Generic Test Cases for Binding Support Function (BSF) of a 5G Network					
Clause No.	**Clause Name**	**Test Case No.**	**Test Case Name**	**Test Case Description (for BSF NF)**	**Expected Results for Pass (for BSF NF)**
2.1.1	**Authentication for Product Management and Maintenance interfaces**	TC 1	TC_MGMT_PROTOCOLS_OEM_DECLARATION	To verify that all management and maintenance protocols available in the DUT are in accordance with the OEM declaration.	The management and maintenance protocols running on the DUT match those specified in the OEM declaration.
		TC 2	TC_MUTUAL_AUTH_BSF	To verify that the BSF supports mutual authentication through Mutual TLS (mTLS) and mutual SSH authentication. These mechanisms ensure that both the BSF and the management entity (client/tester) authenticate each other before communication, in accordance with the 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_BSF_WebUI	To verify that the BSF 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 in accordance with the latest ITSAR.	The BSF WebUI is accessible only through HTTPS/TLS using a valid server certificate. Access to the BSF 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 the management and maintenance interfaces of the DUT enforce mutual authentication using secure cryptographic controls prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.	All protocols deployed on the management and maintenance interfaces of the DUT enforce mutual authentication using secure cryptographic controls prescribed in Table 1 of the latest ITSAR on cryptographic controls.
		TC 5	TC_INSECURE_AUTH_PROTOCOL	To verify that the DUT does not support any insecure or deprecated authentication protocols.	The DUT does not support insecure or deprecated authentication protocols.
2.1.2	**Management Traffic Protection**	TC 1	TC_MGMT_TRAFFIC_PROTECTION_PROTOCOLS_OEM_DECLARATION	To verify that all protocols available on the DUT that handle management traffic to and from the DUT are as per the OEM declaration.	All protocols available on the DUT that handle management traffic to and from the DUT are as per the 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 the latest ITSAR on cryptographic controls.	The DUT ensures that all HTTPS-based management traffic is secured using cryptographic protocols and algorithms compliant with Table 1 of the 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 BSF are protected using industry-standard cryptographic algorithms and secure protocol versions. The test ensures that the BSF supports only approved SSHv2 algorithms in accordance with Table 1 of the latest 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 the DUT strictly use secure cryptographic controls prescribed in Table 1 of the 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.
2.1.3	**Role-based access control policy**	TC1	TC_ROLE_VERIFICATION	To verify that user roles are defined in the BSF according to Role-Based Access Control (RBAC). The BSF shall support at least three distinct user roles — Admin, OAM (privilege management for BSF Management and Maintenance), and User — stored in the database used by the BSF.	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 BSF 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 BSF 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_BSF_CONTAINER	To verify that the BSF 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 (Owner, Group, and Others).
		TC 4	TC_USER_CREATION_WITHOUT_ROLE	To verify that the BSF enforces Role-Based Access Control (RBAC) for new users created without an assigned role.	A new user created without specifying a role is automatically assigned the lowest-privileged role, or user creation without a role is unsuccessful.
2.1.4	**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 at least two authentication mechanisms, such as a public key and password (2FA), when accessed remotely via SSH.	All remote user accounts accessed through SSH on the DUT enforce a combination of at least two authentication mechanisms.
2.1.5	**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 BSF, 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_REMOTE_ADMINISTRATION_SOFTWAR	To verify that the remote root login restriction is effective not only 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 the DUT 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.
2.1.6	**Authorization Policy**	TC1	TC_AUTHORIZATION_LOG_FILE	To verify that only the BSF service account (O&M user) can read and write log files, while an unprivileged user (user1) cannot read, write, modify, or delete them, thereby enforcing least privilege.	The DUT enforces authorization controls on log files such that only the O&M user can perform operations such as reading and writing, while unprivileged users are restricted from accessing or modifying the files.
		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 are 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 root and are fully restricted from access by O&M users and unprivileged users.
		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., BSF) 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 the authorization level of a user who has higher privileges than the lowest-privileged role and lower privileges than the highest-privileged role, and to 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.
2.1.7	**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.	The DUT does not permit multiple users to be created with the 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.	The DUT ensures that the default system configuration does not allow group accounts or shared credentials.
		TC3	TC_ACCOUNT_NAME_UNIQUE	To verify that multiple user accounts cannot be created with the same account name.	The DUT does not permit multiple user accounts to be created with the same account name.
2.2.1	**Authentication Policy**	TC 1	TC_AUTH_PROTOCOLS_OEM_DECLARATION	To verify that all authentication protocols available in the DUT are in accordance with the OEM declaration.	The authentication protocols available in the DUT match those specified in the OEM declaration.
		TC 2	TC_SSH_ACCESS	To verify that the DUT supports SSH access with at least two-factor authentication (2FA).	The DUT supports SSH access with at least two-factor authentication (2FA).
		TC 3	TC_SFTP_ACCESS_WITH_2FA	To verify that the 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 the DUT supports access to the WebUI only after successful two-factor authentication over HTTPS.	The DUT ensures that access to the WebUI is secured through HTTPS and requires at least two authentication attributes.
		TC 5	TC_LOCAL_MANAGEMENT_CONSOLE_ACCESS	To verify that users can log in locally at the system console with at least one authentication attribute.	Authentication is successful with at least one authentication attribute.
		TC 6	TC_HTTPS_ACCESS_CONTROL_VERIFICATION	To verify that the DUT's 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.	The DUT supports at least one authentication attribute for all supported protocols.
		TC 9	TC_COMM_BTW_SYSTEMS	To verify that communications between systems (including BGP, OSPFv2/v3, RIPv2, IS-IS, TACACS+, RADIUS, RADSEC, etc.) require authentication using at least one authentication attribute when communicating with the DUT.	Authentication using at least one authentication attribute is successful.
2.2.2	**Authentication Support – External**	TC 1	TC_EXT_AUTH_PROTOCOLS_OEM_DECLARATION	To verify that all authentication and related service protocols used by the DUT for communicating with an external authentication entity are in accordance with the OEM declaration.	All authentication and related service protocols used by the DUT for communicating with an external authentication entity are in accordance with the OEM declaration.
		TC 2	TC_OTHER_EXT_AUTH_PROTOCOLS	To verify that all authentication protocols (TACACS+, RADIUS, RADSEC 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 time 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 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 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 checking them 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 an automated password-cracking tool.	The DUT enforces strong password complexity requirements and implements protection mechanisms 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 requires the CAPTCHA challenge to be completed successfully before allowing further authentication attempts.
		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 that such passwords cannot be exploited using automated password-guessing tools.	The DUT implements mechanisms 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. The DUT does not permit the absolute minimum password length to be configured below 8 characters.
		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 rejects any password that does not meet these criteria.
		TC3	TC_PASSWORD_CONFIGURE_MIN_LENGTH_SPECIAL_CHAR	To verify that the DUT enforces a configurable minimum password length and configurable sets of allowable special characters, including Unicode-based character-class requirements.	The DUT allows configuration of the minimum password length and the allowed special characters/Unicode character classes, and rejects passwords that do not comply with the configured policy.
		TC4	TC_PASSWORD_STORE	To verify that the DUT does not store passwords in plaintext and that passwords are stored using secure hashing and salting mechanisms.	The DUT does not store passwords in plaintext. Passwords are securely stored using salted and hashed cryptographic mechanisms.
		TC5	TC_WHILE_CHANGING_PWDS	To verify that the DUT/central system checks and enforces the password requirements when a user changes a password or enters a new password.	The DUT/central system checks and enforces the password requirements when a user changes a password or enters a new password.
2.2.5	**Inactivity Session Timeout**	TC1	TC_INACTIVITY_SESSION_TIMEOUT_CONFIGURE	To verify that the DUT enforces an inactivity session timeout for local and remote access for both privileged and non-privileged users, and records the relevant events in the logs.	The DUT implements an inactivity timeout for user sessions, and the user session is terminated after the configured timeout period.
		TC2	TC_INACTIVITY_SESSION_TIMEOUT_VERIFY	To verify that the DUT supports configuration of the inactivity session timeout for local and remote access for both privileged and non-privileged users.	The DUT allows configuration of the inactivity session timeout, and the session automatically terminates after the configured inactivity timeout and requires reauthentication for further access.
2.2.6	**Password Changes**	TC1	TC_PASSWORD_CHANGE	To verify that the DUT allows users to change their passwords at any time and enforces a mandatory password change upon initial login after successful authentication.	The DUT allows users to change their passwords at any time and enforces a 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, provides expiry notifications, and requires a 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 the 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 at least three previously used passwords retained.
		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 password changes until the minimum age requirement has been met.
		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 password input on the DUT is hidden while creating a user and when a user logs in, ensuring that individual characters are not displayed in plaintext during input. This shall be verified 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 not displayed in plaintext and remains hidden from view.
		TC3	TC_MGMT_PROTOCOLS	To verify protected authentication feedback during login using available management authentication protocols.	The DUT enforces protected authentication feedback during login using management protocols.
		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 to be updated upon first login.
		TC2	TC_CRYPTOGRAPHIC_DEFAULT_KEY_REMOVAL_DISABLED	To verify that the DUT removes or replaces all predefined or default cryptographic keys.	The DUT ensures that all predefined or 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, are forced to be updated by following the procedure provided in the OEM manual.	The DUT ensures that all predefined or default authentication attributes, such as default usernames, passwords, or credentials, are no longer available after completion of the procedure.
2.2.9	**Logout Function**	TC1	TC_LOGOUT_FUNCTION	To verify that the DUT allows a user to log out 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 the configured number of consecutive failed login attempts and allows login only after the defined delay.
