Generic Test Cases for Charging Function (CHF) of a 5G Network

Clause No.	Clause Name	Test Case No.	Test Case Name	Test Case Description (for CHF NF)	Expected Results for Pass (for CHF NF)
1.1.1	Authentication for Product Management and Maintenance interfaces	TC 1	TC_MGMT_PROTOCOLS_OEM_DECLARATION	To verify that all the management and maintenance protocols available in the DUT are as per the OEM declaration.	The management and maintenance protocols running on the DUT match the OEM declaration.
		TC 2	TC_MUTUAL_AUTH_CHF	To verify that the CHF supports mutual authentication through both: Mutual TLS (mTLS) and Mutual SSH authentication.These mechanisms ensure both the CHF and the management entity (client/tester) authenticate each other before communication, as per latest ITSAR on cryptographic controls.	Mutual authentication is successfully established when valid credentials are used; however, communication cannot be established if invalid credentials are provided and mutual authentication fails. The protocols and cipher suites used comply with Table 1 of the latest ITSAR on cryptographic controls.
		TC 3	TC_HTTPS_CHF_WebUI	To verify that the CHF WebUI management interface operates exclusively over HTTPS with TLS, using a valid server certificate and secure cryptographic controls to protect all login, API, and operational interactions, with no HTTP access permitted and all database connections secured via SSL/TLS as required by the ITSAR	The CHF WebUI is accessible only through HTTPS/TLS using a valid server certificate. Access to the CHF WebUI over HTTP is not permitted. All API communications and database connections are secured using SSL/TLS.
		TC 4	TC_OTHER_MGMT_PROTOCOLS	To verify that all other protocols deployed on management and maintenance interfaces of DUT enforce mutual authentication methods strictly using Secure Cryptographic Controls prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.	All protocols deployed on management and maintenance interfaces of DUT enforce mutual authentication strictly using secure cryptographic controls prescribed in Table 1 of latest ITSAR on cryptographic controls.
		TC 5	TC_INSECURE_AUTH_PROTOCOL	To verify any insecure or deprecated authentication protocol available in the DUT.	The DUT does not support insecure or deprecated authentication protocols like Telnet etc.
1.1.2	Management Traffic Protection	TC 1	TC_MGMT_TRAFFIC_PROTECTION_PROTOCOLS_OEM_DECLARATION	To verify that all protocols (available in DUT) handling management traffic to and from DUT are as per OEM declaration	All protocols (available in DUT) handling management traffic to and from DUT are as per OEM declaration
		TC 2	TC_PROTECT_HTTPS_DATA_INFO_TRANSFER	To verify that all HTTPS-based management traffic is secured using cryptographic protocols and algorithms compliant with Table 1 of latest ITSAR on cryptographic controls.	The DUT ensures all HTTPS-based management traffic is secured using cryptographic protocols and algorithms compliant with Table 1 of latest ITSAR on cryptographic controls, permitting negotiation only with approved TLS versions and cipher suites. Any attempt to establish communication using deprecated or insecure protocols or cryptographic algorithms is denied.
		TC 3	TC_PROTECT_SSH_DATA_INFO_TRANSFER	To verify that SSH management sessions of the CHF are protected using industry-standard cryptographic algorithms and secure protocol versions. The test ensures that the CHF supports only approved SSHv2 algorithms (as per Table 1 of ITSAR on cryptographic controls and 3GPP TS 33.310 Annex F) and rejects deprecated options.	The DUT ensures that all management traffic over SSH is protected using protocols and cryptographic algorithms compliant with ITSAR requirements, permitting only approved key exchange methods, ciphers, and hashing algorithms while rejecting deprecated or insecure options.
		TC 4	TC_OTHER_MGMT_TRAFFIC_PROTECTION_PROTOCOLS	To verify that all other protocols handling management traffic to and from the DUT strictly use secure cryptographic controls prescribed in Table 1 of the latest ITSAR for Cryptographic Controls.	The DUT ensures that all other protocols handling management traffic to and from DUT strictly use secure cryptographic controls prescribed in Table 1 of latest ITSAR for Cryptographic Controls.
		TC 5	TC_INSECURE_AUTH_PROTOCOL	To verify any insecure or deprecated authentication protocol available in the DUT.	The DUT does not support insecure or deprecated authentication protocols like Telnet etc.
1.1.3	Role-based access control policy	TC1	TC_ROLE_VERIFICATION	To verify that user roles are defined in the CHF as per Role-Based Access Control (RBAC). The CHF shall support at least three distinct user roles — Admin. OAM privilege management for CHF Management and Maintenance, and user — stored in the MongoDB database used by the CHF.	The DUT supports Role-Based Access Control (RBAC) by defining multiple user roles (minimum three) and associating users with specific roles, such that role information is clearly maintained and identifiable within the system, in compliance with ITSAR requirements.
		TC2	TC_ACCESS_ENFORCEMENT_FUNCTIONAL	To verify that the CHF enforces Role-Based Access Control (RBAC) privileges via its HTTPS Management API. Users with the admin role can create and delete user accounts, while other user roles are restricted and cannot perform these actions.	The CHF enforces Role-Based Access Control (RBAC) privileges through its HTTPS Management API such that only users with the admin role are permitted to create or delete user accounts, while users with other roles are restricted from performing these actions.
		TC3	TC_ACCESS_ENFORCEMENT_CHF_CONTAINER	To verify that the CHF container enforces Role-Based Access Control (RBAC) at the operating system level using standard Linux permission roles, namely Owner (root), Group, and Others.	The DUT enforces Role-Based Access Control at the operating system level by applying appropriate file permissions and access restrictions using standard Linux permission roles
		TC 4	TC_USER_CREATION_WITHOUT_ROLE	To verify that the CHF enforces Role-Based Access Control (RBAC) to new users created without an assigned role.	New user created without specifying any role is automatically assigned lowest privileged role or user creation without any role is unsuccessful.
1.1.4	User authentication - Local/Remote	TC1	TC_ACCOUNT_PROTECTION_LOCAL	To verify that all local user accounts on the DUT are protected with at least one authentication attribute	The DUT ensures that all local user accounts are protected with at least one valid authentication attribute such as a password . It is not possible to access any predefined or newly created account without proper authentication.
		TC2	TC_ACCOUNT_PROTECTION_REMOTE	To verify that all remote user accounts on the DUT enforce a combination of two authentication mechanisms—such as a public key and password (2FA)—when accessed remotely via SSH.	All remote user accounts (such as SSH access) on the DUT enforce a combination of at least two authentication mechanisms.
1.1.5	Remote login restrictions for privileged users	TC1	TC_VERIFICATION_OF_REMOTE_ROOT_LOGIN_RESTRICTION	To verify that the security control restricting remote root login is properly configured and enforced on the CHF, permitting direct root login only through the system console.	The DUT restricts remote login for the root or highest privileged user such that remote access via SSH is not permitted. Root access is permitted only through the local system console.
		TC2	TC_VERIFICATION_VIA_APPLICATION_SOFTWARE_REMMINA	To verify that the remote root login restriction is effective not just for command-line tools, but also for graphical remote administration software, as required by the policy.	The DUT ensures that remote root login is restricted across all access methods, including graphical or application-based remote tools.
		TC3	TC_REMOTE_LOGIN_RESTRICTION	To verify that the highest privileged or root user is unable to remotely access using all other supported remote management protocols (e.g., HTTPS, Netconf etc.)	After configuration, the highest privileged user or root is not allowed to connect remotely using any supported remote management protocol. All such remote login attempts are denied.
		TC1	TC_AUTHORIZATION_LOG_FILE	To verify that only the chf service account (O&M user) can read/write log files, while an unprivileged user (user1) cannot read, write, modify, or delete it—enforcing least-privilege.	The DUT enforces authorization controls on log files such that only O&M user is able to perform operations like read and write, while unprivileged users are restricted from accessing or modifying the files.

1.1.6	**Authorization Policy**	TC2	TC_AUTHORIZATION_CONFIGURATION_FILE	To verify that the system configuration file /etc/hosts can only be modified by the root user. O&M users and unprivileged users may read but not write, confirming least-privilege enforcement.	The DUT system configuration file /etc/hosts is modifiable only by the root user. O&M users and unprivileged users may have read access but not permitted to modify the file.
		TC3	TC_AUTHORIZATION_FILE_ACCESS	To verify that /etc/shadow is accessible only by root; both O&M user and unprivileged user must be denied read/write access.	The DUT ensures that sensitive system files such as /etc/shadow are accessible only to privileged users and are fully restricted from access by O&M user and unprivileged user.
		TC4	TC_AUTHORIZATION_STICKYBIT	To verify that the sticky bit is correctly configured on the /tmp directory, ensuring that an unprivileged user cannot delete files created by another user (e.g., chf) within the shared directory, thereby enforcing proper access control and protection of shared resources	The DUT enforces proper authorization controls in shared directories by implementing mechanisms such as the sticky bit, ensuring that users can only modify or delete their own files and cannot interfere with files created by other users.
		TC5	TC_INTERMEDIATE_ROLE_VERIFICATION	To verify authorization level of a user who has higher privileges than lowest and lesser privileges than highest and ensure that access rights are enforced according to the assigned role.	The user is able to perform only those operations permitted for the assigned role. Operations requiring higher privileges are denied.
		TC6	TC_APPLICATION_PRIVILEGE_VERIFICATION	To verify that the applications are not running with system/administrator rights.	No application or service is found to be running with system/administrator privileges in the DUT.
1.1.7	**Unambiguous Identification of the User and Group Accounts**	TC1	TC_ACCOUNT_NUM_UNIQUE	To create multiple user accounts and verify that each account is assigned a unique identifier.	DUT does not support creating multiple users with same unique identifier.
		TC2	TC_ACCOUNT_DEFAULTS	To verify that the default setup of the DUT does not allow the use of group accounts or group credentials.	DUT ensures that default system configuration does not allow group accounts or shared credentials.
		TC3	TC_ACCOUNT_NAME_UNIQUE	To verify that creation of multiple user accounts with same account name is not permitted.	Creation of multiple user accounts with same account name is not permitted
2.2.1	**Authentication Policy**	TC 1	TC_AUTH_PROTOCOLS_OEM_DECLARATION	To verify that all the authentication protocols available in the DUT are as per the OEM declaration.	The authentication protocols available in the DUT match the OEM declaration.
		TC 2	TC_SSH_ACCESS	To verify that DUT supports SSH access with at least two-factor authentication (2FA).	The DUT supports SSH access with atleast 2FA.
		TC 3	TC_SFTP_ACCESS_WITH_2FA	To verify that DUT supports SFTP access with two factor authentication.	The DUT enforces secure authentication for SFTP access using at least two authentication attributes.
		TC 4	TC_WEBUI_ACCESS_WITH_2FA	To verify that DUT supports access to WebUI interface only after successful two-factor authentication using HTTPS.	The DUT ensures that access to the WebUI is secured through HTTPS and requires at least two authentication attribute.
		TC 5	TC_LOCAL_MANAGEMENT_CONSOLE_ACCESS	To verify that users can log in locally at the system console with atleast one authentication attribute.	Authentication is successful with atleast one authentication attribute.
		TC 6	TC_HTTPS_ACCESS_CONTROL_VERIFICATION	To verify that DUT HTTPS Service-Based Interface (SBI) enforces two authentication attributes.	The DUT enforces authentication for HTTPS-based system functions using at least two authentication attributes.
		TC 7	TC_OTHER_AUTH_PROTOCOLS	To verify that all other authentication protocols available in the DUT enforce at least two-factor authentication for user accounts and single-factor authentication for machine accounts or local access.	The DUT ensures that all other authentication protocols available in the DUT enforce at least two-factor authentication for user accounts and single-factor authentication for machine accounts or local access.
		TC 8	TC_MACHINE_ACCOUNT_AUTHENTICATION	To verify that machine accounts can authenticate using at least one authentication attribute and access the permitted system functions.	DUT Supports atleast one Authentication attribute for all supported protocols successfully.
		TC 9	TC_COMM_BTW_SYSTEMS	To verify that communications between systems (includes BGP, OSPFv2 v3, RIPv2, IS-IS, TACACS+, RADIUS, RADSEC, etc.,) requires authentication with atleast one attribute and communicate with DUT.	Authentication with atleast one authentication attribute is successful.
2.2.2	**Authentication Support – External**	TC 1	TC_EXT_AUTH_PROTOCOLS_OEM_DECLARATION	To verify that all the authentication and elated service protocols used by DUT for communicating with external authentication entity are as per the OEM declaration.	All the authentication and elated service protocols used by DUT for communicating with external authentication entity are as per the OEM declaration
		TC 2	TC_OTHER_EXT_AUTH_PROTOCOLS	To verify that all the authentication protocols (TACACS+, RADIUS, RADSEC, LDPA etc.) available in the DUT for communicating with an external authentication entity, use secure cryptographic controls compliant with Table 1 of the latest ITSAR on Cryptographic Controls.	The DUT ensures that all other authentication protocols available in the DUT for communicating with an external authentication entity, use secure cryptographic controls compliant with Table 1 of the latest ITSAR on Cryptographic Controls.
2.2.3	**Protection against Brute Force and Dictionary Attacks**	TC1	TC_INVALID_LOGIN_TIMER_DELAY	To verify that the DUT enforces a configurable timer delay after each incorrect password attempt, preventing rapid repeated login attempts.	The DUT enforces a configurable delay after each incorrect authentication attempt, preventing rapid repeated login attempts.
		TC2	TC_INVALID_LOGIN_ACCOUNT_BLOCKING	To verify that the DUT automatically locks a user account after the configured number of consecutive incorrect password attempts and it provides a secure and controlled account unlock mechanism after lockout.	The DUT locks a user account after a defined number of consecutive failed authentication attempts and also provides a controlled mechanism for unlocking the account.
		TC3	TC_BLACKLISTED_PASSWORD_REJECTION	To verify that the DUT correctly rejects any password that appears in the defined password blacklist (e.g., common or weak passwords).	The DUT enforces a password policy that rejects weak or commonly used passwords by validating against a defined blacklist.
		TC4	TC_BRUTE_FORCE_ATTACK_PROTECTION	To verify that the DUT's password complexity is strong enough to resist brute-force attacks performed using the any automated password cracking tool.	The DUT enforces strong password complexity requirements and implements protection mechanism/s to mitigate brute-force attacks.
		TC5	TC_CAPTCHA_ACTIVATION_AFTER_FAILED_LOGINS	To verify that the DUT activates CAPTCHA after a configured number of consecutive failed authentication attempts.	The DUT enforces CAPTCHA verification after multiple failed login attempts and does not allow further authentication attempts until the CAPTCHA challenge is completed successfully.
		TC6	TC_DICTIONARY_ATTACKS_PROTECTION	To verify that the DUT is protected against dictionary-based attacks by preventing authentication using commonly used or weak passwords from predefined wordlists, ensuring such passwords cannot be exploited using automated password guessing tools.	The DUT implements mechanism/s such as password policies, blacklist enforcement, and account lockout to prevent dictionary attacks through automated password guessing tools.
2.2.4	**Enforce Strong Password**	TC1	TC_PASSWORD_MINIMUM_LENGTH	To verify that the DUT enforces a minimum password length of 8 characters. The DUT must reject any password that does not meet this minimum requirement.	The DUT enforces a minimum password length of at least 8 characters and rejects any password that does not meet this requirement. DUT does not permit setting this absolute minimum length to a lower value by configuration.
		TC2	TC_PASSWORD_COMPLEXITY_4_CATEGORIES	To verify that the DUT enforces password complexity by requiring passwords to contain all four character categories: uppercase letters, lowercase letters, digits, and special characters.	The DUT enforces password complexity requirements such that passwords include at least one uppercase letter, one lowercase letter, one digit, and one special character, and any password not meeting these criteria is rejected.
		TC3	TC_PASSWORD_CONFIGURE_MIN_LENGTH_SPECIAL_CHAR	To verify that the DUT enforces configurable minimum password length and configurable sets of allowable special characters, including Unicode-based character class requirements.	The DUT allows configuration of minimum password length and allowed special character/unicode class, and rejects passwords which do not comply with the configured policy.

