



Information Shield Solution Matrix for Sarbanes-Oxley

Based on COBIT® Control Objectives

This table contains information for organizations that must comply with the Sarbanes-Oxley Act or are otherwise using the COBIT® Framework^[1] to establish audit controls for their information technology systems.^[2] For each domain and process of the COBIT framework, the various control objectives are shown with the corresponding policy category from Information Security Policies Made Easy (ISPME) Version 10. Items marked with a ++ are specifically addressed by policies within ISPME.

COBIT DOMAIN/Process	ISPME Policies and Categories
PLAN & ORGANISE	
P01 Define a Strategic IT Plan	4.01.03-16. Information Security Plans 7.01.01-2. Physical Security Plan 8.03.01-2. Computer Emergency Response Plans 11.03.01-2. Preparation And Maintenance Of Business Contingency Plans
P02 Define the Information Architecture	5.01 Accountability For Assets
2.1 Enterprise Information Architecture Model ++	5.01.01 Inventory Of Assets (12 policies)
2.2 Enterprise Data Dictionary and Data Syntax Rules	5.01.01-4. Corporate Data Dictionary
2.3 Data Classification Scheme ++	5.01.01 Inventory Of Assets (12 policies) 5.02 Information Classification 5.02.01 Classification Guidelines (23 policies) 5.02.02 Information Labeling And Handling (42 policies)
2.4 Integrity Management++	8.04.01 Information Backup 8.06 Media Handling and Security 8.07 Exchanges of Information and Software
P03 Determine Technological Direction	10.01.01 Security Requirements Analysis And Specification (15 policies) 4.01.03-15. Information Security Standards And Procedures 11.01.02 Business Contingency And Impact Analysis (3 policies)
P04 Define the IT Processes, Organization and Relationships	
4.1 IT Process Framework	

4.2 IT Strategy Committee	
4.3 IT Steering Committee	
4.4 Organisational Placement of the IT Function	* Covered in Information Security Roles and Responsibilities Made Easy
4.5 IT Organisational Structure	4.01.01 Management Information Security Forum
4.6 Roles and Responsibilities	4.01.03 Allocation Of Information Security Responsibilities (25 policies)
4.7 Responsibility for IT Quality Assurance	4.01.03-14. Authorization To Review Any Information System
4.8 Responsibility for Risk, Security and Compliance	4.01.03-10. Centralized Information Security 4.01.03- 13. Information Security Department Mission 4.01.02-13. Information Security Department Tasks
4.9 Data and System Ownership ++	4.01.03-1. Information Ownership Assignment 4.01.03- 25. Information Ownership Delegation 4.01.03- 22. Information Custodian 4.01.03- 23. Information Custodian Responsibilities 4.01.03-20. Information Systems Department Ownership Responsibility 4.01.03-19. Assigning Information Ownership 5.01.01-6. Information Ownership
4.11 Segregation of Duties ++	8.01.04 Segregation Of Duties
4.12 IT Staffing ++	6.01.01 Including Security In Job Responsibilities * Covered in Information Security Roles and Responsibilities Made Easy
4.13 Key IT Personnel ++	8.01.01-6. Key Technical Jobs
4.14 Contracted Staff Policies and Procedures ++	4.03.01 - Security Requirements In Outsourcing Contracts
4.15 Relationships	4.01.06 Cooperation Between Organizations
P05 Manage the IT Investment	4.01.03-7. Budgeting For Information Security
P06 Communicate Management Aims and Direction	Chapter 5 Sample Detailed Information Security Policy
6.1 IT Policy and Control Environment	3.01.01 Information Security Policy Document (10 policies) 3.01.12 Policy-Driven Information Systems Security Architecture 4.01.03-10. Centralized Information Security 6.02.01- 10. Training Responsibility
6.2 Enterprise IT Risk and Internal Control Framework	
6.3 IT Policies Management	3.01.02 Policy Review And Evaluation 3.01.02 Exceptions to Policies 12.01.02 Intellectual Property Rights 12.02 Reviews Of Security Policy And Technical Compliance
6.4 Policy Rollout	12.02.01 Compliance With Security Policy
6.5 Communication of IT Objectives and Direction	6.01.01- 1. Policy Quiz 6.01.01- 6. Information Security Training 6.02.01 Information Security Education And Training (21 policies)

