CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)
Introduction must include:
1) CA's Legal Name

"ComSign Ltd."

2) Clear indication (subject and SHA1 or SHA256 fingerprints) about which root certificates are being evaluated, and their full CA hierarchy. In considering a root certificate for inclusion in NSS, Mozilla must also evaluate the current subordinate CAs and the selection/approval criteria for future subordinate CAs. Mozilla's CA Certificate Policy requires full disclosure of non-technically-constrained intermediate certificates chaining up to root certificates in NSS.

"ComSign Global Root CA"
SHA256 fingerprint: 2605875afcc176b2d66dd66a995d7f8d5ebb86ce120d0e7e9e7c6ef294a27d4c

Subordinate CAs:
ComSign Corporations CA
SHA256 fingerprint: 5FB14F5FC0E00717D8FB0E0124E93ABB0548CD9CB2385201D465084C57218871

ComSign Professionals CA
SHA256 fingerprint: 22A65DA9C7540B9B29EE7270AC8E70FA56CB1CE8BBA2417920D4C57EC1F7AD4

ComSign ISA Global CA
SHA256 fingerprint: C925795DD1AA6825B55E8F4ED422BC967DC0EC67F9CA8E1FF916ECDC76FD4062

ComSign Organizational CA
SHA256 fingerprint: CB86CA69C00FE3DAAE45C2ADF945A19B6F0B8C82F95AB114EE862D87275F6B28

Comsign EV SSL CA
SHA256 fingerprint: 2136BADE1B3A613466646C48A4C2F95C756123BE31DC5641606A1746DEDA52FF

3) List the specific version(s) of the BRs that you used. For example: BR version 1.4.2, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.

BR version 1.4.8, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.

4) List the specific versions of the CA's documents that were evaluated, and provide direct URLs to those documents. All provided CA documents must be public-facing, available on the CA's website, and translated into English.

Comsign CPS v4.0. https://www.comsign.co.il/repository or https://www.comsign.co.il/cps

5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.

Note: When you are doing your BR Self Assessment, if you find that the required information is not currently in your CP/CPS documents, then you may indicate what your CA currently does, how it is currently documented, that the next version of your CP/CPS will contain this information, and when the next version of your CP/CPS will be available.

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Comsign CPS v4.0.	All issued and valid certificates were either issued or revoked in compliance with the timetable in the BR section 1.2.1.
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Comsign CPS v4.0.	All issued and valid certificates were either issued or revoked in compliance with the timetable in the BR section 1.2.2
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	Comsign CPS v4.0, section 1.3.2	Comsign Allows for delegated third parties. Delegated Third Parties are complaint with the BR and verified by an external auditor.
2.1. Repositories Provide the direct URLs to the CA's repositories	Comsign CPS v4.0, sections 2.1, 2.2	https://www.comsign.co.il/repository This repository includes links to documents, CA certificates and CRL files.
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	Comsign CPS v4.0, section 2.2	"Comsign conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements those Requirements take precedence over this document"

2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	Comsign CPS v4.0, section 2.2	A valid Subscriber certificate: https://fedir.comsign.co.il/test.html A revoked Subscriber certificate: https://revoked.comsign.co.uk/test.html An expired Subscriber certificate: https://expired.comsign.co.uk/test.html
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	Comsign CPS v4.0, section 2.3	" Changes in the CPS will be published after the approval by the Registrar and no less than once a year. "
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	Comsign CPS v4.0, section 2.4	"Free access to the Repository from Comsign's website is available to sections open to the public. The address of the Revoked Certificates Repository is https://www.comsign.co.il/repository. Access to other sections of the Repository is restricted, except to access authorized individuals according to Comsign's Procedures"
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.0 – Identity authentication for certificates for natural persons. Comsign CPS v4.0, section 3.2.2.1 - Identity authentication for certificates for authenticating servers and websites	Comsign CPS v4.0 section 3.2.2.0 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law. Comsign CPS v4.0, sections 3.2.2.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.2	This section in the CPS complies with the same section in the BRs.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.3	This section in the CPS complies with the same section in the BRs.
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly	Comsign CPS v4.0, section 3.2.2.4	acceptable methods of domain validation: Validating the Applicant as a Domain Contact, Email, Fax, SMS, or Postal Mail to Domain Contact, Phone Contact with Domain Contact, Constructed Email to Domain Contact, Domain Authorization Document, Agreed-Upon Change to Website, DNS Change, IP Address, TLS Using a Random Number

provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.		
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (i)	Confirming the applicant's control over the FQDN by validating the applicant is the Domain Contact directly with the Domain Name Registrar. For this method, Comsign will also authenticate the applicant's identity as specified in section 3.2.2.1 and the authority of the applicant representative under section 3.2.5 of the CPS
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection ii)	Confirming the applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact . The Random Value will be unique in each email, fax, SMS, or postal mail . The Random Value will remain valid for use in a confirming response for no more than 30 days from its creation.
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (iii)	Confirming the applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the applicant's request for validation of the FQDN. Comsign will place the call to a phone number identified by the Domain Name Registrar as the Domain Contact .
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (iv)	Confirming the applicant's control over the requested FQDN by: (a) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an authorization domain name , (b) including a Random Value in the email, and (c) receiving a confirming response utilizing the Random Value. The Random Value will be unique in each email . The Random Value will remain valid for use in a confirming response for no more than 30 days from its creation.
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (v)	Confirming the applicant's control over the requested FQDN by relying upon the attestation to the authority of the applicant to request a certificate contained in a Domain Authorization Document (see section 1.6). The Domain Authorization Document must substantiate that the communication came from the domain contact. Comsign shall verify that the Domain Authorization Document was either (a) Dated on or after the date of the domain validation request or

		(b) That the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (vi)	Confirming the applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of domain validation, on the authorization domain name that is accessible by Comsign CA via HTTP/HTTPS over an Authorized Port (see section 1.6): (a) The presence of Required Website Content (see section 1.6) contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content must not appear in the request used to retrieve the file or web page, or (b) The presence of the Request Token (see section 1.6) or request value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value will not appear in the request
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (vii)	Confirming the applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an authorization domain name or an authorization domain name that is prefixed with a label that begins with an underscore character . If a Random Value is used, Comsign will provide a Random Value unique to the certificate request and will not use the Random Value after 30 days
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (viii)	Confirming the applicant's control over the requested FQDN by confirming that the applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A. Comsign does not use this method	N/A
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.4 subsection (ix)	Confirming the applicant's control over the requested FQDN by confirming the presence of a Random Value within a certificate on the authorization domain name which is accessible by Comsign via TLS over an authorized port.
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.5	This section in the CPS complies with the same section in the BRs.

