NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
	PB9: There is no concept of compensating controls; for example, a CA might want to implement channel authentication as an alternative to physical network segmentation (for example using TLS over VLANs rather than physically segmenting LANs).			
1. GENERAL PROTECTIONS FOR THE NETWORK AND SUPPORTING SYSTEMS				
Each CA or Delegated Third Party SHALL:				
a. Segment Certificate Systems into networks or zones based on their functional, logical, and physical (including location) relationship	PB4: The segmentation requirements are confusing (and possibly contradictory): networks or zones based on their functional, logical, and physical (including location) relationship.	WebTrust § 3.6, Illustrative Control 12 - Controls (e.g., firewalls) are in place to protect the CA's internal network domain from any unauthorized access from any other domain)	ETSI § 7.4.6. a) Controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties.	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
b. Apply the same security controls to all systems co-located in the same zone with a Certificate System	PB3: (See definition of "Certificate System") The scope is far larger than probably intended — it could be viewed as being as far reaching as including CDNs used to distribute CRLs and OCSP responses which have no ability to generate or modify the responses and systems the relay emails to domain contacts which are outside of the CA system	WebTrust § 3.2 - 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	ETSI § 7.4.1 a) The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary.	
c. Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks	PB2: Root CAs are not required to be air gapped at all times. GP1-1: This is a frequent point of discussion because of the term CA system. Is a CA system a fully functioning CA, just a private key, or certain key parts of the whole system? Some CAs feel they are still maintaining a CA system in an offline manner if they move a backup across a network just for a temporary period of time. There are also some CAs that have argued a secure zone only applies to the physical security of the zone (as noted in the definition, but not sure if that is the intent). GP2-6: Treatment of off line roots	WebTrust § 3.6 - Sensitive systems (e.g., Root CA) require a dedicated (isolated) computing environment	ETSI § 7.2.1. a) Certification authority key generation shall be undertaken in a physically secured environment (see clause 7.4.4) ETSI § 7.4.4 f) f) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device preparation (see clause 7.2.9) and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.	
d. Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone		WebTrust § 3.4, Physical and Environmental Security Criteria, Illustrative Control 15 - The CA maintains local network components (e.g., firewalls and routers) in a physically secure environment and audits their configurations periodically for compliance with the CA's configuration requirements	" "	PR.PT-4: Communications and control networks are protected
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		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. WebTrust § 3.4, Illustrative Control 19 - Power and telecommunications, within the facility housing the CA operation, cabling carrying data or supporting CA services is protected from interception or damage; WebTrust § 3.6, Illustrative Controls 12 and 13 - Controls are in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorized users in accordance with the CA's access control policies. The security attributes of all network services used by the CA organization are documented by the CA. 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.	ETSI § 7.4.6 Sensitive data shall be protected against unauthorized access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected **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. **12. Boundary Defense** Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
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	WebTrust: CAs will need to inventory and document their systems. Specifically document what communications are authorized, so auditors can assess the network security systems. There will need to be some type of documentation to document information flows – Data Classification required	WebTrust § 3.6, Illustrative Control 12- Controls (e.g., firewalls) are in place to protect the CA's internal network domain from any unauthorized access from any other domain	ETSI § 7.4.6 a - Controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties.)	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality **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.
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	WebTrust: CAs will need documentation on what is authorized services and accounts are, so auditors can determine whether each active account that is not assigned to an person is authorized or not. Blacklist of prohibited applications, services, protocols, ports, etc.	TSP&C § 3.5, Illustrative Control 1 - Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures. WebTrust § 3.7 - The CA maintains controls to provide reasonable assurance that CA systems development, configuration, and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity	ETSI § 7.4.6a 1 - It is recommended that firewalls be configured to prevent protocols and accesses not required for the operation of the CA.)	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality **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

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
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	GP1-2: Clarify if this can be addressed solely by automated alerting or if there should be a manual human review. The term human review is used at a later point and it would be helpful to be consistent on automated reviews or human review on all required review criteria. WebTrust: CAs will need to document the activities performed weekly for this requirement and document noncompliance and activity to resolve noncompliance. The scope of the activities CAs perform to address this may need to be in more detail and cover other activities than reviewing vulnerability scan reports. If a week is skipped this, would be an audit finding. Baseline configuration and CAs will need to create list of those systems for which configurations are maintained and reviewed and list must include CA systems, security systems, external systems. Ben: Maybe monthly – are there industry requirements? Not included in the CSC criteria are the following: 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	TSP&C § 3.7, Illustrative Control 7 - The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems.	ETSI § 7.4.7b - Change control procedures exist for releases, modifications and emergency software fixes for any operational software.)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained PR.IP-3: Configuration change control processes are in place **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.
i. Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security	WebTrust: CAs will need to retain documentation of this acknowledgement, including for users that had been granted access prior to the effective date.	WebTrust § 3.6 - The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals	ETSI § 7.4.6 - The CA shall ensure that CA system access is limited to properly authorized individuals.)	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established **5. Controlled Use of Administrative Privileges** The [CA implements] processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
j. Implement multi-factor authentication to each component of the Certificate System that supports multi-factor authentication (but see subsection 2.n.(ii) below);	PB5: It assumes passwords are the core authentication credential and does not align with current NIST guidance. Authentication requirements could probably be put in terms of NIST SP 800-63 AAL. PB6: It fails to define "multi-factor authentication". GP2-5: "multi-factor authentication" – (what is acceptable and what is not, is it purely logical authentication, can it be a mix of physical and logical?, Agreement would be useful on how to handle situations where there are multiple layers of physical/logical control around the systems, e.g. does multi-factor authentication at the physical perimeter of the High Security Zone meet the requirement to have multi-factor authentication for administrative access to systems?	WebTrust § 4.4, Illustrative Control 2 - If necessary based on a risk assessment, the activation of the CA private key is performed using multi-factor authentication (e.g., smart card and password, biometric and password, etc.	ETSI § 7.4.6e - CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.)	
k. Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate Systems is changed or revoked; and	WebTrust: Additionally based on the termination criteria in 2L of the Security Requirements, this must happen in 24 hours, not 1 business day. (Non-termination events have a different timeframe.)	WebTrust § 3.3, Illustrative Control 11 - Physical and logical access to CA facilities and systems is disabled upon termination of employment	ETSI § 7.4.6c - The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access)	
l. Apply recommended security patches to Certificate Systems within six months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying	WebTrust: CAs will need to document and sign off on every recommended patch not implemented. Burden of proof is on the CA.	WebTrust § 3.6, Illustrative Control 18 - Operating system and database patches and updates are applied in a timely manner when deemed necessary based on a risk assessment.).		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
2. TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS				
Each CA or Delegated Third Party SHALL:				
a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them		WebTrust §3.3, Illustrative Control 2 - Security roles and responsibilities, as specified in the organization's security policy, are documented in job descriptions	ETSI § 7.4.3c - Security roles and responsibilities, as specified in the CA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified)	
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		WebTrust §3.5, Illustrative Control 3 - Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services	ETSI § 7.4.3d - CA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege)	
c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones		WebTrust § 3.6 Criteria - The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals	ETSI §7.4.6d -Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user)	
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		WebTrust § 3.6 Criteria - The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals	ETSI §7.4.6d -Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user)	
e. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems		WebTrust § 3.6, Illustrative Control 3 - The allocation and use of privileges is restricted and controlled; CA employed personnel are provided direct access only to the services that they have been specifically authorized to use. Illustrative Control 8 - CA employed personnel are provided direct access only to the services that they have been specifically authorized to use	ETSI § 7.4.3d - CA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness; ETSI § 7.4.6d - Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user)	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.