		TC2	TC_FAILED_LOGIN_ATTEMPTS_PERMANENT_LOCK	To verify that the DUT supports permanent lockout for non-administrative accounts and only temporary lockout for administrative accounts after the configured number of 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 the default maximum of 8 consecutive 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 applies an increasing block delay after consecutive failed login attempts, with a default block delay greater than 5 seconds.
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 or configured period of inactivity ("X" days).	The DUT automatically suspends the account after "X" days of non-use, where the number of days is configurable, and prevents login until the account is reactivated.
2.3.1	**Secure Update**	TC1	TC_SW_PKG_INTEGRITY_VALID	To verify the integrity of the software image in accordance with the latest ITSAR on cryptographic controls when 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 of the software image in accordance with the latest ITSAR on cryptographic controls when performing an illegitimate (tampered) software update.	The DUT validates the integrity of the software image as per Table 1 of the latest ITSAR on cryptographic controls and restricts the update in case of a tampered software image.
		TC 3	TC_SW_PKG_INTEGRITY_NO_SIGNATURE	To verify that the DUT does not perform a software update using an unsigned software image.	The DUT does not update the software in the absence of a digital signature on the software image.
		TC 4	TC_SW_PKG_INTEGRITY_UNAUTHORIZED	To verify that a software update cannot be performed on the DUT by an unauthorized user.	The DUT rejects software update requests from unauthorized users.
		TC 5	TC_SW_PKG_INTEGRITY_EXPIRED	To verify that the DUT rejects a software update using an image with an expired digital certificate.	The DUT does not update the software if the digital certificate of the software image has expired.
2.3.2	**Secure Upgrade**	TC1	TC_SW_PKG_INTEGRITY_VALID	To verify the integrity of the software image in accordance with the latest ITSAR on cryptographic controls when 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 of the software image in accordance with the latest ITSAR on cryptographic controls when performing an illegitimate (tampered) software upgrade.	The DUT validates the integrity of the software image as per Table 1 of the latest ITSAR on cryptographic controls and restricts the upgrade in case of a tampered software image.
		TC 3	TC_SW_PKG_INTEGRITY_NO_SIGNATURE	To verify that the DUT does not perform a software upgrade using an unsigned software image.	The DUT does not upgrade the software in the absence of a digital signature on the software image.
		TC 4	TC_SW_PKG_INTEGRITY_UNAUTHORIZED	To verify that a software upgrade cannot be performed on the DUT by an unauthorized user.	The DUT rejects software upgrade requests from unauthorized users.
		TC 5	TC_SW_PKG_INTEGRITY_EXPIRED	To verify that the DUT rejects a software upgrade using an image with an expired digital certificate.	The DUT does not upgrade the software if the digital certificate of the software image has expired.
2.3.3	**Source Code Security Assurance**	TC1	TC_SDoC_Verification	To verify that the OEM has submitted the SDoC in the prescribed format.	The OEM submits the SDoC in the prescribed format.
		TC2	TC_Internal_Report_Verification	To verify the internal test report, excluding intellectual property-related information, and ensuring that it includes a summary of the number of security vulnerabilities/weaknesses classified by risk.	The internal test report is submitted, including a summary of security vulnerabilities/weaknesses classified by risk.
2.3.4	**Known Malware and backdoor Check**	TC1	TC_KNOWN_MALWARE_DECLARATION_VALIDATION	To verify that the OEM submits a Self-Declaration of Conformity (SDoC) in the prescribed format, stating that the product is free from all known malware as per the malware signature database prescribed by NCCS and is also free from backdoors.	The OEM has submitted the SDoC in the 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 - "BSF does not contain software that is not used in the functionality of the BSF."**	**The OEM submits list of necessary software components along with their functions. The OEM submits undertaking - "BSF does not contain software that is not used in the functionality of the BSF."**
		TC1	TC_VERIFICATION_OF_INSTALLED_SOFTWARE_AND_FILES	To verify the inventory of all software components (packages, libraries, binary files, etc.) available in the DUT.	The DUT lists all installed software packages, libraries, and binary files.
		TC2	TC_VERIFICATION_OF_OEM_SUPPLIED_SOFTWARE	To verify the list of necessary software components (along with their functions) submitted by the OEM for accuracy and completeness. To verify that the OEM undertaking is in the prescribed format.	The OEM submits a list of necessary software components, along with their functions, and the undertaking in the prescribed format.
		TC3	TC_CONSOLIDATION_OF_OEM_PROVIDED_AND_INSTALLED_SOFT WARE	To cross-check that the software components actually available in the DUT exactly match the list of components submitted by the OEM.	The software components installed in the DUT match the list of software components submitted by the OEM.
		TC4	TC_VERIFICATION_OF_ORPHANED_AND_UNWANTED_PACKAGES	To verify that the DUT does not contain any orphaned packages or unnecessary files.	The DUT does not contain any orphaned packages or unnecessary files.
2.3.6	**Unnecessary services removal**	TC1	TC_To_verify_OEM_Documentation	To verify that the OEM documentation provides the required protocols and services for the DUT, including a 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 or vulnerable services can be disabled on the DUT and remain disabled after reboot.	The DUT permits unnecessary services to be disabled and restricted.
		TC3	TC_To_verify_protocol_services_disabled_if_vulnerable	To verify that running services do not have any known vulnerabilities.	The DUT has no known vulnerabilities in its running services.
		TC4	TC_SERVICE_SCAN_VERIFICATION	To scan the available services on all interfaces after a factory reset or permanent disabling of the relevant protocol.	The scan report properly documents all available ports for their respective functions, and only documented and required services are found to be available on the DUT.

2.3.7	**Restricting System Boot Source**	TC1	TC_FIRMWARE_PROTECTION	To verify that the DUT firmware has a protection mechanism against unauthorized access.	The DUT firmware is protected against unauthorized access.
		TC2	TC_INTENDED_BOOT_MODE	To verify that the DUT can boot only from the intended memory devices as declared by the OEM.	The DUT boots only from the intended memory devices declared by the OEM.
		TC3	TC_UNINTENDED_BOOT_MODE	To verify that the DUT cannot boot from unintended memory devices.	The DUT does not boot from unintended memory devices and boots only from the intended memory devices declared by the OEM.
2.3.8	**Secure Time Synchronization**	TC1	TC_TIME_SYNC_PROTOCOLS_OEM_DECLARATION	To verify that all protocols available on the DUT for time synchronization are in accordance with the OEM declaration.	All protocols available on the DUT for time synchronization are in accordance with the OEM declaration.
		TC2	TC_Secure Time Synchronization For_ITSAR_Table1_Comparison	To verify that communication between the DUT and the NTP server is secured as prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.	The DUT uses secure protocols for communication with the NTP server as prescribed in Table 1 of the 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.	The DUT logs all events related to changes in time settings.
		TC4	TC_PTP_IMPLEMENTATION	To verify that the DUT implements secure PTP in accordance with the applicable security requirements.	PTP is successfully configured on the DUT with security requirements as per RFC 7384.
		TC5	TC_MANUALLY_CHANGE_TIME	To manually change the time settings on the DUT using a privileged user account and verify that the settings are retained after reboot and power-off.	A privileged user can successfully change the time settings on the DUT manually, and the settings are retained after power-off.
		TC6	TC_NTP_CLIENT_CONFIGURATION	To configure the DUT as an NTP client using a privileged user account to synchronize time with an NTP server, if the DUT does not retain time settings by itself.	If the DUT does not retain time settings on its own, a privileged user can configure the DUT as an NTP client.
		TC7	TC_AUTH_BTW_DUT_AND_NTP	To configure and verify authentication between the DUT and the NTP/PTP server so that the tester can configure the DUT's authentication attributes for accessing the external NTP server.	The tester can successfully configure the authentication attributes of the DUT for accessing the 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 bound to their respective interfaces.	DUT services are not reachable from any interface other than the interface to which they are bound.
		TC2	TC_REACHABILITY_TO_LEGITIMATE_PEERS_ONLY	To verify that only legitimate peers can connect to the DUT.	The DUT is not reachable by 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 and configured management interfaces.	Administrative services (e.g., SSH, HTTPS, RDP, ZTP, NETCONF, SNMP, etc.) are restricted to interfaces in the management plane only and are accessible only through authorized and configured management interfaces.
2.3.10	**Self Testing**	TC1	CRYPTO_MODULE_SELF_TESTING	To perform a self-test to identify failures in security mechanisms during boot-up (power-on or reboot).	The DUT performs a self-test to detect failures in security mechanisms during the boot-up 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 a self-test to identify failures in the security mechanisms when instructed by the administrator.	The DUT performs a self-test to identify failures in its security mechanisms when instructed by the administrator.
		TC4	TC_CRYPTO_MODULE_INTEGRITY_CHECK_FAILS	To verify that the integrity of the cryptographic module is checked before any cryptographic operation is invoked.	The DUT invokes cryptographic operations only after verifying the integrity of the cryptographic module and does not downgrade the module to an insecure state.
		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 appropriate error indicator is displayed.	If the cryptographic module integrity check fails, the module enters an error state, which is verified through the corresponding 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, software, and active services in the DUT.	The DUT lists the installed hardware, software, 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 does not include unused or optional components.	The OEM submits documentation that includes a complete, accurate, and minimal list of software and hardware functions required for the DUT's operation, along with confirmation that no unused functions are present.
		TC3	TC_IDENTIFICATION_OF_DUT_FUNCTIONS_AND_VALIDATION_AG AINST_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 individually deleted, uninstalled, or permanently deactivated.	Unused software functions in the DUT can be individually deleted, uninstalled, or permanently deactivated.
		TC5	TC_VERIFICATION_OF_HARDWARE_FUNC	To verify that unused hardware functions (interfaces) in the DUT can be individually and permanently disabled.	Unused hardware functions (interfaces) in the DUT can be individually and permanently disabled.