3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	Comsign CPS v4.0, section 3.2.2.6	This section in the CPS complies with the same section in the BRs.
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	Comsign CPS v4.0, section 3.2.2.7	This section in the CPS complies with the same section in the BRs.
3.2.3. Authentication of Individual Identity	Comsign CPS v4.0, section 3.2.3.1 – Authentication of individuals for certificates of natural persons. Comsign CPS v4.0, section 3.2.3.2 - Authentication of individuals for certificates of authenticating servers and websites	Comsign CPS v4.0 section 3.2.2.1 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law. Comsign CPS v4.0, sections 3.2.2.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs.
3.2.5. Validation of Authority	Comsign CPS v4.0, section 3.2.5	This section in the CPS complies with the same section in the BRs.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Comsign CPS v4.0, section 3.2.6	Comsign performs and manages issuance using solely the Comsign Issuance system, and does not rely on issuances carried out by any external organization.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	Comsign CPS v4.0, section 4.1.1	"Comsign maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. Comsign use this information to identify subsequent suspicious certificate requests."
4.1.2. Enrollment Process and Responsibilities	Comsign CPS v4.0, section 4.1.2	This section in the CPS complies with the same section in the BRs.
4.2. Certificate application processing		
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	Comsign CPS v4.0, section 4.2.1 – identification and verification for certificates of natural persons. Comsign CPS v4.0, section 4.2.1.1 - identification and verification for certificates of authenticating servers and websites	Comsign CPS v4.0, sections 4.2.1.1 - identification and verification for certificates of authenticating servers and websites: "(i) Comsign will obtain all the required information from the application request filed by the Applicant, from the Applicant itself or from a reliable, independent, third-party data source, provided such third-party information was confirmed with the Applicant. Comsign implements a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant. Applicant information must include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the certificate's SubjectAltName extension . (ii) Documents and data provided to Comsign according to section 3.2 to verify Certificate information may be used to issue Certificates up to 825 days as of the time they were obtained . (iii) Comsign implements a documented procedure that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the CA/Browser Forum Requirements.
4.2.2. Approval or Rejection of Certificate Applications	Comsign CPS v4.0, section 4.2.2 – Approval or Rejection for certificates of natural persons.	Comsign CPS v4.0 section 4.2.2 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law.

	Comsign CPS v4.0, section 4.2.2.1 – Approval or Rejection for certificates of authenticating servers and websites	Comsign CPS v4.0, sections 4.2.2.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs – it is stated that " Comsign will only issue certificates to domains with suffixes that were publicly approved by ICANN, and will not issue certificates with internal domain name suffixes. Comsign will not issue certificates containing a new gTLD under consideration by ICANN. Comsign will only issue certificates to Subscribers after verifying the control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4"
4.3.1. CA Actions during Certificate Issuance	Comsign CPS v4.0, section 4.3.1	This section in the CPS complies with the same section in the BRs.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	Comsign CPS v4.0, section 4.9.1.1	A Certificate will be revoked: (i) If Comsign has been notified by the Subscriber or finds out in another way that a theft, loss, change, unauthorized use, defect or another harm to the signatory device or to the Subscriber's control of the signatory device has occurred. (ii) Immediately when known to Comsign that one of the details of the Certificate is incorrect or the reliability of the Certificate was harmed in another way. (iii) Immediately when known to Comsign of a defect in its secured electronic signature, or its signatory device, or in its hardware and software systems, or in these systems' data security that might harm the reliability of its signature or that of the Electronic Certificates it issues. (iv) Immediately when known to Comsign that the Subscriber died (if a natural person) or an order of dissolution was issued (if a corporation), provided Comsign is assured that the notification is reliable. (v) If Comsign is required to comply with the operational requirements of this CPS. (vi) If a material defect was found in the Certificate issuance process, either a defect originating with Comsign, the Applicant or any other party involved in the issuance process . (vii) The certificate owner or his/her agent or another third party which is explicitly authorized in the subscriber agreement, requests the certificate revocation in writing, or via email or via phone (and is authenticated according to section 3.4. (viii) The certificate owner notifies Comsign that the original certificate request was not authorized and does not retroactively grant authorization (ix) Comsign is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use. (x) Comsign is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted. (xi) Comsign is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name. (xii) Comsign is made aware of a material change in the information contained in the certificate.