P07 Manage IT Human Resources	
7.1 Personnel Recruitment and Promotion	6.01.03 Confidentiality Agreements (5 policies) 6.01.01 Including Security In Job Responsibilities
7.2 Personnel Competencies ++	6.01.04 Terms And Conditions Of Employment
7.3 Staffing of Roles ++	6.01.01 Including Security In Job Responsibilities
7.4 Personnel Training ++	6.02.01 Information Security Education And Training (21 policies)
7.5 Dependence Upon Individuals	06.02.01-18. Technical Training And Apprenticeship 08.04.01 - 1. Job Rotation
7.6 Personnel Clearance Procedures ++	6.01.02 Personnel Screening And Policy (22 policies)
7.7 Employee Job Performance Evaluation	06.01.01- 2. Performance Evaluations
7.8 Job Change and Termination ++	06.01.04- 18. Notification Of Worker Terminations 09.02.01- 20. Deletion Of Terminated Worker Files 6.03.05 Disciplinary Process
P08 Manage Quality	
P09 Assess and Manage IT Risks	
	4.01.03- 4. Risk Assessments 4.01.02 Information Security Coordination 4.02.01 Identification Of Risks From Third-Party Access (16 policies) 11.01.02-3. Business Impact Analysis 12.01.01- 6. System Risk Assessments Appendix L: Management Risk Acceptance Memo
P010 Manage Projects	

ACQUIRE & IMPLEMENT	
AI1 Identify Automated Solutions	8.02.02- 8. Information Security Impact Analysis 10.05.05 Outsourced Software Development 4.03.01 Security Requirements In Outsourcing Contracts (15 policies)
AI2 Acquire and Maintain Application Software	10.02 Security In Application Systems 10.05.01 Change Control Procedures (25 policies) 10.05.03 Restrictions On Changes To Software Packages (2 policies)
AI3 Acquire and Maintain Technology Infrastructure	7.02.04 Equipment Maintenance (6 policies) 7.02.06 Secure Disposal Or Re-Use Of Equipment

AI4 Enable Operation and Use	8.01.01 Documented Operating Procedures (14 policies)
AI5 Procure IT Resources	
AI6 Manage Changes	8.01.02 Operational Change Control (7 policies)
AI7 Install and Accredite Solutions and Changes	8.02 System Planning And Acceptance 8.02.02 System Acceptance (12 policies) 8.02.03-5. Production Application Acceptance 10.05.02 Technical Review Of Operating System Changes

DELIVER & SUPPORT	
DS1 Define and Manage Service Levels	
DS2 Manage Third-Party Services	4.02.01 Identification Of Risks From Third-Party Access (16 policies) 4.02.02 Security Requirements In Third-Party Contracts (21 policies) 4.03.01 Security Requirements In Outsourcing Contracts (15 policies) 10.05.05 Outsourced Software Development
DS3 Manage Performance and Capacity	8.02.01 Capacity Planning (2 policies)
DS4 Ensure Continuous Service	
4.1 IT Continuity Framework	11.01.01 Business Continuity Management Process (5 policies) 11.01.04 Business Continuity Planning Framework (3 policies)
4.2 IT Continuity Plan	11.01.02 Business Contingency And Impact Analysis 11.01.03 Writing And Implementing Contingency Plans (3 policies)
4.3 Critical IT Resources	11.01.01-3. Vendors Providing Mission Critical Hardware & Software 4.02.01-14. Critical Vendor Financial Review
4.4 Maintenance of the IT Continuity Plan	11.01.05 Testing, Maintaining, And Re-Assessing Business Continuity Plans (6 policies)
4.5 Testing of the IT Continuity Plan	(See 11.01.05)
4.6 IT Continuity Plan Training	
4.7 Distribution of IT Continuity Plan	11.01.01-2. Contingency Plan Accessibility