2.4.2	**No Unsupported Components**	TC1	TC_No_Unsupported_components	To verify that all hardware and software components present and running in the DUT are still supported and have not reached end of life (EoL) or end of support (EoS).	The DUT does not contain any hardware or software components that have reached EoL or EoS.
		TC2	TC_OEM_UNDERTAKING	To verify that the OEM has submitted the undertaking in the prescribed format.	The 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 BSF 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 the OEM has submitted the undertaking in the prescribed format.	The OEM submits the undertaking in the prescribed format.
2.5.1	**Audit trail storage and protection**	TC1	TC_AUDIT_LOG_ACCESS_CONTROL_CLI	To verify local access control for read, write, and delete operations on security event log files for privileged, non-privileged, and administrator users.	Only authorized users with appropriate privileges have local access to the security event log files.
		TC2	TC_AUDIT_LOG_ACCESS_CONTROL_SSH	To verify remote access control for read, write, and delete operations on security event log files for privileged, non-privileged, and administrator users.	Only authorized users with appropriate privileges have remote access to the security event log files.
		TC1	TC_INCORRECT_LOGIN_ATTEMPTS	To verify that the DUT records all incorrect user login attempts.	The DUT successfully records incorrect login attempts by users. The logs contain the username, source IP address, event outcome, and timestamp.
		TC2	TC_ADMINISTRATOR_ACCESS	To verify that the DUT records all access attempts to accounts with system privileges.	The DUT successfully records user details for all access attempts to accounts with system privileges. The logs contain the username, source IP address, event outcome, session duration, and timestamp.
		TC3	TC_ACCOUNT_ADMINISTRATION	To verify that the DUT records all account administration activities, including configuration, deletion, enabling, and disabling.	The DUT successfully records all account administration activities, including configuration, deletion, enabling, and disabling. The logs contain the administrator username, administered account, activity performed, event outcome (success or failure), and timestamp.
		TC4	TC_RESOURCE_USAGE	To verify that the DUT records events triggered when system parameter values, such as disk space and CPU load, exceed their defined thresholds for a specified period.	The DUT successfully records events triggered when system parameter values, such as disk space and CPU load, exceed their defined thresholds. The logs contain the exceeded parameter, threshold value, event outcome, and timestamp.
		TC5	TC_CONFIGURATION_CHANGE	To verify that the DUT records all configuration changes.	The DUT successfully records all configuration changes. The logs contain the event, username of the account that initiated the change, details of the changes made, timestamp, and event outcome.

2.5.2	**Audit Event Generation**	TC6	TC_REBOOT/SHUTDOWN/CRASH	To verify that the DUT records any actions that cause a reboot, shutdown, or crash of the DUT.	The DUT successfully records any action that causes a reboot or shutdown and any unintentional crash of the DUT. The logs contain the action performed, username, event outcome, 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 its interfaces. The logs contain the interface name and type, interface status, event outcome, and timestamp.
		TC8	TC_CHANGE_OF_GROUP_MEMBERSHIP_OR_ACCOUNTS	To verify that the DUT records all changes to group membership for user accounts.	The DUT successfully records all changes to group membership for user accounts. The logs contain the administrator username, administered account, activity performed (group added or removed), event outcome, and timestamp.
		TC9	TC_RESETTING_PASSWORDS	To verify that the DUT records resetting of user account passwords by the administrator.	The DUT successfully records password resets performed by the administrator. The logs contain the administrator username, administered account, activity performed, event outcome, and timestamp.
		TC10	TC_SERVICES	To verify that the DUT records starting and stopping of services on the DUT.	The DUT successfully records the starting and stopping of services. The logs contain the service identity, activity performed (start, stop, etc.), timestamp, and event outcome.
		TC11	TC_X.509_CERTIFICATE_VALIDATION	To verify that the DUT records unsuccessful attempt to validate a certificate.	The DUT successfully records unsuccessful certificate validation attempts. The logs contain the timestamp, reason for failure, subject identity, and event type.
		TC12	TC_SECURE_UPDATE	To verify that the DUT records attempts to initiate a manual update, initiation of the update, and completion of the update.	The DUT successfully records: a. Attempts to initiate a manual update b. Initiation of the update c. Completion of the update The logs contain the user identity, timestamp, event outcome, and activity performed.
		TC13	TC_TIME_CHANGE	To verify that the DUT records changes in time settings.	The DUT successfully records changes in its time settings. The logs contain the old time value, new time value, timestamp, origin of the attempt to change the time (IP address), subject identity, event outcome, and user identity.
		TC14	TC_SESSION_UNLOCKING/TERMINATION	To verify that the DUT records any attempt to unlock an interactive session, termination of a remote session by the session-locking mechanism, and termination of an interactive session.	The DUT successfully records: a. Attempts to unlock an interactive session b. Termination of a remote session by the session-locking mechanism c. Termination of an interactive session The logs contain the user identity, timestamp, event outcome, subject identity, activity performed, and event type.
		TC15	TC_TRUSTED_COMMUNICATION_PATHS_WITH_IT_ENTITIES_AND_FOR_AUTHORIZED_REMOTE_ADMINISTRATORS	To verify that the DUT records the initiation, termination, and failure of trusted communication paths.	The DUT successfully records the initiation, termination, and failure of trusted communication paths. The logs contain the timestamp, initiator identity (as applicable), target identity (as applicable), user identity (in case of remote administrator access), event type, and event outcome (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 contain the timestamp, event type (audit data deletion or modification), event outcome, subject identity, user identity, origin of the attempt to change the audit data (IP address), and details of the data deleted or modified.
		TC17	TC_USER_LOGIN_AND_LOGOFF	To verify that the DUT records all uses of identification and authentication mechanisms during user login.	The DUT successfully records all uses of identification and authentication mechanisms during user login. The logs contain the user identity, origin of the attempt (IP address), timestamp, and event outcome.
		TC18	TC_ACL_RULE	To verify that the DUT records any packet-matching failure against an ACL or a rule that allows packet traversal through the router.	The DUT successfully records any packet-matching failure against an ACL or a rule that allows packet traversal through 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 for exporting logs match those specified in the OEM declaration.
		TC2	TC_FORWARDING_SECURITY_EVENT	To verify that the DUT forwards security event logs to an external (syslog) server.	The DUT forwards security event logs to an 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 generates audit logs locally without an external log server and retains at least two days of audit data.
		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 the DUT, with approved cryptographic controls/protocols as per Table 1 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 the latest ITSAR on cryptographic controls.
		TC5	TC_LOG_BUFFER_BEYOND_THRESHOLD	To verify the behavior of the DUT when the log buffer exceeds its default threshold size.	Do not finalize this Expected Result until you confirm what the applicable requirement specifies for log-buffer overflow.
		TC6	TC_DUT_ALERTS_ADMIN_IN_CASE_LOG_BUFFER_EXCEEDS	To verify that the DUT sends an alert to the administrator when the log buffer reaches or exceeds the default threshold.	The DUT sends an alert to the administrator when the log buffer reaches or exceeds the default threshold.
2.5.4	**Logging access to personal data**	TC1	TC_LOGGING_ACCESS_TO_PERSONAL_DATA	To verify that the DUT logs access to personal data and identifies the user who accessed it. The log must contain information identifying who accessed which data. The log must not reveal personal data in clear text.	The DUT successfully logs access to personal data. The logs contain information about the user and the data accessed. Personal data is not revealed in clear text.
		TC2	TC_SECURING_SUBSCRIBER_PRIVACY	To verify that personal data stored in the log files does not allow direct identification of a subscriber and does not result in a privacy violation.	Personal data stored in the log files does not allow direct identification of a subscriber and does not result in a 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 used to communicate with external connected entities are in accordance with the OEM declaration.	All protocols available in the DUT used to communicate with external connected entities are in accordance with the OEM declaration.
		TC2	TC_API_ACCESS_OVER_TLS	To verify that the BSF 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 or TLS 1.3 with approved cipher suites.
		TC3	TC_REJECT_API_ACCESS_WITHOUT_TLS	To verify that the BSF supports only cipher suites compliant with Table 1 of the latest ITSAR on cryptographic controls and does not support weak TLS versions.	The DUT rejects weak TLS versions and denies any API access attempted without TLS. The DUT supports only cipher suites compliant with Table 1 of the latest ITSAR on cryptographic controls.
		TC4	TC_ALLOW_SSH_WITH_STRONG_CIPHERS	To verify that the BSF accepts SSH connections on the OAM interface using only approved ciphers as per Table 1 of the latest ITSAR on cryptographic controls.	The DUT allows SSH connections using SSHv2 with strong, approved cipher suites as per Table 1 of the latest ITSAR on cryptographic controls.
		TC5	TC_REJECT_SSH_WITH_WEAK_CIPHERS	To verify that attempts to connect using weak or null SSH ciphers are rejected by the BSF and that non-compliant ciphers are blocked.	The DUT rejects SSH connections that attempt to use weak or non-approved cipher suites.
		TC6	TC_VERIFY_DATABASE_TLS_CONNECTION	To verify that the BSF communicates securely with its internal database using only approved cryptographic controls, as per Table 1 of the latest ITSAR on cryptographic controls.	The DUT ensures that the internal database connection uses TLS to encrypt and secure data in transit.

		TC7	TC_OTHER_SECURE_COMM_PROTOCOLS	To verify that all other protocols available in the DUT used to communicate with connected entities strictly use secure cryptographic controls prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.	The DUT ensures that all other protocols available in the DUT used to communicate with connected entities strictly use secure cryptographic controls prescribed in Table 1 of the latest ITSAR on Cryptographic Controls.
