

▶ Looking at the SANS 20 Critical Security Controls

Mapping the SANS 20 to NIST 800-53 to ISO 27002
by Brad C. Johnson

© Copyright 2011 SystemExperts Corporation. All rights reserved.

Looking at the SANS 20 Critical Security Controls

The SANS 20 Overview

SANS has created the “20 Critical Security Controls” as a way of providing effective cyber defense against current and likely future Internet based attacks. Following these 20 controls will help establish, in their words, a “prioritized baseline of information security measures and controls.” The target audience is Federal enterprise environments but it certainly could be used by commercial organizations. Let’s take a quick look at the specifics of what the control areas are and how they are organized.

Control Area Organization

Each of the 20 critical areas is organized using the same subsections:

- › How do attackers exploit the lack of this control?
- › How can this control be implemented, automated, & its effectiveness measured?
- › Associated NIST SP 800-53 Priority 1 Controls
- › Procedures & tools for implementing & automating this control
- › Control metric (what the control should deal with)
- › Control test (how to evaluate the control)

Critical Security Controls

The 20 Critical Controls are broken into two categories: the first set of 15 controls lend themselves to automation.

Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized & Unauthorized Devices
2. Inventory of Authorized & Unauthorized Software
3. Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, & Switches
5. Boundary Defense
6. Maintenance, Monitoring, & Analysis of Audit Logs

7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment & Remediation
11. Account Monitoring & Control
12. Malware Defenses
13. Limitation & Control of Network Ports, Protocols, & Services
14. Wireless Device Control
15. Data Loss Prevention

Additional Critical Controls

16. Secure Network Engineering
17. Penetration Tests & Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment & Appropriate Training to Fill Gaps

Is This a New Standard?

No, the SANS 20 Critical Security Controls is not a new standard. This is a set of recommendations developed by a consortium of companies with the purpose of identifying specific controls that will make systems safer. In addition, most of the controls can be automated (to various degrees) through the use of tools.

There is a direct mapping between the 20 controls areas and the NIST standard “Recommended Security Controls for Federal Information Systems and Organizations” which is referred to as NIST Special Publication (SP) 800-53. The SANS 20 Critical Security Controls represent a subset of the NIST SP 800-53 controls (in fact, it covers about one third of the 145 controls identified in NIST 800-53).

From SANS’s point of view, focusing on these 20 areas will help an organization be prepared for the most important actual threats that exist in today’s Internet world. In addition, the first 15 control areas lend themselves to tool based assessments so an organization has a chance to fulfill most of them in an automated or semi-automated way. Most of

▶ Looking at the SANS 20 Critical Security Controls

the control areas are focused on technical controls and not so much on operational or management oriented NIST controls.

Therefore, SANS believes that following their 20 Critical Security Controls will directly help protect your systems against current threats and cyber attacks.

Mapping the SANS 20 to ISO 27002

If you are not a government agency, however, you probably are not using the NIST SP 800-53 security standard as a framework for auditing your IT environment. Many private organizations instead use the ISO 27001/27002 information security standards.

From my point of view, focusing on control areas that provide practical and tangible progress for preventing or detecting actual threats is a good idea. To help understand how these control areas map to a standard that you are probably more familiar with or are already using to evaluate your own environment, I have created a table that shows how the SANS 20 Critical Security Controls maps to the NIST 800-53 standard and then how those controls map to the ISO 27002 standard.

Understanding the big picture

SANS has done a good job of trying to distill a complex problem (protecting your networked resources from cyber attacks) into a series of

straightforward security controls. There are other things you should consider if you are going to use the 20 Critical Security Controls as a benchmark.

In all likelihood, management and operational controls, policies, and procedures are going to provide the security umbrella you need to protect corporate assets and information. Tools are helpful for automating tasks, but tools and technologies are only as useful as the management and operational infrastructure that is using them. Being prepared for serious problems such as Advanced Persistent Threats are not going to be solved by technology alone.

SANS has identified a set of tools that have been “vetted” by users to help automate some of the Security Control areas. This list is largely based on input from users who have been involved in helping to create the SANS 20 recommendation. There are other third-party and public domain tools that are similar to the ones listed or may be more appropriate for you to use.