4.8 IT Services Recovery and Resumption	7.02.02-2. Redundant Utility Suppliers 7.02.05 Security Of Equipment Off-Premises 08.05.01-9. Multiple Carriers 11.01.05-1. Reversion To Manual Procedures 11.01.05-2. Off-Site Personnel Rotation
4.9 Off-site Back-up Storage ++	7.02.01-7. Backup Data Center Infrastructure
4.10 Post Resumption Review	(See 11.01.05) 6.03.04 Learning From Incidents
DS5 Ensure Systems Security	
5.1 Management of IT security Measures	4.01 Information Security Infrastructure 4.01.01 Management Information Security Forum 4.01.03 Allocation Of Information Security Responsibilities 4.01.07 Independent Review Of Information Security 12.02.02 Technical Compliance Checking (4 policies)
5.2 IT Security Plan	4.01.03-16. Information Security Plans
5.3 Identity Management	9.01.01 Access Control Policy 9.01.01 - 9. Centralized Access Control Database 9.02.03 User Password Management (12 policies) 9.05.03 User Identification And Authentication (6 policies) 9.05.04 Password Management System (26 policies) 9.03.02 Unattended User Equipment
5.4 User Account Management ++	9.02.01 User Registration (26 policies) 9.02.02 Privilege Management (12 policies) 9.02.04 Review Of User Access Rights 9.03 User Responsibilities 9.03.01 Password Use (24 policies)
5.5 Security testing, Surveillance and Monitoring ++	9.07 Monitoring System Access And Use 12.03.01 System Audit Controls (3 policies) 12.03.02 Protection Of System Audit Trails
5.6 Security Incident Definition ++	6.03.01 Reporting Security Incidents (30 policies) 6.03 Responding To Security Incidents And Malfunctions (5 sections) 8.01.03 Incident Management Procedures (2 policies)
5.7 Protection of Security Technology	9.07.01 Event Logging (14 policies) 9.07.02 Monitoring System Use (25 policies)
5.8 Cryptographic Key Management	10.03 Cryptographic Controls 10.03.02 Encryption (14 policies) 10.03.05 Key Management (34 policies)
5.9 Malicious Software prevention, detection and correction	8.03.01 Controls Against Malicious Software (26 policies)
5.10 Network Security	Chapter 20 Sample Firewall Policy 9.04.07 Network Connection Control (6 policies) 9.04.08 Network Routing Control 9.04.09 Security Of Network Services
5.11 Exchange of Sensitive Data	8.07 Exchanges Of Information And Software 8.07.02 Security Of Media In Transit (6 policies) 8.07.04 Security Of Electronic Mail (47 policies) 8.07.01 Information And Software Exchange Agreements (6 policies) 10.02.01 Input Data Validation (4 policies) 10.02.03 Message Authentication (2 policies)

