The Top 20 Most Critical Controls for Cyber Security

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[](http://itmanagersinbox.com/wp-content/uploads/2009/03/4.jpg)A consortium of federal agencies and private organizations have released Version 1.0 of the **Consensus Audit Guidelines** (CAG) that define the most critical security controls to protect federal and contractor information and information systems.

For each of the 20 controls, the experts identified specific (actual) attacks that the control stops or mitigates, illuminated best practices in automating the control (for 15 controls that can be automated)and defined tests that can determine whether each control is effectively implemented. The resulting document is called the Consensus Audit Guidelines and, once fully vetted, is expected to become the standard baseline for measuring computer security in organizations that are likely to be under attack.

Twenty critical security controls were agreed upon by knowledgeable individuals from the groups listed above. The list of controls includes fifteen that are able to be validated in an automated manner and five that must be validated manually.

Critical Controls Subject to Automated Measurement and Validation:

1. Inventory of Authorized and Unauthorized Hardware.
2. Inventory of Authorized and Unauthorized Software.
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.
4. Secure Configurations of Network Devices Such as Firewalls and Routers.
5. Boundary Defense
6. Maintenance and Analysis of Complete Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
10. Continuous Vulnerability Testing and Remediation
11. Dormant Account Monitoring and Control
12. Anti-Malware Defenses
13. Limitation and Control of Ports, Protocols and Services
14. Wireless Device Control
15. Data Leakage Protection

Additional Critical Controls (not directly supported by automated measurement and validation):

1. Secure Network Engineering
2. Red Team Exercises
3. Incident Response Capability
4. Data Recovery Capability
5. Security Skills Assessment and Training to Fill Gaps