2.6.2	**Cryptographic Module Security Assurance**	TC1	TC_CRYPTOGRAPHIC_MODULE_SECURITY_ASSURANCE	To verify that the OEM has submitted self-certified test reports for the cryptographic module embedded in the BSF (in the form of hardware, software, or firmware) that provides security services such as authentication, integrity, and confidentiality, and that the module is designed and implemented in compliance with FIPS 140-2 or later, as prescribed by applicable NIST standards.	The OEM submits the required self-certified test report for the cryptographic module.
		TC2	TC_OEM_DECLARATION	To verify that the OEM has submitted the undertaking in the prescribed format stating that the cryptographic module embedded in the DUT (in the form of hardware, software, or firmware) that provides security services such as authentication, integrity, and confidentiality is designed and implemented in compliance with FIPS 140-2 or later, as prescribed by applicable 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 the OEM has submitted self-certified test reports regarding the cryptographic algorithms implemented in the cryptographic module of the BSF and that they comply with the respective latest FIPS standards for the specific cryptographic algorithms.	The OEM has submitted the required self-certified test reports for the implemented cryptographic algorithms.
		TC2	TC_OEM_DECLARATION	To verify that the OEM has submitted an undertaking and self-certified test reports declaring that all cryptographic algorithms implemented within the DUT's cryptographic module comply with the respective latest FIPS standards.	The OEM submits the undertaking in the prescribed format.
2.6.4	**Protecting data and information – Confidential System Internal Data**	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.
		TC2	TC_CONFIDENTIAL_SYSTEM_INTERNAL_DATA	To verify that the DUT does not reveal confidential system internal data (such as error logs and trace files) in clear text through any function or interface during normal or debug operation when the system is not under maintenance (normal operational mode). To verify that error logs, trace files, and alarms/monitors do not reveal 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 that the configuration backup package does not reveal 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 are not stored in clear text and are protected using encryption or scrambling.	The DUT does not store identification and authentication data in clear text and protects such data using encryption or scrambling mechanisms.
		TC3	TC_STORED_FILE_INTEGRITY_PROTECTION	To verify that stored files and sensitive system files of the BSF are protected against unauthorized modification using approved cryptographic integrity and non-repudiation controls.	The DUT protects stored files and sensitive system files against unauthorized modification 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 on Cryptographic Controls and does not store such 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 are permitted only for authenticated and authorized users.	The DUT allows data-copying functions only for authenticated and authorized users.
		TC2	TC_LOGGING_AND_AUDITING_OF_UNAUTHORIZED_ACCESS	To verify that the use of system functions for copying data in use or in transit is logged.	The DUT logs the use of system functions for copying data in use or in transit.
		TC3	TC_UNAUTHORIZED_DATA_COPY_PREVENTION	To verify all protective measures implemented in the DUT against the use of available system functions or software residing in the BSF to create copies of data for illegal transmission.	The DUT implements protective measures that prevent copying 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 the BSF has mechanisms to prevent data exfiltration attacks involving the 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 is forbidden when they are auto-initiated or auto-originated by the BSF.	The DUT prevents auto-origination of outbound overt-channel connections.
		TC3	TC_Session_logs_generation_of_any_session	To verify that session logs are generated for the establishment of every session initiated by either the user or the DUT.	The DUT generates session logs for every session initiated by the 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 an overt channel such as SFTP or SCP.	An authorized user is able to perform outbound data export (file transfer) using an overt channel such as SFTP or SCP.
		TC5	TC_UNAUTH_USER_DATA_TRANSFER	To verify that an unauthorized user cannot perform outbound data transfer using an overt channel such as SFTP, SCP, or any other supported mechanism.	An unauthorized user cannot perform outbound data transfer using an overt channel such as SFTP, SCP, or any other supported mechanism.
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 the BSF has mechanisms to prevent data exfiltration attacks involving the 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 is forbidden when they are auto-initiated or auto-originated by the BSF.	The DUT prevents auto-origination of outbound covert-channel connections.
		TC3	TC_Session_logs_generation_of_any_session	To verify that session logs are generated for the establishment of every session initiated by the user or the DUT.	The DUT generates session logs for every session initiated by the user or the DUT.
		TC1	JSON input length validation	To verify that the BSF responds correctly to a request containing a valid JSON payload and safely handles a JSON payload with excessive length received from an NF consumer.	The DUT safely handles oversized JSON input without crashing or exhibiting abnormal behavior and returns a valid error response.
		TC2	JSON data type and structure validation	To verify the BSF's response to JSON fields with incorrect data types or an invalid 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 BSF validates received JSON requests for the presence of mandatory information elements.	The DUT rejects JSON requests that are missing mandatory fields.
		TC4	HTTP method error handling	To verify that the BSF correctly handles protocol-level errors caused by unsupported or invalid HTTP methods.	The DUT rejects unsupported HTTP methods with appropriate HTTP error codes.

2.6.9	**System robustness against Unexpected Input**	TC5	JSON nesting depth handling	To verify that the BSF safely handles complex input structures containing excessive JSON nesting depth.	The DUT safely handles deeply nested JSON payloads without crashing or causing service disruption.
		TC6	JSON input value whitelisting	To verify that the BSF properly validates and handles input values containing characters outside the permitted value set.	The DUT rejects JSON payloads containing invalid characters or disallowed escape sequences through input validation.
		TC7	HTTP/2 protocol robustness fuzz testing	To verify the BSF's behavior and resilience when subjected to malformed or fuzzed HTTP/2 traffic on its exposed application port.	The DUT securely handles malformed or fuzzed HTTP/2 inputs without impacting service availability or stability during fuzz testing.
		TC8	TLS handshake robustness fuzz testing	To evaluate the BSF's robustness against malformed or fuzzed TLS handshake packets at the transport layer.	The DUT securely handles malformed or fuzzed 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 bypasses, or abnormal behavior.	The DUT securely validates and processes 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 the DUT provides a mechanism to back up sensitive data, configuration data, and log files.	The DUT supports a mechanism to securely store backups of sensitive data, configuration data, and log files.
		TC2	TC_BACKUP_AND_RESTORATION_VERIFICATION	To verify that an effective backup and restoration strategy is implemented and documented for the DUT.	An effective backup and restoration strategy is implemented and documented for the DUT.
2.6.11	**Secure deletion of sensitive data**	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.
		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 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 and audit 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 affecting 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 the 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 the 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 the 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 the 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 the DUT allows only management-plane traffic through the OAM interface.	The DUT allows only management-plane traffic through the OAM interface.
		TC2	TC_OAM_to_DUT_via_SBI_Interface	To verify that the DUT denies management-plane traffic through the control-plane interface.	The DUT rejects management-plane traffic through the control-plane interface.
		TC3	TC_AMF_to_DUT_via_SBI_Interface	To verify that the DUT allows only control-plane traffic through the control-plane interface.	The DUT allows only control-plane traffic through the control-plane interface.
		TC4	TC_AMF_to_DUT_via_OAM_Interface	To verify that the DUT denies control-plane traffic through the OAM interface.	The DUT rejects control-plane traffic through the OAM interface.
		TC5	TC_PHYSICAL_SEPARATION	To verify that control-plane and O&M traffic are physically separated through out-of-band management.	The control-plane and O&M networks are physically separated and independently configurable through distinct hardware ports.
		TC6	TC_LOGICAL_SEPARATION	To verify that control-plane and O&M traffic are logically separated through in-band management when using a single physical interface.	The control-plane and O&M networks are logically separated through distinct configurations, such as VLANs, on the same physical interface.
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 mechanisms against DDoS attacks, as documented and verified through the OEM documentation.
		TC2	TC_Syn Flood.	To verify that the DUT has a network-level DDoS attack prevention mechanism.	The DUT possesses a network-level DDoS attack prevention mechanism.
		TC3	TC_Http2 High Request Rate Flood	To verify that the DUT has an application-level DDoS attack prevention mechanism.	The DUT possesses an application-level DDoS attack prevention mechanism.
		TC4	TC_Http2 Large Payload Flood	To verify that the DUT properly handles requests that may lead to memory exhaustion or DDoS conditions by rejecting such requests or degrading gracefully without crashing or restarting.	The DUT has mechanisms to protect against memory exhaustion and DDoS conditions and does not become impaired, unresponsive, crash, or restart.
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 the OEM documentation regarding the system protection mechanisms for overload situations.	The OEM documentation specifies the system protection mechanisms and procedures for overload situations.
		TC2	TC_Excessive Overload Scenario	To verify that the DUT does not enter an insecure state during an excessive overload situation, as specified in the OEM documentation.	The DUT acts predictably during an excessive overload situation in accordance with the OEM documentation.
		TC3	TC_Large Data to API Endpoints	To verify that the DUT handles large payloads without memory exhaustion and maintains a stable and secure state without crashes or undefined behavior.	The DUT behaves predictably under excessive overload conditions caused by large payloads or memory exhaustion.
2.8.3	**Interface Robustness Requirements**	TC1	TC_VERIFY_ROBUSTNESS_AGAINST_SYN_FLOOD_ATTACK	To verify that the DUT's performance does not degrade under a SYN flood attack due to excessive CPU or memory utilization.	The performance of the DUT does not degrade under a SYN flood attack.
		TC2	TC_VERIFY_ROBUSTNESS_AGAINST_LAND_ATTACK	To verify that the DUT's performance does not degrade under a LAND attack due to excessive CPU or memory utilization.	The performance of the DUT does not degrade under a LAND attack.
		TC3	TC_VERIFY_ROBUSTNESS_AGAINST_SMURF_ATTACK	To verify that the DUT's performance does not degrade under a Smurf attack due to excessive CPU or memory utilization.	The performance of the DUT does not degrade under a Smurf attack.
		TC4	TC_VERIFY_ROBUSTNESS_AGAINST_TEARDROP_ATTACK	To verify that the DUT's performance does not degrade under a Teardrop attack due to excessive CPU or memory utilization.	The performance of the DUT does not degrade under a Teardrop attack.

