CSC #	Description	WTCA #	Description	Detailed Requirements Included in NSR not in CSC
1	**Inventory of Authorized and Unauthorized Devices** Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	WTCA 3.2	**Asset Classification and Management** The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.	
		WTCA 3.6	System Access Management The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals.	
		NSR 1.e	Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks;	
2	**Inventory of Authorized and Unauthorized Software** Actively manage (inventory, tack, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	NONE	Currently there is not criteria that requires this level of software inventory. This could be covered in some of the NSR requirements around system configuration.	
3	**Secure Configurations for Hardware and Software** Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	NSR 1.g	Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;	General Protections for networks and supporting systems • Defined security zones based on type of assets • Required air gapped/offline roots • Required review of system configurations on a weekly basis • Apply security patches within six months
		NSR 1.h	Review configurations of Issuing Systems, Certificate management Systems, Security Support Systems, and Front-End / Internal-Support Systems on at least a weekly basis to determine whether any changes violated the CA's security policies;	
		NSR 3.a	Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems;	
4	**Continuous Vulnerability Assessment and Remediation** Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	WTCA 3.1	Security Management (cont) The CA maintains controls to provide reasonable assurance that: • security is planned, managed and supported within the organization; • security risks are identified and managed; • the security of CA facilities, systems and information assets accessed by third parties is maintained; and • the security of subscriber and relying party information is maintained when the responsibility for CA sub-functions has been outsourced to another organization or entity.	Vulnerability Detection and Patch Management • Perform vulnerability scan within one week of a request from the Browser Forum, significant changes, once per quarter • Annual penetration test • Remediation plan within 96 hours of discovering a critical vulnerability
		NSR 4.a	Implement detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against viruses and malicious software;	
		NSR 4.c	Undergo or perform a Vulnerability Scan (i) within one week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems;	

		NSR 4.d	Undergo a Penetration Test on the CA’s and each Delegated Third Party’s Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;	
5	**Controlled Use of Administrative Privileges** The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	WTCA 3.6	**System Access Management** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: - operating system and database access is limited to authorized individuals with predetermined task privileges; - access to network segments housing CA systems is limited to authorized individuals, applications and services; and - CA application use is limited to authorized individuals.	
		NSR 2	Each CA or Delegated Third Party SHALL: a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them; b. Document the responsibilities and tasks assigned to Trusted Roles and implement “separation of duties” for such Trusted Roles based on the security-related concerns of the functions to be performed; c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; d. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; e. Require employees and contractors to observe the principle of “least privilege” when accessing, or when configuring access privileges on, Certificate Systems; f. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems;	
6	**Maintenance, Monitoring, and Analysis of Audit Logs** Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	3.10	**Audit Logging** The CA maintains controls to provide reasonable assurance that • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	Logging, Monitoring, and Alerting • Automated alerting of security related system changes and critical security events • Conduct a human review of log integrity every 30 days
		NSR 3	a. Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems; b. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity; c. Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events; d. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events; e. Conduct a human review of application and system logs at least every 30 days and validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log-integrity verification functions are operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool); and f. Maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.	

7	**Email and Web Browser Protections** Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.	NSR 1.e - g	e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks; f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA’s or Delegated Third Party’s operations and allowing only those that are approved by the CA or Delegated Third Party;	
8	**Malware Defenses** Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	NSR 4.a	a. Implement detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against viruses and malicious software;	
		WTCA 3.5	Operations Management The CA maintains controls to provide reasonable assurance that: • the correct and secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimized; • the integrity of CA systems and information is protected against viruses and malicious software; • damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and • media are securely handled to protect them from damage, theft and unauthorized access.	
9	**Limitation and Control of Network Ports** Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	NSR 1.e - g	e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks; f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA’s or Delegated Third Party’s operations and allowing only those that are approved by the CA or Delegated Third Party;	General Protections for networks and supporting systems • Defined security zones based on type of assets • Required air gapped/offline roots