Author Information

Brad C. Johnson
ISACA/CISM, NSA/IAM
Vice President
SystemExperts Corporation
Email: brad.johnson@systemexperts.com
Phone: 401-348-3099

▶ Looking at the SANS 20 Critical Security Controls

SANS 20 Critical Security Controls	NIST SP 800-53 (control numbers)	ISO 27002 (control heading numbers)
Control 1: Inventory of Authorized & Unauthorized Devices	CM-8	7.1.1, 7.1.2
	PM-5	7.1.1, 7.1.2
	PM-6	None
Control 2: Inventory of Authorized & Unauthorized Software	CM-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 10.1.2, 12.4.1, 12.5.1, 15.1.1, 15.2.1
	CM-2	10.1.4, 12.4.1
	CM-3	10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2, 12.5.3
	CM-5	10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3
	CM-7	None
	CM-8	7.1.1, 7.1.2
	CM-9	6.1.3, 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.4.3, 12.5.1, 15.2.1
	PM-6	None
	SA-6	12.4.1, 12.5.5, 15.1.2
	SA-7	12.4.1, 12.5.5, 15.1.2
Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, & Servers	CM-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 10.1.2, 12.4.1, 12.5.1, 15.1.1, 15.2.1
	CM-2	10.1.4, 12.4.1
	CM-3	10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2, 12.5.3
	CM-5	10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3
	CM-6	None
	CM-7	None
	SA-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 6.2.1, 8.1.1, 10.1.1, 12.1.1, 12.5.5, 15.1.1, 15.2.1
	SA-4	12.1.1, 12.5.5
	SI-7	10.4.1, 12.2.2, 12.2.3
	PM-6	None
Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	AC-4	10.6.1, 10.8.1, 11.4.5, 11.4.7, 11.7.2, 12.4.2, 12.5.4
	CM-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 10.1.2, 12.4.1, 12.5.1, 15.1.1, 15.2.1
	CM-3	10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2, 12.5.3
	CM-5	10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3
	CM-6	None
	CM-7	None
	IA-2	11.3.2, 11.5.1, 11.5.3
	IA-5	11.2.1, 11.2.3, 11.3.1, 11.5.2, 11.5.3
	IA-8	10.9.1, 11.4.2, 11.5.1, 11.5.2
	RA-5	12.6.1, 15.2.2
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
	SC-9	10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.3.1

▶ Looking at the SANS 20 Critical Security Controls

SANS 20 Critical Security Controls	NIST SP 800-53 (control numbers)	ISO 27002 (control heading numbers)
Control 5: Boundary Defense	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-20	7.1.3, 8.1.1, 8.1.3, 10.6.1, 10.8.1, 11.4.1, 11.4.2
	CA-3	6.2.1, 6.2.3, 10.6.1, 10.8.1, 10.8.2, 10.8.5, 11.4.2
	IA-2	11.3.2, 11.5.1, 11.5.2, 11.5.3
	IA-8	10.9.1, 11.4.2, 11.5.1, 11.5.2
	RA-5	12.6.1, 15.2.2
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
	SC-18	10.4.2
	SI-4	10.10.2, 13.1.1, 13.1.2
	PM-7	None
Control 6: Maintenance, Monitoring & Analysis of Security Audit Logs	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-19	10.4.1, 11.1.1, 11.4.3, 11.7.1
	AU-2	10.10.1, 10.10.4, 10.10.5, 15.3.1
	AU-3	10.10.1
	AU-4	10.10.1, 10.3.1
	AU-5	10.3.1, 10.10.1
	AU-6	10.10.2, 10.10.5, 13.1.1, 15.1.5
	AU-8	10.10.1, 10.10.6
	AU-9	10.10.3, 13.2.3, 15.1.3, 15.3.2
	AU-12	10.10.1, 10.10.4, 10.10.5
SI-4	10.10.2, 13.1.1, 13.1.2	
Control 7: Application Software Security	CM-7	None
	RA-5	12.6.1, 15.2.2
	SA-3	12.1.1
	SA-4	12.1.1, 12.5.5
	SA-8	10.4.1, 10.4.2, 11.4.5, 12.5.5
	SI-3	10.4.1
	SI-10	12.2.1, 12.2.2
Control 8: Controlled Use of Administrative Privileges	AC-6	6.1.3, 8.1.1, 11.1.1, 11.2.2, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.3
	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-19	10.4.1, 11.1.1, 11.4.3, 11.7.1
	AU-2	10.10.1, 10.10.4, 10.10.5, 15.3.1
Control 9: Controlled Access Based on Need to Know	AC-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.4.1, A.11.7.1, 11.7.2, 15.1.1, 15.2.1
	AC-2	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1
	AC-3	10.8.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2
	AC-4	10.6.1, 10.8.1, 11.4.5, 11.4.7, 11.7.2, 12.4.2, 12.5.4
	AC-6	6.1.3, 8.1.1, 11.1.1, 11.2.2, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.3
	MP-3	7.2.2, 10.7.1, 10.7.2
	RA-2	7.2.1, 14.1.2
	RA-3	6.2.1, 10.2.3, 12.6.1, 14.1.2
Control 10: Continuous Vulnerability Assessment & Remediation	RA-5	12.6.1, 15.2.2
Control 11: Account Monitoring & Control	AC-2	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1
	AC-3	10.8.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2

