**Self-evaluation form for testing items**

**1. Preface**

(1) This document is provided to allow vendors to independently evaluate whether their respective communication products and integrated systems meet the feasibility criteria for certification testing (hereafter referred to as "testability"). Interpretations and approvals or rejections related to certification testing of secure equipment are subject to the administrative guidance of the competent authority.

(2) The self-assessment required in this form encompasses three major categories: cryptographic security, communication security, and information security.

(3) The secure equipment requiring certification testing includes:

Primary equipment, such as encryption devices.

Auxiliary equipment, such as encoders, key generation, and management mechanisms.

(4) Secure equipment must be implemented in hardware form.

A NOTE FROM THE ORBIS TEAM: While this document is focused on hardware-based cryptography and security, Orbis acknowledges that Catalyst uses an integrated software-based cryptographic solution that can use either software key management or hardware security modules when required. The Orbis Catalyst system uses software-based encryption, specifically cryptography that is fully compliant with the CRYSTALS-Kyber standard. CNSA Suite 2.0 is the replacement (required by 2025) for the Commercial National Security Algorithm Suite, the cryptographic standard for software-based implementations. CNSA Suite-approved algorithms are equal to the hardware-based Suite A / Type 1 cryptographic implementations  (<https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF>). Kyber cryptography is resistant to the attacker advantages provided by quantum computing against other algorithms in accordance with Federal Information Processing Standards 203 (FIPS 203). Data providers utilize Catalyst provided libraries for validating identity and connecting to Catalyst using TLS 1.3 with Post-Quantum keys or by implementing mTLS between services. Clients access Catalyst through the Catalyst Gateway which supports TLS 1.3 with Post-Quantum keys if supported by the partner's application stack.

(5) Encryption algorithms must be replaceable.

(6) The security design of secure equipment must be verifiable.

The design must be accompanied by documentation.

**2. Verification Methods Include (But Are Not Limited To) the Following:**

* Review and Testing of Software and Hardware Components: This includes reviewing numerical values within the software and hardware, as well as measuring equipment signals.
* Test samples can be executed using test prototypes, development boards, or testing platforms.
* Some testing procedures are destructive, so vendors intending to participate must consider the required quantity of test samples.
* Vendors intending to participate must provide support with equipment relevant to the testing process.
* Upon passing the security certification testing and being adopted by the institute, a security assessment must be conducted once every three years as per regulations. If any deficiencies are found during the assessment, modifications must be completed before re-evaluation. Once re-evaluation is passed, all equipment versions must be updated accordingly.

(7) During the lifecycle of the secure equipment, if there are any changes to software, hardware, or firmware related to the security of the equipment, partial or complete security certification testing must be conducted based on the scope of the impacted security boundary before the equipment can be used.

