

# Using the SANS Top 20 Critical Controls to support CDS requirements

## “The SANS Top Twenty Critical Controls

These 20 critical security controls were agreed upon by knowledgeable individuals from the groups listed above. The list includes 15 controls that can be validated at least in part in an automated manner and five that must be validated manually. It is important to note that the 20 control categories are *not* presented in order of priority. The process of gathering these specific controls and subcontrols focused on identifying the highest priority defenses and represent a subset of controls found in other audit guidelines and documents. Each of the 20 categories is important and offers high-priority techniques for thwarting real-world attacks.”

The SANS Website.

Ahead of version 1.3 of the CDS, this document will briefly identify the relationship between the CDS Levels 1-9 and the SANS Top 20 Critical Controls.

The controls identified by SANS are excellent and have been developed by seasoned IT Security Practitioners based upon evidence, experience and post incident analysis. The reader is strongly encouraged to review the list of contributors before discounting the value of this Top 20. (<http://www.sans.org/cag/guidelines.php>)

Excellent though they are the SANS Top 20 Critical Controls are not always achievable every industry sectors (through user resistance, a lack of consideration of the risk or a lack of funds). That said they should not be discarded as too difficult or not relevant as there is something to be learnt from every control.

This short document aims to show the reader how the detail from the SANS Top 20 Critical Controls can be used to assist those seeking to follow the CDS roadmap to a more secure system. With the next release of the CDS (version 1.3 in November 2009), the table will be expanded to include every CDS requirement and the SANS controls that can be implemented to support the achievement of the requirement.

Note: The SANS top 20 Critical Controls are detailed and many of their Advanced or Configuration/Hygiene are long term implementation requirements, depending upon the CDS level aimed for, the initial results of the Quick Wins can be sufficient to meet the CDS requirements, although organizations are strongly encouraged to implement additional long term controls and measures wherever possible.

The SANS controls are listed at [www.sans.org/cag](http://www.sans.org/cag) and the table below references version 2.1

Mapping the SANS 20 Critical Controls to the Certified Digital Security Levels

<b>CDS Level</b>	<b>Comment and applicability of the SANS control in meeting the CDS Requirements.</b>	<b>SANS Control Number</b>	<b>Control Title</b>
1 & 4	There are good quick wins from the SANS list that will assist levels 1 where users have individual accounts and level 4 where servers are locked down	11	Account Monitoring and Control
1	The SANS top 20 give excellent guidance on how to control and monitor the use of administrator accounts. CDS requires that the accounts are use sparingly and that admin's have lower privileged accounts for normal activities.	8	Controlled Use of Administrative Privileges
1	The implementation of Anti Virus is just the start, and the SANS section 12 gives good quick win tips that will augment standard AV software installations	12	Malware Defenses
2	The auditing can be achieved by means of a SANS Control 1 quick win, but should be supported and enforced by other measures like the use of monitoring software.	1	Inventory of Authorized and Unauthorized Devices
2	Asset registers and security management plans can be defined and described in many ways. The use of the	9	Controlled Access Based on Need to Know
2	Wireless must be controlled in the environment; quick wins can help identify rogue access points. For many organizations this is enough control, for other larger organizations the Configuration and Hygiene controls will assist in maintaining secure WLANs and perimeter.	14	Wireless Device Control
3	The SANS control will lent itself to the software purge of illegal, unauthorized and unnecessary software that is found on corporate LANs.	2	Inventory of Authorized and Unauthorized Software
4	The server lockdowns and hardening activities can take good advice from this SANS control.	13	Limitation and Control of Network Ports, Protocols, and Services
4	Servers secured and maintained at level 4, Workstations patched at level 2, software audited at level 3 and laptops encrypted with USB lockdown at level 5	3	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

CDS Level	Comment and applicability of the SANS control in meeting the CDS Requirements.	SANS Control Number	Control Title
2 & 4	The logging requirements at levels 2 and 4 can be supported by almost all of the Quick Wins and the larger ones can validate their in place activities with the Visibility and Attribution elements. Highly secure organizations should look at the Advanced element.	6	Maintenance, Monitoring, and Analysis of Security Audit Logs
6	Forensics concepts need to be considered and the potential impact upon how an incident is handled needs consideration in the cold light of day - not when the incident is running. Linked to the organizations Business Continuity Plan, recovery of data is vital if hackers have destroyed logs, hard drives or whole systems	19	Data Recovery Capability
5 & 6	The requirement to undergo regular reviews and Vulnerability Assessment supports the Level 5 requirement to review barriers and the over all security and the Level 6 requirement for Vulnerability Assessments. The internal work to get ready for these can be undertaken with guidance from the SANS Control 10, but the CDS requirement will need the Vulnerability Assessment to be conducted by an independent 3 <sup>rd</sup> Party.	10	Continuous Vulnerability Assessment and Remediation
7 & 4	These can be used to support the hardening of the servers and the network, but the Control 16 is more about the design of the network and this is level 7 and above material. In the Advanced levels the requirements are more about ensuring the network has been designed and managed correctly.	16	Secure Network Engineering
7	As per the Level 6 and 5 requirements the CDS requirements can be supported by internal staff undertaking the quick win aspects of the SANS control 17. They must have legal authority to use any tools in and on the organization, but they can reduce the costs of an external pen test by removing the easy targets first - plus they learn from the activity and add to the overall skills pool of the team - part of the requirement for multi-skilled staff.	17	Penetration Tests and Red Team Exercises
CDS Level	Comment and applicability of the SANS control in meeting the CDS Requirements.	SANS Control Number	Control Title

4 & 5	Public facing services and internet Servers are secured at level 4. Barriers are required to be audited at level 5. The tips and quick wins in the Control 4 are excellent and should be used by Administrators as crub sheets of 'what to do next'.	4	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
3 & 7	Firewalling, IPS/IPS requirements are supported by Control 5 as it identifies how a boundary can be made and reinforced.	5	Boundary Defense
3, 4 & 5	If an organization wants to completely control the data on their system then the tips in this SANS control are well worth considering and implementing - especially on large networks where links are big and fast and huge volumes of data can be exported in seconds.	15	Data Loss Prevention
2, 5 & 6	Training is a core element of the CDS. The pointers from the SANS last control are well worth considering when implementing user and administrator training requirements and requests.	20	Security Skills Assessment and Appropriate Training to Fill Gaps
3, 6 & 7	The need for an Incident Response capability is introduced early in CDS and its importance is raised as the levels increase. The 18 <sup>th</sup> Control from SANS will assist the initial stages of the capability development, but training, resources, support and practice are the main requirments.	18	Incident Response Capability
6, 7 & 8	This is a theme rather than a strict requirement in CDS, as it depends upon the size and type or organization as to the importance or relevance of any Application Security will have. However, in the development of a application that will be subject to the levels 6-8 testing (the main one being the penetration testing at level 7), the organization would be strongly advised to review the SANS Critical Control 7 - its more about the journey as CDS will validate the destination.	7	Application Software Security