		TC4	TC_PASSWORD_STORE	To verify that the DUT does not store passwords in clear text and that passwords are stored using hashing and salting mechanisms.	The DUT does not store passwords in clear text. Passwords are securely stored using salted and hashed cryptographic mechanisms.
		TC5	TC_WHILE_CHANGING_PWDS	To verify that the DUT/central system checks and ensures that it meets the password requirements when a user is changing a password or entering a new password.	The DUT/central system checks and ensures that it meets the password requirements when a user is changing a password or entering a new password.
2.2.5	Inactivity Session Timeout	TC1	TC_INACTIVITY_SESSION_TIMEOUT_CONFIGURE	To verify that the DUT enforces inactive session timeout for local and remote access for both privileged and non privileged users. To verify the logs.	The DUT implements inactivity timeout for user sessions. The user is logged out after timeout period.
		TC2	TC_INACTIVITY_SESSION_TIMEOUT_VERIFY	To verify that the DUT supports configuration of inactive session time out in DUT for local and remote access for both privileged and non privileged users.	The DUT allows configuration of inactive session timeout and session automatically terminates after the configured inactive session timeout and require reauthentication for access.
2.2.6	Password Changes	TC1	TC_PASSWORD_CHANGE	To verify that the DUT allows users to change their password at any time. Password change shall be enforced after initial login (after successful authentication).	The DUT allows users to change their passwords at any time and enforces mandatory password change upon initial login after successful authentication.
		TC2	TC_PASSWORD_EXPIRE	To verify that the DUT enforces password expiry and notifies users before expiry.	The DUT enforces password expiry, provide expiry notification, and also requires password change upon expiry.
		TC3	TC_PASSWORD_HISTORY	To verify that the DUT enforces password history and prevents reuse of previous passwords. The DUT must store at least last three passwords and prevent their reuse. The number of disallowed previous passwords shall be configurable and greater than zero.	The DUT enforces a password history policy that prevents reuse of previously used passwords, with a configurable history value greater than zero and a minimum of three previously used passwords stored.
		TC4	TC_PASSWORD_AGE	To verify that the DUT enforces a minimum password age policy of one day. The DUT must restrict password change attempts until the minimum age period has passed.	The DUT enforces a minimum password age of at least one day, preventing immediate password reuse or cycling.
		TC5	TC_PASSWORD_CHANGE_OF_USER_ROLES	To verify that the DUT enforces password change upon user role modification.	The DUT enforces password change when user roles or privileges are modified.
2.2.7	Protected Authentication feedback	TC1	TC_HIDING_PASSWORD_DISPLAY	To verify that the password entry on the DUT is hidden while creating user and when user logins, ensuring that individual characters are not displayed in plain text during input. To verify this for local login, remote login and web access.	The DUT ensures that password input is not displayed in plaintext.
		TC2	TC_HIDING_CHANGE_PASSWORD_DISPLAY	To verify that the DUT hides password input during password change operations.	The DUT ensures that password input during password change operations is protected from display and is not visible.
		TC3	TC_MGMT_PROTOCOLS	To check any available management authentication protocol	DUT enforces protected authentication feedback during login using management protocol.
		TC4	TC_MANAGEMENT_PROTOCOL	To verify that the DUT enforces protected authentication feedback during login using management protocol.	The DUT enforces protected authentication feedback.
2.2.8	Removal of Predefined or default authentication attributes	TC1	TC_PREDEFINED_AUTHENTICATION_ATTRIBUTES_DELETED_DISABLED	To verify that all predefined or default authentication attributes (such as default usernames and passwords) in the DUT are deleted, disabled, or forced for updation during forst login.	The DUT ensures that all predefined or default authentication attributes such as default usernames, passwords, or credentials are either deleted, disabled, or forced for updation upon first login.
		TC2	TC_CRYPTOGRAPHIC_DEFAULT_KEY_REMOVAL_DISABLED	To verify that the DUT removes or replaces predefined/default cryptographic keys.	The DUT ensures that predefined/default cryptographic keys are removed or replaced with securely generated keys.
		TC3	TC_OEM_MANUAL	To verify that all predefined or default authentication attributes (such as default usernames and passwords) in the DUT are forced for updation by following the procedure given in OEM's manual.	The DUT ensures that all predefined or default authentication attributes such as default usernames, passwords, or credentials are not available after completion of procedure.
2.2.9	Logout Function	TC1	TC_LOGOUT_FUNCTION	To verify that the DUT allows a user to logout at any time and terminates all associated processes and sessions.	The DUT successfully terminates all user sessions and associated processes upon logout.
		TC2	TC_DEBUGGING_MODE_DETACHED_PROCESS_CONTINUES_AFTER_LOGOUT	To verify that the DUT allows detached/debug processes to continue running after user logout (if supported).	The DUT allows detached/debug processes to continue after logout while terminating the interactive session.
2.2.10	Policy regarding consecutive failed login attempts	TC1	TC_FAILED_LOGIN_ATTEMPTS_TEMPORARY_LOCK	To verify that the DUT enforces a configurable limit on consecutive failed login attempts and applies a temporary lock for user and administrative accounts.	The DUT temporarily locks the account after exceeding the configured consecutive number of failed login attempts and allows login only after a defined delay.
		TC2	TC_FAILED_LOGIN_ATTEMPTS_PERMANENT_LOCK	To verify that the DUT supports permanent lock for non-administrative accounts and only temporary lock for administrative accounts after exceeding failed login attempts.	The DUT permanently locks non-administrative accounts after exceeding the configured number of failed attempts, while administrative accounts are temporarily locked and regain access after the defined delay.
		TC3	TC_FAILED_LOGIN_ATTEMPTS_DEFAULT	To verify that the DUT enforces a default maximum value of consecutive failed login attempts as less than or equal to 8.	The DUT temporarily locks the account after exceeding 8 consecutive number of failed login attempts.
		TC4	TC_FAILED_LOGIN_ATTEMPTS_BLOCK_DELAY	To verify that the DUT applies a block delay (increasing the delay after every failed attempt) with default value as greater than 5s.	The DUT blocks the account for 5s after maximum failed login attempts.
2.2.11	Suspend Account on Non-Use	TC1	TC_ACCOUNT_EXPIRY_FUNCTION	To verify that the DUT automatically suspends a user account after a defined/configured period of inactivity ('X' days).	The DUT automatically suspends the account after 'X' days (number of days is configurable) of non-usage and prevents login until reactivation.
2.3.1	Secure Update	TC1	TC_SW_PKG_INTEGRITY_VALID	To verify the integrity in accordance with the latest ITSAR on cryptographic controls while performing a legitimate (non-tampered) software update.	The DUT updates the software only after validating the integrity of the software image in accordance with Table 1 of the latest ITSAR on cryptographic controls.
		TC2	TC_SW_PKG_INTEGRITY_TAMPERED	To verify the integrity in accordance with the latest ITSAR on cryptographic controls ITSAR while performing a illegitimate (tampered) software update.	The DUT validates integrity of the software image as per Table 1 of latest ITSAR on cryptographic controls and restricts update in case of an illegitimate (tampered) software.
		TC 3	TC_SW_PKG_INTEGRITY_NO_SIGNATURE	To verify that a software update does not happen on the DUT while using a non-signed image.	The DUT does not update the software in absence of a digital signature on the software image.
		TC 4	TC_SW_PKG_INTEGRITY_UNAUTHORIZED	To verify that a software update can not be performed on the DUT by an unauthorized user.	The DUT restricts software update request given by an aunauthorized user.
		TC 5	TC_SW_PKG_INTEGRITY_EXPIRED	To verify the DUT rejects the software update of an image with expired digital certificate.	The DUT does not update the software if digital certificate of the software image is expired.
2.3.2	Secure Upgrade	TC1	TC_SW_PKG_INTEGRITY_VALID	To verify the integrity in accordance with the latest ITSAR on cryptographic controls while performing a legitimate (non-tampered) software upgrade.	The DUT upgrades the software only after validating the integrity of the software image in accordance with Table 1 of the latest ITSAR on cryptographic controls.
		TC2	TC_SW_PKG_INTEGRITY_TAMPERED	To verify the integrity in accordance with the latest ITSAR on cryptographic controls while performing a illegitimate (tampered) software upgrade.	The DUT validates integrity of the software image as per Table 1 of latest ITSAR on cryptographic controls and restricts upgrade in case of an illegitimate software.
		TC 3	TC_SW_PKG_INTEGRITY_NO_SIGNATURE	To verify that a software upgrade should not happen on the DUT while using a non-signed image.	The DUT does not upgrade the software in absence of a digital signature on the software image.

		TC 4	TC_SW_PKG_INTEGRITY_UNAUTHORIZED	To verify that a software upgrade can not be performed on the DUT by an unauthorized user.	The DUT restricts software upgrade request given by an aunauthorized user.
		TC 5	TC_SW_PKG_INTEGRITY_EXPIRED	To verify the DUT rejects the software upgrade of an image with expired digital certificate.	The DUT does not upgrade the software if digital certificate of the software image is expired.
2.3.3	**Source Code Security Assurance**	TC1	TC_SDoC_Verification	To verify that the OEM has submitted SDoC in prescribed format	OEM submits SDoC in prescribed format.
		TC2	TC_Internal_Report_Verification	To verify internal test report, excluding Intellectual Property related information, but mandatorily including a summary of number of security vulnerabilities/weaknesses classified by risk.	Internal test report is submitted including the security vulnerabilities/weaknesses classified by risk.
2.3.4	**Known Malware and backdoor Check**	TC1	TC_KNOWN_MALWARE_DECLARATION_VALIDATION	To verify that OEM shall submit Self Declaration of Conformity in the enclosed proforma/format stating that the product is free from all known malware as per the malware signature database prescribed by NCCS and also it is free from backdoors.	The OEM has submitted SDOC in prescribed format
2.3.5	**No Unused Software**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain complete list of necessary software components available in the DUT along with their functions. Obtain OEM undertaking - "CHF does not contain software that is not used in the functionality of the CHF."**	**The OEM submits list of necessary software components along with their functions. The OEM submits undertaking - "CHF does not contain software that is not used in the functionality of the CHF."**
		TC1	TC_VERIFICATION_OF_INSTALLED_SOFTWARE_AND_FILES	To verify inventory of all software components (packages, libraries, binaries files etc.) available in the DUT.	The DUT lists all installed software packages, libraries, binaries files.
		TC2	TC_VERIFICATION_OF_OEM_SUPPLIED_SOFTWARE	To verify the list of necessary software components (along with functions) submitted by OEM w.r.t accuracy, completeness. To verify that the OEM undertaking is in prescribed format only	OEM submits list of necessary software components along with their functions and also submits undertaking in the prescribed format
		TC3	TC_CONSOLIDATION_OF_OEM_PROVIDED_AND_INSTALLED_SOFTWARE	To cross check that the software components actually available in DUT exactly match the list of components submitted by OEM.	Software components installed in DUT match with the list of software components submitted by OEM
		TC4	TC_VERIFICATION_OF_ORPHANED_AND_UNWANTED_PACKAGES	To verify that the DUT does not contain any orphaned packages, unnecessary files.	The DUT does not contain any orphaned package and unnecessary file.
2.3.6	**Unnecessary services removal**	TC1	TC_To_verify_OEM_Documentation	To verify that the OEM documentation provides required protocols and services for the DUT, including the complete communication matrix.	The OEM documentation clearly specifies the required protocols and services for the DUT, including a complete and accurate communication matrix.
		TC2	TC_To_verify_Unnecessary_services_are_disabled	To verify that unnecessary/vulnerable services can be disabled if needed in the DUT and verify the same after reboot.	The DUT permits restriction of unnecessary services.
		TC3	TC_To_verify_protocol_services_disabled_if_vulnerable	To verify that running services do not have any known vulnerability.	The DUT has no known vulnerabilities present in the running services.
		TC4	TC_SERVICE_SCAN_VERIFICATION	To scan available services on all interfaces after factory reset /after permanent disabling of protocol.	The scan report with all ports are documented properly for respective function and only documented, required services are found to be available on the DUT.
2.3.7	**Restricting System Boot Source**	TC1	TC_FIRMWARE_PROTECTION	To verify that DUT firmware is having protection mechanism against unauthorized access.	The DUT firmware is password protected.
		TC2	TC_INTENDED_BOOT_MODE	To verify that DUT can boot from only intended memory devices as declared by the OEM.	DUT boots from intended memory devices only as declared by the OEM.
		TC3	TC_UNINTENDED_BOOT_MODE	To verify that DUT can't boot from unintended memory devices.	DUT does not boot from unintended memory devices. DUT boots from intended memory devices only as declared by the OEM.
2.3.8	**Secure Time Synchronization**	TC1	TC_TIME_SYNC_PROTOCOLS_OEM_DECLARATION	To verify that all the protocols (for time synchronization) available in DUT are as per the OEM declaration.	All the protocols (for time synchronization) available in DUT are as per the OEM declaration.
		TC2	TC_Secure Time Synchronization For_ITSAR_Table1_Comparison	To verify that DUT and NTP server communication is secured as prescribed in Table-1 of latest ITSAR on Cryptographic Controls.	DUT uses secure protocols for NTP server communication as prescribed in Table-1 of latest ITSAR on Cryptographic Controls.
		TC3	TC_Audit Log Verification	To verify that audit logs are generated by the DUT for all changes to time settings.	DUT logs all the events related to time settings.
		TC4	TC_PTP_IMPLEMENTATION	To verify a secure PTP implementation in the DUT.	PTP is successfully configured in DUT with security requirements as per RFC 7384
		TC5	TC_MANUALLY_CHANGE_TIME	To manually change the time settings in DUT by a privileged user and retain these time settings after reboot and power off.	Privileged user can successfully change the time settings in DUT manually. These settings are retained after a power off.
		TC6	TC_NTP_CLIENT_CONFIGURATION	To configure DUT as an NTP client by a privileged user to synchronize time with NTP server, if it does not have time retention by itself.	If the device does not retain the time settings on its own, privileged user is able to configure DUT as an NTP client.
		TC7	TC_AUTH_BTW_DUT_AND_NTP	To configure and verify authentication between DUT and NTP/PTP server so that the tester is able to configure authentication attributes of DUT for accessing external NTP server.	The tester is able to configure authentication attributes of DUT for accessing external NTP server.
2.3.9	**Restricted Reachability of Services**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of essential services required for the operation of the DUT, as declared by the OEM.**	**OEM submits the list of essential services required for the operation of the DUT.**
		TC1	TC_SERVICE_BINDING_TO_SPECIFIC_INTERFACES	To verify that running services are binded to their respective interfaces.	DUT services are not reachable from any interface other than the one to which they are bound.
		TC2	TC_REACHABILITY_TO_LEGITIMATE_PEERS_ONLY	To verify that only legitimate peers are able to connect to the DUT	DUT is not reachable from illegitimate peers.
		TC3	TC_ADM_SERVICES_RESTRICTION	To verify that administrative services (e.g. SSH, HTTPS, RDP, ZTP, NETCONF, SNMP etc.) are restricted to interfaces in the management plane only and are reachable only through authorized/configured management interfaces only.	Administrative services (e.g. SSH, HTTPS, RDP etc.) are restricted to interfaces in the management plane only
2.3.10	**Self Testing**	TC1	CRYPTO_MODULE_SELF_TESTING	To perform self test to identify failures in security mechanism during boot (power on or reboot).	The DUT performs self-test to verify failure in security mechanism (during booting of cryptographic modules, software, firmware etc.)
		TC2	CRYPTO_MODULE_CONDITIONAL_TESTING	To verify that the DUT performs a conditional self-test whenever a cryptographic algorithm is initiated.	The DUT performs a conditional self-test each time a cryptographic algorithm is initiated.
		TC3	TC_SEC_MECH_FAIL	To perform self-tests to identify failures in its security mechanism when administrator instructs.	DUT shall verify the failures in its security mechanism when administrator instructs the DUT.
		TC4	TC_CRYPTO_MODULE_INTEGRITY_CHECK_FAILS	To verify that the integrity of the cryptographic module is checked before invoking any cryptographic operation.	The DUT invokes cryptographic operation only after verification of integrity of the cryptographic module and does not downgrade the module for insecure operation.

