

Supply Chain Risk Management

Applying Secure Acquisition Principles to
Ensure a Trusted Technology Product

Ken Sigler, Dan Shoemaker, and Anne Kohnke



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

AN AUERBACH BOOK

Contents

Forewordxi
Preface.....xiii
Authors.....xvii
Contributions.....xix
Chapter Structure and Summary.....xxi

1 Why Secure Information and Communication Technology

Product Acquisition Matters 1
Introduction to the Book 1
Underwriting Trust and Competence2
Justification and Objectives of the Book.....3
The Five-Part Problem.....4
Putting Product Assurance into Practice7
The Supply Chain and the Weakest Link.....8
Visibility and Control9
Building Visibility into the Acquisition Process 11
The Seven Phases of ICT Acquisition Practice 13
 Practice Area One: Procurement Program Initiation and Planning 14
 Practice Area Two: Product Requirements Communication
 and Bidding 16
 Practice Area Three: Source Selection and Contracting..... 16
 Practice Area Four: Supplier Considerations.....20
 Practice Area Five: Customer Agreement Monitoring.....21
 Practice Area Six: Product Acceptance.....22
 Practice Area Seven: Project Closure.....23
Building the Foundation: The Role of Governance in Securing the
 ICT Supply Chain23
The Use of Standard Models of Best Practice32
Chapter Summary33
Key Concepts38
Key Terms39
References 40

2	Building a Standard Acquisition Infrastructure	41
	ISO/IEC 12207	42
	Agreement Processes: Overview	45
	Acquisition Process.....	47
	Acquisition Activity: Acquisition Preparation	50
	Concept of Need.....	51
	Define, Analyze, and Document System Requirements	52
	Consideration for Acquiring System Requirements	53
	Preparation and Execution of the Acquisition Plan.....	54
	Acceptance Strategy Definition and Documentation	55
	Prepare Acquisition Requirements.....	56
	Acquisition Activity: Acquisition Advertisement	57
	Acquisition Activity: Supplier Selection	58
	Acquisition Activity: Contract Agreement.....	59
	Acquisition Activity: Agreement Monitoring.....	60
	Acquisition Activity: Closure	61
	Supply Process.....	61
	Supply Activity: Opportunity Identification.....	63
	Supply Activity: Supplier Tendering	63
	Supply Activity: Contract Agreement.....	65
	Supply Activity: Contract Execution	67
	Supply Activity: Product/Service Delivery and Support.....	74
	Supply Activity: Closure	75
	Chapter Summary.....	75
	Key Terms	76
	References	77
3	The Three Building Blocks for Creating Communities of Trust	79
	Introduction to Product Trust	79
	Building a Basis for Trust	81
	The Hierarchy of Sourced Products	82
	The Problem with Sourced Products.....	88
	Promoting Trust through Best Practice	92
	Moving the Product up the Supply Chain	93
	The Standard Approach to Identifying and Controlling Risk.....	95
	The Three Standard Supply Chain Roles	96
	The Acquirer Role.....	97
	The Supplier Role	101
	The Integrator Role.....	104
	Information and Communication Technology Product Assurance.....	105
	Adopting a Proactive Approach to Risk	107
	People, the Weakest Link	108

Chapter Summary.....	110
Key Concepts.....	114
Key Terms.....	115
References.....	115
4 Risk Management in the Information and Communication Technology (ICT) Product Chain.....	117
Introduction.....	117
Supply Chain Security Control Categorization.....	119
Categorization Success through Collaboration.....	123
Supply Chain Security Control Selection.....	124
The Eight Tasks of Control Selection.....	128
Documentation Prior to Selection.....	128
Select Initial Security Control Baselines and Minimum Assurance Requirements.....	128
Determine Need for Compensating Controls.....	131
Determine Organizational Parameters.....	132
Supplement Security Controls.....	132
Determine Assurance Measures for Minimum Assurance Requirements.....	134
Complete Security Plan.....	135
Develop a Continuous Monitoring Strategy.....	136
Supply Chain Security Control Implementation.....	137
Implement the Security Controls Specified in the Security Plan.....	138
Security Control Documentation.....	141
Supply Chain Security Control Assessment.....	142
The Four Tasks of Security Control Assessment.....	144
Implications of Security Control Authorization to the Supply Chain.....	149
The Four Tasks of Security Control Authorization.....	151
Supply Chain Risk Continuous Monitoring.....	155
The Seven Tasks of Security Continuous Monitoring.....	157
Determine the Security Impact of Changes.....	158
Assess Selected Security Controls.....	159
Conduct Remediation Actions.....	159
Update the Security Plan, Security Assessment Report, and POA&M.....	160
Report the Security Status.....	160
Review the Reported Security Status on an Ongoing Basis.....	161
Implement an ICT System Decommissioning Strategy.....	162
Chapter Summary.....	162
Key Terms.....	164
References.....	165