10	**Data Recovery Capability** The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	3.8	**Business Continuity Management** The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: - the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; - the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; - the storage of backups of systems, data and configuration information at an alternate location; and - the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.	
11	**Secure Configurations for Network Devices** Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	NSR 1.g	Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;	General Protections for networks and supporting systems • Defined security zones based on type of assets • Required air gapped/offline roots • Required review of system configurations on a weekly basis • Multi-factor authentication requirement • Apply security patches within six months
		NSR 1.h	Review configurations of Issuing Systems, Certificate management Systems, Security Support Systems, and Front-End / Internal-Support Systems on at least a weekly basis to determine whether any changes violated the CA's security policies;	
		WTCA 3.7	**Systems Development and Maintenance** The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	
12	**Boundary Defense** Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	NSR 1.e - g	e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks; f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;	General Protections for networks and supporting systems • Defined security zones based on type of assets • Required air gapped/offline roots
13	**Data Protection** The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	3.5	**Operations Management** The CA maintains controls to provide reasonable assurance that: - the correct and secure operation of CA information processing facilities is ensured; - the risk of CA systems failure is minimized; - the integrity of CA systems and information is protected against viruses and malicious software; - damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and - media are securely handled to protect them from damage, theft and unauthorized access.	

14	**Controlled Access Based on the Need to Know** The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	3.2	**Asset Classification and Management** The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.	Trusted Roles, Delegated Third Parties, and System Accounts • Specific password requirements based on security zone • Required workstation lockout • Required access reviews every 90 days • Required system lockout after 5 failed attempts • Removal of access within 24 hours after termination • Multi-factor authentication requirement to Issuing Systems and Certificate Management Systems
		WTCA 3.4	Physical and Environmental Security The CA maintains controls to provide reasonable assurance that • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	
		WTCA 3.6	**System Access Management** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: - operating system and database access is limited to authorized individuals with predetermined task privileges; - access to network segments housing CA systems is limited to authorized individuals, applications and services; and - CA application use is limited to authorized individuals.	
		NSR 2	Each CA or Delegated Third Party SHALL: a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them; b. Document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed; c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; d. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; e. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems; f. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems;	
	Wireless Access Control The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	WTCA 3.6	**System Access Management** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: - operating system and database access is limited to authorized individuals with predetermined task privileges; - access to network segments housing CA systems is limited to authorized individuals, applications and services; and - CA application use is limited to authorized individuals.	

15		NSR 1.e - g	e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks; f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;	
16	**Account Monitoring and Control** Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	WTCA 3.6	**System Access Management** The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: - operating system and database access is limited to authorized individuals with predetermined task privileges; - access to network segments housing CA systems is limited to authorized individuals, applications and services; and - CA application use is limited to authorized individuals.	Trusted Roles, Delegated Third Parties, and System Accounts • Specific password requirements based on security zone • Required access reviews every 90 days
		NSR 2	Each CA or Delegated Third Party SHALL: a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them; b. Document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed; c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; d. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; e. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems; f. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems;	
		NSR 2.j	j. Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;	
		NSR 2.l	l. Implement a process that disables all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party;	
17	**Security Skills Assessment and Appropriate Training to Fill Gaps** For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	WTCA 3.3	**Personnel Security** The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	
18	**Application Software Security** Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	WTCA 3.7	**Systems Development and Maintenance** The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	General Protections for networks and supporting systems • Required review of system configurations on a weekly basis

19	**Incident Response and Management** Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.	WTCA 3.5	**Operations Management** The CA maintains controls to provide reasonable assurance that: • the correct and secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimized; • the integrity of CA systems and information is protected against viruses and malicious software; • damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and • media are securely handled to protect them from damage, theft and unauthorized access.	Vulnerability Detection and Patch Management • Perform vulnerability scan within one week of a request from the Browser Forum, significant changes, once per quarter • Remediation plan within 96 hours of discovering a critical vulnerability
		NSR 4.b	b. Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities;	
		NSR 4.f	f. Do one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA’s vulnerability correction process: i. Remediate the Critical Vulnerability; ii. If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or iii. Document the factual basis for the CA’s determination that the vulnerability does not require remediation because (a) the CA disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.	
20	**Penetration Tests and Red Team Exercises** Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.	NSR 4.c	Undergo or perform a Vulnerability Scan (i) within one week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA’s or Delegated Third Party’s Certificate Systems;	Vulnerability Detection and Patch Management • Annual penetration test
		NSR 4.d	Undergo a Penetration Test on the CA’s and each Delegated Third Party’s Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;	