		TC5	TC_CRYPTO_MODULE_FAILURE_INDICATOR	To verify that if the cryptographic module integrity verification fails, the cryptographic module enters an error state and an error indicator is displayed.	If the cryptographic module integrity checking mechanism fails, the module enters an error state and the same is verified through alarms and logs.
2.4.1	**No Unused Functions**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain OEM declaration for the list of software and hardware functions available in the DUT along with their functionality.**	**The OEM submits list of software and hardware components available in DUT, along with their functionality.**
		TC1	TC_VERIFICATION_OF_INSTALLED_SOFTWARE_AND_ACTIVE_SERVICES	To verify the list of installed hardware, softwares and active services in the DUT.	The DUT lists installed hardware, softwares and active services.
		TC2	TC_VERIFICATION_OF_OEM_DECLARED_FUNCTIONS_LIST	To verify that the OEM declaration accurately documents all functions required for operation and excludes unused or optional components.	OEM submits documentation which includes a complete, accurate, and minimal list of required software functions for DUT, along with confirmation of no unused functions.
		TC3	TC_IDENTIFICATION_OF_DUT_FUNCTIONS_AND_VALIDATION_AGAINST_ REQUIREMENT	To verify that the hardware and software functions available within the DUT, exactly match the list of necessary functions declared by the OEM	The hardware and software functions available within the DUT, exactly match the list of necessary functions declared by the OEM
		TC4	TC__VERIFICATION_OF_SOFTWARE_FUNC	To verify that unused software functions in the DUT can be deleted, uninstalled or permanently deactivated individually.	Unused software functions in the DUT can be deleted, uninstalled or permanently deactivated individually.
		TC5	TC_VERIFICATION_OF_HARDWARE_FUNC	To verify that unused hardware functions (interfaces) in the DUT can be permanently disabled individually.	Unused hardware functions (interfaces) in the DUT can be permanently disabled individually.
2.4.2	**No Unsupported Components**	TC1	TC_No_Unsupported_components	To verify that all hardware and software components running in the DUT are still supported and have not reached end-of-life or end-of-support.	The DUT does not contain any EoL/EoS hardware and software components.
		TC2	TC_OEM_UNDERTAKING	To verify that OEM has submitted the undertaking in the prescribed format.	OEM has submitted the undertaking in the prescribed format as recommended on 15/09/2025.
2.4.3	**Avoidance of Unspecified mode of Access**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain undertaking from OEM "The CHF does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel." .**	**The OEM submits the required undertaking.**
		TC1	TC_COVERT_CHANNEL_OEM_UNDERTAKING	To verify that OEM has submitted the undertaking in prescribed format.	OEM submits undertaking in prescribed format.
2.5.1	**Audit trail storage and protection**	TC1	TC_AUDIT_LOG_ACCESS_CONTROL_CLI	To verify the local access control operations (read, write and delete) on security event log files for both privileged, non privileged users and administrator.	Only authorized users with appropriate privileges have local access to the security event log files.
		TC2	TC_AUDIT_LOG_ACCESS_CONTROL_SSH	To verify the remote access control operations (read, write and delete) on security event log files for both privileged, non-privileged users and administrator.	Only authorized users with appropriate privileges have remote access to the security event log files.
2.5.2	**Audit Event Generation**	TC1	TC_INCORRECT_LOGIN_ATTEMPTS	To verify that the DUT records any user incorrect login attempts to the DUT.	The DUT successfully records incorrect login attempts by the user. The logs contain username, source IP address, outcome of event and timestamp.
		TC2	TC_ADMINISTRATOR_ACCESS	To verify that the DUT records any access attempt to accounts that have system privileges.	The DUT successfully records user details for any access attempts to accounts that have system privileges. The logs contain username, source IP address, outcome of event, length of session and timestamp.
		TC3	TC_ACCOUNT_ADMINISTRATION	To verify that the DUT records all account administration activity, i.e. Configure, delete, enable, and disable.	The DUT successfully records all account administration activity, i.e. Configure, delete, enable, and disable. The logs contain Administrator username, Administered account, Activity performed, (configure, delete, enable and disable), Outcome of event (Success or failure), Timestamp.
		TC4	TC_RESOURCE_USAGE	To verify that the DUT records events that have been triggered when system parameter value such as disk space and CPU load over a longer period have exceeded their defined thresholds.	The DUT successfully records events that have been triggered when system parameter value such as disk space and CPU is being loaded over a long period and has exceeded its defined thresholds. The logs on the DUT mention the value exceeded, value reached (threshold value), outcome of event and timestamp.
		TC5	TC_CONFIGURATION_CHANGE	To verify that the DUT records all the changes to configuration.	The DUT successfully records all the changes to configuration of the DUT. The logs contain the event and username of the account that initiated changes to configuration in DUT. The logs mention the changes made on the DUT, timestamp, outcome of event and username.
		TC6	TC_REBOOT/SHUTDOWN/CRASH	To verify that the DUT records any actions performed on the DUT that forces a reboot or shutdown or crash of the DUT.	The DUT successfully records any action that forces a reboot or shutdown or an unintentional crash of the DUT. The logs mention the action performed,Username, Outcome of the event and timestamp.
		TC7	TC_INTERFACE_STATUS_CHANGE	To verify that the DUT records all changes in the status of interfaces of the DUT.	The DUT successfully records all changes in the status of interfaces of the DUT. The logs contain interface name and type, interface status, outcome of event and timestamp.
		TC8	TC_CHANGE_OF_GROUP_MEMBERSHIP_OR_ACCOUNTS	To verify that the DUT records any change of group membership for accounts.	The DUT successfully records any change of group membership for accounts. The logs mention administrator username, administered account, activity performed (group added or removed), outcome of event and timestamp.
		TC9	TC_RESETTING_PASSWORDS	To verify that the DUT records resetting of user account passwords by the administrator.	The DUT successfully records resetting of user account passwords by the administrator. The logs do mention administrator username, administered account, activity performed (configure, delete, enable and disable), outcome of event and timestamp.
		TC10	TC_SERVICES	To verify that the DUT records starting and stopping of services on the DUT.	The DUT successfully records starting and stopping of services on the DUT. The logs do mention service identity, activity performed (start, stop, etc.), timestamp and outcome of event.
		TC11	TC_X.509_CERTIFICATE_VALIDATION	To verify that the DUT records unsuccessful attempt to validate a certificate.	The DUT successfully records unsuccessful attempt to validate a certificate. The logs must mention Timestamp, Reason for failure, Subject identity, Type of event.
		TC12	TC_SECURE_UPDATE	To verify that the DUT records attempt to initiate manual update, initiation of update and completion of update.	The DUT successfully records: a. Attempt to initiate manual update b. Initiation of update c. Completion of update The logs mention user identity, timestamp, outcome of event and activity performed.
		TC13	TC_TIME_CHANGE	To verify that the DUT records changes in time settings.	The DUT successfully records changes in time settings of the DUT. The logs mention old value of time, new value of time, timestamp, origin of attempt to change time (IP address), subject identity, outcome of event and user identity.
		TC14	TC_SESSION_UNLOCKING/TERMINATION	To verify that the DUT records any attempt at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session.	The DUT successfully records: a. Any attempts at unlocking of an interactive session, b. Termination of a remote session by the session locking mechanism c. Termination of an interactive session. The logs mention user identity, timestamp, outcome of event, subject Identity, activity performed and type of event.

		TC15	TC_TRUSTED_COMMUNICATION_PATHS_WITH_IT_ENTITIES_AND_FOR_AUTHORIZED_REMOTE_ADMINISTRATORS	To verify that the DUT records Initiation, Termination and Failure of trusted Communication paths.	The DUT successfully records Initiation, Termination and Failure of trusted Communication paths. The logs mention Timestamp, Initiator identity (as applicable) Target identity (as applicable),User identity (in case of Remote administrator access), Type of event, Outcome of event (Success or failure, as applicable)
		TC16	TC_AUDIT_DATA_CHANGES	To verify that the DUT records changes to audit data including deletion of audit data.	The DUT successfully records changes to audit data including deletion of audit data. The logs must include timestamp, type of event (audit data deletion/audit data modification), outcome of event, subject identity, user identity, origin of attempt to change time (IP address) and details of data deleted or modified.
		TC17	TC_USER_LOGIN_AND_LOGOFF	To verify that the DUT records all use of identification and authentication mechanisms during login(s).	The DUT successfully records all use of identification and authentication mechanisms during login(s). The logs must mention the user identity, origin of attempt (IP address), timestamp and outcome of event.
		TC18	TC_ACL_RULE	To verify that the DUT records any failure of packet to match an ACL or a rule allowing traversal of the router.	The DUT successfully records any failure of packet to match an ACL or a rule allowing traversal of the router.
2.5.3	**Secure Log Export**	TC1	TC_LOG_EXPORT_PROTOCOLS_OEM_DECLARATION	To verify that all the protocols available in the DUT to export the logs are as per the OEM declaration.	The protocols available in the DUT to export the logs match OEM declaration.
		TC2	TC_FORWARDING_SECURITY_EVENT	To verify that the DUT forwards security event logging from DUT to external (syslog) server.	The DUT forwards security event logging from DUT to external (syslog) server.
		TC3	LOCAL_STORAGE	To verify that the DUT stores audit logs locally and has sufficient storage to retain at least two days of audit data.	The DUT ensures that attempt to generate log files without any external log server and check that log files are properly generated and audit data of last two days is stored locally in the DUT
		TC4	SECURE_LOG_TRANS_TO_CENTR_STORAGE	To verify that the DUT securely exports security event logs to a centralized or external system using rsyslog, SFTP or any other protocol used by DUT, using approved cryptographic controls/protocols as per Table1 of the latest ITSAR on cryptographic controls	The DUT successfully transmits security logs to the centralized server using approved cryptographic controls/protocols as per Table 1 of latest ITSAR on cryptographic controls.
		TC5	TC_LOG_BUFFER_BEYOND_THRESHOLD	To overflow the log buffer of the DUT beyond default threshold size limit.	The DUT overwrites either newer or older logs when log buffer size is full. If the log file is emptied and new logs are written it is a fail case.
		TC6	TC_DUT_ALERTS_ADMIN_IN_CASE_LOG_BUFFER_EXCEEDS	To verify that the DUT sends alerts to the administrator when the log buffer reaches the default threshold.	The DUT sends an alert to the administrator when the log buffer reaches the default threshold.
2.5.4	**Logging access to personal data**	TC1	TC_LOGGING_ACCESS_TO_PERSONAL_DATA	To verify that the DUT generates and identifies user whenever personal data is accessed . The log must contain who accessed what data. Log must not reveal personal data in clear text.	The DUT successfully logs access to personal data. The logs contain information about user and what data was accessed. Personal data is not revealed in clear text.
		TC2	TC_SECURING_SUBSCRIBER_PRIVACY	To verify that the personal data stored in the log files do not allow direct identification of a subscriber and there is no privacy violation.	The personal data stored in the log files do not allow direct identification of a subscriber and there is no privacy violation.
2.6.1	**Cryptographic Based Secure Communication**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of connected entities with DUT and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication with each entity and any other details required.**	**The OEM submits information as per pre-requisite.**
		TC1	TC_SECURE_COMM_PROTOCOLS_OEM_DECLARATION	To verify that all protocols available in the DUT which are used to communicate with external connected entities are as per the OEM declaration.	All the protocols available in the DUT which are used to communicate with external connected entities are as per the OEM declaration.
		TC2	TC_API_ACCESS_OVER_TLS	To verify that the CHF establishes secure cryptographic communication with other NFs over the SBI interface using only approved TLS protocols and cipher suites.	The DUT establishes communication strictly using TLS 1.2/1.3 with approved cipher suites.
		TC3	TC_REJECT_API_ACCESS_WITHOUT_TLS	To verify that the CHF supports only those ciphers which are as per Table 1 of latest ITSAR on cryptographic controls and does not support weak TLS versions.	The DUT rejects weak TLS versions, and deny any API access attempted without TLS. DUT supports only those ciphers which are as per Table 1 of latest ITSAR on cryptographic controls
		TC4	TC_ALLOW_SSH_WITH_STRONG_CIPHERS	To verify that the CHF accepts SSH connections on the OAM interface only approved ciphers as per Table 1 of latest ITSAR on cryptographic controls	The DUT allows SSH connection using SSHv2 with strong, approved cipher suites as per Table-1 of latest ITSAR on cryptographic controls
		TC5	TC_REJECT_SSH_WITH_WEAK_CIPHERS	To verify that attempts to connect with weak or null SSH ciphers are rejected by the CHF (non-compliant ciphers are blocked).	The DUT rejects SSH connections that attempt to use weak or non-approved cipher suites.
		TC6	TC_VERIFY_MONGODB_TLS_CONNECTION	To verify that the CHF communicates securely with its connected MongoDB internal database using only approved cryptographic controls, as per Table 1 of latest ITSAR on cryptographic controls	The DUT ensures that the MongoDB connection within the DUT uses TLS to ensure data in transit is encrypted and secure.
		TC7	TC_OTHER_SECURE_COMM_PROTOCOLS	To verify that all other protocols available in the DUT which are use to communicate with connected entities strictly use secure cryptographic controls prescribed in Table 1 of the latest ITSAR for Cryptographic Controls.	DUT ensures that all other protocols available in the DUT which are use to communicate with connected entities strictly use secure cryptographic controls prescribed in Table 1 of the latest ITSAR for Cryptographic Controls.
2.6.2	**Cryptographic Module Security Assurance**	TC1	TC_CRYPTOGRAPHIC_MODULE_SECURITY_ASSURANCE	To verify that OEM has submitted self certified test reports regarding cryptographic module embedded inside the CHF (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.	The OEM submits self certified test report regarding cryptographic module as required.
		TC2	TC_OEM_DECLARATION	To verify that the OEM has submitted the undertaking in the prescribed format stating that Cryptographic module embedded inside the DUT (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.	The OEM provides the undertaking in the prescribed format.
2.6.3	**Cryptographic Algorithms implementation Security Assurance**	TC1	TC_CRYPTOGRAPHIC_ALGORITHMS_IMPLEMENTATION_SECURITY_ASSURANCE	To verify that OEM has submitted self certified test reports regarding cryptographic algorithm implemented inside the Crypto module of the CHF shall be in compliance with the respective latest FIPS standards (for the specific cryptographic algorithm).	The OEM has submitted self certified test reports regarding cryptographic algorithms.
		TC2	TC_OEM_DECLARATION	To verify that OEM undertaking and self-certified test reports declaring that all cryptographic algorithms implemented within the DUT cryptographic module comply with the respective latest FIPS standards.	The OEM submits undertaking in the prescribed format
		TC1	TC_MAINTENANCE_MODE_VERIFICATION	To verify that the DUT provides a configurable maintenance mode option to authorized privileged users only.	The DUT provides a configurable maintenance mode option to authorized privileged users only.