		TC5	TC_VERIFY_ ROBUSTNESS_AGAINST_PING_OF_DEATH_ATTACK	To verify that the DUT's performance does not degrade under a Ping of Death attack due to excessive CPU or memory utilization.	The performance of the DUT does not degrade under a Ping of Death attack.
		TC6	TC_VERIFY_ROBUSTNESS_AGAINST_UNCORRELATED_REPLY_PACKET_ATTACK	To verify that the DUT's performance does not degrade when uncorrelated reply packets are received.	The performance of the DUT does not degrade when uncorrelated reply packets are received.
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 the network and application levels that are subjected to fuzzing are as per the OEM declaration.	All protocols available in the DUT at the network and application levels that are subjected to fuzzing match the OEM declaration.
		TC2	TCP_Protocol_Fuzzing	To fuzz the TCP-IPv4 protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The TCP-IPv4 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC3	IPv4_Protocol_Fuzzing	To fuzz the IPv4 protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The IPv4 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC4	IPv6_Protocol_Fuzzing	To fuzz the IPv6 protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The IPv6 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC5	ARP_Protocol_Fuzzing	To fuzz the ARP client protocol using mutation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The ARP client protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC6	SSH_Protocol_Fuzzing	To fuzz the SSHv2 server protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The SSHv2 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC7	SNMP_Protocol_Fuzzing	To fuzz the SNMPv3 protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The SNMPv3 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC8	IPSec_Protocol_Fuzzing	To fuzz the IPsec protocol using mutation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The IPsec protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC9	Diameter_Protocol_Fuzzing	To fuzz the Diameter protocol using generation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The Diameter protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC10	HTTP2_Protocol_Fuzzing	To fuzz the HTTP/2 protocol using mutation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The HTTP/2 protocol passes the fuzzing test, and the DUT remains in a stable state. The same is verified through the DUT logs.
		TC11	TLS_Handshake_Fuzzing	To fuzz the TLS handshake using mutation-based fuzzing and verify the DUT logs for stable operation during fuzzing.	The TLS handshake passes the fuzzing test, and the DUT remains in a stable state. The same is verified through 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 externally reachable protocols at the network and application levels available in the DUT and verify the DUT logs for stable operation during fuzzing.	The DUT remains in a stable state when all externally reachable protocols at the network and application levels 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 availability of network services on the documented ports that 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 interfaces of the DUT and verify the results against the list of documented ports.	The list of open ports identified through TCP scanning matches the list of documented ports required for the operation of the DUT.
		TC3	TC_VERIFICATION_OF_PORT_SCANNING_UDP	To perform a UDP port scan on all interfaces of the DUT and verify the results against the list of documented ports.	The list of open ports identified through UDP scanning matches the list of documented ports required for the operation of the DUT.
		TC4	TC_VERIFICATION_OF_PORT_SCANNING_SCTP	To perform an SCTP port scan on all interfaces of the DUT and verify the results against the list of documented ports.	The list of open ports identified through SCTP scanning matches the list of documented ports required 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 a vulnerability assessment/scanning tool against all IP interfaces of the DUT.	The credential-based vulnerability scan report does not contain any known vulnerabilities. Any identified vulnerabilities have an appropriate remediation plan in place to mitigate the associated risks.
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 limits for dynamic or growing content, such as 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 and enforcement of dynamic or growing content limits. The DUT enforces the configured limits 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 whether the DUT supports file-system monitoring, such as alerts or alarms, for growing or dynamic content, as specified in the OEM documentation.	The DUT supports file-system monitoring, such as alerts or alarms, for growing or dynamic content, and the monitoring mechanism is successfully verified.
		TC3	TC_DYNAMIC_CONTENT_FILESYSTEM_MONITORING_VERIFICATION	To verify whether the DUT supports file-system monitoring, such as alerts or alarms, for growing or dynamic content, as specified in the OEM documentation.	The DUT supports file-system monitoring, such as alerts or alarms, for growing or dynamic content, and the monitoring mechanism is successfully verified.
		TC4	TC_QUOTA_AND_FILESYSTEM_MONITORING_STABILITY_VERIFICATION	To verify that events related to quota exceedance and file-system monitoring are logged and that the DUT maintains stable performance during such events by monitoring CPU and memory utilization.	The DUT maintains stable performance during events where dynamic or growing content exceeds the configured threshold, and such events are appropriately 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.**
		TC1	TC_ICMPV4_UNSUPPORTED_TYPE_SUPPORT_VERIFICATION	To verify that the DUT does not support sending ICMPv4 types that are not mentioned in the permitted/optional list in ITSAR, as per the OEM documentation.	The DUT does not support sending any ICMPv4 type other than those permitted/optional in ITSAR or specified in the OEM documentation.

2.10.2	**Handling of ICMP**	TC2	TC_ICMPV6_UNSUPPORTED_TYPE_SUPPORT_VERIFICATION	To verify that the DUT does not support sending ICMPv6 types that are not mentioned in the permitted/optional list in ITSAR, as per the OEM documentation.	The DUT does not support sending any ICMPv6 type other than those permitted/optional in ITSAR or 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 that are not mentioned in the permitted/optional list in ITSAR (ICMP Types 5, 13, and 14).	The DUT does not support sending, responding to, or processing any ICMPv4 type other than those permitted/optional in ITSAR or 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 that are not mentioned in the permitted/optional list in ITSAR (ICMP Type 137).	The DUT does not support sending, responding to, or processing any ICMPv6 type other than those permitted/optional in ITSAR or 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 privilege escalation.	The DUT does not allow unauthenticated privilege escalation.
		TC2	TC_LIST_B_FUNCTIONS_PERMISSION_VERIFICATION	To ensure that all List B functions, including SUID, SGID, and Linux capability-enabled files present on the DUT, match the OEM-provided list, follow secure permission configurations, and do not allow unauthorized privilege escalation.	All files in List B provide only the specific and limited functions justified by the OEM documentation and do not permit unauthorized privilege escalation.
2.10.4	**System Account Identification**	TC1	TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION	To verify that existing account UIDs are assigned uniquely in the DUT system.	The DUT ensures that all existing account UIDs are unique.
		TC2	TC_NEW_USER_ACCOUNT_IDENTIFICATION	To create a new user account on the DUT and verify the assigned user account identifier.	The DUT is able to create a new user account with a unique identifier.
		TC3	TC_DUPLICATE_USER_ACCOUNT_IDENTIFICATION	To attempt to create a duplicate user account on the DUT.	The DUT does not permit the creation of a duplicate user account with the same account identifier or account name.
		TC4	TC_VERIFY_NON_REPUDIATION_CONTROLS	To verify that users cannot deny actions they performed by validating the non-repudiation controls.	Audit logs accurately record actions performed by the user against their unique UID. Logs contain sufficient information for accountability, including UID, action, date/time, and 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 and functions required for the operation of the DUT are available.	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 has the Proxy ARP feature disabled by default.
		TC4	TC_DIRECTED_BROAD_DISABLING	To verify that directed broadcast is disabled by default on the DUT after a factory reset.	The DUT has directed broadcast disabled 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 that multicast route caching and forwarding are disabled by default after a factory reset.	The DUT discards all multicast IPv4 packets, and multicast route caching and forwarding are 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 has the Gratuitous ARP feature disabled 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 does not respond to ICMP broadcast or multicast packets by default.
2.10.6	**No Automatic Launch of Removable Media for BSF NF**	TC1	NO_AUTOMATIC_LAUNCH_OF_REMOVABLE_MEDIA	To verify that the DUT does not automatically mount or launch an application when a removable media device is connected.	The DUT does not automatically mount or launch an application when a removable media device is connected.
		TC2	TC_AUTOMATIC_LAUNCH_OF_REMOVABLE_MEDIA_DEACTIVATION	To verify the activation/deactivation of automatic launching of compatible scripts/applications from a USB drive or removable media.	The DUT deactivates automatic launching of compatible applications/scripts from 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 protection mechanisms are mentioned in the OEM documentation.	The buffer overflow protection mechanisms are clearly described in the OEM documentation.
		TC2	TC_PROTECTION_FROM_BUFFER_OVERFLOW	To verify that the DUT implements robust buffer overflow protection mechanisms as per the OEM documentation.	The DUT implements robust buffer overflow protection mechanisms as per the OEM documentation, and the same is verified through testing.
2.10.8	**External file system mount restriction**	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 implemented for normal users against the mounting or use of removable media for data transfer.	The DUT provides a mechanism to prevent normal users from mounting or using removable media for data transfer.
		TC3	TC_Privilege_escalation_non_support_for_normal_users	To verify that the DUT prevents privilege escalation attempts using an external file system containing writable SUID/SGID files.	The DUT prevents privilege escalation attempts using externally prepared file systems containing writable SUID/SGID files and blocks unauthorized access attempts.
		TC4	TC_Privilege_escalation_attempt_from_external_filesystem	To verify that execution of privilege escalation payloads from a mounted file system is blocked.	The DUT blocks the execution of privilege escalation payloads 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 permitted to modify only those files, data, directories, or file systems for which they are authorized according to the OEM documentation.	The DUT ensures that OS-level access permissions are correctly configured for all users. Users are able to modify only those files, data, directories, or file systems for which they have the necessary privileges.
		TC2	TC_AUTHORISED_USER_Modify	To verify that an authorized user with the necessary privileges can modify at least one file and directory.	The DUT allows authorized users to modify the file or directory.
		TC3	TC_UNAUTHORISED_USER_Modify	To verify that an unauthorized user with insufficient privileges cannot modify a file or directory.	The DUT does not allow unauthorized users to modify the file or directory.