		(xiii) Comsign is made aware that the certificate was not issued in accordance with the CA/Browser Forum requirements or this CPS document. (xiv) Comsign ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate. (xv) Comsign is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate. (xvi) The technical content or format of the Certificate presents an unacceptable risk to application software suppliers or relying parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk)
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	Comsign CPS v4.0, section 4.9.1.2	The Issuing CA will revoke a Subordinate CA Certificate within seven (7) days of being notified if one or more of the following occurs: (i) The Subordinate CA requests revocation in writing. (ii) The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization. (iii) The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6. (iv) The Issuing CA obtains evidence that the Certificate was misused. (v) The Issuing CA is made aware that the Certificate was not issued in accordance with or that subordinate CA has not complied with this CPS. (vi) The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading. (vii) The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate. (viii) Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice statement. (ix) The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk
4.9.2. Who Can Request Revocation	Comsign CPS v4.0, section 4.9.2	This section in the CPS complies with the same section in the BRs.
4.9.3. Procedure for Revocation Request	Comsign CPS v4.0, section 4.9.3	This section in the CPS complies with the same section in the BRs.
4.9.5. Time within which CA Must Process the Revocation Request	Comsign CPS v4.0, section 4.9.5	This section in the CPS complies with the same section in the BRs.
4.9.7. CRL Issuance Frequency	Comsign CPS v4.0, section 4.9.7	This section in the CPS complies with the same section in the BRs.
4.9.9. On-line Revocation/Status Checking Availability	Comsign CPS v4.0, section 4.9.9 – On-line Revocation/Status Checking Availability for certificates of natural persons.	Comsign CPS v4.0 section 4.9.9 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law. OCSP service is only optional.

	Comsign CPS v4.0, section 4.9.9.1 – On-line Revocation/Status Checking Availability for certificates of authenticating servers and websites	Comsign CPS v4.0, sections 4.9.9.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs – it is stated that " Comsign always includes the AIA field for OCSP status checking in certificates of authenticating servers accessible through the Internet, and maintains the OCSP responder service for these certificates. OCSP responses will either (i) Be signed by the CA that issued the Certificates whose revocation status is being checked, or (ii) Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. In the latter case, the OCSP signing Certificate will contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960"
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	Comsign CPS v4.0, section 4.9.10 – On-line Revocation Checking requirements for certificates of natural persons. Comsign CPS v4.0, section 4.9.10.1 – On-line Revocation Checking requirements for certificates of authenticating servers and websites	Comsign CPS v4.0 section 4.9.10 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law. OCSP service is only optional. Comsign CPS v4.0, sections 4.9.10.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs – it is stated that " (i) Comsign supports OCSP capability using the GET method for Certificates issued. (ii) For the status of Subscriber Certificates: Comsign updates information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service always have an expiration time of less than ten days. (iii) For the status of Subordinate CA Certificates: Comsign updates information provided via an Online Certificate Status Protocol at least (i) Every twelve months and (ii) Within 24 hours after revoking a Subordinate CA Certificate. (iv) When the OCSP responder receives a request for status of a certificate that has not been issued, then the responder responds with a status of "unknown"."
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Comsign CPS v4.0, section 4.9.11	Comsign OCSP services do not rely on stapling.
4.10.1. Operational Characteristics	Comsign CPS v4.0, section 4.10.1	This section in the CPS complies with the same section in the BRs.
4.10.2. Service Availability	Comsign CPS v4.0, section 4.10.2	This section in the CPS complies with the same section in the BRs.
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	Comsign CPS v4.0, section 5	This section in the CPS complies with the same section in the BRs.
5.2.2. Number of Individuals Required per Task	Comsign CPS v4.0, section 5.2.2	This section in the CPS complies with the same section in the BRs.
5.3.1. Qualifications, Experience, and Clearance Requirements	Comsign CPS v4.0, section 5.3.1	This section in the CPS complies with the same section in the BRs.
5.3.3. Training Requirements and Procedures	Comsign CPS v4.0, section 5.3.3	This section in the CPS complies with the same section in the BRs.
5.3.4. Retraining Frequency and Requirements	Comsign CPS v4.0, section 5.3.4	This section in the CPS complies with the same section in the BRs.
5.3.7. Independent Contractor Controls	Comsign CPS v4.0, section 5.3.7	This section in the CPS complies with the same section in the BRs.
5.4.1. Types of Events Recorded	Comsign CPS v4.0, section 5.4.1	This section in the CPS complies with the same section in the BRs.
5.4.3. Retention Period for Audit Logs	Comsign CPS v4.0, section 5.4.3	This section in the CPS complies with the same section in the BRs.