2.6.4	**Protecting data and information – Confidential System Internal Data**	TC2	TC_CONFIDENTIAL_SYSTEM_INTERNAL_DATA	To verify that the DUT does not reveal confidential system internal data (such as error logs, trace files etc.) in cleartext through any function or interface during normal or debug operation when the system is not under maintenance (normal operational mode). To verify error logs, trace files and alarms/monitor for reveal of any confidential system internal data.	The DUT does not reveal confidential system internal data in clear text through any function or interface during normal or debug operation.
		TC3	TC_CONFIG_BACKUP_EXPORT	To verify the configuration backup-package export for any reveal of confidential system internal data.	The configuration backup package export does not reveal any confidential system internal data.
2.6.5	**Protecting data and information in storage**	TC1	TC_SENSITIVE_DATA_ACCESS_PROTECTION	To verify that read access to sensitive data stored in the DUT is restricted to authorized users only.	The DUT restricts read access to sensitive data and allows access only to authorized users.
		TC2	TC_CLEAR_TEXT_AUTHENTICATION_DATA_PROTECTION	To verify that identification and authentication data requiring readable access for operations is not stored in clear text and is protected using encryption or scrambling.	The DUT does not store identification and authentication data in clear text and protects it using encryption or scrambling mechanisms.
		TC3	TC_STORED_FILE_INTEGRITY_PROTECTION	To verify that stored files and sensitive system files of the CHF are protected against unauthorized modification using approved cryptographic integrity and non-repudiation controls.	The DUT protects stored files and sensitive system files against manipulation using approved cryptographic integrity and non-repudiation controls.
		TC4	TC_SENSITIVE_DATA_HASHING	To verify that sensitive data not requiring clear-text access is hashed using approved cryptographic controls.	The DUT hashes sensitive data using cryptographic controls prescribed in the latest ITSAR for Cryptographic Controls and does not store the data in clear text.
2.6.6	**Protection against Copy of Data**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of system functions, software components and services available in DUT for copying the data in transit or in use.**	**OEM provides the list of system functions, software components and services available in DUT for copying the data in transit or in use.**
		TC1	TC_DATA_COPY_PROTECTION_MECHANISMS	To verify that data copying functions for data in use or transit is permitted to an authenticated and authorized users only.	The DUT allows data copying functions to authenticated and authorized user only.
		TC2	TC_LOGGING_AND_AUDITING_OF_UNAUTHORIZED_ACCESS	To verify that use of system functions for copying the data in use or in transit is logged.	The DUT logs use of system functions for copying the data in use or in transit
		TC3	TC_UNAUTHORIZED_DATA_COPY_PREVENTION	To verify all other protective measures that exist in DUT against use of available system functions / software residing in the CHF to create a copy of data for illegal transmission.	Protective measures are available in DUT which prevent copy of data for illegal transmission.
2.6.7	**Protection against data exfiltration - Overt channel**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of overt channels such as FTP, HTTP, HTTPS IM, P2P, Email etc. available in the DUT.**	**OEM submits list of overt channels that can be configured and initiated in DUT.**
		TC1	TC_Prevention_of_data_exfiltration_attack.	To verify that CHF shall have mechanism to prevent data exfiltration attacks for theft of data in use and data in transit.	The DUT prevents data exfiltration over overt channels.
		TC2	TC_Forbid_auto-initiation_of_outbound_overt_channels.	To verify that establishment of outbound overt channels are to be forbidden if they are auto-initiated by/auto-originated from the CHF.	The DUT prevents auto-origination of outbound overt channel connections.
		TC3	TC_Session_logs_generation_of_any_session	To verify that session logs shall be generated for establishment of any session initiated by either user or the DUT.	The DUT generates session logs for every session initiated by user or the DUT.
		TC4	TC_AUTH_USER_DATA_TRANSFER	To verify that an authorized user is able to perform outbound data export (file transfer) using overt channel (SFTP, SCP etc).	An authorized user is able to perform outbound data export (file transfer) using overt channel (SFTP, SCP etc).
		TC5	TC_UNAUTH_USER_DATA_TRANSFER	To verify that an unauthorized user cannot perform outbound data transfer using overt channel (SFTP, SCP or any other).	An unauthorized user cannot perform outbound data transfer using overt channel (SFTP, SCP or any other).
2.6.8	**Protection against data exfiltration - Covert channel**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of services such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. available in the DUT.**	**OEM provides the list of tunneling services that can be configured and initiated in DUT**
		TC1	TC_Prevention_of_data_exfiltration_attack	To verify that CHF has mechanism to prevent data exfiltration attacks for theft of data in use and data in transit.	The DUT prevents data exfiltration over covert channels.
		TC2	TC_Forbid_auto-initiation_of_outbound_covert_channels	To verify that establishment of outbound covert channels and tunnels are forbidden if they are auto-initiated by/auto-originated from the CHF.	The DUT prevents auto-origination of outbound covert channel connections.
		TC3	TC_Session_logs_generation_of_any_session	To verify that session logs shall be generated for establishment of any session initiated.	The DUT generates session logs for every session initiated.
2.6.9	**System robustness against Unexpected Input**	TC1	JSON input length validation	To verify that the CHF responds as expected to a request with valid JSON payload and safely handles JSON payload with excessive length received from an NF consumer.	The DUT safely handles oversized JSON input without crash or abnormal behavior, returning a valid error response.
		TC2	JSON data type and structure validation	To verify CHFs response to JSON fields with incorrect data types and incorrect JSON payload structure	The DUT rejects malformed or incorrectly typed JSON payloads with appropriate error responses.
		TC3	JSON specification compliance validation	To verify that the CHF validates received input data against requests with missing mandatory information elements.	The DUT rejects JSON requests missing mandatory fields.
		TC4	HTTP method error handling	To verify that the CHF correctly handles protocol-level errors like invalid methods being used.	The DUT rejects unsupported HTTP methods with appropriate error codes.
		TC5	JSON nesting depth handling	To verify that the CHF safely handles complex input structures with excessive nesting.	The DUT safely handles deeply nested JSON payloads, without crash or service disruption.
		TC6	JSON input value whitelisting	To verify that the CHF properly validates and handles input values containing characters outside the allowed value margins.	The DUT rejects JSON payloads containing special characters and escape sequences through input value validation.
		TC7	HTTP/2 protocol robustness fuzz testing	To verify the CHF's behaviour and resilience when subjected to malformed or fuzzed HTTP/2 traffic on its exposed application port.	The DUT securely and correctly handles malformed or fuzzed HTTP/2 inputs while maintaining service availability and stability during fuzz testing.
		TC8	TLS handshake robustness fuzz testing	To evaluate the CHF's robustness against malformed or fuzzed TLS handshake packets at the transport layer.	The DUT securely and correctly handle malformed TLS handshake inputs at the transport layer without impacting service stability or availability.
		TC9	TC_OTHER_PROTOCOLS_INTERFACES_COMM_CHANNELS	To verify that the DUT securely validates, rejects, and handles malformed, invalid, unexpected, oversized, or fuzzed inputs across all supported protocols, interfaces, APIs, message formats, and communication channels without causing crashes, resource exhaustion, service disruption, security bypass, or abnormal behavior.	The DUT securely validates and processes all unexpected, malformed, invalid, oversized, deeply nested, protocol-violating, or fuzzed inputs by rejecting them with appropriate error responses while maintaining service availability, stability, integrity, and security.
2.6.10	**Security of backup data**	TC1	TC_Mechanism_for_secure_backup_of_sensitive_data	To verify that DUT has mechanism to backup the sensitive data, configurations and log files.	The DUT supports mechanism to store backup of sensitive data, configurations, and log files.
		TC2	TC_BACKUP_AND_RESTORATION_VERIFICATION	To verify that an effective backup and restoration strategy is in place in the DUT and documented.	An effective backup and restoration strategy is in place in the DUT and documented.
2.6.11	**Secure deletion of**	TC1	TC_SECURE_DELETION_OF_SENSITIVE_DATA	To verify that the DUT supports secure deletion of sensitive data by authorized users.	The DUT allows only authorized users to perform secure deletion of sensitive data.

2.6.11	sensitive data	TC2	TC_SENSITIVE_DATA_RECOVERY_VERIFICATION	To verify that sensitive data deleted from the DUT cannot be recovered through forensic means.	Sensitive data securely deleted from the DUT cannot be recovered through any forensic means.
2.7.1	Traffic Filtering – Network Level Requirement	TC1	TC_PACKET_FILTERING_LOGGING	To verify that the DUT supports logging of dropped packets and records filtering actions for troubleshooting purposes.	The DUT generates logs for dropped packets and records filtering actions as configured for troubleshooting and audit purposes.
		TC2	TC_PACKET_FILTERING_IP_PORT_BASED	To verify that the DUT can filter packets based on source IP address, destination IP address, port number, and protocol header values.	The DUT successfully filters traffic based on configured source IP addresses, destination IP addresses, port numbers, and protocol header values.
		TC3	TC_PACKET_FILTERING_RESET_ACCOUNTING	To verify that the DUT provides a mechanism to reset accounting counters associated with filtering rules without affecting active filtering rules.	The DUT successfully resets accounting counters without impacting active filtering rules or traffic filtering operations.
		TC4	TC_PACKET_FILTERING_ENABLE_DISABLE	To verify that the DUT provides a mechanism to individually enable or disable configured filtering rules.	The DUT allows individual filtering rules to be enabled or disabled without affecting other configured filtering rules.
		TC5	TC_PACKET_FILTERING_ACCEPT_NETWORK_LAYER	To verify that the DUT can filter packets at Network Layer, perform permit (accept) actions based on configured filtering rules, and maintain accounting counters for accepted traffic.	The DUT successfully filters packets at the Network Layer according to configured permit rules and accurately maintains accounting counters for accepted traffic.
		TC6	TC_PACKET_FILTERING_DENY_NETWORK_LAYER	To verify that the DUT can filter packets at Network Layer, perform deny (drop) actions based on configured filtering rules, and maintain accounting counters for dropped traffic.	The DUT successfully filters packets at the Network Layer according to configured deny rules and accurately maintains accounting counters for dropped traffic.
		TC7	TC_PACKET_FILTERING_ACCEPT_TRANSPORT_LAYER	To verify that the DUT can filter packets at Transport Layer, perform permit (accept) actions based on configured filtering rules, and maintain accounting counters for accepted traffic.	The DUT successfully filters packets at the Transport Layer according to configured permit rules and accurately maintains accounting counters for accepted traffic.
		TC8	TC_PACKET_FILTERING_DENY_TRANSPORT_LAYER	To verify that the DUT can filter packets at Transport Layer, perform deny (drop) actions based on configured filtering rules, and maintain accounting counters for dropped traffic.	The DUT successfully filters packets at the Transport Layer according to configured deny rules and accurately maintains accounting counters for dropped traffic.
2.7.2	Traffic Separation	TC1	TC_OAM_to_DUT_via_OAM_Interface	To verify that DUT allows only Management plane traffic via OAM interface.	The DUT allows only Management plane traffic via OAM interface.
		TC2	TC_OAM_to_DUT_via_SBI_Interface	To verify that DUT deny Management traffic via control plane interface.	The DUT rejects Management traffic via control plane interface.
		TC3	TC_AMF_to_DUT_via_SBI_Interface	To verify that DUT allows only control plane traffic via control plane interface.	The DUT allows only control plane traffic via control plane interface.
		TC4	TC_AMF_to_DUT_via_OAM_Interface	To verify that DUT denies control plane traffic via OAM interface	The DUT rejects control plane traffic over OAM interface.
		TC5	TC_PHYSICAL_SEPARATION	To Verify that control plane and O&M traffic are separated physically (out of band management).	The control plane and O&M networks are physically separated and independently configurable on distinct hardware ports.
		TC6	TC_LOGICAL_SEPARATION	To Verify that control plane and O&M traffic are separated logically (in band management) in a single physical interface.	The control plane and O&M networks are cleanly separated via distinct logical configurations (such as VLANs) on the same hardware port.
2.7.3	Traffic Protection – Anti-Spoofing	TC1	TC_SOURCE_ADDRESS_REACHABILITY_VERIFICATION	To verify that the DUT validates whether the source IP address of an incoming packet is reachable through the incoming interface.	The DUT successfully validates the reachability of the source IP address through the incoming interface before processing the packet.
		TC2	TC_ANTI_SPOOFING_PACKET_REJECTION	To verify that the DUT rejects or discards packets received on an interface when the source IP address is not reachable through that interface.	The DUT discards spoofed packets with unreachable source addresses and does not process such packets.
2.8.1	Network Level and Application Level DDoS	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of available protection mechanisms against DDoS attacks.**	**OEM provides the list of available protection mechanisms against DDoS attacks.**
		TC1	TC_OEM, Vendor, etc., document Verification.	To verify the list of available protection mechanisms in the DUT against DDoS attacks through OEM documentation	The DUT has protection mechanism against DDoS attacks which is verifiable through the OEM documentation.
		TC2	TC_Syn Flood.	To verify that DUT has network level DDoS attack prevention mechanism.	The DUT possesses network level DDoS attack prevention mechanism.
		TC3	TC_Http2 High Request Rate Flood	To verify application level DDoS attack prevention mechanism.	The DUT possesses application level DDoS attack prevention mechanism.
		TC4	TC_Http2 Large Payload Flood	To verify that DUT properly handles requests that may lead to memory exhaustion or DDoS conditions, by rejecting them or degrading gracefully without crashing or restarting.	The DUT has a protection mechanism against memory exhaustion, DDoS condition. The DUT does not become impaired or unresponsive.
2.8.2	Excessive Overload Protection	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of available protection mechanisms against Excessive overload.**	**OEM provides the list of available protection mechanisms against Excessive overload.**
		TC1	TC_OEM, Vendor, etc., document Verification.	To verify OEM documentation regarding the system protection on overload situation.	The OEM documentation and it lists the system protection procedures in overload situation.
		TC2	TC_Excessive Overload Scenario	To verify that the DUT does not fall into an insecure state in excessive overload situation as per OEM documentation.	The DUT acts predictably under excessive overload situation as per OEM documentation.
		TC3	TC_Large Data to API Endpoints	To verify that DUT handles large payloads without memory exhaustion, maintaining a stable and secure state without crashes or undefined behavior.	The DUT behaves predictably when under excessive overload situation created by memory overload.
2.8.3	Interface Robustness Requirements	TC1	TC_VERIFY_ROBUSTNESS_AGAINST_SYN_FLOOD_ATTACK	To verify that DUT performance does not degrade under SYN FLOOD attack(by an excessive CPU and memory usage).	The performance of DUT does not degrade under SYN FLOOD attack
		TC2	TC_VERIFY_ROBUSTNESS_AGAINST_LAND_ATTACK	To verify that DUT performance does not degrade under LAND attack(by an excessive CPU and memory usage).	The performance of DUT does not degrade under LAND attack.
		TC3	TC_VERIFY_ROBUSTNESS_AGAINST_SMURF_ATTACK	To verify that DUT performance does not degrade under SMURF attack(by an excessive CPU and memory usage).	The performance of DUT does not degrade under SMURF attack.
		TC4	TC_VERIFY_ROBUSTNESS_AGAINST_TEARDROP_ATTACK	To verify that DUT performance does not degrade under TEARDROP attack(by an excessive CPU and memory usage).	The performance of DUT does not degrade under TEARDROP attack.
		TC5	TC_VERIFY_ROBUSTNESS_AGAINST_PING_OF_DEATH_ATTACK	To verify that DUT performance does not degrade under PING-OF-DEATH attack(by an excessive CPU and memory usage).	The performance of DUT does not degrade under PING-OF-DEATH attack.
		TC6	TC_VERIFY_ROBUSTNESS_AGAINST_UNCORRELATED_REPLY_PACKET_ATTACK	To verify that DUT performance does not degrade when uncorrelated reply packets are sent.	The performance of DUT does not degrade when uncorrelated reply packets are sent.