5	Establishing a Substantive Control Process	167
	Introduction: Using Formal Models to Build Practical Processes	167
	Why Formal Models Are Useful	169
	NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems	170
	The 21 Principles for SCRM	172
	Principle 1: Maximize Acquirer’s Visibility into the Actions of Integrators and Suppliers in the Process.....	173
	Principle 2: Ensure That the Uses of Individual Supply Chain Components Are Kept Confidential	174
	Principle 3: Incorporate Conditions for Supply Chain Assurance in Specifications of Requirements	175
	Principle 4: Select Trustworthy Elements and Components	176
	Principle 5: Enable a Diverse Supply Chain—Do Not Sole Source	176
	Principle 6: Identify and Protect Critical Processes and Elements.....	176
	Principle 7: Use Defensive Design in Component Development.....	176
	Principle 8: Protect the Contextual Supply Chain Environment.....	177
	Principle 9: Configure Supply Chain Elements to Limit Access and Exposure.....	177
	Principle 10: Formalize Service/Maintenance Agreements.....	177
	Principle 11: Test throughout the SDCL.....	178
	Principle 12: Manage All Pertinent Versions of the Configuration	178
	Principle 13: Factor Personnel Considerations into Supply Chain Management.....	179
	Principle 14: Promote Awareness, Educate, and Train Personnel on Supply Chain Risk	179
	Principle 15: Harden Supply Chain Delivery Mechanisms.....	179
	Principle 16: Protect/Monitor/Audit the Operational Supply Chain System	180
	Principle 17: Negotiate and Manage Requirements Changes.....	180
	Principle 18: Manage Identified Supply Chain Vulnerabilities.....	181
	Principle 19: Reduce Supply Chain Risks during Software Updates and Patches.....	181
	Principle 20: Respond to Supply Chain Incidents	181
	Principle 21: Reduce Supply Chain Risks during Disposal.....	182
	Making Control Structures Concrete: FIPS 200 and NIST 800-53(Rev 4)	182
	Application of FIPS 200 and NIST 800-53(Rev 4) to Control Formulation.....	183
	The Generic Security Control Set.....	186

NIST 800-53 Control Baselines	186
Detail of Controls	187
Six Feasibility Considerations for NIST 800-53	188
NIST 800-53 Catalog of Baseline Controls	190
Implementing Management Control Using the Standard	
NIST SP 800-53 Rev. 4 Control Set	191
Practical Security Control Architectures	192
Control Statements	192
Supplemental Guidance	193
Control Enhancements	193
Real-World Control Formulation and Implementation	193
Limitations of the 800-53 Approach in SCRM	194
Chapter Summary	196
Key Concepts	199
Key Terms	200
References	201
6 Control Sustainment and Operational Assurance.....	203
Sustaining Long-Term Product Trust.....	203
Step 1: Establish and Maintain Situational Awareness	205
Step 2: Analyze Reported Vulnerability and Understand	
Operational Impacts	209
Environmental Monitoring.....	210
Vulnerability Reporting	210
Vulnerability Response Management	211
Step 3: Obtain Management Authorization to Remediate	212
Understand Impacts.....	213
Communicating with Authorization Decision-Makers.....	215
Step 4: Manage and Oversee the Authorized Response	216
Responding to Known Vulnerabilities with Fixes	217
Responding to Known Vulnerabilities without Fixes	217
Fixing an Identified ICT Supply Chain Vulnerability.....	218
Step 5: Evaluate the Correctness and Effectiveness of the	
Implemented Response	219
Step 6: Assure the Integration of the Response into the Larger	
Supply Chain Process.....	223
Establishing a Supply Chain Assurance Infrastructure	225
Policies for Operational Assurance: Method, Measurement,	
and Metrics	226
Building a Practical Supply Chain Sustainment Function.....	228
Generic Management Roles.....	230
Conducting the Day-to-Day Operational Response Process	230

Response Management Process Planning.....231

Deciding What to Secure232

Enforcing Management Control232

Status Assessment.....233

Maintaining Documentation Integrity234

Chapter Summary.....234

Key Concepts.....237

Key Terms237

References238

7 Building a Capable Supply Chain Operation.....239

Introduction.....239

Why a Capability Maturity Model?.....241

A Staged Model for Increasing Capability in Supply

 Chain Management242

 Level One: The Initial Level244

 Level Two: The Repeatable Level244

 Level Two: Acquisition Planning.....246

 Level Two: Solicitation247

 Level Two: Requirements Development and Management248

 Level Two: Project Management249

 Level Two: Contract Tracking and Oversight250

 Level Two: Evaluation251

 Level Two: Transition to Support251

 Level Three: The Defined Level253

 Level Three: Process Definition and Maintenance254

 Level Three: User Requirements.....256

 Level Three: Project Performance Management.....257

 Level Three: Contract Performance Management.....257

 Level Three: Acquisition Risk Management258

 Level Three: Training Program Management.....259

 Level Four: The Quantitative Level.....260

 Level Four: Quantitative Process Management.....260

 Level Four: Quantitative Acquisition Management261

 Level Five: The Optimizing Level.....262

 Level Five: Continuous Process Improvement262

 Level Five: Acquisition Innovation Management.....263

Practical Evaluation of Supply Chain Process Maturity.....264

Maturity Rating Schemes266

Chapter Summary.....267

Key Terms272

References272