2.10.10	**SYN Flood attacks Prevention for BSF 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 the DUT supports a SYN flood prevention mechanism by default after a factory reset, as described in the vendor documentation.	The SYN flood prevention mechanism or technique is enabled by default on 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 an ACL filtering rule on the DUT to drop packets with IPv4 options enabled and apply the rule to the appropriate interface of the DUT, as per the OEM documentation.	The DUT drops IPv4 packets containing IPv4 options and does not send a response.
		TC2	TC_IPV6_EXTENSION_HEADERS_ACL_Drop	To configure an ACL filtering rule on the DUT to drop 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 IPv6 packets containing IPv6 extension headers and does not send a response.
		TC3	TC_IP_OPTIONS_IPV6_EXTENSION_HEADERS_ACL_Allow_Exception	To configure and apply an ACL for handling exceptional requirements that allow IP options and extension headers, as per the OEM documentation.	The tester is able to configure a filtering rule (ACL) on the DUT to allow IPv4/IPv6 packets with IP options and extension headers and apply the rule to the appropriate interface. The IPv4/IPv6 packets with IP options and extension headers are received by the DUT, and the corresponding responses are 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 such as backups, disk monitoring, and maintenance can be executed only by privileged users.	The DUT ensures that backup, disk-space monitoring, system maintenance, and script/batch-process/macro execution 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 execution of scripts, batch processes, or macros is restricted to authorized users only.	The DUT ensures that only authorized users can execute scripts, batch processes, or macros. Normal users are unable to execute these operations.
		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) are 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_BSF_RESTRICTIONS_ON_SOFT_RESTART	To verify that the BSF system restricts the use of software-based system restart options among different users.	The DUT ensures that attempts by normal users to execute system restart commands are denied. Attempts by a normal user to execute the reboot command are also denied.
		TC2	TC_BSF_RESTRICTION_ON_KEY_COMBINATIONS	To restrict software restarts initiated through key combinations, specifically CTRL+ALT+DEL, for users operating within the BSF.	The DUT does not allow system restart through the CTRL+ALT+DEL key combination.
2.11.1	**HTTPS**	TC1	TC _HTTPS	To verify that communication between the web server and the client is secure using authorized TLS 1.2 or above, and that downgrade to lower TLS versions and the use of NULL ciphers are not permitted.	The DUT supports HTTPS configuration using TLS 1.2 or above. Attempts to configure TLS 1.0, TLS 1.1, or NULL ciphers are 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 handshake and negotiates authorized cryptographic suites as per the cryptographic controls prescribed in Table 1 of the 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 the access timestamp, source IP address, account (if known), attempted login name (if the associated account does not exist), relevant fields in the HTTP request (including the URL whenever possible), and the web server response status code.
		TC2	TC_VERIFICATION_OF_WEBSERVER_FAILED_LOGIN_WRONG_CREDENT IAL	To verify that the web server logs failed access attempts.	The DUT logs all failed login attempts with the access timestamp, source IP address, account (if known), attempted login name (if the associated account does not exist), relevant fields in the HTTP request (including the URL whenever possible), and the web server response status code.
2.11.3	**HTTP Input Validation**	TC1	TC_USERNAME_Injection	To verify that the username field is protected against command injection and cross-site scripting (XSS).	The DUT ensures that the username field is not vulnerable to command injection or cross-site scripting (XSS).
		TC2	TC_PASSWORD_Injection	To verify that the password field is protected against command injection and cross-site scripting (XSS).	The DUT ensures that the password field is not vulnerable to command injection or cross-site scripting (XSS).
		TC3	TC_Manual_Testing_for_XSS_SQL_Injection	To verify manually that all input fields, such as text boxes, buttons, check boxes, and tick boxes, supported by the DUT are protected against command injection and cross-site scripting (XSS).	The DUT ensures that all supported input fields, including 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 the DUT web server prevents XSS and command injection attacks using an appropriate tool, preferably an automated crawler.	The DUT ensures that all supported input fields 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 the DUT web server is able to filter, escape, encode, and validate all user-controllable input fields.	The DUT web server filters, escapes, encodes, and validates 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 runs 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 runs under a non-system, non-root user account with least privileges.
		TC3	.TC_SYSTEM_PRIVILEGES_DROP_TO_NO_SYSTEM_PRIVILEGES_SE RVER	To verify that if the web server process starts with system privileges, it drops those privileges and transfers execution to a non-privileged user account after startup.	The DUT web server process transfers execution to a non-privileged user account after startup if it initially 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 the required HTTP methods, such as GET, HEAD, and POST, as applicable to its operation.
		TC2	TC_NO_TRACK_TRACE_Method	To verify that the DUT web server does not allow the TRACK or TRACE methods.	The DUT web server does not allow the TRACK or TRACE methods.
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 when they are not required.	The DUT permits deactivation of CGI or other scripting components, Server Side Includes (SSI), and WebDAV when they are not required.
		TC2	TC_NO_OTHER_COMPONENTS	To verify that no unnecessary components are installed on the web server using an automated tool.	The DUT does not have any unnecessary web server components installed, as verified 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 directories used for CGI or other scripting components do not contain compilers, interpreters, or operating system shells (e.g., Perl® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler, or operating system shells).	The web server in the DUT does not contain compilers, interpreters, or operating system shells in 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 directories with write permission for the web server do not contain executable scripts, CGI programs, or other executable code.	Directories with write permission for the web server do not contain executable scripts, CGI programs, or other executable code.
		TC2	TC_DIR_CONFIGURED	To verify that directories configured for CGI/scripting do not have write permissions for the web server.	The CGI/scripting directories do 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 execution of system commands using the exec directive in an SSI file is disabled, both with and without valid system commands.	The DUT does not execute any system commands using the exec directive through SSI.
		TC2	TC_EXEC_DIRECTIVE_SYSTEM_COMMAND_BLOCKING	To verify that execution of system commands using the exec directive in an SSI file is disabled, both with and without valid system commands.	The DUT does not execute any system commands using the 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 to all web server configuration files and configuration directories.	The DUT ensures that only the owner of the web server process and users with system privileges have read and write access to 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 to newly created web server configuration files and configuration directories.	The DUT ensures that only the owner of the web server process and users with system privileges have read and write access to newly created web server configuration files and directories.
2.11.11	**No Default Content**	TC1	TC_NO_DEFAULT_CONTENT	To verify whether any default content, such as example files, help files, documentation, or aliases, is available on the web server.	The DUT does not have any default content, such as example files, help files, documentation, or aliases, on the web server.
2.11.12	**No Directory Listings**	TC1	TC_DIRECTORY_LISTING_DISABLED	To verify that directory listing/browsing is disabled in the web server configuration.	The DUT ensures that directory browsing is disabled.
		TC2	TC_NO_DIRECTORY_LISTING	To verify that directory listing/browsing is not allowed on all endpoints, including domains, subdomains, and directories, offered by the web server.	The DUT does not allow directory browsing through the web server.
2.11.13	**Web Server Information in HTTPS Headers**	TC1	TC_NO_WEB_SERVER_HEADER_INFORMATION	To verify that response headers sent by HTTP requests do not disclose the web server version or the modules/add-ons used, such as server name or version.	The DUT web server ensures that HTTP response headers do not contain web server identification details, such as server name or version.
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 replaces the default error pages with user-defined error pages.
		TC2	TC_NO_USER_DEFINED_ERROR_PAGES_INFORMATION	To verify that user-defined error pages do not include version information about the web server or the modules/add-ons used.	The DUT ensures that error pages do not display internal information such as the server version, server name, or other sensitive implementation details.
		TC3	TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION	To verify that error messages/pages, as per the OEM documentation, do not include internal information such as internal server names, error codes, modules, add-ons used, or other sensitive implementation details.	The DUT web server ensures that the custom error page is displayed without exposing internal information.
2.11.15	**Minimized File Type Mappings**	TC1	TC_VERIFY_FILE_TYPES_SUPPORTED	To verify which file types/script handlers are supported and confirm that only the required file types and script handlers 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 (e.g., PHP, PHTML, SH, EXE, etc.) are not handled or executed by the DUT web server.	The DUT does not allow file types or script handlers that are not required for its operation.
2.11.16	**Restricted File Access**	TC1	TC_RESTRICTED_FILE_ACCESS_DEFAULT	To verify that newly created directories/files present in the DUT web server document directory are owned by the user running the web server and are not writable by other users.	The DUT web server ensures that newly created directories/files in the web server document directory are owned by the user running the web server and are not writable by other users.
		TC2	TC_RESTRICTED_FILE_ACCESS_EXISTING	To verify that existing directories/files present in the DUT web server document directory are owned by the user running the web server and are not writable by other users.	The DUT web server ensures that existing directories/files in the web server document directory are owned by the user running the web server and are not writable by other users.
		TC3	TC_VERIFY_USER_RUNNING_WEB_SERVER	To verify that the user running the web server is an unprivileged user account.	The DUT ensures that the user running the web server is an unprivileged user account.
		TC4	TC_CHROOT_ENVIRONMENT	To verify that the web server runs inside a jail or chrooted environment for operating systems that support chrooted environments. If a chrooted environment is not used, the web server or other system functionality shall be configured to restrict access to file directories.	The DUT ensures that files and directories outside the web server's permitted directory cannot be accessed.
2.11.17	**HTTP User Sessions**	TC1	TC_SESSION_ID_UNIQUENESS	To verify that session IDs are unique for different users and different sessions.	The DUT web server ensures that session IDs for all users and sessions are unique.
		TC2	TC_SESSION_ID_UNPREDICTABILITY	To verify that session IDs are unpredictable.	The DUT web server ensures that session IDs have sufficient entropy and are unpredictable.