2.8.4	**GTP-C Filtering (when 5GC is interworking with EPC)**	TC1	TC_GTPC_SENDER_AUTHORIZATION_VERIFICATION	To verify that the DUT validates whether the sender of a GTP-C message is authorized to send messages pertaining to the GTP-C protocol.	The DUT verifies the authorization of the sender before processing GTP-C messages and permits only authorized senders to send messages pertaining to the GTP-C protocol.
		TC2	TC_GTPC_FILTERING_ACTIONS_VERIFICATION	To verify that the DUT supports Accept, Discard and Account actions for GTP-C messages based on configured filtering rules.	The DUT supports Accept, Discard, and Account actions for GTP-C messages and accurately accounts for messages processed under the configured filtering rules.
		TC3	TC_GTPC_FILTERING_CAPABILITY_DECLARATION	To verify that the OEM documentation specifies whether the DUT supports GTP-C filtering capability or requires a separate entity to provide the capability.	The OEM documentation clearly states whether the DUT supports GTP-C filtering capability. If the capability is not supported, the documentation identifies the separate entity responsible for providing the capability.
2.9.1	**Fuzzing Network and Application Level**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of all the protocols supported by DUT at network and application level.**	**OEM provides a document containing list of all protocols supported by DUT at network and application level.**
		TC1	TC_PROTOCOLS_UNDER_OEM_DECLARATION	To verify that all protocols available in the DUT at network and application level, which are subjected to fuzzing, are as per the OEM declaration.	All the protocols available in the DUT at network and application level, which are subjected to fuzzing, are as per the OEM declaration.
		TC2	TCP_Protocol_Fuzzing	To fuzz TCP-IPv4 protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The TCP IPv4 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC3	IPv4_Protocol_Fuzzing	To fuzz IPv4 protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The IPv4 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC4	IPv6_Protocol_Fuzzing	To fuzz TCP-IPv6 protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The TCP-IPv6 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same can be verified from the DUT logs.
		TC5	ARP_Protocol_Fuzzing	To fuzz ARP Client protocol using mutation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The ARP Client protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC6	SSH_Protocol_Fuzzing	To fuzz SSHv2 Server protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The SSHv2 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC7	SNMP_Protocol_Fuzzing	To fuzz SNMPv3 protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The SNMPv3 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC8	IPSec_Protocol_Fuzzing	To fuzz IPSec protocol using mutation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The IPSec protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC9	Diameter_Protocol_Fuzzing	To fuzz Diameter protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The Diameter protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC10	HTTP2_Protocol_Fuzzing	To fuzz HTTP2 protocol using mutation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The HTTP2 protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC11	TLS_Handshake_Fuzzing	To fuzz TLS protocol using mutation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The TLS protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC12	GTP_Protocol_Fuzzing	To fuzz GTP protocol using generation based fuzzing and verify the DUT logs for stable operation during fuzzing.	The GTP protocol is PASSED by the fuzzing tool and DUT behaves in a stable state. The same is verified from the DUT logs.
		TC13	TC_OTHER_PROTOCOLS_FUZZING	To fuzz all other protocols (at network and application level) available in the DUT which are externally reachable and verify the DUT logs for stable operation during fuzzing.	DUT behaves in a stable manner when all protocols (at network and application level) which are externally reachable are subjected to fuzzing.
2.9.2	**Port Scanning**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of all services and ports required for the functioning of the DUT.**	**OEM submits the list of ports and services associated with these ports.**
		TC1	TC_VERIFICATION_OF_NETWORK_SERVICES	To verify the available network services on the documented ports which are necessary for the operation of the DUT.	Only the documented network services on the specified ports are available and responding.
		TC2	TC_VERIFICATION_OF_PORT_SCANNING_TCP	To perform a TCP port scan on all the interfaces of the DUT and verify with the list of documented ports.	The list of open ports identified by the TCP match the list of the documented ports that are necessary for the operation of the DUT.
		TC3	TC_VERIFICATION_OF_PORT_SCANNING_UDP	To perform a UDP port scan on all the interfaces of the DUT and verify with the list of documented ports.	The list of open ports identified by the UDP match the list of the documented ports that are necessary for the operation of the DUT.
		TC4	TC_VERIFICATION_OF_PORT_SCANNING_SCTP	To perform a SCTP port scan on all the interfaces of the DUT and verify with the list of documented ports.	The list of open ports identified by the SCTP match the list of the documented ports that are necessary for the operation of the DUT.
2.9.3	**Vulnerability scanning**	TC1	TC_Vulnerability scanning using tool	To conduct a credential-based vulnerability scan using Vulnerability assessment/scanning tool against all IP interfaces of the DUT.	The report of credential-based vulnerability scan using Vulnerability assessment/scanning tool does not contain any known vulnerabilities. The identified vulnerabilities have a remediation plans in place to mitigate them.
2.10.1	**Growing content handling**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a documentation on dynamic content sources like e.g. log files and their paths, and measures that are taken to protect system functions from growing or dynamic content that may exhaust file system capacity usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.**	**OEM submits a documentation on dynamic content sources like e.g. log files and their paths, and measures that are taken to protect system functions from growing or dynamic content that may exhaust file system capacity usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.**
		TC1	TC_GROWING_CONTENT_HANDLING	To verify that the DUT logs an event with appropriate message parameters when a file system reaches its maximum capacity and supports configuration and enforcement of dynamic or growing content limits (quotas) by exceeding log file size or file upload limits as specified in the OEM documentation.	The DUT generates an event log with appropriate message parameters when the file system reaches its maximum capacity and supports configuration of dynamic or growing content limits (quotas) and enforces the configured quota by preventing log file growth or file uploads beyond the defined limits in accordance with the OEM documentation.
		TC2	TC_DYNAMIC_CONTENT_FILESYSTEM_MONITORING_VERIFICATION	To verify that whether the DUT support any separate file system for growing or dynamic contents (other than the main file system) (as per OEM documentation).	DUT supports separate file system for growing or dynamic contents.
		TC3	TC_DYNAMIC_CONTENT_FILESYSTEM_MONITORING_VERIFICATION	To verify that whether DUT support any file system monitoring (eg, alerts, alarms etc.) for growing or dynamic contents. (as per OEM documentation).	DUT supports any file system monitoring (eg, alerts, alarms etc.) for growing or dynamic contents and it is verified.
		TC4	TC_QUOTA_AND_FILESYSTEM_MONITORING_STABILITY_VERIFICATION	To verify that any events of quota exceeding, file system monitoring are logged and the DUT's performance is stable during such incidents (by verification of CPU/Memory usages)	The DUT performance shall be stable during any event of dynamic/growing contents exceeding a threshold and such events shall be logged.
		PRE_REQ	**PRE-REQUISITE**	**Obtain the documentation on necessary ICMP types required for the DUT to function.**	**OEM submits the documentation on necessary ICMP types required for the DUT to function.**

2.10.2	**Handling of ICMP**	TC1	TC_ICMPV4_UNSUPPORTED_TYPE_SUPPORT_VERIFICATION	To verify that the DUT does not support the sending of the ICMPv4 types which are not mentioned in the permitted/optional list in ITSAR (As per OEM documentation).	The DUT does not support sending of any ICMPv4 Type other than permitted/optional in ITSAR or not specified in the OEM documentation.
		TC2	TC_ICMPV6_UNSUPPORTED_TYPE_SUPPORT_VERIFICATION	To verify that the DUT does not support the sending of the ICMPv6 types which are not mentioned in the permitted/optional list in ITSAR (As per OEM documentation).	The DUT does not support sending of any ICMPv6 Type other than permitted/optional in ITSAR or not specified in the OEM documentation.
		TC3	TC_ICMPV4_UNSUPPORTED_TYPE_PROCESSING_VERIFICATION	To verify that the DUT does not send, respond to or process ICMPv4 types which are not mentioned in the permitted/optional list in ITSAR (ICMP Type 5, 13, 14).	The DUT does not support sending, responding to or processing of any ICMPv4 Type other than permitted/optional in ITSAR or not specified in the OEM documentation.
		TC4	TC_ICMPV6_UNSUPPORTED_TYPE_PROCESSING_VERIFICATION	To verify that the DUT does not send, respond to or process ICMPv6 types which are not mentioned in the permitted/optional list in ITSAR (ICMP Type 137).	The DUT does not support sending, responding to or processing of any ICMPv6 Type other than permitted/optional in ITSAR or not specified in the OEM documentation.
2.10.3	**Authenticated Privilege Escalation only**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the following lists from OEM: list A (operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured) and list B (operating system commands, GUI functions, and files which will execute specifically limited tasks automatically with higher privileges, even when used by a low-privileged user).**	**OEM submits list A (operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured) and list B (operating system commands, GUI functions, and files which will execute specifically limited tasks automatically with higher privileges, even when used by a low-privileged user).**
		TC1	TC_PRIVILEGE_ESCALATION_AUTHENTICATION_VERIFICATION	To verify that the DUT requires authentication when a low-privileged user attempts to perform a privilege escalation.	DUT does not allow unauthenticated privilege escalation.
		TC2	TC_LIST_B_FUNCTIONS_PERMISSION_VERIFICATION	To ensure that all list "B" functions (SUID, SGID, and Linux capability-enabled files) present on the network product match the OEM-provided list, follow secure permission configurations, and do not allow privilege escalation.	All files in List B provides only the specific, limited functions justified by OEM documentation.
2.10.4	**System Account Identification**	TC1	TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION	To check that existing account UIDs are assigned uniquely in the DUT system.	The DUT ensures that all existing account UIDs are assigned uniquely.
		TC2	TC_NEW_USER_ACCOUNT_IDENTIFICATION	To create new user account on the DUT and to verify the user account identifier.	The DUT is able to create a new user account with a unique identifier.
		TC3	TC_DUPLICATE_USER_ACCOUNT_IDENTIFICATION	To create a duplicate user account on the DUT.	The DUT does not permit the creation of a duplicate user account or is able to overwrite the existing credentials when such an attempt is made.
		TC4	TC_VERIFY_NON_REPUDIATION_CONTROLS	To verify that users cannot deny actions they performed (non-repudiation controls).	Audit logs accurately record actions performed by the user against their unique UID. Logs contain sufficient information for accountability (UID, action, date/time, result).
2.10.5	**OS Hardening - Minimized Kernel Network Functions**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain documentation on OS hardening undertaken to sufficiently harden the OS and limit kernel based applications/functions only for the operation of the DUT, from the OEM.**	**OEM submits documentation on OS hardening undertaken to sufficiently harden the OS and limit kernel based applications/functions only for the operation of the DUT.**
		TC1	TC_KERNEL_BASED_APPLICATION	To verify that only the KERNEL based applications or functions required for the operation are available in the DUT.	The DUT ensures that only the kernel-based applications and functions required for its operation are present.
		TC2	TC_IP_PACKET_FORWARDING_DISABLING	To verify that IP packet forwarding between interfaces is disabled by default on the DUT (after a factory reset).	The DUT restricts IP packet forwarding between interfaces by default.
		TC3	TC_PROXY_ARP_DISABLING	To verify that the Proxy ARP feature is disabled by default on the DUT (after a factory reset).	The DUT restricts the Proxy ARP feature by default.
		TC4	TC_DIRECTED_BROAD_DISABLING	To verify that the Directed broadcast is disabled by default on the DUT (after a factory reset).	The DUT restricts directed broadcast by default.
		TC5	TC_ IP_MULTICAST_HANDLING	To verify that the DUT discards all multicast IPv4 packets (IP ranges 224.0.0.0 through 239.255.255.255) and multicast route caching and forwarding are also disabled by default (after a factory reset).	The DUT discards all multicast IPv4 packets and multicast route caching and forwarding are also disabled by default.
		TC6	TC_GRATUITOUS_ARP_DISABLING	To verify that the Gratuitous ARP feature is disabled by default on the DUT (after a factory reset).	The DUT restricts Gratuitous ARP feature by default.
		TC7	TC_BROADCAST_ICMP_HANDLING	To verify that responses to ICMP broadcast packets are disabled by default on the DUT (after a factory reset).	The DUT restricts responses to ICMP broadcast and multicast packets by default.
2.10.6	**No Automatic Launch of Removable Media for CHF NF**	TC1	NO_AUTOMATIC_LAUNCH_OF_REMOVABLE_MEDIA	To verify that the DUT does not automount and launch an application automatically when a removable media device is connected.	the DUT does not automount and launch an application automatically when a removable media device is connected.
		TC2	TC_AUTOMATIC_LAUNCH_OF_REMOVABLE_MEDIA_DEACTIVATION	To verify activation/deactivation of automatic launch of compatible scripts/applications from USB drive or removable media.	The DUT deactivates automatic launch of compatible applications/scripts in USB or removable media.
2.10.7	**Protection from Buffer Overflows**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a document from OEM which includes a detailed technical description of the system's buffer overflow protection mechanisms and ways to verify the same.**	**OEM submits a document which includes a detailed technical description of the system's buffer overflow protection mechanisms and ways to verify the same.**
		TC1	TC_DOC_REVIEW_PROTECTION_FROM_BUFFER_OVERFLOW	To verify that the buffer overflow mechanisms are mentioned in the OEM documentation.	The buffer overflow mechanisms is clearly mentioned in OEM documentation.
		TC2	TC_PROTECTION_FROM_BUFFER_OVERFLOW	To verify that the DUT implements robust buffer overflow protection mechanisms as per OEM documentation	The DUT implements robust buffer overflow protection mechanism as per OEM documentation and the same is verified by testing.
	External file	TC1	TC_OS-level_restrictions_to_mount_external_file_systems	To verify that OS-level mount policies and restrictions (such as nosuid or noexec flags) are properly configured for removable media	The DUT ensures that OS-level mount policies and restrictions (such as nosuid or noexec flags) are properly configured for removable media
		TC2	TC_OS-level_restrictions_for_Normal_user	To verify that OS-level restrictions are possible for a normal user against the mount/use of removable media for data transfer.	The DUT OS have the facility to prevent the normal user against the mount/use of removable media for data transfer.

