ANNEX A

FOLLOW-UP OF IDENTIFIED GAPS

No	Requirements	Issues Noted	Status
1	Principle 1, Criterion 1 requires that CA discloses 2 on its website its: · Certificate practices, policies and procedures, all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue), and its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. Principle 1, Criterion 3 requires that issuing CA documents in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the SSL Baseline Requirements. Principle 1, Criterion 4 requires that Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually. Principle 1, Criterion 5 requires that CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	We noted that audit reports at Certsuperior web site: - The policies, procedures and agreements are not available for consulting. - The CPS published is illegible. - The CPS version published lacks of compliance clause. - The CPS has not a 24 hours availability model. - Furthermore, we noted that CPS lacks of section to specify the Policy Identifier. As result, we noted that Certsuperior did not meet Principle 1, Criteria 3, 4 and 5 during the examination period.	Remedied
2	Principle 2, Criterion 4.4 requires that CA maintains controls and procedures to provide reasonable assurance that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request. Principle 2, Criterion 6.2 requires that CA maintains controls to provide reasonable assurance that: · the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. - The CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. - Validation Specialists engaged in Certificate issuance maintains skill levels consistent with the CA's training and performance programs. - The CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. - The CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.	During our request validation by Certsuperior process revision, we noted: - Lack of implemented and documented control for requests validation sent by personnel authorized. - Lack of training plan for employee that include issues like PKI fundamentals, authentications, policies and procedures, phishing techniques or social engineering. As result, we noted that Certsuperior did not meet Principle 2, Criteria 4.4 and 6.2, during the examination period.	Remedied

3	Principle 3, Criterion 2 requires that CA performs a risk assessment at least annually that: - Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; - Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate - Management Processes; and Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats. Principle 3, Criterion 3 requires that CA develops, implement, and maintain a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan: - includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. - takes into account then-available technology and the cost of implementing the specific measures, and - is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.	During our revision we noted lack of annual risk analysis over computer equipment's, technological infrastructure, facilities, etc., and lack of security program to manage the possible solutions that were identified in the annual risk analysis. As result, we noted that Certsuperior did not meet Principle 3, Criteria 2 and 3, during the examination period.	Remedied
4	Principle 4, Criterion 1 requires that CA maintains controls to provide reasonable assurance that: - Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship; - The same security controls for Certificate Systems apply to all systems co-located in the same zone; - Root CA Systems are located in a High Security Zone and in an offline state or air-gapped from all other networks; Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in at least a Secure Zone; - Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in at least a Secure Zone; - Security Support Systems are implemented and configured to 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; - Networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations; - Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are configured 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; - Configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies; - Administration access to Certificate Systems are granted only to persons acting in Trusted Roles and receive their accountability for the Certificate System's security; - Multi-factor authentication is implemented to each component of the Certificate System that supports it; - Authentication keys and passwords for any privileged account or service account on a Certificate System is changed, when a person's authorization to administratively access that account on the Certificate System is changed or revoked. - Recommended security patches are applied 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 the security patch.	Through diagram documented of network communication, equipment configuration policy and firewall configuration, we noted: - Lack of network segmentation for distinguish between equipment with access to application and with other ones that are not part of validation process. - The firewall implemented doesn't filter from internal network traffic to allow only communication with secure ports. - Lack of firewall between internal network and equipment that access to application. As result, we noted that Certsuperior did not meet Principle 4, Criterion 1(sub-bullet 1, 2, 4, 6), during the examination period.	Remedied

5	Principle 4, Criterion 2 requires that CA maintains controls to provide reasonable assurance that: - A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed; - The responsibilities and tasks assigned to Trusted Roles are documented and “separation of duties” for such Trusted Roles based on the risk assessment of the functions to be performed is implemented; - Only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones; - Individuals in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role; - Employees and contractors observe the principle of “least privilege” when accessing, or when configuring access privileges on, Certificate Systems; - Trusted Role use a unique credential created by or assigned to that person for authentication to Certificate Systems; - Trusted Role using an username and password to authenticate shall configure accounts to include but not be limited to: o Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones); o Configure passwords for accounts that are accessible from outside a Secure Zone or High Security Zone to have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, and not be one of the user’s previous four passwords; and implement account lockout for failed access attempts; OR o 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. - Trusted Roles log out of or lock workstations when no longer in use; - Workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user; - Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations; - Revoke 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; - Disable 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; - Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems; Each Delegated Third Party, shall be: o Required to use multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate; or o Be technically constrained that restrict the Delegated Third Party’s ability to approve certificate issuance for a limited set of domain names; and - Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: o 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, o The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and o The remote connection is made to a designated intermediary device meeting the following: - Located within the CA’s network, - Secured in accordance with these Requirements, and - Mediates the remote connection to the Issuing System.	During our revision we noted roles of users that are not confidence with access to validation request at the web application. As result, we noted that Certsuperior did not meet Principle 4, Criterion 2 (sub-bullet 5), during the examination period.	Remedied

6	Principle 4, Criterion 4 requires that CA maintains controls to provide reasonable assurance that: - Detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against viruses and malicious software; - A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities; Perform a Vulnerability Scan 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 based on the following: o Within one week of receiving a request from the CA/Browser Forum, o After any system or network changes that the CA determines are significant, and o At least once per quarter; Perform 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; - Document that Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; and - Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process: - Remediate the Critical Vulnerability; 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 the following: o 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 o 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 o Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: - The CA disagrees with the NVD rating; - The identification is a false positive; - The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or - Other similar reasons.	During our revision of technical vulnerabilities, we noted: - Lack of documented process for technical vulnerabilities management - The scans performed omitted private IP address of equipment with access to the application - The scans performed has not suitable periodicity and only had been executed over the https://www.certsuperior.com web site - The scans performed were executed by personnel without technical skills, ethic code and independence. As result, we noted that Certsuperior did not meet Principle 4, Criterion 4 (sub-bullet 1, 4), during the examination period.	Remedied