		TC3	TC_SESSION_ID_NO_SENSITIVE_INFORMATION	To verify that session IDs do not contain sensitive information in clear text, such as account numbers or other sensitive identifiers.	The DUT web server ensures that session IDs do not contain sensitive information in clear text.
		TC4	TC_SESSION_MAX_LIFETIME_TIMEOUT	To verify that the web server has a session idle timeout period beyond which the web server terminates idle sessions, deletes the session ID, and forces the user to re-authenticate to establish a new session. The default maximum session lifetime shall be 8 hours and shall be configurable.	The DUT web server ensures that the session is terminated and the session ID is deleted after the configured idle timeout period. The default maximum session lifetime is 8 hours and is configurable.
		TC5	TC_SESSION_ID_REGENERATION	To verify that the session ID is regenerated for each new session, such as each time a user logs in.	The DUT web server ensures that a new session ID is generated each time a user logs in.
		TC6	TC_SESSION_ID_NO_REUSE	To verify that the web server does not allow reuse or renewal of a session ID in subsequent sessions.	The DUT web server restricts reuse or renewal of session IDs in subsequent sessions.
		TC7	TC_SESSION_COOKIE_NO_PERSISTENCE	To verify that the BSF uses only session cookies and does not use persistent cookies; the Max-Age and Expires attributes shall not be set in the cookies.	The DUT web server ensures that session cookies are not stored permanently. The Max-Age and Expires 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 attribute is set to true.
		TC9	TC_SESSION_COOKIE_PATH_RESTRICTION	To verify that the session cookie Path attribute is set.	The DUT web server ensures that the Path attribute of the session cookie is set and valid.
		TC10	TC_SESSION_COOKIE_DOMAIN_RESTRICTION	To verify that the session cookie Domain attribute is set.	The DUT web server ensures that the Domain attribute of the session cookie is set and valid.
		TC11	TC_SESSION_ID_NOT_ACCEPTED_FROM_GET_POST	To verify that the network product does not accept session identifiers through GET/POST variables.	The DUT web server does not accept session identifiers through GET/POST variables.
		TC12	TC_SERVER_GENERATED_SESSION_ID ONLY	To verify that the DUT is configured to accept only server-generated session IDs.	The DUT web server does not accept client-supplied session IDs and accepts only 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 the JSON parser does not execute code-like strings contained in JSON payloads.	The DUT rejects JSON payloads containing executable code and does not execute any code.
		TC2	TC_JSON_LOCAL_FILE_INCLUSION_ATTEMPT	To verify that the JSON parser does not include or read local files from the DUT.	The DUT rejects JSON payloads referencing local files and does not access the referenced files in the DUT.
		TC3	TC_JSON_REMOTE_URI_INCLUSION_ATTEMPT	To verify that the JSON parser does not fetch external resources through a URI.	The DUT rejects JSON payloads containing external URIs and does not fetch or access external resources.
		TC4	TC_JSON_MALFORMED_AND_OVERSIZED_INPUT_HANDLING	To verify that the DUT safely handles malformed and oversized JSON payloads.	The DUT rejects malformed and oversized JSON payloads with appropriate error responses and maintains predictable and stable operation.
2.12.2	**Validation of the unique key values in Information Elements (IEs)**	TC1	TC_DUPLICATE_KEY_VALIDATION	To verify that the DUT rejects JSON messages containing duplicate key names within an Information Element (IE).	The DUT accepts valid JSON requests and rejects requests containing duplicate keys with an appropriate error response.
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 containing more than 16,000 leaf IEs and accepts requests within the specified 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 payloads within the permitted size limit.
		TC3	TC_NESTING_DEPTH_OF_LEAVES_NOT_EXCEED_32	To verify that the DUT enforces the maximum JSON nesting depth of 32 levels.	The DUT rejects JSON payloads with a nesting depth greater than 32 levels and accepts payloads within the permitted 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 and documented inventory of all active service interface protocols running on the DUT. The list 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 1.2 or above for NF-to-NF communications and rejects connections using 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 rejected.
		TC3	TC_MUTUAL_TLS_AUTHENTICATION_USING_CLIENT_AND_SERVER_CERTIFICATES	To verify that the DUT enforces mutual authentication between the 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 successfully completed 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 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 deployed transport-layer protection mechanism. 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 required 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 an NF Service Request when the access token signature has been tampered with.	The DUT rejects the NF Service Request when the access token signature has been tampered with and returns an appropriate 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 authorization failure.
		TC4	TC_AUTH_INCORRECT_AUDIENCE	To verify that the DUT correctly rejects an NF Service Request when the 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 does not match the DUT's specific identity or its NF Type.
		TC5	TC_AUTH_INCORRECT_SCOPE	To verify that the DUT correctly rejects an NF Service Request when the scope claim in 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 an S-NSSAI list that includes S-NSSAIs not served by the DUT.	The DUT rejects the NF Service Request when the token contains S-NSSAIs that are not served by the DUT.
		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 that are not supported by the 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 information 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 verify 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 JSON structural control characters, such as double quotes and backslashes, supplied in input fields, ensuring that they are treated strictly as literal string values and do not alter the structure 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 to perform 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 remote login to the DUT is permitted only for authorized users and that unauthorized users are not allowed to log in remotely.	The DUT allows only authorized users to log in remotely. Root and unauthorized users are not permitted to log in remotely.
		TC2	TC_VERIFICATION_OF_REMOTE_DIAGNOSTIC_LOGGING	To verify that all remote diagnostic activities performed by remote users on the DUT are properly logged, including required parameters such as ID, timestamp, interface type, event level, and result, where applicable as per the troubleshooting guide/alarm maintenance requirements.	The DUT captures logs of all activities performed by remote users, including required parameters such as ID, timestamp, interface type, event level, and result, where applicable as per the troubleshooting guide/alarm maintenance requirements.
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 when the system password is reset.	When a password reset is successfully performed, the DUT does not allow the deleted configuration to be retrieved or recovered through any means.
		TC2	TC_NO_SYSTEM_ROOT_PASSWORD_RECOVERY	To verify that no system/root password recovery mechanism is provided 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 be performed only by users with administrator privileges.	The DUT permits software image rollback only for 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 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 installation or upgrade on the DUT ensures software integrity in accordance with Table 1 of the latest ITSAR on cryptographic controls.	The DUT performs the software installation or upgrade only after validating the integrity of the software image using the cryptographic controls specified in Table 1 of the latest ITSAR on cryptographic controls.
		TC2	TC_SW_PKG_INTEGRITY_TAMPERED	To verify that an illegitimate (tampered) software installation or upgrade 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 installation or 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 the integrity of a legitimate software image during the boot process.	The DUT verifies the integrity of the legitimate software image during the boot process using the cryptographic controls specified in Table 1 of the latest ITSAR on cryptographic controls, matches the image against the expected reference value, and successfully completes the boot process.
		TC2	TC_SW_BOOT_INTEGRITY_NEG	To verify that the DUT detects and rejects an illegitimate (tampered) software image 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) software image during boot and rejects the image, preventing the boot process from proceeding with the tampered 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 DUT.**	**OEM provides the list of the default used Physical/Logical Interfaces/Ports that are necessary for the operation of the DUT.**
		TC1	TC_verify_physical_and_logical_interfaces	To verify the physical and logical interfaces available on the DUT.	The DUT provides a list of all available physical and logical interfaces.
		TC2	TC_verify_disabled_physical_and_logical_interfaces	To verify that unused physical and logical interfaces on the DUT can be permanently disabled.	The DUT allows all unused physical and logical interfaces to be permanently disabled.
		TC3	TC_UNUSED_INTERFACE_PORT_DISABLE_BY_ADMINISTRATOR	To verify that an administrator can permanently 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 each unauthorized 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 remain inactive 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 or 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 identify all predefined/default accounts with known or null authentication attributes stored in the DUT (such as passwords, password hashes, tokens, etc.) and verify them against the OEM documentation.	The list of all predefined/default accounts in the DUT matches the OEM documentation.
		TC2	TC_PREDEFINED_ACCOUNT_DELETION	To verify that all predefined or default user accounts (except Admin/Root) with known or null authentication attributes can be deleted or disabled on the DUT.	All predefined/default user accounts with known or null authentication attributes, 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 to the DUT is denied.
		TC4	TC_PREDEFINED_ACCOUNT_PERSISTENCE_AFTER_REBOOT	To verify that deleted or disabled predefined user accounts remain deleted or disabled after a system reboot.	Deleted accounts are not recreated, and disabled accounts remain disabled 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, a correct audience claim, and a matching NF Instance ID.	The DUT accepts and processes NF Service Requests when the client credentials assertion contains a valid signature, valid timestamps, a correct audience claim, and a matching NF Instance ID.
		TC2	TC_AUTH_TAMPER_TOKEN	To verify that the DUT rejects NF Service Requests when the access token signature has been altered or tampered with.	The DUT rejects any request received from an NF when the access token has a tampered or invalid signature.
		TC3	TC_AUTH_INCORRECT_AUDIENCE	To verify that the DUT rejects NF Service Requests when the aud claim in the access token does not match the DUT's identity.	The DUT rejects any request received from an NF with an invalid or mismatched 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 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 matches the NF Instance ID embedded in the public-key certificate used to sign the assertion, and rejects the request if there is a mismatch.	The DUT validates that the NF Instance ID (nfInstanceId) contained in the client credentials assertion matches the NF Instance ID verified from the signing certificate. If a mismatch is detected, the DUT rejects the client credentials assertion and denies the NF Service Request.
