


Common Required Technical Security Solutions

The purpose of this worksheet is to list _required_ solutions that are part of a comprehensive security program.

		<div> ISO PCI HIPAA SANS CSA FISMA LOW FISMA MOD FISMA HIGH FedRAMP LOW FedRAMP MOD </div>										PCI	NIST SP800-53A†
Common Required Technical Security Solutions		Description											
Data Segmentation / Boundary Protection		FW											
1	Network (N) and Host (H) Firewall	Segment and protect networks	●	●	●	●	●	●	●	●	●	1	SC-7
Infrastructure Management		PM; CM											
2	Configuration Management	Protect infrastructure	●	●	●	●	●	●	●	●	●	2.1, 2.2	SI-2, SA-10, CM-1/2/6
3	Patch Management	Protect infrastructure	●	●	●	●	●	●	●	●	●	6.1	CM-2, SI-2
Exploit and Malware Protection		IPS; FIM; AV; WAF; DLP											
4	Intrusion Prevention System	Identify attacks	●	●	●	●	●	●	●	●	●	11.4	SI-3, SI-4
5	File Integrity Monitoring	Identify changed files	●	●	●	●	●	●	●	●	●	11.5	SI-7
6	Server and Endpoint Antivirus	Protect against malware	●	●	●	●	●	●	●	●	●	5	SI-3
7	Web Application Firewall*	Protect user services	●	●	●	●	●	●	●	●	●	6.6	SI-3, SI-4, SC-7
8	Data Leakage Protection**	Identify sensitive data		**	**								
Encryption		DIME; DARE											
9	Data At Rest Encryption	Protect data	●	●	●	●	●	●	●	●	●	3.4, 3.5, 3.6	SC-12/13/28, IA-7
10	Data In Motion Encryption	Protect data	●	●	●	●	●	●	●	●	●	2.3, 4, 8.4	SC-9/12/13, IA-7
Identity & Access Management		IdM; AAA; 2FA											
11	Two Factor Authentication	Authenticate users	●	●	●	●	●	●	●	●	●	8.3	IA-2 (1), IA-4
12	Identity Management	Provision and deprovision users	●	●	●	●	●	●	●	●	●	8.1, 8.2, 8.5.1	IA-2, IA-4
13	Authentication, Authorization, Accounting (3A)	Identity interaction nonrepudiation	●	●	●	●	●	●	●	●	●	7, 8.5	IA-5, AC-3
Systems Monitoring		SIEM; DBM											
14	Security Information Event Monitoring	Log and correlate environment data	●	●	●	●	●	●	●	●	●	10, A.1.3	SI-4, AU-2/3/6/10/12
15	Database Monitoring	Protect database environment	●	●	●	●	●	●	●	●	●	10, A.1.3	SI-4
Vulnerability Assessment		PT; VAM											
16	Vulnerability Assessment and Management	Identify and track vulnerabilities	●	●	●	●	●	●	●	●	●	6.2, 6.5, 6.6, 11.2	RA-5
17	Penetration Testing	Validate vulnerabilities	●	●	●	●	●	●	●	●	●	11.3	CA-2
Data Protection		BU											
18	System Backups	Systems survivability	●	●	●	●	●	●	●	●	●	10.5.3, 12.9.1	CP-9

* Specifically called out in some authorities and implied control in others. Highly recommended where the Internet will be the primary use case.

** Not _specifically_ called out in any authority. However, often used as a control for healthcare and financial verticals.

† Sampling of controls that apply.

Comments or suggestions: Chris.Davis@VCE.com