5.4.8. Vulnerability Assessments	Comsign CPS v4.0, section 5.4.8	This section in the CPS complies with the same section in the BRs.
5.5.2. Retention Period for Archive	Comsign CPS v4.0, section 5.5.2	This section in the CPS complies with the same section in the BRs.
5.7.1. Incident and Compromise Handling Procedures	Comsign CPS v4.0, section 5.7.1	This section in the CPS complies with the same section in the BRs.
6.1.1. Key Pair Generation	Comsign CPS v4.0, section 6.1.1	This section in the CPS complies with the same section in the BRs.
6.1.2. Private Key Delivery to Subscriber	Comsign CPS v4.0, section 6.1.2	This section in the CPS complies with the same section in the BRs.
6.1.5. Key Sizes	Comsign CPS v4.0, section 6.1.5	This section in the CPS complies with the same section in the BRs.
6.1.6. Public Key Parameters Generation and Quality Checking	Comsign CPS v4.0, section 6.1.6	This section in the CPS complies with the same section in the BRs.
6.1.7. Key Usage Purposes	Comsign CPS v4.0, section 6.1.7	This section in the CPS complies with the same section in the BRs.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	Comsign CPS v4.0, section 6.2	This section in the CPS complies with the same section in the BRs.
6.2.5. Private Key Archival	Comsign CPS v4.0, section 6.2.5	This section in the CPS complies with the same section in the BRs.
6.2.6. Private Key Transfer into or from a Cryptographic Module	Comsign CPS v4.0, section 6.2.6	This section in the CPS complies with the same section in the BRs.
6.2.7. Private Key Storage on Cryptographic Module	Comsign CPS v4.0, section 6.2.7	This section in the CPS complies with the same section in the BRs.
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	Comsign CPS v4.0, section 6.3.2 – Certificate operational periods for certificates of natural persons. Comsign CPS v4.0, section 6.3.2.1 – Certificate operational periods for certificates of authenticating servers and websites	Comsign CPS v4.0 section 6.3.2 deals with certificates for natural persons only (including Secure Email EKU) and complies with the Israeli Law. OCSP service is only optional. Comsign CPS v4.0, sections 6.3.2.1 deals with certificates for authenticating servers and websites and complies with the CABF BRs – it is stated that "Subscriber Certificates that will be issued after 1 March 2018 will have a validity period no greater than 825 days. Subscriber Certificates that will be issued after 1 July 2016 but prior to 1 March 2018 will have a validity period no greater than 39 months"
6.5.1. Specific Computer Security Technical Requirements	Comsign CPS v4.0, section 6.5.1	This section in the CPS complies with the same section in the BRs.
7.1. Certificate profile	Comsign CPS v4.0, section 7.1	This section in the CPS complies with the same section in the BRs.
7.1.1. Version Number(s)	Comsign CPS v4.0, section 7.1.1	This section in the CPS complies with the same section in the BRs.
7.1.2. Certificate Content and Extensions; Application of RFC 5280		
7.1.2.1 Root CA Certificate	Comsign CPS v4.0, section 7.1.2.1	This section in the CPS complies with the same section in the BRs.
7.1.2.2 Subordinate CA Certificate	Comsign CPS v4.0, section 7.1.2.2	This section in the CPS complies with the same section in the BRs.
7.1.2.3 Subscriber Certificate	Comsign CPS v4.0, section 7.1.2.3	This section in the CPS complies with the same section in the BRs.
7.1.2.4 All Certificates	Comsign CPS v4.0, section 7.1.2.4	This section in the CPS complies with the same section in the BRs.
7.1.2.5 Application of RFC 5280	N/A	Comsign does not implement any Certificate Transparency mechanisms
7.1.3. Algorithm Object Identifiers	Comsign CPS v4.0, section 7.1.3	This section in the CPS complies with the same section in the BRs.
7.1.4. Name Forms	Comsign CPS v4.0, section 7.1.4	"Different names may appear in the Certificates issued by Comsign in accordance with subsection 3.1. The names may be one of the following: (i) Name of a person or an organization as it appears in the document used for identification, as described in subsection 3.2 .