	10.03.03 Digital Signatures (2 policies) 10.03.04 Non-Repudiation Services
DS6 Identify and Allocate Costs	
DS7 Educate and Train Users	6.02.01 Information Security Education And Training (21 policies)
DS8 Manage Service Desk and Incidents	6.03.01 Reporting Security Incidents (30 policies) 6.03.01-3. Centralized Problem Reporting
DS9 Manage the Configuration	8.03.01 Controls Against Malicious Software 8.03.01 - 4. Downloading Software 8.03.01 - 5. Software Scanning 8.03.01 - 13. System Integrity Checking 8.02.02 System Acceptance 8.02.02 -12. Systems Configuration Templates
DS10 Manage Problems *	6.03 Responding To Security Incidents And Malfunctions (5 sections)
10.1 Identification and Classification of Problems	6.03.01 Reporting Security Incidents (30 policies) 6.03.02 Reporting Security Weaknesses
10.2 Problem Tracking and resolution ++	6.03.01-3. Centralized Problem Reporting
10.3 Problem Closure	
10.4 Integration of Change, Configuration and Problem management	
DS11 Manage Data	8.04.01 Information Backup (23 policies) 8.06 Media Handling and Security 8.06.01 Management of Removable Computer Media (3 policies) 8.06.02 Disposal of Media (13 policies) 8.06.03 Information Handling Procedures (25 policies) 12.01.03 Safeguarding Of Organizational Records (19 policies)
DS12 Manage the Physical Environment *	
12.1 Site Selection and Layout	7.01.05 Isolated Delivery And Loading Areas 7.02.01 Equipment Siting And Protection 6.01.04-9. Workplace Hazards
12.2 Physical Security ++	7 Physical And Environmental Security 7.01.01 Physical Security Perimeter 7.01.02 Physical Entry Controls (29 policies) 7.01.03 Securing Offices, Rooms, And Facilities (5 policies) 7.01.04 Working In Secure Areas (9 policies) 7.03.01 Clear Desks And Clear Screen Policy (8 policies)

	7.03.02 Removal Of Property
12.3 Physical Access	7.01.02-29. Computer Facility Tours 7.01.02-11. Physical Access Of Terminated Workers 7.01.02-22. Unescorted Visitors
12.4 Protection Against Environmental Factors	7.02.01- 4. Computer Center Environmental Controls 7.02.01-13. Computer Center Locations 7.02.03 Cabling Security
12.4 Physical Facilities Management	6.01.04-8. Health And Safety Information 7.02.02 Power Supplies (2 policies)
DS13 Manage Operations	
	8.01 Operational Procedures And Responsibilities 8.01.01 Documented Operating Procedures (14 policies) 8.01.02 Operational Change Control (7 policies)

MONITOR and EVALUATE	
ME1 Monitor and evaluate IT performance	8.04.02 Operator Logs (3 policies) 9.07.01 Event Logging (14 policies) 9.07.02 Monitoring System Use (25 policies) 6.03.04 Learning From Incidents 12.03.01 System Audit Controls (3 policies) 12.03.02 Protection Of System Audit Trails (2 polices)
ME2 Monitor and evaluate internal control	12.02.01 Compliance With Security Policy (7 policies) 12.02.02 Technical Compliance Checking (6 policies)
ME3 Ensure regulatory compliance	4.01.07 Independent Review Of Information Security (2 policies) 12.01 Compliance With Legal Requirements 12.01.01 Identification Of Applicable Legislation 12.01.04 Data Protection And Privacy Of Personal Information 12.01.02 Intellectual Property Rights
ME4 Provide IT Governance	4.01.07 Independent Review Of Information Security (2 policies) 4.02.01 Identification Of Risks From Third-Party Access 4.03.01- 1. Independent Control Reports

[1] This product includes COBIT® 4th Edition, which is used by permission of the IT Governance Institute (ITGI). ©1996, 1998, 2000 IT Governance Institute. All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.”

[2] While the actual Sarbanes-Oxley legislation does not specify a set of detailed requirement for information security, most organizations have used the COBIT® framework as a reference for filling in the detailed information technology control requirements. Sarbanes-Oxley does specify that organizations must use a standard control framework which has international support, such as the COSO framework published by the Committee for Sponsoring Organizations (COSO). While COSO is a general framework for all controls, auditors and information technology consultants have looked to the COBIT framework to provide more detail within the information technology area.

[3] Note: ISPME V10 is topically organized around the ISO 17799:2000 information security framework, and is based upon information security leading practices. COBIT, while containing many overlaps with information security, is based around the more general information technology functions. Therefore, in the areas where COBIT overlaps strongly with the traditional information security requirements, ISPME will have a high-level of policy coverage. ISPME will have little or no policy coverage in control areas that do not involve information security.