2.10.8	**system mount restriction**	TC3	TC_Privilege_escalation_non_support_for_normal_users	To verify that the DUT prevents privilege escalation attempts using an external filesystem prepared with writable SUID/GUID files.	The DUT prevents privilege escalation attempts using externally prepared filesystems containing writable SUID/GUID files and blocks any such unauthorized access attempts.
		TC4	TC_Privilege_escalation_attempt_from_external_filesystem	To verify that execution of privilege escalation payloads from a mounted filesystem is blocked."	The DUT blocks execution of privilege escalation payload from a mounted file system
2.10.9	**File-System Authorization Privileges**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a document from OEM, describing how access control is configured for the filesystems in the DUT.**	**OEM submits a document describing how access control is configured for the filesystems in the DUT.**
		TC1	TC_FILESYSTEM_AUTHORIZATION_PRIVILEGES	To verify that users are only permitted to modify files, data, directories or file systems for which they have been authorized according to the vendor documentation.	The DUT ensures that OS-level access permissions are set correctly for all users. Users are only able to modify files, data, directories, or file systems for which they have the necessary privileges.
		TC2	TC_AUTHORISED_USER_Modify	To verify that an authorised user with necessary privileges can modify at least one file and directory.	The DUT allows the Authorized users to modify the file or directory.
		TC3	TC_UNAUTHORISED_USER_Modify	To verify that an unauthorised user with insufficient privileges cannot modify file and directory.	The DUT does not allow Unauthorized users to modify the file or directory.
2.10.10	**SYN Flood attacks Prevention for CHF NF**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a documentation from OEM, describing the SYN flood attack prevention mechanism or setting and where to check for them.**	**OEM submits a documentation, describing the SYN flood attack prevention mechanism or setting and where to check for them.**
		TC1	TC_SYN_FLOOD_PREVENTION	To verify that DUT supports SYN Flood Prevention mechanism by default (after a factory reset) as described in vendor's documentation).	SYN flood mechanism or technique is enabled by default in the DUT and the DUT does not become inoperative when subjected to a SYN FLOOD attack.
2.10.11	**Handling of IP options and extensions**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a documentation from OEM, listing the IP Header Options (IPv4) and IP Header Extensions (IPv6) which are required for DUT operation, with justification (exception list).**	**OEM submits a documentation, listing the IP Header Options (IPv4) and IP Header Extensions (IPv6) which are required for DUT operation, with justification (exception list).**
		TC1	TC_IPV4_OPTIONS_ACL_Drop	To configure the filtering rule (ACL) on DUT to drop any packets with IPv4 options enabled and apply the rule to the appropriate interface of the DUT, as per the OEM documentation.	The DUT drops the IPv4 packet with any IPv4 Options extension header and no response is being sent by the DUT.
		TC2	TC_IPV6_EXTENSION_HEADERS_ACL_Drop	To configure the filtering rule (ACL) on DUT to drop any packets with IPv6 extension headers enabled and apply the rule to the appropriate interface of the DUT, as per the OEM documentation.	The DUT drops the IPv6 packet with any IPv6 extension header and no response is being sent by the DUT.
		TC3	TC_IP_OPTIONS_IPV6_EXTENSION_HEADERS_ACL_Allow_Exception	To configure and apply ACL for handling exceptional requirement of allowing IP options and extension headers as per OEM documentation.	The tester is able to configure the filtering rule (ACL) on the DUT to allow any IPv4/v6 packets with IP options and extension headers and apply the rule to the appropriate interface of the DUT. The IPv4/v6 packets with IP options and extension headers is received by the DUT and the corresponding response is being sent by the DUT.
2.10.12	**Restrictions on running Scripts / Batch-processes**	TC1	TC_RESTRICTIONS_ON_RUNNING_SCRIPTS_OR_BATCH-PROCESSES	To verify that scheduled tasks like backups, disk monitoring, and maintenance can only be executed by privileged users.	The DUT ensures that backup, disk space monitoring, system maintenance, and script/batch-process/macro executions is permitted only for privileged users. Normal users are denied access to these operations.
		TC2	TC_RESTRICTIONS_ON_RUNNING_SCRIPTS_OR_BATCH-PROCESSES_AUTHORISED_USER	To verify that the running script batch processes or macros are restricted to authorised users only.	The DUT ensures that only authorized users can execute scripts, batch processes, or macros. Normal users are unable to execute scripts, batch processes, or macros.
		TC3	TC_RESTRICTIONS_ON_SCHEDULED_TASKS_CRON_JOB_USAGE	To verify that the system permits only privileged users to configure, schedule, or execute automated tasks (such as cron-jobs).	The DUT ensures that administratively configured scheduled tasks (cron jobs) shall be permitted only for privileged users. Normal users are unable to schedule, modify, or execute cron jobs.
2.10.13	**Restrictions on Soft-Restart**	TC1	TC_CHF_RESTRICTIONS_ON_SOFT_RESTART	To verify that the CHF system shall restrict software-based system restart options usage among various users.	The DUT ensures that attempts to run system restart commands by normal users is denied and attempts by a normal user to run the reboot command is failed.
		TC2	TC_CHF_RESTRICTION_ON_KEY_COMBINATIONS	To restrict software restarts initiated via key combinations, specifically CTRL+ALT+DEL, for users operating within the CHF .	The DUT does not allow restart via key combination (CTRL+ALT+DEL).
2.11.1	**HTTPS**	TC1	TC _HTTPS	To verify that the communication between the web server and the client is secure using authorised TLS1.2 or above. To verify that downgrade option to lower versions and NULL ciphers shall not be allowed.	The DUT supports configuration of HTTPS using TLS1.2 or above. Attempt to configure using TLSv1.0, TLSv1.1 and NULL cipher is unsuccessful.
		TC2	TC_IPSEC IKEv2	To verify that encrypted tunnels are established and IKEv2 negotiation is successfully completed.	The DUT successfully establishes a secure tunnel by completing the IKEv2 four-way handshake and negotiates authorized cryptographic suites as per cryptographic controls prescribed in Table 1 of latest ITSAR on cryptographic controls
2.11.2	**Web Server Logging**	TC1	TC_VERIFICATION_OF_WEBSERVER_SUCCESSFUL_LOGIN	To Verify that the Web Server logs successful access attempts.	The DUT logs all successful login attempts with Access timestamp, Source IP address, Account (if known), attempted login name (if associated account does not exist), Relevant fields in http request(the URL should be included whenever possible) and Status code of web server response.
		TC2	TC_VERIFICATION_OF_WEBSERVER_FAILED_LOGIN_WRONG_CREDENTIAL	To Verify that the Web Server logs the failed access attempts.	The DUT logs all failed login attempts with Access timestamp, Source (IPaddress), Account (if known), Attempted login name (if the associated account does not exist), Relevant fields in http request(the URL should be included whenever possible) and Status code of web server response.
	HTTP Input	TC1	TC_USERNAME_Injection	To verify that the Username field is free from command injection and cross-site scripts	The DUT ensures that the username field is not vulnerable to command injection and cross site scripting.
		TC2	TC_PASSWORD_Injection	To verify that the Password field is free from command injection and cross-site scripts	The DUT ensures that the password field is not vulnerable to command injection and cross site scripting.

2.11.3	**HTTP Input Validation**	TC3	TC_Manual_Testing_for_XSS_SQL_Injection	To verify manually that all input fields (like tick box, buttons, check box) supported by the DUT are free from command injection and cross site scripts.	The DUT ensures that all supported input fields (e.g., text boxes, buttons, check boxes, and tick boxes) are protected against command injection and cross-site scripting (XSS) vulnerabilities during manual testing.
		TC4	TC_Automated_testing_for_XSS_SQL_Injection_using_tool	To verify that DUT web server prevents executing XSS and command injection attack using an appropriate tool (preferably using an automated crawler).	The DUT ensures that all supported input fields (e.g., text boxes, buttons, check boxes, and tick boxes) are protected against command injection and cross-site scripting (XSS) vulnerabilities during automated testing.
		TC5	TC_Filter_escape_validate_encode_with_all_input_fields	To verify that DUT web server is able to filter, escape, encode and validate all user controllable input fields.	The DUT web server is able to filter, escape, encode and validate all user controllable input fields.
2.11.4	**No System Privileges**	TC1	TC_NO_SYSTEM_PRIVILEGES_WEB_SERVER	To verify the current user account and privilege level under which the web server process is running.	The DUT web server is running under a non-system (non-root) user account with least privileges.
		TC2	TC_SYSTEM_PRIVILEGES_Not_Running_with_Root_user	To verify that the web server process is not running with root or system-level privileges.	The DUT web server is running under a non-system (non-root) user account with least privileges.
		TC3	TC_SYSTEM_PRIVILEGES_DROP_TO_NO_SYSTEM_PRIVILEGES_SERVER	To verify that if the web server process starts with system privileges, it is transferred to a non privileged user account for execution after startup.	The DUT web server process transfers execution to a non privileged user account if the web server process starts with system privileges.
2.11.5	**No Unused HTTPS Methods**	TC1	TC_NO_UNUSED_HTTP_METHODS	To identify the HTTP methods currently allowed by the web server on the DUT.	The DUT allows only GET, HEAD and POST methods.
		TC2	TC_NO_TRACK_TRACE_Method	To verify that the DUT webserver shall not run the methods TRACK or TRACE.	The DUT webserver does not allow TRACK or TRACE method.
2.11.6	**No Unused Add-Ons**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list from OEM of add-ons or scripting tools for Web server components needed for system operation.**	**OEM submits a list of add-ons or scripting tools for Web server components needed for system operation.**
		TC1	TC_NO_UNUSED_ADD-ONS	To verify that CGI or other scripting components, Server Side Includes (SSI), and WebDAV are deactivated if they are not required.	The DUT permits deactivation of CGI or other scripting components, Server Side Includes (SSI), and WebDAV, if not required.
		TC2	TC_NO_OTHER_COMPONENTS	To verify that no other component is installed on the web server, using an automated tools.	The DUT verifies that no other component is available in the web server using an automated tool.
2.11.7	**No Compiler, Interpreter, or Shell via CGI or other Server Side Scripting**	TC1	TC_NO_COMPILER_FOR_CGI	To verify that all directories used for CGI or other scripting components shall not contain compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).	The web server in the DUT does not contain compilers or interpreters, or CGI or other scripting directories.
2.11.8	**No CGI or other Scripting for Uploads**	TC1	TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS	To verify that the directories with write permission to Webserver, do not contain any executable scripts, CGI programs, or other executable code	The directories with write permission do not contain any executable scripts, CGI programs or other executable code
		TC2	TC_DIR_CONFIGURED	To verify that the directories configured for CGI/Scripting do not have write permissions for the web server.	The CGI/ Scripting directories does not not have write permissions for the web server.
2.11.9	**No Execution of System Commands with SSI**	TC1	TC_NO_Execution_of_System_Commands_with_SSI	To verify that whether execution of system commands is disabled in the web server configuration.	The DUT does not execute any system commands.
		TC2	TC_NO_Execution_of_System_Commands_with_SSI	To verify execution of system commands by using the exec directive in SSI file with and without system commands	The DUT does not execute any system commands by using exec directive through SSI.
2.11.10	**Access Rights for Web Server Configuration**	TC1	TC_ACCESS_RIGHTS_WEB_SERVER_FILES	To verify that only the owner of the web server process and users with system privileges have "read" and "write" access rights for all web server configuration files and configuration directories.	The DUT ensures that only owner of the web server process and users with system privileges have "read" and "write" access rights for all web server configuration files and directories.
		TC2	DEFAULT_PERMISSION_OF_NEW_FILES.	To verify that only the owner of the web server process and users with system privileges have "read" and "write" access rights for all newly created web server configuration files and configuration directories.	The DUT ensures that only owner of the web server process and users with system privileges have "read" and "write" access rights for all newly created web server configuration files and directories.
2.11.11	**No Default Content**	TC1	TC_NO_DEFAULT_CONTENT	To verify that if any default content (such as example files, help files, documentation, or aliases) is available with the webserver.	The DUT does not have any default content(such as example files, help files, documentation, or aliases) in the web server.
2.11.12	**No Directory Listings**	TC1	TC_DIRECTORY_LISTING_DISABLED	To verify Directory Listing/Browsing is disabled in configuration	The DUT ensures that directory browsing is disabled.
		TC2	TC_NO_DIRECTORY_LISTING	To verify that Directory listing / Directory browsing is not allowed on all endpoints (domains, subdomains and directories) offered by the web server	The DUT does not allow directory browsing through web server.
2.11.13	**Web Server Information in HTTPS Headers**	TC1	TC_NO_WEB_SERVER_HEADER_INFORMATION	To verify that the response headers sent by HTTP requests do not disclose the web server version and the modules/add-ons used(eg., server name, version etc).	The DUT Web server ensures that HTTP response headers do not contain any server identification details(server name,version etc).
2.11.14	**Web Server information in Error Pages**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain a documentation on user-defined error pages (e.g. location, content, where configured) and messages and a list of potential parameters/commands to trigger events resulting in an http status code 3xx, 4xx, 5xx.**	**OEM provides a documentation on user-defined error pages (e.g. location, content, where configured) and messages and a list of potential parameters/commands to trigger events resulting in an http status code 3xx, 4xx, 5xx.**
		TC1	TC_DEFAULT_ERROR_PAGE_REPLACED	To verify that default error pages are replaced by user defined error pages.	The DUT replaced default error pages by the user defined error pages.
		TC2	TC_NO_USER_DEFINED_ERROR_PAGES_INFORMATION	To verify that user-defined error pages does not include version information about the web server and the modules/addons used.	The DUT ensures that the error pages should not display internal information such as the server version, server name, or error codes.
		TC3	TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION	To verify that error messages/pages (as per the OEM documentation) does not include any internal information such as internal server names, error codes, modules, add-ons used, etc.	The DUT Web server ensures that the custom error page is displayed, and no internal information is present in the error message.
2.11.15	**Minimized File Type Mappings**	TC1	TC_VERIFY_FILE_TYPES_SUPPORTED	To verify which file types /script handlers are supported and confirm only required ones are configured.	The DUT ensures that only the file types and script handlers required for its operation are enabled.
		TC2	TC_NO_WEB_SERVER_FILE_TYPE MAPPINGS	To verify that disallowed script/file types (php, phtml, sh, exe, etc.) are not handled or executed by the DUT's web server.	The DUT does not allow file types/ script handlers which are not required

