

Addressing Compliance from One Infrastructure: Cisco Unified Compliance Solution Framework



The Cross-Walk

Organizations responsible for handling and storing customer information must protect personal data, including health records and financial information. In the United States and abroad, regulatory statutes such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX) and the Payment Card Industry Data Security Standard (PCI DSS) have been established to define responsibilities and practices, and are backed by financial penalties for public or private organizations that fail to comply, or where personal data is actually breached.

Although achieving compliance requires more than just technology, the network is critical in supporting organizations' compliance strategies. Cisco offers a Unified Compliance Solution Framework with guidelines that enable you to address multiple regulatory compliance requirements from one network infrastructure. The Cisco[®] Compliance Solution includes the following mandates which are mapped to Cisco products to create a cross-walk:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes–Oxley (SOX)

The set of integrated and audited architectures that incorporate technology from Cisco and Cisco technology partners helps enterprises meet these complex mandates and requirements. The cross-walk and assessments were completed in partnership with an external auditor, Verizon Global Services Group.

Simplified Crosswalk – HIPAA, PCI, and SOX

Title	Citation	PCI Cross Reference	SOX Cross Reference
Security Management Process	164.308(a)(1)(i)	12.1, 12.1.1, 12.1.1.1, 12.1.3, 12.2, 12.6, 12.9, 12.9.1, 12.9.2, 12.9.3, 12.9.4, NA – ALL	CA (DS5) Monitoring CE (ME12) Internal Control Program
Risk Analysis	164.308(a)(1)(ii)(A)		CA (A16) Risk Assessment
Risk Management	164.308(a)(1)(ii)(B)		CA (A16) Risk Assessment
Information System Activity Review	164.308(a)(1)(ii)(D)	10.2.7 (Y), 10.3, 10.3.1 (Y), 10.3.2 (Y), 10.3.3 (Y), 10.3.4 (Y), 10.3.5 (Y), 10.3.6 (Y), 10.6, 11.5, 12.9.6	CA (DS5) Monitoring
Assigned Security Responsibility	164.308(a)(2)		CA (DS5) Monitoring
Authorization and/or Supervision	164.308(a)(3)(ii)(A)	2.2.3, 7.1.4 (Y), 7.2, 7.2.3 (Y), 8.2 (Y), 8.5.1, 8.5.16, 10.2.7 (Y), 10.3, 10.3.1 (Y), 10.3.2 (Y), 10.3.3 (Y), 10.3.4 (Y), 10.3.5 (Y), 10.3.6 (Y), 10.6, 11.5	
Termination Procedures	164.308(a)(3)(ii)(C)	8.2 (Y), 8.5.1, 8.5.16	
Isolating Health Care Clearinghouse Function	164.308(a)(4)(ii)(A)	2.1.1, 2.2.3, 6.6, 7.1.4 (Y), 12.8.2	
Access Authorization	164.308(a)(4)(ii)(B)	2.2.3, 7.1.4 (Y), 7.2, 7.2.3 (Y), 8.2 (Y), 8.5.1, 8.5.16	
Access Establishment and Modification	164.308(a)(4)(ii)(C)	8.2 (Y), 8.5.1, 8.5.16	
Protection from Malicious Software	164.308(a)(5)(ii)(B)	5.1, 5.1.1, 5.2, NA – ALL	CA (DS9) Manage Configuration
Log-in Monitoring	164.308(a)(5)(ii)(C)	10.1 (Y), 10.2, 10.2.1 (Y), 10.2.5 (Y), 10.2.7 (Y), 10.3, 10.3.1 (Y), 10.3.2 (Y), 10.3.3 (Y), 10.3.4 (Y), 10.3.5 (Y), 10.3.6 (Y), 10.5.4 (Y), 10.6, 11.5	CA (DS5) Monitoring
Password Management	164.308(a)(5)(ii)(D)	2.1, 2.1.1, 8.4 (Y), 8.5, 8.5.2, 8.5.3, 8.5.7, 8.5.8 (Y), 8.5.9 (Y), 8.5.10 (Y), 8.5.11 (Y), 8.5.12 (Y), 8.5.13 (Y), 8.5.14 (Y)	
Response and Reporting	164.308(a)(6)(ii)	12.6, 12.9, 12.9.1, 12.9.2, 12.9.3, 12.9.4, 12.9.6, NA – ALL	CA (DS5) Monitoring
Contingency Plan	164.308(a)(7)(i)	9.1.1 NA	
Evaluation	164.308(a)(8)	11.3, 12.1, 12.1.1, 12.1.2, 12.1.3, 12.2, NA – ALL	CA (DS5) Monitoring
Facility Access Control and Validation Procedures	164.310(a)(2)(iii)	NA	CA (DS12) Physical Security
Unique User Identification	164.312(a)(2)(i)	3.2, 8.1 (Y), 8.2 (Y), 8.5.1, 8.5.8 (Y), 8.5.16, 12.3.2	
Emergency Access Procedure	164.312(a)(2)(ii)	7.1.4 (Y)	
Automatic Logoff	164.312(a)(2)(iii)	8.5.15 (Y), 12.3.8	
Encryption and Decryption	164.312(a)(2)(iv)	3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, NA – ALL	
Audit Controls	164.312(b)	10.1 (Y), 10.2, 10.2.1 (Y), 10.2.5 (Y), 10.2.7 (Y), 10.3, 10.3.1 (Y), 10.3.2 (Y), 10.3.3 (Y), 10.3.4 (Y), 10.3.5 (Y), 10.3.6 (Y), 10.5.4 (Y), 10.6, 11.5	
Data Integrity	164.312(c)(1)	2.3, 4.1 (Y), 4.1.1 (Y)	CA (DS9) Manage Configuration
Person or Entity Authentication	164.312(d)	3.2, 8.1 (Y), 8.2 (Y), 8.5.1, 8.5.8 (Y), 8.5.16, 12.3.2	
Integrity Controls	164.312(e)(2)(i)	2.1.1, 4.1 Y, 4.1.1	
Encryption	164.312(e)(2)(ii)	2.1.1, 4.1 Y, 4.1.1	



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

DRMKT-19117 06/14