File 20090224.2251: There is a new 'Consensus Audit Guidelines' list published by NSA, US-CERT, and DoD the other day. See the full list at `http://www.sans.org/cag`.

Consensus Audit Guidelines Draft 1.0

- Consensus Audit Guidelines—Introduction (Draft 1.0)
- Critical Control 1: Inventory of authorized and unauthorized hardware.
- Critical Control 2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software.
- Critical Control 3: Secure configurations for hardware and software on laptops, workstations, and servers.
- Critical Control 4: Secure configurations of network devices such as firewalls, routers, and switches.
- Critical Control 5: Boundary Defense
- Critical Control 6: Maintenance, Monitoring and Analysis of Complete Audit Logs
- Critical Control 7: Application Software Security
- Critical Control 8: Controlled Use of Administrative Privileges
- Critical Control 9: Controlled Access Based On Need to Know
- Critical Control 10: Continuous Vulnerability Testing and Remediation
- Critical Control 11: Dormant Account Monitoring and Control
- Critical Control 12: Anti-Malware Defenses
- Critical Control 13: Limitation and Control of Ports, Protocols and Services
- Critical Control 14: Wireless Device Control
- Critical Control 15: Data Leakage Protection
- Critical Control 16: Secure Network Engineering
- Critical Control 17: Red Team Exercises
- Critical Control 18: Incident Response Capability
- Critical Control 19: Data Recovery Capability
- Critical Control 20: Security Skills Assessment and Appropriate Training To Fill Gaps

[1]

References

[1] John Gilligan. Consensus audit guidelines—draft 1.0, February 23, 2009. `http://www.sans.org/cag`.