 

Auditing IT Infrastructures for Compliance
 Second Edition
Transition Guide

By Martin Weiss & Michael Solomon
ISBN-13: 9781284090703
Paperback • 400 Pages • ©2016

**Main Updates**

* New studies and statistics throughout
* Includes references to updated federal laws, including FISMA and the DoD
* Includes references to updated standards such as COBIT, SANS, ISACA, ISO/IEC 27001 and CRMA
* Discusses new technology including social networking sites and electronics
* Incorporates new and updated tables and figures
* Provides new website resources, key concepts and terms, and assessment questions

**Major Chapter Changes Are Listed Below**

**Chapter 1**

* Material on the integrity of information systems updated

**Chapter 2**

* Material on IT compliance requirements updated
* Information on regulatory agencies added
* Federal Information Security Management Act of 2002 (FISMA) updated to include information regarding 2014 amendment by Federal Information Security Modernization Act
* “Laws and Regulations of the DoD” section updated to clarify information on The Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the E-Government Act of 2002
* Information added on NIST six-step risk management framework (RMF), as well as a comparison between RMF and C&A
* Figure 2-1 updated
* Information Assurance (IA) replaced with cybersecurity
* New section “Children’s Online Privacy Protection Act (COPPA)” added

**Chapter 3**

* Definitions added for gap analysis, identity theft, privacy office*,* LAN, and WAN
* Information on SANS updated to include 2013 transfer of Critical Security Controls to Council on CyberSecurity
* Description of 20 critical controls updated
* Table 3-2 updated

**Chapter 4**

* Information on COBIT updated due to 2014 changes and to reflect COBIT 5
* Information on ISACA added
* Figure 4-2 updated
* “SAS 70 Compliance” section replaced with “Service Organization Control (SOC) Reports” section
* Additional information security series included
* Table 4-3 replaced with new Table 4-2
* Information on ISO/IEC 27001 updated
* Section on the NIST “Cybersecurity Framework” added

**Chapter 5**

* Definitions added for scope creep and CPO
* “Threat Analysis” section updated
* Information on quantitative risk analysis added
* COBIT control objectives updated
* Consensus Audit Guidelines updated to Critical Security Controls

**Chapter 6**

* Topics and Goals updated
* Various line edits
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 7**

* Topics and Goals updated to reflect new sections
* “Maturity modeling” section replaced and updated
* Tables 7-2, 7-3, and 7-6 updated
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 8**

* Key Concepts and Terms updated with new entries
* Various line edits
* Assessment Questions updated

**Chapter 9**

* New Figure 9-2
* Technology references updated to include smartphones, tablets, etc.
* “Wardialing” and “wardriving” entries updated
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 10**

* Table 10-2 updated
* Definitions added for WLANs and networking devices
* New website resources added
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 11**

* New website resources added for network management tools and NAC software products
* Key Concepts and Terms updated with new entries
* Various line edits
* Assessment Questions updated

**Chapter 12**

* New section on “cloud computing”
* Figure 12-4 updated
* New website resources added for WAN optimization tools
* Section on “WAN Service Provider SOC Compliance” updated
* Table 12-5 updated
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 13**

* User Datagram Protocol (UDP) defined
* A-I-C updated to C-I-A
* Various line edits
* Key Concepts and Terms updated with new entries
* Assessment Questions updated

**Chapter 14**

* A-I-C updated to C-I-A
* New website resources added for application performance monitoring software
* Table 14-3 updated
* Key Concepts and Terms updated
* Assessment Questions updated

**Chapter 15**

* “ISACA seven guiding principles” updated
* URLs updated
* “(ISC)2 Code of Ethics” updated with new information regarding the Certified Authorization Professional (CAP), Certified Cyber Forensics Professional (CCFP), and Healthcare Information Security and Privacy Practitioner (HCISPP) certifications
* “CompTIA certifications” updated to include the CompTIA Cloud, Mobility, Storage, Cloud Essentials, Healthcare IT Technician, Social Media Security Professional (SMSP), IT Fundamentals, and Advanced Security Practitioner (CASP) certifications
* New section on “Certification in Risk Management Assurance (CRMA)” added
* “SANS” section updated with new 2015 data and updated Table 15-1 on Global Information Assurance Certification (GIAC) programs
* Key Concepts and Terms updated with new entries
* Assessment Questions updated