**2. Cryptographic Security**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Test item | Test description | Testability | | Description |
| Y | N |
| 1 | Secure equipment (modules) must be implemented in hardware form. | **Hardware implementation is required for secure cryptographic modules.** | **Y** |  | **Google Cloud HSM is implemented as a FIPS 140-2 Level 3 certified hardware module.** |
| 2 | Encryption algorithms, algorithm parameters, and cryptographic keys must be modifiable and replaceable. | **Flexibility to modify and replace cryptographic components.** | **Y** |  | **Catalyst supports key rotation and parameter updates through GCP’s unified API.** |
| 3 | Provide a description of the secure equipment, including its purpose, security functions, operating environment and methods, intended users, and security management procedures. | **Detailed description of secure hardware.** | **Y** |  | **Catalyst integrates with Google Cloud HSM for secure key storage and management, leveraging hardware security and robust API controls.** |
| 4 | Outline the storage and management procedures for the secure equipment and its critical auxiliary devices. | **Describe storage and management of critical devices.** | **Y** |  | **Cryptographic keys are securely stored in HSMs, with geographic controls and centralized management.** |
| 5 | Specify the security boundary scope of the secure equipment submitted for certification testing. The boundary scope should be defined sequentially from the inside out as follows: cryptographic module security boundary, cryptographic device security boundary, and cryptographic system security boundary. | **Define security boundary of hardware and system.** | **Y** |  | **GCP defines cryptographic boundaries for HSMs, ensuring strict separation of hardware and system operations.** |
|  | Interface security |  |  |  |  |
| 6 | Secure equipment interfaces are classified as follows (but not limited to the listed interfaces; vendors may supplement based on the characteristics of their equipment): Data Input Interface, Data Output Interface, Status Display Interface, Control Signal Input Interface. Vendors must provide explanations ensuring that each interface is logically independent and separate. | **Logical separation of interfaces.** | **Y** |  | **Google Cloud HSM uses isolated interfaces for secure communication, aligned with industry standards like PKCS#11.** |
| 7 | Sensitive data within secure equipment must not be accessed, modified, or deleted via any interface without proper authorization. | **Authorization for all data access.** | **Y** |  | **IAM policies ensure that only authorized users can access or modify keys in the HSM.** |
| 8 | When the security equipment is in an error state, the equipment functions are locked and users cannot communicate normally. Data output from all data output interfaces is prohibited. Only status information can be output through the status output interface to identify the error status category. | **Error state behavior.** | **Y** |  | **HSM modules in Google Cloud automatically lock outputs during error states and provide status indicators.** |
| 9 | During self-testing, secure equipment must prevent any data from being output through the data output interface.  Status information displaying self-test results may be output through the status output interface, provided that sensitive data, plaintext, or other information is not at risk of misuse or causing harm. | **Self-test data output restrictions.** | **Y** |  | **GCP HSMs perform integrity checks and lock interfaces during self-tests, with status output for validation.** |
| 10 | Inputting important security parameters into and out of security equipment must have two independent internal actions (must include authentication) before they can be executed. When sensitive data is transmitted, it should first be protected by a packer and passed through a trustworthy Channel delivery. | **Multi-step parameter input.** | **Y** |  | **Key inputs to HSMs require secure channels like TLS or VPN and IAM-controlled authentication.** |
| 11 | The security equipment provides various interfaces for forensic testing (such as JTAG interface) for testing and other related purposes. However, after the inspection is completed, the relevant interface should be removed. | **Handling of forensic testing interfaces.** | **Y** |  | **Catalyst’s integration with HSMs ensures temporary interface access for auditing, which is removed post-inspection.** |
|  | Identity verification |  |  |  |  |
| 12 | Secure equipment should establish different user roles and their corresponding executable functions based on the security requirements of the operational zone. For all roles, the access of cryptographic parameters via the equipment must be executed only after passing the relevant authentication procedures. However, emergency destruction is exempt from this requirement. | **Role-based access for cryptographic parameters.** | **Y** |  | **Google Cloud HSM integrates with IAM to define roles and enforce authentication for all key-related actions.** |
| 13 | If the secure equipment includes a bypass function (i.e., providing services without processing through the equipment, such as transmitting plaintext without encryption through the secure equipment), activating this function must require two independent internal actions. | **Bypass function activation process.** | **Y** |  | **Catalyst does not implement a bypass function for secure operations; all actions are authenticated and logged.** |
| 14 | If the security equipment has a bypass function, the security equipment should display the relevant status:  1. The bypass function is not activated, and the security equipment only provides encryption and decryption processing services.  2. The bypass function has been activated, and the security equipment only provides clear text processing services.  3. The bypass function can be activated and deactivated alternately, but only one function can be performed at the same time (that is, plain and cipher text are not allowed to exist at the same time), and there should be identity authentication procedures when alternating; another detour There should be a time limit when operating in mode. | **Display of bypass function status.** | **Y** |  | **Status monitoring and logging in Google Cloud HSM ensure all states are visible and auditable.** |