▶ Looking at the SANS 20 Critical Security Controls

SANS 20 Critical Security Controls	NIST SP 800-53 (control numbers)	ISO 27002 (control heading numbers)
Control 12: Malware Defenses	SC-18	10.4.2
	SC-26	None
	SI-3	10.4.1
Control 13: Limitation and Control of Network Ports, Protocols, & Services	CM-6	None
	CM-7	None
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
Control 14: Wireless Device Control	AC-17	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	AC-18	10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2
	SC-9	10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.3.1
	SC-24	None
	SI-4	10.10.2, 13.1.1, 13.1.2
Control 15: Data Loss Prevention	AC-4	10.6.1, 10.8.1, 11.4.5, 11.4.7, 11.7.2, 12.4.2, 12.5.4
	MP-2	7.2.2, 10.7.1, 10.7.3
	MP-4	10.7.1, 10.7.3, 10.7.4, 15.1.3
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
	SC-9	10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.3.1
	SC-13	12.3.1, 15.1.6
	SC-28	None
	SI-4	10.10.2, 13.1.1, 13.1.2
Control 16: Secure Network Engineering	PM-7	None
	IR-4	6.1.2, 13.2.2, 13.2.3
	SA-8	10.4.1, 10.4.2, 11.4.5, 12.5.5
	SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.2, 11.4.5, 11.4.6
	SC-20	10.6.1
	SC-21	10.6.1
	SC-22	10.6.1
Control 17: Penetration Tests & Red Team Exercises	PM-7	None
	CA-2	6.1.8, 10.3.2, 15.2.1, 15.2.2
	CA-7	6.1.8, 15.2.1, 15.2.2
	RA-3	6.2.1, 20.2.3, 12.6.1, 14.1.2
	RA-5	12.6.1, 15.2.2
Control 18: Incident Response Capability	SA-12	12.5.5
	IR-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 13.1.1, 13.2.1, 15.1.1, 15.2.1
	IR-2	8.2.2
	IR-4	6.1.2, 13.2.2, 13.2.3
	IR-5	None
	IR-6	6.1.6, 13.1.1
Control 19: Data Recovery Capability	IR-8	None
	CP-9	9.1.4, 10.5.1, 14.1.3, 15.1.3
Control 20: Security Skills Assessment & Appropriate Training To Fill Gaps	CP-10	9.1.4, 14.1.3
	AT-1	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1, 10.10.2, 15.1.1, 15.2.1, 15.3.1
	AT-2	6.2.2, 8.1.1, 8.2.2, 9.1.5, 10.4.1
	AT-3	8.1.1, 8.2.2, 9.1.5

▶ Looking at the SANS 20 Critical Security Controls

NIST 800-53 Security Control Identifiers, Families, and Classes

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

ISO 27002 Security Categories

SECTION	CATEGORY
4	Risk Assessment & Treatment
5	Security Policy
6	Organization of Information Security
7	Asset Management
8	Human Resources Security
9	Physical & Environmental Security
10	Communications & Operations Management
11	Access Control
12	Information Systems Acquisition, Development & Maintenance
13	Information Security Incident Management
14	Business Continuity Management
15	Compliance