2.11.16	**Restricted File Access**	TC1	TC_RESTRICTED_FILE_ACCESS_DEFAULT	To verify that the newly created directories/files present in the DUT web server document directory are owned by the user that runs the web server and are not writable to others.	The DUT Web server ensures that the newly created directories/files present in the web server document directory are owned by the user that runs the web server and are not writable to others.
		TC2	TC_RESTRICTED_FILE_ACCESS_EXISTING	To verify that the existing directories/files present in the DUT web server document directory are owned by the user that runs the web server and are not writable to others.	The DUT Web server ensures that the existing directories/files present in the web server document directory are owned by the user that runs the web server and are not writable to others.
		TC3	TC_VERIFY_USER_RUNNING_WEB_SERVER	To verify that the user running the web server is an unprivileged account.	The DUT ensures that the user running the web server is an unprivileged account.
		TC4	TC_CHROOT_ENVIRONMENT	To verify that the web server runs inside a jail or chrooted environment for Operating Systems that have chrooted environments. If the chrooted environment is not used, the web server or system functionality can be used to restrict access to file directories.	The DUT ensures that the Files outside the web server directory cannot be accessed.
2.11.17	**HTTP User Sessions**	TC1	TC_SESSION_ID_UNIQUENESS	To verify that the session IDs are uniquely identified for different users as well as different sessions.	The DUT Web server ensures that session IDs of all users and sessions are unique.
		TC2	TC_SESSION_ID_UNPREDICTABILITY	To verify that the session IDs are not predictable.	The DUT Web server ensures that entropy of these length of Session ID is higher and unpredictable
		TC3	TC_SESSION_ID_NO_SENSITIVE_INFORMATION	To verify that session ID shall not contain sensitive information in clear text (e.g. Account number, social security, etc.)	The DUT Web server ensures that session IDs in the DUT does not contain sensitive information in clear text.
		TC4	TC_SESSION_MAX_LIFETIME_TIMEOUT	To verify that the web server shall have session idle timeout period beyond which the web server shall terminate the idle sessions, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for maximum lifetime of a session shall be 8 hours and it shall be configurable.	The DUT Web server ensures that the session is terminated and the session ID is deleted after idle timeout period. The default maximum lifetime session time is 8 hours and duration is configurable.
		TC5	TC_SESSION_ID_REGENERATION	To verify that session ID shall be regenerated for each new session (e.g., each time a user logs in).	The DUT Web server ensures that each new session generate new session ID each time when a user logs in the web server.
		TC6	TC_SESSION_ID_NO_REUSE	To verify that web server should not allow reuse or renewal of session ID in subsequent sessions.	The DUT Web server restricts reuse or renewal of session ID in subsequent sessions.
		TC7	TC_SESSION_COOKIE_NO_PERSISTENCE	To verify that the CHF uses only session cookies and does not use persistent cookies i. e.; the max-age and expiry attributes shall not be set in the cookies.	The DUT Web server ensures that the session cookies are not stored permanently. The max age and expiry attributes are not set in the cookies.
		TC8	TC_SESSION_COOKIE_HTTPONLY_ATTRIBUTE	To verify that the session cookie attribute 'HttpOnly' is set to true.	The DUT Web server ensures that the' HttpOnly' is set to true.
		TC9	TC_SESSION_COOKIE_PATH_RESTRICTION	To verify that the session cookie attribute 'path' shall be set.	The DUT Web server ensures that the 'path' of a session cookie is set and is valid.
		TC10	TC_SESSION_COOKIE_DOMAIN_RESTRICTION	To verify that the session cookie attribute 'domain' shall be set.	The DUT Web server ensures that the 'domain' of a session cookie is set and is valid.
		TC11	TC_SESSION_ID_NOT_ACCEPTED_FROM_GET_POST	Verify that network product shall not accept session identifiers from GET/POST variables.	The DUT Web server does not accept session identifiers from GET/POST variables.
		TC12	TC_SERVER_GENERATED_SESSION_ID_ONLY	To verify that the DUT shall be configured to only accept server generated session IDs.	The DUT web server does not accept session IDs from client and accept server generated session IDs.
2.12.1	**No Code Execution or Inclusion of External Resources by JSON parsers**	TC1	TC_JSON_CODE_EXECUTION_ATTEMPT	To verify that JSON parser does not execute code-like strings in JSON.	The DUT rejects JSON payloads containing executable code and does not execute any code.
		TC2	TC_JSON_LOCAL_FILE_INCLUSION_ATTEMPT	To verify that JSON parser does not include/read local files in the DUT.	The DUT rejects JSON payloads referencing local files and does not access the files in the DUT
		TC3	TC_JSON_REMOTE_URI_INCLUSION_ATTEMPT	To verify that JSON parser does not fetch external resources via URI.	The DUT rejects JSON payloads containing external URIs and does not fetch external resources.
		TC4	TC_JSON_MALFORMED_AND_OVERSIZED_INPUT_HANDLING	To verify safe handling of malformed and oversized JSON payloads.	The DUT rejects malformed and oversized JSON payloads with appropriate errors and behaves in a predictable, stable manner.
2.12.2	**Validation of the unique key values in Information Elements (IEs)**	TC1	TC_DUPLICATE_KEY_VALIDATION	To verify that DUT rejects JSON messages containing duplicate key names within an Information Element (IE).	The DUT accepts valid JSON requests and reject requests containing duplicate keys with an error.
2.12.3	**Validation of the IEs limits**	TC1	TC_IE_SHALL_NOT_EXCEED_16000	To verify that the DUT enforces the maximum limit of 16,000 leaf Information Elements (IEs) in a JSON request.	The DUT rejects requests where the number of leaf IEs exceeds 16,000 and accepts only valid requests within the limit.
		TC2	TC_JSON_PAYLOAD_HTTPS_REQUEST_EXCEEDS_16MB	To verify that the DUT enforces the maximum JSON payload size limit of 16 MB.	The DUT rejects JSON payloads exceeding 16 MB and accepts payload within the allowed size.
		TC3	TC_NESTING_DEPTH_OF_LEAVES_NOT_EXCEED_32	To verify that the DUT enforces the maximum JSON nesting depth limit of 32 levels.	The DUT rejects JSON payloads with nesting depth greater than 32 and accepts payload within the allowed depth.
2.12.4	**Protection at the Transport Layer**	TC1	TC_TRANSPORT_PROTECTION_PROTOCOLS_OEM_DECLARATION	To verify and document all service interface protocols, API endpoints, and associated transport ports available on the DUT as officially declared by the OEM.	The OEM provides a comprehensive, documented inventory of all active service interface protocols running in the DUT. The list must explicitly identifies the transport and security protocols used by each interface.
		TC2	TC_TLS_1_2_OR_HIGHER_ENFORCEMENT	To verify that the DUT supports only TLS version 1.2 or above for NF-to-NF communications and rejects connections attempting to use unsupported or legacy TLS versions.	The DUT successfully establishes a secure connection using TLS 1.2 or above only when both client and server certificates are mutually validated. Connection attempts using legacy TLS versions or missing certificates are strictly rejected.
		TC3	TC_MUTUAL_TLS_AUTHENTICATION_USING_CLIENT_AND_SERVER_CERTIFICATES	To verify that the DUT enforces mutual authentication between NF consumer and NF producer by validating both server-side and client-side certificates during connection establishment.	The DUT successfully establishes a secure connection only when both the server and client present valid certificates. Mutual authentication is completed successfully before communication is permitted.
		TC4	TC_MISSING_CLIENT_OR_SERVER_CERTIFICATE_REJECTION	To verify that the DUT rejects NF-to-NF connection attempts when either the client certificate or server certificate is absent during the TLS handshake.	The DUT rejects the connection when the client certificate, server certificate, or both are missing. No communication session is established without successful mutual certificate validation.

		TC5	TC_INVALID_OR_UNTRUSTED_CERTIFICATE_REJECTION	To verify that the DUT rejects NF-to-NF connection attempts when expired, revoked, malformed, or untrusted certificates are presented during authentication.	The DUT rejects the connection and prevents communication when invalid, expired, revoked, malformed, or untrusted certificates are detected.
		TC6	TC_INTRA_PLMN_TRANSPORT_PROTECTION	To verify that NF-to-NF communication within the same PLMN successfully uses the deployed transport-layer protection mechanism for authentication and secure communication.	The DUT successfully authenticates and communicates with peer NFs within the same PLMN using the active transport-layer protection solution. Unauthenticated communication attempts are rejected.
2.12.5	**Authorization Token Verification Failure Handling within one PLMN**	TC1	TC_VALID_ACCESS_TOKEN_SERVICE_EXECUTION	To verify that the NF Service Producer successfully processes an NF Service Request when the access token passes all verification checks.	The DUT successfully validates the access token, executes the requested service operation, and returns the appropriate service response to the NF Service Consumer.
		TC2	TC_TOKEN_INTEGRITY_HANDLING	To verify that the DUT correctly rejects a NF Service Request when the access token signature has been tampered.	The DUT rejects the NF service request when the access token signature has been tampered, based on OAuth 2.0 error response.
		TC3	TC_OAUTH2_ERROR_RESPONSE_ON_TOKEN_VERIFICATION_FAILURE	To verify that the DUT returns the appropriate OAuth 2.0 error response when access token verification fails.	The DUT rejects the request and returns a compliant OAuth 2.0 error response indicating the reason for the authorization failure.
		TC4	TC_AUTH_INCORRECT_AUDIENCE	To verify that the DUT correctly rejects NF Service Requests when the audience (aud) claim in the access token matches neither the DUT's identity nor its NF Type.	The DUT rejects the NF service request when the aud claim in the access token does not match the DUT's specific identity and does not match its NF Type
		TC5	TC_AUTH_INCORRECT_SCOPE	To verify that the DUT correctly rejects an NF Service Request when the scope claim inside the access token does not authorize the requested DUT operation.	The DUT rejects the NF service request when the "scope" claim does not authorize the requested operation.
		TC6	TC_AUTH_EXPIRED_ACCESS_TOKEN	To verify that the DUT correctly rejects an NF Service Request when the access token has expired.	The DUT rejects the NF service request when the "exp" claim in the JWT is earlier than the current system time.
		TC7	TC_AUTH_INCORRECT_S_NSSAI_LIST	To verify that the DUT correctly rejects an NF Service Request when the access token contains a list of S-NSSAIs that the DUT does not serve.	The DUT rejects the NF service request when the token contains S-NSSAIs the DUT does not serve.
		TC8	TC_AUTH_INCORRECT_NSI_LIST	To verify that the DUT correctly rejects an NF Service Request when the access token contains an incorrect list of NSI IDs.	The DUT rejects the NF service request when the token contains NSI IDs not supported by DUT.
		TC9	TC_AUTH_INCORRECT_NF_SET_ID	To verify that the DUT correctly rejects an NF Service Request when the access token contains an incorrect NF Set ID.	The DUT rejects the NF service request when the token contains an incorrect NF Set ID.
		TC10	TC_AUTH_INCORRECT_ADDITIONAL_SCOPE	To verify that the DUT correctly rejects an NF Service Request when the access token contains incorrect additional scope information.	The DUT rejects the NF service request when the token contains additional scope that does not match the requested DUT service operation.
2.12.6	**Authorization Token Verification Failure Handling in Different PLMNs**	TC1	TC_HOME_PLMNID_MATCH_VERIFICATION	To verify that the DUT accepts an NF Service Request when the home PLMN ID contained in the audience claim of the access token matches the DUT's own PLMN identity.	The DUT successfully validates the PLMN ID claim, accepts the NF Service Request, and proceeds with normal authorization processing.
		TC2	TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_INCORRECT_PLMN_ID	To verify that the DUT rejects an NF Service Request when the home PLMN ID contained in the audience claim of the access token belongs to a different PLMN than the DUT's identity.	The DUT rejects the NF service consumer's service request when the token contains an incorrect home PLMN ID in the audience claim.
		TC3	TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_MISSING_PLMN_ID	To verify that the DUT rejects an NF Service Request when the access token does not contain the home PLMN ID within the audience claim required for inter-PLMN authorization.	The DUT rejects the NF service consumer's service request when the mandatory home PLMN ID is absent from the audience claim in the token.
2.12.7	**Protection against JSON injection attacks**	TC1	TC_Verification_of_Unsafe_Function_Usage	To confirm that the DUT software does not use unsafe functions such as "eval()" for processing JSON data.	The DUT does not use unsafe evaluation functions such as "eval()" for processing JSON data.
		TC2	TC_SANITIZE_JSON_DATA	To verify that the DUT properly sanitizes and contextually escapes data fields before serializing them into outbound JSON payloads, preventing structural server-side JSON injection.	The DUT properly serializes all outbound payloads by escaping structural JSON control characters (such as unescaped double quotes, backslashes, and commas) supplied in input fields, ensuring they are treated strictly as literal string values and do not alter the structural schema of the generated JSON.
		TC3	TC_JSON_SCRIPT_INJECTION_ATTEMPT	To verify that the DUT rejects or safely handles JSON payloads containing embedded JavaScript, script tags, or executable content intended for JSON injection attacks.	The DUT rejects or safely processes the malicious JSON payload without executing any embedded script or executable content.
2.13.1	**Remote Diagnostic Procedure – Verification**	TC1	TC_VERIFICATION_OF_REMOTE_DIAGNOSTIC_ACCESS	To verify that DUT remote login shall be permitted only for authorized users, and that unauthorized users shall not be allowed to login remotely.	The DUT allows only authorized users to log in remotely. Root and unauthorized users are not permitted to login remotely.
		TC2	TC_VERIFICATION_OF_REMOTE_DIAGNOSTIC_LOGGING	To verify that all remote diagnostic activities performed by remote users on the DUT shall be properly logged, including required parameters such as id, timestamp, interface type, event level, result (if applicable as per troubleshooting guide/alarm maintenance).	The DUT captures logs of all activities performed by remote users, including required parameters such as id, timestamp, interface type, event level, result (if applicable as per troubleshooting guide/alarm maintenance).
2.13.2	**No System Password Recovery**	TC1	TC_VERIFY_ENTIRE_CONFIG	If system password reset functionality is present, verify that the entire configuration of the DUT is irretrievably deleted in the event of system password reset.	Attempt to password reset is made and if successful, the DUT does not allow to retrieve the configuration through any means.
		TC2	TC_NO_SYSTEM_ROOT_PASSWORD_RECOVERY	To verify that no provision shall exist for system/root password recovery on the DUT.	The DUT does not provide any system/root password recovery mechanism.
2.13.3	**Secure System Software Revocation**	TC1	TC_SOFTWARE_ROLLBACK_ADMINISTRATOR_ACCESS_ONLY	To verify that software image rollback on the DUT can only be performed by users with administrator privileges.	The DUT permits software image rollback only to authorized administrator accounts.
		TC2	TC_UNAUTHORIZED_SOFTWARE_IMAGE_ROLLBACK_REJECTION	To verify that the DUT rejects software image rollback attempts initiated by unauthorized or non-administrator users.	The DUT denies the rollback request, prevents the rollback operation from being executed, and generates an appropriate security or audit log entry for the unauthorized attempt.
		TC3	TC_SOFTWARE_ROLLBACK_NON_REPUDIATION_LOGGING	To verify that all software image rollback actions performed by an administrator are protected by non-repudiation controls and are recorded in audit logs.	The DUT records each rollback event with sufficient information in tamper-resistant audit logs, ensuring accountability and non-repudiation.
2.13.4	**Software Integrity - Installation**	TC1	TC_SW_PKG_INTEGRITY_VALID	To verify that a legitimate software upgrade/install on the DUT shall ensure software integrity in accordance with Table 1 of the latest ITSAR on cryptographic controls.	The DUT performs software upgrade only after validating the integrity of the software image using cryptographic controls specified in Table 1 of the latest ITSAR document on cryptographic controls.
		TC2	TC_SW_PKG_INTEGRITY_TAMPERED	To verify that an illegitimate (tampered) software upgrade/install on the DUT fails integrity verification in accordance with Table 1 of the latest ITSAR on cryptographic controls.	The DUT fails the integrity verification check, immediately aborts the upgrade process, and ensures that the tampered software is neither executed nor installed.