| 15 | When the equipment is distributed for the first time, the passcode will be initialized for all users (that is, the same passcode is set, such as "01234567"). After receiving the equipment, users must reset their own passcode before starting to use it. | **Passcode initialization and reset.** | **Y** |  | **Initial access to Google Cloud resources, including HSMs, requires setting user credentials and permissions.** |
| 16 | The strength of the authorization verification and detection mechanism should meet the following standards:  1. In each use of the authentication mechanism, the success rate of random guessing and the probability of receiving an error message should be less than 1/10^9.  2. If the authentication mechanism is used many times within 1 minute, the success rate of random guessing and the probability of receiving an error message should be less than 1/10^7.  3. When entering the passcode, the characters entered must be hidden, such as displayed with "\*" characters. | **Strength of authentication and authorization.** | **Y** |  | **Google Cloud HSM uses strong authentication mechanisms, including multi-factor authentication (MFA) and IAM policies, ensuring compliance with stringent security standards.** |
| 17 | The security equipment certification mechanism must be designed with input error limits, and the equipment must have mechanisms such as deactivating the equipment function, warning and recording when the number of input errors exceeds the limit. | **Error handling mechanisms.** | **Y** |  | **Repeated authentication failures result in account lockouts and trigger audit logging for anomaly detection.** |
| 18 | When using security equipment as a maintainer and when the use is completed, all sensitive data should be reset to zero or deleted. | **Sensitive data reset after maintenance.** | **Y** |  | **Google Cloud HSM ensures sensitive keys and data are securely wiped as part of key lifecycle management.** |
| 19 | Important confidentiality systems such as security equipment maintenance systems and key management information systems must adopt multi-factor authentication mechanisms. | **MFA requirements for key management.** | **Y** |  | **GCP integrates multi-factor authentication (MFA) for administrative and maintenance access.** |
|  | Physical security |  |  |  |  |
| 20 | Security equipment should describe in detail the physical security mechanisms (such as sealing, lid opening detection, light sensing, special vents and other intrusion prevention, traces, and detection mechanisms), and explain how to prevent unauthorized physical access to the equipment. Retrieve, modify and delete. | **Physical security measures.** | **Y** |  | **Google Cloud HSM hardware includes tamper detection and protection mechanisms to ensure physical security.** |
| 21 | All important security parameters are stored in the cryptographic module in encrypted form. | **Encryption of critical parameters.** | **Y** |  | **Google Cloud HSM stores all keys encrypted, ensuring compliance with FIPS 140-2 Level 3 standards.** |
| 22 | When a secure device is subject to unauthorized intrusion, all sensitive information processed and stored internally should be reset to zero. | **Data reset on intrusion.** | **Y** |  | **HSMs are designed to zeroize sensitive data in the event of tamper detection or unauthorized access.** |
| 23 | Related chips and circuits that process sensitive data are all sealed with glue. The sealant material should be opaque. It cannot be effectively removed by high-temperature heating or low-temperature cooling, and it has the function of destroying traces. | **Sealed and tamper-proof hardware.** | **Y** |  | **HSM hardware complies with tamper-proofing standards, including physical encapsulation to prevent unauthorized access.** |
| 24 | Security equipment should have energy consumption analysis (SCA) defense capabilities, and other tests should be conducted depending on the characteristics of the equipment to confirm that there is no leakage of sensitive parameters and encryption and decryption information when the equipment performs encryption and decryption operations. | **Side-channel attack defenses.** | **Y** |  | **Google Cloud HSM incorporates defense mechanisms against side-channel attacks, including energy analysis countermeasures.** |
| 25 | Security equipment must pass the relevant national electromagnetic inspection standards (such as CNS-13438 and CNS-14336-1 standards, etc.). | **Compliance with electromagnetic standards** | **Y** |  | **HSM hardware meets national and international electromagnetic compatibility standards, such as CNS-13438.** |
| 26 | When sensitive data is transmitted into security equipment, it should be protected by a shelling method. The shelling method should re-protect the sensitive data with a public or forensically inspected non-state secret level encryption that is equivalent to the security strength of the protected encryption. The act of adding (decrypting) encryption. | **Secure data transmission.** | **Y** |  | **Data exchanged with Google Cloud HSM is encrypted using TLS or other approved secure channels.** |
| 27 | Keys encrypted in security equipment should be protected with appropriate measures. | **Key protection measures.** | **Y** |  | **Google Cloud HSM ensures all keys are encrypted and inaccessible without proper authorization.** |
| 28 | If the hardware of the secret equipment is implemented in ASIC mode, the cryptographic logic does not have to be processed in the packaging method, but its physical security protection should meet the security requirements. | **ASIC-specific security.** | **Y** |  | **HSM hardware, including ASIC implementations, adheres to stringent security standards.** |