		(ii) Email address, according to standard RFC822 . (iii) Distinguish name according to standard RFC1770, including fields such as O, CN, T, SN, G, C, OU. (iv) Fully-Qualified Domain Names (v) IP addresses"
7.1.4.1 Issuer Information	Comsign CPS v4.0, section 7.1.4.1 and section 7.1.2	These sections in the CPS comply with the same section in the BRs.
7.1.4.2 Subject Information	Comsign CPS v4.0, section 7.1.4.2 and section 7.1.2	These sections in the CPS comply with the same section in the BRs.
7.1.4.3 Subject Information - Subordinate CA Certificates	Comsign CPS v4.0, section 7.1.4.3 and section 7.1.2	These sections in the CPS comply with the same section in the BRs.
7.1.5. Name Constraints	Comsign CPS v4.0, section 7.1.5	"Comsign does not limit names, provided that the names match the conditions described in subsection 3.1. The NameConstraints extension is not used."
7.1.6. Certificate Policy Object Identifier	Comsign CPS v4.0, section 7.1.6 and section 7.1.2	Electronic Certificates issued by Comsign conform Comsign's policy that holds the following object identifier: OID: 1.3.6.1.4.1.19389.2.1.1
7.1.6.1 Reserved Certificate Policy Identifiers	Comsign CPS v4.0, section 7.1.6 and section 7.1.2	Comsign may also use other policy identifiers such as OID 2.23.140.1.2.1, OID 2.23.140.1.2.2 – see Comsign CPS v4.0 section 7.1.2
7.1.6.2 Root CA Certificates	Comsign CPS v4.0, section 7.1.6 and section 7.1.2	These sections in the CPS comply with section 7.1.6.2 in the BRs.
7.1.6.3 Subordinate CA Certificates	Comsign CPS v4.0, section 7.1.6 and section 7.1.2	These sections in the CPS comply with section 7.1.6.3 in the BRs.
7.1.6.4 Subscriber Certificates	Comsign CPS v4.0, section 7.1.6 and section 7.1.2	These sections in the CPS comply with section 7.1.6.4 in the BRs.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	Comsign CPS v4.0, section 8.1	This section in the CPS complies with section 8 in the BRs.
8.1. Frequency or circumstances of assessment	Comsign CPS v4.0, section 8.1	This section in the CPS complies with the same section in the BRs.
8.2. Identity/qualifications of assessor	Comsign CPS v4.0, section 8.2 and section 8.3	These sections in the CPS comply with section 8.2 in the BRs.
8.4. Topics covered by assessment	Comsign CPS v4.0, section 8.4	This section in the CPS complies with the same section in the BRs.
8.6. Communication of results	Comsign CPS v4.0, section 8.6	This section in the CPS complies with the same section in the BRs.
8.7. Self-Audits	Comsign CPS v4.0, section 8.7	This section in the CPS complies with the same section in the BRs.
9.6.1. CA Representations and Warranties	Comsign CPS v4.0, section 9.6.1	This section in the CPS complies with the same section in the BRs.
9.6.3. Subscriber Representations and Warranties	Comsign CPS v4.0, section 9.6.3	This section in the CPS complies with the same section in the BRs.
9.8. Limitations of liability	Comsign CPS v4.0, section 9.8	This section in the CPS complies with the same section in the BRs.
9.9.1. Indemnification by CAs	Comsign CPS v4.0, section 9.9.1	This section in the CPS complies with the same section in the BRs.
9.16.3. Severability	Comsign CPS v4.0, section 9.16.3	This section in the CPS complies with the same section in the BRs.