2.13.5	**Software Integrity Check - Boot**	TC1	TC_SW_BOOT_INTEGRITY_Pos	To verify that the DUT successfully validates boot integrity of the legitimate software image during the boot process.	The DUT verifies the integrity of the legitimate software image during the boot process using cryptographic controls specified in Table 1 of the latest ITSAR on cryptographic controls, matches it to the expected reference value, and proceeds to complete the boot process successfully.
		TC2	TC_SW_BOOT_INTEGRITY_NEG	To verify that the DUT detects and rejects illegitimate (tampered) software images during boot integrity verification in accordance with Table 1 of the latest ITSAR on cryptographic controls	The DUT verifies the integrity of the illegitimate (tampered) image during boot and rejects the illegitimate image.
2.13.6	**Unused physical and logical interfaces disabling**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of the default used Physical/Logical Interfaces/Ports that are necessary for the operation of the IP Router.**	**OEM provides the list of the default used Physical/Logical Interfaces/Ports that are necessary for the operation of the IP Router.**
		TC1	TC_verify_physical_and_logical_interfaces	To verify the available physical and logical interfaces on the DUT.	The DUT lists all physical and logical interfaces available on the DUT.
		TC2	TC_verify_disabled_physical_and_logical_interfaces	To verify that unused interfaces on the DUT can be permanently disabled.	The DUT is able to permanently disable all unused interfaces.
		TC3	TC_UNUSED_INTERFACE_PORT_DISABLE_BY_ADMINISTRATOR	To verify that an administrator can disable unused interfaces and ports on the DUT.	The DUT allows only an administrator to disable unused interfaces and ports, and the selected interfaces/ports are successfully disabled.
		TC4	TC_UNAUTHORIZED_INTERFACE_PORT_DISABLE_REJECTION	To verify that unauthorized users cannot disable interfaces or ports on the DUT.	The DUT rejects attempts by unauthorized users to disable interfaces or ports and logs the unauthorized action attempt.
		TC5	TC_DISABLED_INTERFACE_PORT_PERSISTENCE_AFTER_REBOOT	To verify that interfaces and ports disabled by an administrator remain disabled after a system reboot.	The DUT retains the disabled state of the configured interfaces and ports after reboot, and the interfaces/ports do not become active unless explicitly re-enabled by an authorized administrator.
		TC6	TC_DISABLED_INTERFACE_PORT_INACCESSIBILITY_VERIFICATION	To verify that disabled interfaces and ports cannot be accessed or used for communication.	The DUT does not accept connections, traffic, or service requests through disabled interfaces and ports.
2.13.7	**Predefined accounts shall be deleted or disabled**	**PRE_REQ**	**PRE-REQUISITE**	**Obtain the list of all predefined accounts in the DUT.**	**OEM provides the list of all predefined accounts in the DUT.**
		TC1	TC_VERIFY_PREDEFINED_ACCOUNTS	To search for all default accounts with known or nil authentication attributes stored in DUT (like password, hash value, token, etc.) and verify with OEM document.	List of all default accounts in the DUT is as per OEM documentation.
		TC2	TC_PREDEFINED_ACCOUNT_DELETION	To verify that all predefined or default user accounts (except Admin/Root) with known or nil authentication attribute can be deleted or disabled on the DUT.	All predefined/default user accounts with known or nil authentication attribute (other than Admin/Root) are successfully deleted or disabled.
		TC3	TC_PREDEFINED_ACCOUNT_LOGIN_REJECTION	To verify that disabled predefined user accounts cannot be used to access the DUT.	Login attempts using disabled predefined accounts are rejected and access is denied.
		TC4	TC_PREDEFINED_ACCOUNT_PERSISTENCE_AFTER_REBOOT	To verify that deleted or disabled predefined user accounts remain deleted or disabled even after a system reboot.	Deleted accounts are not recreated and disabled accounts remain disabled even after reboot.
2.13.8	**Correct Handling of Client Credentials Assertion Validation Failure**	TC1	TC_VALID_CLIENT_CREDENTIALS_ASSERTION_ACCEPTANCE	To verify that the DUT accepts and processes NF service requests when the client credentials assertion contains a valid signature, valid timestamps, correct audience claim, and matching NF Instance ID.	The DUT accepts and processes NF service requests when the client credentials assertion contains a valid signature, valid timestamps, correct audience claim, and matching NF Instance ID.
		TC2	TC_AUTH_TAMPER_TOKEN	To verify that the DUT rejects NF service requests when the access token signature is altered.	The DUT rejects any request received from an NF with a tampered or invalid signature.
		TC3	TC_AUTH_INCORRECT_AUDIENCE	To verify that the DUT rejects NF service requests when the audience (“aud”) claim in the access token does not match the DUT identity.	The DUT rejects any request received from an NF with an invalid audience claim.
		TC4	TC_AUTH_EXPIRED_ACCESS_TOKEN	To verify that the DUT rejects NF service requests when the access token has expired, i.e., when the “exp” (expiration time) claim in the JWT is earlier than the current system time.	The DUT rejects any request received from an NF with an expired access token.
		TC5	TC_AUTH_NF_INSTANCE_ID_MATCH_PUBLICKEY	To verify that the DUT validates that the client NF Instance ID (nfInstanceId) contained within the client credentials assertion precisely matches the NF Instance ID embedded in the public key certificate used for signing that assertion, rejecting the request if there is a mismatch (spoofing attempt).	The DUT validates that the NF Instance ID (nfInstanceId) contained in the client credentials assertion matches the DUT instance ID. The DUT detects the mismatch, rejects the client credentials assertion, and denies the NF service request. The DUT does not accept the request when the token's identity claim fails to match the identity verified by the signing certificate.
		TC6	TC_CLIENT_CREDENTIALS_ASSERTION_INVALID_IAT_TIMESTAMP	To verify that the DUT correctly handles client credentials assertions containing an invalid issued-at (iat) timestamp, such as a timestamp significantly in the future or otherwise outside the acceptable validation window.	The DUT rejects the client credentials assertion and does not process the NF service request when timestamp validation fails.
2.13.9	**Isolation of Compromised Element**	TC1	TC_COMPROMISED_DUT_NETWORK_LEVEL_ISOLATION	To verify that the DUT can be isolated at the network level in the event of a security compromise.	The DUT can be isolated from network communications using the available network isolation mechanisms. Network traffic to and from the DUT is successfully restricted or blocked as configured.
		TC2	TC_COMPROMISED_DUT_COMPUTE_STORAGE_LEVEL_ISOLATION	To verify that the DUT can be isolated at the compute and/or storage level in the event of a security compromise.	The DUT can be isolated using the available compute and/or storage isolation mechanisms, preventing unauthorized access to compromised resources.
		TC3	TC_COMPROMISED_DUT_ISOLATION_PROCEDURE_DOCUMENTATION	To verify that documented procedures and provisions exist for isolating the DUT at the network and/or compute/storage level following a security compromise.	The OEM provides documented procedures, operational guidance, and recovery instructions describing how to isolate the DUT at the network and/or compute/storage level.
		TC4	TC_COMPROMISED_DUT_POST_ISOLATION_ACCESS_RESTRICTION	To verify that, after isolation, the DUT is prevented from continuing normal communication or access to protected resources.	The isolated DUT cannot establish unauthorized network communication or access protected compute/storage resources until isolation is removed through authorized procedures.
3.1	**Secure Communication over the GTP Prime (GTP') based Interface, Ga**	TC1	TC_GA_INTERFACE_PROTOCOL_AND_PORT_INVENTORY	To verify and document all communication protocols, application versions, and transport ports available on the DUT for the Ga interface as per OEM declaration.	All communication protocols, application versions, and transport ports exposed on the Ga interface are identified and match the OEM declaration.
		TC2	TC_GTP_PRIME_CONFIDENTIALITY_PROTECTION	To verify that GTP' communication between the DUT and CGF over the Ga interface is protected against unauthorized disclosure of transmitted information.	The DUT ensures that GTP' traffic is encrypted using NDS/IP protection mechanisms and transmitted information cannot be interpreted from captured network traffic.
		TC3	TC_GTP_PRIME_INTEGRITY_PROTECTION	To verify that GTP' communication between the DUT and CGF over the Ga interface is protected against unauthorized modification of transmitted data.	The DUT detects and rejects the tampered or modified GTP' packets. Integrity violations are not accepted by the DUT.
		TC4	TC_GTP_PRIME_REPLAY_PROTECTION	To verify that GTP' communication between the DUT and CGF over the Ga interface is protected against replay attacks.	The DUT detects and discards the replayed GTP' packets. Previously transmitted packets cannot be successfully reused to establish or manipulate communication.
		TC5	TC_NDS_IP_IPSEC_ESP_IKEV2_ENFORCEMENT	To verify that NDS/IP protection is implemented for the Ga interface using IPSec ESP and IKEv2 as specified in 3GPP TS 33.210.	The DUT uses IPSec ESP and IKEv2 to secure GTP' communication over the Ga interface in accordance with 3GPP TS 33.210.

3.2	**Secure Communication over the Diameter based interfaces, Rc and Re**	TC1	TC_RC_RE_INTERFACE_PROTOCOL_INVENTORY	To verify that the protocols, application versions, and transport ports available on the Rc and Re interfaces are as per the OEM declaration.	All protocols, application versions, and transport ports exposed on the Rc and Re interfaces are identified and match the OEM declaration.
		TC2	TC_DIAMETER_CONFIDENTIALITY_PROTECTION_RC_RE	To verify that Diameter communication over the Rc and Re interfaces is protected against unauthorized disclosure of information.	Diameter traffic is encrypted and transmitted information cannot be interpreted from captured network traffic.
		TC3	TC_DIAMETER_INTEGRITY_PROTECTION_RC_RE	To verify that Diameter communication over the Rc and Re interfaces is protected against unauthorized modification.	Modified or tampered Diameter messages are detected and rejected by the DUT.
		TC4	TC_DIAMETER_REPLAY_PROTECTION_RC_RE	To verify that Diameter communication over the Rc and Re interfaces is protected against replay attacks.	Replayed Diameter messages are detected and discarded by the DUT.
		TC5	TC_TLS_DTLS_1_2_OR_HIGHER_SUPPORT_RC_RE	To verify that the DUT supports TLS/DTLS version 1.2 or higher for Diameter communications over the Rc and Re interfaces.	Diameter communication can be established using TLS/DTLS 1.2 or higher. Unsupported versions are not accepted.
		TC6	TC_NDS_IP_SUPPORT_FOR_DIAMETER_INTERFACES	To verify that protection of the Diameter interfaces is supported using NDS/IP as specified in TS 33.210.	The DUT supports NDS/IP protection for Diameter communications in accordance with TS 33.210.
		TC7	TC_DTLS_TLS_PROFILE_COMPLIANCE_TS33210_TS33310	To verify that when TLS/DTLS is used, its implementation and usage follow the profiles specified in TS 33.210 and TS 33.310.	TLS/DTLS implementation and configuration comply with the requirements and profiles defined in TS 33.210 and TS 33.310.
		TC8	TC_RC_RE_CRYPTOGRAPHIC_CONTROL_COMPLIANCE	To verify that all other protocols available on the Rc and Re interfaces use secure communication channels and cryptographic controls as prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.	All additional protocols operating on the Rc and Re interfaces comply with the applicable ITSAR cryptographic requirements.
3.3.1	**Charging Data Record File Integrity**	TC1	TC_VERIFICATION_OF_CHF_DATABASE_CONFIGURATION	To verify CHF Database configuration integrity, and the internal structure of the associated database.	The DUT maintains integrity of its configuration and ensures correct initialization of the internal database structure, including the presence of all required databases and schema versions.
		TC2	TC_VERIFICATION_OF_CHF_CDR_FILE_INTEG	To verify the integrity and authenticity of Charging Data Record (CDR) files generated by the CHF, including the following: a. CDR files are written to the configured output path b. CDR files are generated only after real traffic c. CDR files are protected using SHA-256 integrity hashing d. CDR files are protected using RSA-2048 digital signatures e. Any modification of the CDR files is detected.	The CHF generates CDR files in the designated output path only upon detection of valid traffic. Each generated file is protected using approved integrity cryptographic hashing and digital signatures in accordance with Table 1 of the latest ITSAR to ensure data integrity and authenticity.
		TC3	TC_VERIFICATION_OF_CHF_DATABASE_INTEG	To verify the integrity of the CHF database using cryptographic controls specified in Table 1 of the latest ITSAR on cryptographic controls.	The DUT ensures that integrity of the CHF database is maintained using the cryptographic controls specified in Table 1 of the latest ITSAR on cryptographic controls.
3.3.2	**Charging Data Records Availability**	TC1	_TC_VERIFICATION_OF_CDR_GEN_AND_INITIAL_AVAILABILITY	To verify that CDRs are correctly generated by the DUT and are immediately available in the host persistent storage.	The DUT generates accurate Charging Data Records (CDRs) upon trigger and securely commit them to the host persistent storage immediately after generation.
		TC2	TC_VERIFICATION_OF_CDR_PERSISTENCE_ACROSS_RESTARTS_AND_FAILURES	To verify that CDR files remain available across component restarts, system reboot, and FTP delivery failures.	The DUT ensures that all generated CDR files are retained in persistent storage and remain accessible following component restart, system reboot, or FTP delivery failure.
		TC3	TC3TC_VERIFICATION_OF_CDR_DURING_FTP_FAILURE	To verify the high availability of the DUT, ensuring that charging records are stored in the database regardless of the Management Plane status and that delivery resumes automatically when the transport path is restored.	The DUT ensures reliable capture and storage of all charging records within the database persistence layer, even during unavailability of the FTP or WebUI management planes, with no loss of data.
		TC4	TC_DOCUMENTATION	To verify that OEM provides documentation describing the mechanisms implemented to ensure Charging Data Record (CDR) availability, persistence, recovery, and delivery continuity.	OEM provides documentation describing the mechanisms implemented to ensure Charging Data Record (CDR) availability, persistence, recovery, and delivery continuity.
3.3.3	**Secured backups of Charging Data Records**	TC1	TC_VERIFICATION_OF_CDR_BACKUP_GENERATION	To verify that all charging data generated by the CHF is backed up.	The DUT successfully backs up all generated charging data.
		TC2	TC_VERIFICATION_OF_CDR_BACKUP_RESTORE_AND_INTEGRITY	To verify the restoration capability of the charging data backups.	The DUT ensures that all backups related to charging data are successfully restored.
3.3.4	**CDR file Protection**	TC1	TC_VERIFICATION_OF_CDR_CRYPTOGRAPHIC_PROTECTION	To verify that CDR files are protected using Table 1 of the latest ITSAR on Cryptographic Controls.	The DUT shall ensure that all CDR files are protected using cryptographic algorithms in accordance with Table 1 of the latest ITSAR on cryptographic controls.
		TC2	TC_VERIFICATION_OF_CDR_TAMPER_DETECTION	To verify tamper protection of the CDR files in the DUT.	The DUT has tamper protection mechanism and is able to detect any tampering in CDR files.