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		WebTrust § 3.6, Illustrative Control 21 - All CA personnel users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual	ETSI § 7.4.6c - The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access)	
g. If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, implement the following controls:		WebTrust § 3.6 Illustrative Control 6 - Users are required to follow defined policies and procedures in the selection and use of passwords;	ETSI § 7.4.6 - The CA shall ensure that CA system access is limited to properly authorized individuals	
For accounts that are not publicly accessible (accessible only within Secure Zones or High Security Zones), require that passwords:	PB5: It assumes passwords are the core authentication credential and does not align with current NIST guidance. Authentication requirements could probably be put in terms of NIST SP 800-63 AAL.	" "	" "	
i. Have at least twelve (12) characters		" "	" "	

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
ii. For accounts that are accessible from outside a Secure Zone or High Security Zone, require that passwords have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, that are not a dictionary word or on a list of previously disclosed human-generated passwords and not be one of the user's previous four passwords; and implement account lockout for failed access attempts in accordance with subsection k; OR	WebTrust: Non-auditable portion is "that are not a dictionary word or on a list of previously disclosed human-generated passwords," PB5: It assumes passwords are the core authentication credential and does not align with current NIST guidance. Authentication requirements could probably be put in terms of NIST SP 800-63 AAL.	" "	" "	
iii. Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.	WebTrust: CAs have the burden of proof demonstrating their password management scheme is of equivalent security to the first two password configuration requirements.	" "	" "	
h. Require Trusted Roles to log out of or lock workstations when no longer in use	GP1-4: The term workstation here can be out dated. Is this intended to apply to any user connection into a CA system that is not designed to be persistent?	WebTrust § 3.4, Illustrative Control 23 - Procedures require that personal computers and workstations are logged off or protected by key locks, passwords or other controls when not in use	" "	
i. Configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user (the CA or Delegated Third Party MAY allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock)	GP1-4: The term workstation here can be out dated. Is this intended to apply to any user connection into a CA system that is not designed to be persistent?	WebTrust § 3.6, Illustrative Control 23 - Inactive terminals serving CA systems require re-authentication prior to use	" "	
j. Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations	GP1-5: The criteria as written causes a lot of compliance discussions. The first issue is many CAs design procedures to perform this on a quarterly basis rather than every 90 days. This causes reviews to drift a few days after 90 days. This also raises a lot of points about when the 90 day clock start and ends. If the next review starts 90 days after the last review ends, does that mean the review has to be completed and remediation activity performed by the 90th day or does the review process just need to have started? The term "system accounts" has also led to a lot of conversations. Is this intended to only be automated users or service accounts or does it include all users, human or machine? There is also discussion about which systems are in scope for these reviews. Should all CA, RA, and supporting systems be included along with supporting databases? GP2-10: Reviews of account configurations every 90 days (why not quarterly?) - very prescriptive, making it extremely easy to audit and extremely easy to fail, while not necessarily practical, or consistent WebTrust: If on day 91 the review is performed, this will be an audit finding and qualification.	WebTrust § 3.6 – Illustrative Control 5 - Access rights for users with trusted roles are reviewed at regular intervals and updated	ETSI § 7.4.6c - The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access)	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **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.
k. Lockout account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control	GP1-3: We see a lot of CAs that feel rigid password and lockout requirements become less necessary when multi-factor access is required as listed in other criteria. WebTrust: CAs cannot use 6 or more failed attempts before lockout.	WebTrust 3.6 – Illustrative Control 20 - Access to CA systems requires a secure logon process	ETSI § 7.4.6 - The CA shall ensure that CA system access is limited to properly authorized individuals	
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	GP1-6: The 24 hour threshold has been a criteria that is difficult for large organizations that have multiple teams supporting networking and other services and team members rotating amongst various services on a frequent basis. This is also difficult for offline systems that are touched infrequen-ly. WebTrust: Must be 24 hours not 1 business day. So if termination occurs on a weekend the accounts access must be revoked. 25+ hours after termination the access is revoked will be potentially a qualification. Also to revoke access, the authentication to shared accounts must be changed. The CA's will also have to retain system evidence of when the account's access was terminated for auditors to test this or it will be a disclaimer of opinion due to inability of the auditor to test this criteria. GP2-9: Responses are provided within 24hrs for revocation of access - very prescriptive, making it extremely easy to audit and extremely easy to fail,	WebTrust § 3.3, Illustrative Control 11 - Physical and logical access to CA facilities and systems is disabled upon termination of employment	ETSI § 7.4.6c - The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access);	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
m. Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems	PB6: It fails to define "multi-factor authentication".	WebTrust § 3.4, Illustrative Control 10 - Access to CA operational facilities is controlled and restricted to authorized persons through the use of multi-factor authentication controls;	ETSI 7.2.7 c) The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees.	
n. For each Delegated Third Party, (i) require multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate or (ii) implement technical controls that restrict the Delegated Third Party's ability to approve certificate issuance to a limited set of domain names	PB6: It fails to define "multi-factor authentication".	" "	ETSI 7.4.1 b) The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties. c) The CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
o. Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:	WebTrust: All remote access or offsite "VPN". Remote access can be interpreted as access from outside the subnet the CA systems sit on or through terminal services or SSH. By definition of Security Support System, this will include systems such as but not limited to, Active Directory, logging systems, firewalls, routers, L3 switches, AV, Vulnerability scanners, etc., which may not employ this level of control for remote access. How will the CA's document and track the approved external IP addresses, most end users will have dynamic IP addresses for example from coffee shop, home, air cards. Does external IP address include any IP address not within the Security zone (subnet CA systems are on for example)? No access – so no roaming IP. PB7: It fails to define "remote" (used as part of "remote administration or access"); Is remote anything other than using a keyboard and monitor	WebTrust § 3.6, Illustrative Controls 8-10 - CA employed personnel are provided direct access only to the services that they have been specifically authorized to use. The path from the user terminal to computer services is controlled. Remote access to CA systems, made by CA employees or external systems, if permitted, requires authentication. Connections made by CA employees or CA systems to remote computer systems are authenticated)		PR.AC-3: Remote access is managed PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
(i) the remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address,	WebTrust: Does this mean devices owned or controlled by the CA's must originate from a pre-approved external IP address or only for devices owned or controlled by the delegated 3rd party? The former and must be a device owned or controlled. A1: With multi-factor authorization and VPNs widely used today, is it really necessary that remote access to "an Issuing System, Certificate Management System, or Security Support System" come only via a "pre-approved external IP address?			
(ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and				
(iii) the remote connections is made to a designated intermediary device (a) located within the CA's network, (b) secured in accordance with these Requirements, and (c) that mediates the remote connection to the Issuing System	WebTrust: VPN gateways will need to be protected in a Secure Zone meeting these requirements.			
			ETSI § 7.2.7c - The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees).	
3. LOGGING, MONITORING, & ALERTING	GP2-7: The 3% audit requirement is not clear about the parameters that need to be reviewed for in the self-assessment of the issued certificates. Right now anyone can do anything as long as it covers 3% newly issued certs, and there is no guidance on what minimum sufficient procedures should be (if it is to be called self-audit). This is a separate thread on the forum from what I see anyway.			
Certification Authorities and Delegated Third Parties SHALL:				
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	WebTrust: SIEM, IDS, IDP, etc will need to be managed by and be under the control of "Trusted Roles" and not under a shared services team.	WebTrust § 3.9 - The CA maintains controls to provide reasonable assurance that … the effectiveness of the system audit process is maximized and interference to and from the system audit process is minimized and unauthorized CA system usage is detected.)		**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.
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		WebTrust § 3.9, Illustrative Control 13 - Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorized or suspicious activity. Alerting mechanisms are implemented to detect unauthorized access	ETSI § 7.4.6. i - k i) - Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources); j) - Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources. k) - Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
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		WebTrust § 3.9, Illustrative Control 13 - Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorized or suspicious activity. Alerting mechanisms are implemented to detect unauthorized access)		DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed DE.AE-2: Detected events are analyzed to understand attack targets and methods DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors DE.AE-4: Impact of events is determined DE.AE-5: Incident alert thresholds are established
d. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events	WebTrust: Follow-up requires some documentation of what was performed, not just close a ticket.	WebTrust § 3.10, Illustrative Control 13 - Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorized or suspicious activity. Alerting mechanisms are implemented to detect unauthorized access)		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
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)	GP1-7: The 30 day requirement is particularly difficult because some CAs establish this is a monthly control. We also see a lot of confusion in regards to the scope of this human review. Some CAs have interpreted this as a human review of log activity and feel it is not practical or effective to perform human review of log activity. Others feel this is more of a check up on the automated log monitoring in place. GP2-8: System logs are reviewed every 30 days (why not monthly?) - very prescriptive, making it extremely easy to audit and extremely easy to fail, while not necessarily practical, or consistent	WebTrust § 3.10 - audit logs are reviewed periodically by authorized personnel		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.DP-3: Detection processes are tested
f. Maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation		accordance with disclosed business practices. WebTrust § 3.10 - 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	ETSI § 7.4.11e - Records concerning certificates shall be held for a period of time as indicated in the CA's terms and conditions (see clause 7.3.4) in accordance with applicable legislation)	
4. VULNERABILITY DETECTION AND PATCH MANAGMENT				
Certification Authorities and Delegated Third Parties SHALL:				
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	GP1-8: Many CAs see this as a requirement to have anti-virus (AV) software installed and feel AV software is not required in some cases and opens more risks than it prevents. WebTrust: This does not mean that the entire AV system and control consoles have to be under the control of a CA/RA trusted role this can still be performed by a "Shared Service"	WebTrust § 3.5, Illustrative Control 8 – Detection and prevention controls to protect against viruses and malicious software are implemented. Employee awareness programs are in place	ETSI §7.4.5a - The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software)	DE.CM-4: Malicious code is detected ID.RA-3: Threats, both internal and external, are identified and documented **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. **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.
b. Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities	Provisions in the NetSec Requirements that aren't in the CSC criteria: **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	**WT 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. **WebTrust § 3.5 Illustrative Control 11** - Procedures exist and are followed for reporting hardware and software malfunctions		PR.IP-12: A vulnerability management plan is developed and implemented RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk PR.IP-7: Protection processes are continuously improved **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
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	WebTrust: Cannot test (i) unless event happens. For (ii) the CA will have the burned of proof to demonstrate to the auditor that changes questioned were not significant if an vulnerability scan was not performed in a reasonable timeframe (interpreted to be a week based on what the CA/B Forum interprets to be a reasonable timeframe) after the change was			DE.CM-8: Vulnerability scans are performed
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	WebTrust: The CA will have the burned of proof to demonstrate to the auditor that changes questioned were not significant if an penetration test was not performed in a reasonable timeframe after the change was made.			**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
e. Record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test and	GP1-9: A lot of CAs are looking for more guidance on the level of documentation that is required when assessing a penetration tester or tool for vulnerability scans. Many larger organizations have questions on the "independence" criteria and if a security element within the company but outside the PKI group is independent.			

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
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:	GP2-11: Then there is infamous 96 hrs. requirement for action in case of detection of Critical Vulnerability, which is both very prescriptive (i.e. if action is taken within 97 hrs., does criterion fail resulting in qualification to the report), as well as ambiguous (as in, when does the 96 hr. countdown start? From a discovery of vulnerability or from the moment it was determined to be a critical one? What determines moment of discovery – the moment it was logged, or the moment the log was reviewed, the moment issue entered into ticketing system, the moment it was escalated? If it takes management a week to determine that it is critical, does it mean they automatically failed the criterion, regardless how quickly they respond once this conclusion has been reached, or is it OK? WebTrust: The CA will have the burned of proof to demonstrate to the auditor that changes questioned were not significant if an vulnerability scan was not performed in a reasonable timeframe (interpreted to be a week based on what the CA/B Forum interprets to be a reasonable timeframe) after the change was made.			D.RA-2: Threat and vulnerability information is received from information sharing forums and sources RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks ID.GV-4: Governance and risk management processes address cybersecurity risks
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.	WebTrust: The CA needs to document this for each new vulnerability, and will have the burden of proof.			
	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.			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
	The Network Security Requirements do not specify backup criteria for CAs.	WT 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		**10 Data Recovery Capability** The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
	Wireless security is not called out separately in the CABF Network Security Reqs			**15. 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
	Training is discussed in the Baseline Requirements - "user management, separate trusted-role assignments, education, awareness, and training"			
	Software development is not called out separately in the CABF NetSec Reqs	**WT 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.		**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.
	Inventorying hardware was not called out separately - it was implied.			**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.
DEFINITIONS	One of the biggest things that cause confusion is discussion about definitions of terms used within this document. Example terms include CA System (defined but leads to more questions), Issuing System, or system accounts. We often see many different interpretations of secure zones.			
Certificate Management System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.	PB8: Certificate Management System and Security Support System definitions are both very broad. At least one interpretation prevents usage of any system accessible to persons who are not in Trusted Roles, even if such usage is not critical to system security. For example, the CA might have a corporate policy to send logs to a central log server in addition to CA specific log servers. It is not clear this is allowed.			

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS	Commentary	WebTrust	ETSI	CSC Criteria & NIST Cybersecurity Framework
Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.	GP2-1: "Certificate systems", "Certificate management system", "Security support system" – how far and wide are we going with this? Are we referring to the servers hosting the CA's or supporting systems as well?			
Common Vulnerability Scoring System (CVSS): A quantitative model used to measure the base level severity of a vulnerability.				
Critical Security Event: Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of	GP2-2: "Critical security events" – as defined by whom? Right now, considering the use of the phrase "event that could lead to…" and the long list of potential consequences, this is pretty open for interpretation.			
Critical Vulnerability: A system vulnerability that has a CVSS score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating, or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.				
Delegated Third Party: A natural person or legal entity that is not the CA and that operates any part of a Certificate System				
Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.				
Front End / Internal Support System: A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.	GP2-3: "Internal support systems" – how do we scope the boundaries of the system? If you use a ticketing system does that by default mean that all of these requirements apply to it?			
High Security Zone: A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.				
Issuing System: A system used to sign certificates or validity status information.				
National Vulnerability Database (NVD): A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems.				
OWASP Top Ten: A list of application vulnerabilities published by the Open Web Application Security Project.				
Penetration Test: A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.				
Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.				
SANS Top 25: A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities.				
Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.				
Security Support System: A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.				
System: One or more pieces of equipment or software that stores, transforms, or communicates data.				
Trusted Role: An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.				
Vulnerability Scan: A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.				
Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.	GP2-4: "Zones" (we've had a number of discussions on this one, particularly about applicability of various requirements across the zones)			