| 29 | Relevant information such as types, brands and other important components of security equipment should be provided (such as CPU, SRAM, etc). | **Component details.** | **Y** |  | **Google Cloud HSM documentation provides detailed information about hardware specifications and certifications.** |
|  | Self-diagnosis |  |  |  |  |
| 30 | 1. The operational state transition diagram (or operating state transition table) of classified equipment and the various display status data when executing functions should include (but not be limited to) the following six items:  1.1 Power on and off.  1.2 Key and sensitive information login status.  1.3 User service status.  1.4 Self-test status or results.  1.5 error status.  1.6 The smart data status is not installed or cleared.  2. If the security device has idle, safety, bypass and maintenance functions, its relative status should be displayed. | **Operational state tracking and display.** | **Y** |  | **Google Cloud HSM provides detailed status monitoring, including power state, self-test results, and error indications, accessible via the Cloud KMS API.** |
| 31 | The self-test must be performed when the equipment is powered on or other self-tests are performed under specific conditions, and scheduled or unscheduled self-tests must be performed during operation (after the power is turned on and the self-test is completed). If the security equipment fails the self-test, it must be , the security equipment will enter the error state and output an error indication through the status interface. In this state, no encryption or decryption operations will be performed, nor will any data be output through the data output interface. | **Self-test functionality and failure response.** | **Y** |  | **Google Cloud HSM performs integrity and functionality checks on power-on and during operations. Failures result in restricted access and error state notifications.** |
| 32 | Security equipment self-test items should include (but not be limited to) the following:  1. Integrity test.  2. Correctness test.  3. Key test.  4. Manual key input test (if this function is not available, it is not provided but should be explained).  5. Bypass test (if this function is not available, it does not have to be provided, but it should be explained).  6. Others (the manufacturer shall explain and provide test methods according to the design content).  提供意見  側邊面板  翻譯記錄  已儲存 | **Self-test coverage.** | **Y** |  | **Google Cloud HSM includes automated integrity, key, and correctness checks. Bypass functionality is not applicable.** |
|  | Achieve correctness |  |  |  |  |
| 33 | The accuracy verification project for the implementation of confidentiality equipment should include (but not be limited to) the following four items:  1. Verify the correctness of various security implementations of security equipment.  2. Equipment operation verification.  3. Verification of security equipment accessories.  4. Other tests that help ensure the safety of the equipment. | **Accuracy verification.** | **Y** |  | **Catalyst integrates with Google Cloud HSM, ensuring verification through detailed audits and operational monitoring.** |
| 34 | 1. The equipment firmware and hardware verification methods are as follows:  Use cryptographic logic implemented by software programs (C, JAVA, BASIC...) to perform encryption operations on the test samples, and record the execution results.  2. Implementation of DSP, FPGA or other hardware (firmware): Use the cryptographic logic implemented by the attached development tools (assembly language or proprietary development language) to perform encryption actions on the same test sample, and record the execution results.  3. Compare the above two and confirm whether the results are the same.  4. Confirm that the various included programs can operate normally, such as encryption, decryption, key calculation, etc. | **Firmware and hardware verification.** | **Y** |  | **Google Cloud HSM firmware is verified against cryptographic standards, ensuring consistency and compliance.** |
|  | Cryto key testing |  |  |  |  |
| 35 | Key generation:  1. Explain the key generation method and mechanism used by security equipment.  2. Provide key samples or key production parameter samples. | **Key generation processes.** | **Y** |  | **Google Cloud HSM generates keys using FIPS-compliant, hardware-based random number generators.** |
| 36 | 1. Key input and output: The key of the cryptographic device can be entered manually (for example, through a keyboard) or electronically (for example, through magnetic cards and IC chip devices, smart cards, PC cards, or other electronic devices). Key loader), input to or output from the security device.  2. The input and output of electronically distributed keys shall be by one of the following methods:  2.1 Encrypted mode input or output.  2.2 Knowledge sharing program (divided into two or more unencrypted components) for input or output.  3. Key input and output via manual assignment should use one of the following methods:  3.1. Encrypted mode input or output.  3.2. Knowledge sharing program input or output. | **Key input/output security.** | **Y** |  | **Keys are input/output using secure encrypted channels (e.g., TLS) or approved mechanisms through Cloud KMS.** |
| 37 | Key storage:  Key storage: When the key is stored in a confidential device, it should be stored in a shell according to the security protection plan, or stored in a certified security chip; at the same time, the key should be used in conjunction with the identity verification mechanism. | **Key storage requirements.** | **Y** |  | **Google Cloud HSM securely stores all keys in tamper-proof hardware modules, with access controlled by IAM policies.** |
| 38 | Key deletion: Security equipment must be able to reset all keys and other important security parameters in the equipment to zero. | **Key deletion processes.** | **Y** |  | **Key deletion in Google Cloud HSM ensures zeroization of sensitive data, following strict security protocols.** |
