

Contents

Acknowledgments	xv
Introduction	xvii

PART I

Defining the Value of and the Need for IAM

1	Who's Where, and Why Do You Care?	3
	The Value of Identity to User and Enterprise	4
	General Benefits of IAM	6
	The Value of Identity to the Enterprise	6
	Self-Service, Part I	6
	Privacy, Part I	7
	Productivity, Part I	7
	Managing the Masses	8
	The Value of Identity to the End User	9
	Exceptions	10
	Self-Service, Part II	10
	Privacy, Part II	11
	Productivity, Part II	11
	Getting What You Need from IAM	11
2	Determining Your Need for an IAM Framework	13
	Investigating Your Internal Necessities	14
	Starting from Scratch	14
	Time for Compliance	14
	All-Manual Processes	15
	Hard-Coded Security	16
	Expansion of the Business	16
	Expansion or Sudden Popularity of a Resource	16
	Replacing or Augmenting IAM	17
	Persistent All-Manual Processes	17

Too Much Customization	18
Insufficient Business Support	18
Patchwork Systems	18
Purely Business Reasons	19
Nonintegrated Systems	19
Vendor No Longer in Business	20
Inadequate Workflow Capabilities	20
Mergers and Acquisitions (M&A)	20
Obsolete Systems	21
Throughput Expansion	21
User Expansion	21
Excessive Cost	21
Augmentation of Existing Systems	22
A Bad First Choice	22
Making the Business Case, Round One	22

PART II

Preparing the Enterprise for IAM

3	Planning an IAM Project	29
	Resources, Both Digital and Human	30
	The Processes	30
	The Requirements	31
	The Pieces	32
	The People	32
	The Resources	33
	The Design	33
	The Roll-Out	34
	Remembering the Goal	34
	Getting Ready to Break Things	35
	Determining Specific Requirements	36
	The Essentials of IAM	37
	Governance by Committee	38
	Engage Stakeholders	40
	Which Committees to Assemble	40
	An Iterative Process	43
4	Compliance Considerations	45
	What Compliance Typically Includes	46
	Compliance Components	47
	What Compliance Should Include	47
	Controls	48
	Privacy	49
	Attestation and Reconciliation	49
	Segregation of Duties (SoD)	50
	Audit Support	50

	Event Scheduling	51
	Enterprise Reporting	51
	Forensics	52
	Analytics	52
	Data Retrieval	53
	Regulatory Compliance Laws	54
	The United States	55
	Greater North America	60
	Latin America	60
	Asia-Pacific	61
	Europe, the Middle East, and Africa (EMEA)	64
	The Takeaways	65
5	Making the Business Case	67
	Round Two in Front of Management	68
	Sell the Business Value	68
	Look Organized	68
	Believe in Your Message	69
	Prioritize	69
	Compile Real Evidence	69
	Anticipate Objections	69
	Getting Help with Your Pitch	70
	Request Budget	71
	Return on Investment (ROI)	71
	Hard ROI	72
	Soft ROI	72
	Preserving Your Existing Investment	74
	Asking for Help, One More Time	74
	Finalizing the Request	75
6	Achieving Pitfalls: Common Mistakes in IAM	77
	Mistakes Both Large and Small	78
	Boiling the Ocean	78
	Failure to Communicate	79
	Trust, But Verify	79
	No Corporate Sponsorship	80
	Lack of a Governance Committee	80
	Scope Creep	80
	Being Nailed to Legacy Systems	80
	Overselling	81
	Failing to Meet Deliverables	81
	Presuming Everybody's on Board	82
	Failing to Plan for Integration	82
	Investing Before Analyzing	82
	Failure to Invest the Internal Resources	83
	Forgetting the Goal	83

PART III

The Oracle Identity and Access Solution

7	Designing an Oracle IAM Framework	87
	The Latest and Greatest	88
	The Purpose of the Framework	90
	The Oracle Identity Suite	91
	Defining Your Organization, Top to Bottom	92
	Defining Your Resources	93
	Preparing Resources for the Job of Provisioning	94
	Source(s) of Truth and Authority	95
	What Goes into Those Authoritative Sources?	96
	Oracle Directory Services: OID, OVD, and ODSEE	97
	Populate Your Authoritative Source(s)	102
	Service Accounts	103
	Enabling Your Population: Roles, Privileges, and Access	103
	When the Tail Wags the Dog	108
	Authenticating and Authorizing Your Population	109
	Governance, Compliance, and Reporting in the Design	113
	Centralized and Delegated Administration	116
	Security in the Development Process	117
	The End Process: Termination	118
	Cleanup and the Creation of Artifacts	120
	Deciding When Design Is Completed	121
8	User Account Creation	123
	Bulk Loading	124
	One-Time Reconciliation	126
	Identity Management System	126
	HR Event	126
	Customer Service	127
	Self-Registration	127
	Universal Requirements	128
9	Provisioning: Now That I'm In, What Can I Have?	131
	Oracle Provisioning	133
	Organizations and Groups	136
	Defined Resources and Connectors	137
	User Profiles	139
	Legacy IDs	141
	Workflow Definitions	142
	Workflow Designer	143
	Workflow Events	146
	Workflow Separation	146
	Notifications	147
	Manual Provisioning	148
	Impersonation and Proxy Users	148

