

Compliance Rosetta Stone

Most regulations have these common characteristics:

Perimeter security

SOX CO.03 Limiting external access to systems (Computer operations)
PCI 1 Install and maintain a firewall configuration to protect data (Secure network)
HIPAA 45 CFR Parts 164.310(a)(1) Facility Access Controls
GLBA 16 CFR Part 314.4(b), 314.4(c)

Access to programs and data

SOX APD.01 Password policies
SOX APD.02 User account and group security
SOX APD.03 System audit configuration (Access to programs and data)
PCI 2 Do not use vendor-supplied defaults for system passwords and other security parameters (Secure network)
PCI 3 Protect stored data (Protect cardholder data)
PCI 4 Encrypt transmission of cardholder data and sensitive info across public networks (Protect cardholder data)
PCI 7 Restrict access to data by business need-to-know (Strong access control)
PCI 8 Assign a unique ID to each person with computer access (Strong access control)
PCI 10 Track and monitor all access to network resources and cardholder data (Monitor, test networks)
HIPAA 45 CFR Parts 164.312(a)(1) Access Control
GLBA 16 CFR Part 314.4(c)

Unintended programs and endpoint security

SOX CO.02 Operate reliable systems (Computer operations)
PCI 5 Use and regularly update antivirus software (Vulnerability management)
HIPAA 45 CFR Parts 164.312(c)(1) Mechanism to Authenticate Electronic Protected Health Information
HIPAA 45 CFR Parts 164.312(d) Health Information Person or Entity Authentication
GLBA 16 CFR Part 314.4(b)

Program development and change management

SOX PDC.01 Acquire and maintain applications
SOX PDC.02 Acquire and maintain systems (Program development and change management)
PCI 6 Develop and maintain secure systems and applications (Vulnerability management)
HIPAA 164.308(a)(7) Testing and Revision Procedure
GLBA 16 CFR Part 314.4(b)

Physical security

SOX CO.04 Protect physical assets (Computer operations)
PCI 9 Restrict physical access to cardholder data (Strong access control)
HIPAA 45 CFR Parts 164.310(a)(1) Facility Access Controls
GLBA 16 CFR Part 314.4(b)

Policy, procedures, and testing

SOX APD.01 Security policies
SOX CO.01 Managed 3rd party services
SOX APD.04 Access provisioning
PCI 11 Regularly test security systems and processes (Monitor, test networks)
PCI 12 Maintain a policy that addresses information security (Information security policy)
HIPAA 45 CFR Parts 164.308(a)(1) Security Management Process
HIPAA 45 CFR Parts 164.308(a)(8) Evaluation
HIPAA 45 CFR Parts 164.308(b)(1) Business Associate Contracts and Other Arrangement
GLBA 16 CFR Part 314.4(c)

References

1. Tool Talk Webcast: How to Reach Compliance Nirvana if You are Subject To Payment Card Industry (PCI) & Government Regulatory Compliance

<https://www.sans.org/webcasts/access.php?id=90725>

2. Department of Health and Human Services

45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule

<http://www.hhs.gov/ocr/hipaa/>

3. Federal Trade Commission

16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule

<http://www.ftc.gov/os/2002/05/67fr36585.pdf>

4. PCI Security Standards Council

Download the PCI

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm