTA for Non-SAP ERP Applications .....                                                 | 58        |
| 4.2.1    | Integration with Oracle .....                                                          | 59        |
| 4.2.2    | Integration with PeopleSoft .....                                                      | 63        |
| 4.2.3    | Integration with JDE .....                                                             | 63        |
| 4.2.4    | Integration with Legacy Systems .....                                                  | 64        |
| 4.2.5    | RTA Deployment .....                                                                   | 64        |
| 4.2.6    | Connector Creation .....                                                               | 64        |
| 4.3      | Summary .....                                                                          | 64        |
| <b>5</b> | <b>Configuration and Operation of the Data Extractor .....</b>                         | <b>65</b> |
| 5.1      | System Connector .....                                                                 | 67        |
| 5.2      | Configure Extraction Process .....                                                     | 67        |
| 5.2.1    | Extraction Process in Legacy Systems .....                                             | 68        |
| 5.2.2    | Extraction Process in SAP Access Control .....                                         | 70        |
| 5.3      | Production .....                                                                       | 80        |
| 5.4      | Summary .....                                                                          | 80        |
| <b>6</b> | <b>Risk Analysis for Cross-Enterprise Systems .....</b>                                | <b>81</b> |
| 6.1      | Scheduling Background Jobs .....                                                       | 81        |
| 6.1.1    | Scheduling Synchronization Jobs, Including Methods<br>for Legacy/Offline Systems ..... | 82        |
| 6.1.2    | Scheduling Batch Risk Analysis .....                                                   | 84        |
| 6.2      | Management Report Updates .....                                                        | 85        |
| 6.3      | Real Time Risk Analysis .....                                                          | 86        |
| 6.4      | Cross-Enterprise Execution in the AC Application .....                                 | 87        |
| 6.5      | Offline Risk Analysis .....                                                            | 92        |
| 6.6      | Summary .....                                                                          | 93        |
| <b>7</b> | <b>Mitigation and Alerts .....</b>                                                     | <b>95</b> |
| 7.1      | Mitigation Controls .....                                                              | 95        |
| 7.2      | Mitigated Users/Roles/Profiles/HR Objects .....                                        | 96        |
| 7.2.1    | How to Create a Mitigation Control .....                                               | 96        |

|     |                                    |     |
|-----|------------------------------------|-----|
| 7.3 | Alert Generation .....             | 101 |
| 7.4 | Alert Dashboard .....              | 103 |
| 7.5 | Alert Clearing and Archiving ..... | 104 |
| 7.6 | Summary .....                      | 105 |

## **8 Continuous Compliance ..... 107**

|     |                                                |     |
|-----|------------------------------------------------|-----|
| 8.1 | Best Practices for Continuous Compliance ..... | 107 |
| 8.2 | Simulation .....                               | 109 |
| 8.3 | Monitoring and Control .....                   | 112 |
| 8.4 | Summary .....                                  | 112 |

## **Appendices ..... 113**

|      |                                                       |     |
|------|-------------------------------------------------------|-----|
| A    | Rule Library File Templates .....                     | 115 |
| A.1  | Business Process Template .....                       | 115 |
| A.2  | Function Template .....                               | 115 |
| A.3  | Function-Business Process Relationship Template ..... | 116 |
| A.4  | Function-Action Relationship Template .....           | 116 |
| A.5  | Function-Permission Relationship Template .....       | 116 |
| A.6  | Rule Set Template .....                               | 117 |
| A.7  | Risk Definition Template .....                        | 117 |
| A.8  | Risk Description Template .....                       | 118 |
| A.9  | Risk to Rule Set Relationship Template .....          | 119 |
| B    | Legacy System Templates .....                         | 121 |
| B.1  | User File Template .....                              | 121 |
| B.2  | User Action File Template .....                       | 122 |
| B.3  | User Permission File Template .....                   | 122 |
| B.4  | Role File Template .....                              | 124 |
| B.5  | Role Action File Template .....                       | 124 |
| B.6  | Role Permission File Template .....                   | 125 |
| B.7  | Profile File Template .....                           | 126 |
| B.8  | Profile Action File Template .....                    | 126 |
| B.9  | Profile Permission File Template .....                | 127 |
| B.10 | Action File Template .....                            | 127 |
| B.11 | Permission File Template .....                        | 128 |
| B.12 | Field File Template .....                             | 129 |
| B.13 | Value File Template .....                             | 130 |

## Contents

|     |                                          |     |
|-----|------------------------------------------|-----|
| C   | Information Sources .....                | 133 |
| C.1 | Installation and Upgrades .....          | 133 |
| C.2 | SAP Help Portal for Access Control ..... | 134 |
| D   | The Author .....                         | 135 |
|     | Index .....                              | 137 |