Automated Provisioning	149
Access Policies	150
Pre-Provisioning	150
Reconciliation	151
Role-Based Provisioning	152
What's in a Role?	154
Building Roles	156
Role Life Cycle	156
Role History	157
Database Security and Provisioning	157
Reporting and Compliance	158
10 Authentication and SSO: Accessing What I've Been Granted	161
Authentication Architecture	162
Simple Authentication	165
Defining the Authentication Scheme for a Resource	166
Single Sign-On	167
Strong Authentication, Historically	170
Very Strong Authentication, Alternatively	170
Protecting the User	176
Gated Security	178
11 Authorization: Now That I've Got It, How Do I Get to It?	181
Layers of Authorization	182
Coarse-Grained Authorization	184
Coarse-Grained Protection of Web Services	185
Authorization Rules	186
Extending the Authorization Model	187
Basing Authorization on Risk, Activity, and Behavior	187
Fine-Grained Entitlements	188
OES Architecture	190
Federation	194
Oracle's Federation Solution	197
Federation Types	198
Database Security	198
12 Compliance Support	201
Common Elements of Regulatory Compliance	202
Privacy Requirements	203
PCI	206
Certification: The Ugliest Compliance Process?	211
Automated, Simplified Certification	213
The Value of Automated Certification	216
Role Governance	218
Reconciliation of User Accounts	218

Segregation of Duties	220
How Deep Should SoD Go?	221
Preventive Versus Detective SoD	222
Database-Level SoD	226
Keeping Things from Getting Away from You	226
Audit Support	227
Build Your Own Security Audit	228
Scheduled Reports	229
Real-Time Audit Support	230
Compliance and the Cloud	231
Forensics	231
Post-Visit Audit Requests	231
13 The Time Bomb Everybody Forgets: Things Change	235
Impact Analysis	237
Changes to Users and Policies	238
Identity Changes	238
Source of Authority on User Changes	240
When Temporary Changes Become Permanent	241
Changes to Roles	241
Changes to the Organization	242
Changes to Resources	244
Schema Changes	245
Validating Policy Changes: Impact Analysis	245
Evolution of Risk Models	248
Adding Federation	249
Accepting Recommendations from Auditors	249
Changes to Infrastructure	250
Twenty-Four/Seven Availability	251
14 Legacy Considerations	253
Definition of Legacy	254
Legacy Business, Legacy Identity	254
IAM Components to Keep	255
Help Desk	255
Workflow	257
Directories	257
Authentication Schemes	258
Scripts, Libraries, and Other Provisioning Bits	258
IdM Discards	259
IdM Sources to Mine for Data	260
Historic Activity Data	260
Reclaiming User Accounts	260
Role Mining/Discovery/Definition	261
Legacy Business Components	265

15	Testing Your Framework	269
	Incremental Testing	270
	Integration Testing	273
	Regression Testing	273
	Load Testing	274
	Load Testing in Increments	275
	Penetration Testing	276

PART IV

Pre- and Post-Implementation Advice

16	Choosing Software	281
	Buy vs. Build	282
	So You've Decided to Build	283
	Open Source	284
	So You've Decided to Buy (or at Least Shop)	284
	Big vs. Little	285
	How to Look	285
	Vendor Visits	286
	What's Truly Important?	287
	Get Some Help Shopping	288
	Customization	289
	Go with Experience	290
	Go with Commitment to the Space	290
	Watch the Strictly Proprietary Stuff	291
	Non-Disclosure Agreements	292
	RFPs	292
	POCs and Pilots	296
	References: Getting One, Being One	297
	CPU Pricing vs. Seat-Based Pricing	298
	Cloud Computing	298
	One Last Thing about Vendors	299
17	Getting Help with Your IAM Project	301
	Types of External Resources	302
	When the Seller and the Builder Are a Package Deal	303
	Small-to-Medium Integrators	304
	Larger Integrators	305
	References	305
	Transfer of Knowledge	305
	Keeping the Peace	306
18	Notes on the Actual Implementation	309
	Keep People in the Loop (Sort Of)	310
	Governance	311
	Mid-Stream Changes	312

xiv Designing an IAM Framework with Oracle Identity and Access Management Suite

Phased Deployment	313
Cut-Overs	313
Training	314
Rounding Up the Stragglers	315
Make Sure Everybody Plays Nice	316
Control the Communications	316
Everybody Protects Everybody Else	317
Educate the Masses	317
Establish Ownership and Responsibilities	318
19 Post-Implementation: Keeping the Framework Running	319
Adoption	320
Show Results	321
Monitor Those First Transactions	321
Pass That Audit	322
Accountability	322
Monitor, Maintain, Modify	323
Monitor and Manage the Pieces	323
OAAM and the Evolution of Policies	324
Deploying the Next Phase	325
Standards Support	325
What Did We Learn From All of This?	327
Index	329