		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 are available 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 accessing 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 on Nbsf Interfaces**	TC1	C_SECURE_COMMUNICATION_ON_NBSF_DATAREPOSITORY_INTERFACE	To verify that communication over the Nbsf_DataRepository interface between BSF Network Functions is protected using HTTPS with mutual TLS, ensuring confidentiality, integrity, authentication, and protection against unauthorized access using cryptographic controls compliant with the latest ITSAR on Cryptographic Controls.	The DUT successfully established secure communication over the Nbsf_DataRepository interface using HTTPS with mutual TLS. Communication was encrypted, mutually authenticated, and protected against unauthorized access in accordance with the latest ITSAR on Cryptographic Controls.
		TC2	TC_SECURE_COMMUNICATION_BETWEEN_BSF_AND_PCF	To verify that communication between the BSF and PCF over the Nbsf interface is protected using HTTPS with mutual TLS, ensuring confidentiality, integrity, replay protection, and authentication in accordance with the latest ITSAR on Cryptographic Controls.	The DUT successfully established secure communication between the BSF and PCF using HTTPS with mutual TLS. Confidentiality, integrity, authentication, and replay protection were ensured, and unauthorized connection attempts were rejected.
3.2	**Secure Communication on the Diameter Interface**	TC1	TC_DIAMETER_FIREWALL_PROTECTION	To verify that the Diameter firewall protects the Diameter interface by allowing authorized Diameter signaling while detecting and blocking unauthorized or malicious Diameter traffic.	The DUT successfully verified that the Diameter firewall permitted authorized Diameter signaling and blocked unauthorized or malicious Diameter traffic on the Diameter interface.
		TC2	TC_SECURE_DIAMETER_COMMUNICATION	To verify that the Diameter interface is protected using TLS/DTLS 1.2 or above over TCP/SCTP, providing confidentiality, integrity, replay protection, and cryptographic controls compliant with the latest ITSAR on Cryptographic Controls.	The DUT successfully verified that the Diameter interface was protected using TLS/DTLS 1.2 or above. Confidentiality, integrity, replay protection, and approved cryptographic controls were ensured.
		TC3	TC_DIAMETER_NDSIP_PROTECTION	To verify that the Diameter interface supports NDS/IP protection using IPsec with Security Gateway (SEG) termination in accordance with TS 33.210.	The DUT successfully verified NDS/IP protection for the Diameter interface. IPsec tunnels were terminated at the Security Gateway (SEG), ensuring secure Diameter communication in accordance with TS 33.210.
3.3.1	**Removal of Default Accounts in database**	TC1	TC_REMOVAL_OF_DEFAULT_DATABASE_ACCOUNTS	To verify that all default, anonymous, and predefined database accounts are removed from the BSF database.	The DUT successfully verified that no default, anonymous, or predefined database accounts were present in the BSF database.

3.3.2	**Renaming of root/admin account in the database**	TC1	TC_NON_GUESSABLE_DATABASE_ADMIN_ACCOUNT	To verify that the BSF database does not contain administrative accounts with default or guessable names such as root or admin.	The DUT successfully verified that no administrative accounts with default or guessable names were present in the BSF database.
		TC2	TC_NON_GUESSABLE_SUPERUSER_ACCOUNT_CREATION	To verify that the DUT supports creation of a superuser account with a non-guessable name and permits authorized administrative operations.	The DUT successfully verified creation of a superuser account with a non-guessable name. The account successfully performed authorized administrative operations.
3.3.3	**No default databases in BSF Bindings**	TC1	TC_REMOVAL_OF_DEFAULT_DATABASES	To verify that all default or test databases have been removed from the BSF database.	The DUT successfully verified that only operational databases were present and no default or test databases existed.
3.3.4	**Password management and validation policy for Database**	TC1	TC_DATABASE_MUTUAL_AUTHENTICATION	To verify that access to the BSF database is protected using mutual authentication.	The DUT successfully verified that mutual authentication was enforced before database access was granted.
		TC2	TC_DATABASE_PASSWORD_COMPLEXITY_POLICY	To verify that the BSF database enforces the configured password complexity policy.	The DUT successfully verified enforcement of the configured password complexity policy. Non-compliant passwords were rejected.
		TC3	TC_DATABASE_PASSWORD_REUSE_POLICY	To verify that the BSF database prevents reuse of previously used passwords.	The DUT successfully verified enforcement of the password reuse policy. Previously used passwords were rejected.
3.3.5	**Restricted access to sensitive Information**	TC1	TC_RESTRICTED_ACCESS_TO_SENSITIVE_INFORMATION	To verify that access to sensitive database information is restricted to authorized users only.	The DUT successfully verified that sensitive database information was accessible only to authorized users and processes.
3.3.6	**Encryption of the BSF Binding Database**	TC1	TC_DATABASE_ENCRYPTION_AT_REST	To verify that sensitive database information is stored in encrypted form using cryptographic controls compliant with the latest ITSAR on Cryptographic Controls.	The DUT successfully verified that sensitive database information was stored in encrypted form using approved cryptographic controls.
3.3.7	**BSF Database specific logging**	TC1	TC_DATABASE_SECURITY_EVENT_LOGGING	To verify that security-relevant database events are recorded with sufficient audit information.	The DUT successfully verified that all required security-relevant database events were recorded with sufficient audit information.
		TC2	TC_DATABASE_AUTHENTICATION_LOG_PROTECTION	To verify that authentication-related attributes are protected within database logs.	The DUT successfully verified that sensitive authentication-related attributes were protected and not exposed in database logs.
		TC3	TC_SECURE_LOG_TRANSFER_USING_RSYSLOG	To verify that database logs are securely transferred to a centralized logging server using a secure log-transfer mechanism (e.g., rsyslog) and approved cryptographic controls.	The DUT successfully verified secure transfer of database logs to the centralized logging server using approved cryptographic controls.
		TC4	TC_SECURE_LOG_TRANSFER_USING_SFTP	To verify that database logs are securely transferred to an external system using SFTP.	The DUT successfully verified secure transfer of database logs to the external system using SFTP.
3.3.8	**User privileges**	TC1	TC_DATABASE_ROLE_BASED_ACCESS_CONTROL	To verify that database users can perform only the operations permitted by their assigned privileges.	The DUT successfully verified that database users could perform only authorized operations according to their assigned privileges.
3.3.9	**Protection from attacks**	TC1	TC_DATABASE_INJECTION_PROTECTION	To verify that the database is protected against injection attacks.	The DUT successfully verified protection against database injection attacks. Unauthorized database access through injection attempts was prevented.
		TC2	TC_DATABASE_ACCESS_CONTROL_AND_PORT_SECURITY	To verify that database access is restricted through mutual authentication and secure port configuration.	The DUT successfully verified secure database access using mutual authentication and protected port configuration. Unauthorized access attempts were rejected.
		TC3	TC_DATABASE_SECURE_RECOVERY	To verify that the database supports secure backup and restoration following data loss or corruption.	The DUT successfully verified secure backup and restoration of the database. Database data was successfully recovered following restoration.
		TC4	TC_DATABASE_DDOS_PROTECTION	To verify that the database enforces mechanisms to protect against denial-of-service and overload conditions.	The DUT successfully verified enforcement of mechanisms to prevent database overload and denial-of-service conditions.
		TC5	TC_DATABASE_TOCTOU_PROTECTION	To verify that the database is protected against Time-of-Check to Time-of-Use (TOCTOU) race condition attacks.	The DUT successfully verified protection against Time-of-Check to Time-of-Use (TOCTOU) race condition attacks.
		TC6	TC_DATABASE_INPUT_VALIDATION	To verify that database inputs are validated and encoded to prevent malformed input and injection attacks.	The DUT successfully verified that malformed or malicious inputs were rejected through input validation and encoding mechanisms.
3.3.10	**Unique Identity**	TC1	TC_DATABASE_UNIQUE_USER_IDENTITY	To verify that each database user account has a unique identity.	The DUT successfully verified that all database user accounts possessed unique identities and duplicate accounts were not permitted.
3.3.11	**BSF Database Integrity**	TC1	TC_DATABASE_CONFIGURATION_INTEGRITY	To verify the integrity of the database configuration and internal database structures.	The DUT successfully verified the integrity of the database configuration and internal database structures.
		TC2	TC_DATABASE_BACKUP_INTEGRITY	To verify the integrity and authenticity of database backups.	The DUT successfully verified the integrity and authenticity of the database backup.
3.3.12	**BSF Database Availability**	TC1	TC_DATABASE_SERVICE_AVAILABILITY	To verify that database services remain operational and continuously available.	The DUT successfully verified that database services remained operational and continuously available.
		TC2	TC_DATABASE_RESTORATION	To verify that database restoration successfully recovers data after corruption or loss.	The DUT successfully verified successful restoration of database data following recovery procedures.
		TC3	TC_DATABASE_REDUNDANCY_AND_FAILOVER	To verify that database redundancy and automatic failover mechanisms ensure service continuity.	The DUT successfully verified database redundancy and automatic failover while maintaining data availability and service continuity.
3.3.13	**Secured BSF database backups**	TC1	TC_SECURE_DATABASE_BACKUP_INTEGRITY	To verify that database backups are securely created and protected against unauthorized modification.	The DUT successfully verified secure creation of database backups and their integrity using approved verification mechanisms.
		TC2	TC_DATABASE_CLUSTER_REDUNDANCY_FAILOVER	To verify that clustered database deployment provides redundancy and automatic failover.	The DUT successfully verified clustered database redundancy and automatic failover while maintaining database availability.
3.4	**Valid AF session**	TC1	TC_VALID_AF_SESSION_AUTHORIZATION	To verify that the BSF authorizes valid AF sessions, rejects unauthorized session requests, and performs Diameter signaling validation in accordance with security requirements.	The DUT successfully verified authorization of valid AF sessions. Unauthorized or invalid session requests were rejected, and Diameter signaling validation was enforced in accordance with security requirements.

ASHISH VYAS

Digitally signed by ASHISH VYAS
Date: 2026.08.20 17:45:44 +05'30'