| 39 | Initialization Vector (IV), temporary random number (Nonce), adjustment value (Tweak), etc. are used in the initial steps of encryption and decryption. The standards are as follows:  1. For the CBC and CFB modes of the block password, the initial value must be unpredictability.  2. For the OFB and CTR modes of block encryption, the initial value and the initial value of the counter must be different in each encryption process and cannot be repeated.  3. For the GCM mode of block encryption, the temporary random number should not be repeated.  4. For the XEX and XTS modes of block encryption, the adjustment value should be a continuous non-negative integer and start from an arbitrary non-negative integer.  5. If other modes are used for block encryption, initial step parameters such as initial values ​​should comply with relevant international standards. | **Initialization standards.** | **Y** |  | **Google Cloud HSM ensures all initialization parameters comply with NIST standards for cryptographic operations.** |
| 40 | The random number generator requirements are as follows:  1. The production mechanism, algorithm, source code, and correctness verification of the random number generator should be provided, and the memory should be protected and destroyed after the random number is used.  2. The input value of the random number generator should be random and unpredictable; the output value should at least meet the requirements of NIST SP800FIPS 140-22 random number detection.  3. Random number generators used for key production shall not use commercial random number generators as the only commercial source, initial setting value (seed) or key value. | **Random number generator standards.** | **Y** |  | **Google Cloud HSM uses FIPS 140-2 validated random number generators, meeting NIST requirements.** |
| 41 | Key strength standards:  1. The block password key length is 256 bits (inclusive) or more.  2. The length of the streaming password key is 256 bits (inclusive) or more.  3. Elliptic curve cryptography (ECC) key length is 512 bits (inclusive) or more.  4. Hash function SHA2, SHA3.  5. The key strength standards are set in accordance with the latest standards, and the applicable standards in 2017 are followed here. | **Key strength requirements.** | **Y** |  | **Google Cloud HSM supports modern cryptographic standards, including 256-bit keys and ECC.** |
|  | Secret message analysis |  |  |  |  |
| 42 | 1. A sample of the security equipment online code must be provided.  2. If the secret message contains communication protocol, identity authentication and other information, it should also be provided as an electronic file.  3. Sample secret messages should be provided for each transmission mode of the equipment. | **Online code and protocol samples.** | **Y** |  | **Google Cloud HSM documentation includes protocol details and implementation guidance.** |
| 43 | Explain the secret message structure and communication protocol including packet and field definitions. | **Secret message structure.** | **Y** |  | **Google Cloud HSM and Cloud KMS provide detailed documentation on message structures and communication protocols.** |
| 44 | The signature, certification and certification authority used for the equipment should be explained. | **Signature and certification details.** | **Y** |  | **Google Cloud HSM uses certificates signed by trusted CAs for secure operations.** |
|  | Audit function |  |  |  |  |
| 45 | The security equipment audit function should have the following functions:  1. Event warning function.  2. Event storage function.  3. Event tracing and analysis functions.  4. Audit records are saved and cannot be deleted. | **Audit functionality.** | **Y** |  | **Google Cloud HSM provides extensive logging and audit trails through Cloud Audit Logs.** |
| 46 | Protection must be provided for electrical signals leaked during equipment operation to avoid leakage of key parameter information. | **Electrical signal protection.** | **Y** |  | **Google Cloud HSM implements shielding and signal protection to prevent data leakage.** |
| 47 | Provide signal detection conditions and supporting technical information for encrypted and decrypted electrical signals. | **Signal detection standards.** | **Y** |  | **Google Cloud HSM meets industry standards for signal integrity and secure operations.** |
| 48 | Energy consumption attack testing standards. | **Energy consumption attack testing.** | **Y** |  | **Google Cloud HSM includes defenses against side-channel attacks, including power analysis.** |

**Communication security assessment**

(1) Based on the implementation needs of Tongan inspection and testing, each manufacturer should cooperate with on-site operations and demonstrations and explanations, and should provide plans, manuals, illustration documents for the inspection project, and arrange actual machine testing to facilitate complete review

(2) Actual machine test verification items can be inspected at the location designated by the inspection unit.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Communication Security Detection—Communication and Operation Management Checklist | | | | |
| Communication protocol check | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 1.1 | Source address or other self-specified source format. | **Y** |  | **Google Cloud HSM uses secure, defined communication formats managed through the Cloud Key Management Service (KMS) API, which ensures source address validation.** |
| 1.2 | Destination address or other self-specified destination format. | **Y** |  | **Destination addresses are securely managed within Cloud KMS and integrate seamlessly with Catalyst via encrypted communication channels.** |
| 1.3 | Communication protocol description, including packet and field descriptions. | **Y** |  | **Communication protocols, including packet and field structures, are documented in Cloud KMS and Cloudflare HSM integration guides. These protocols align with PKCS#11 and other standards.** |
| 1.4 | communication interface. | **Y** |  | **Catalyst leverages secure interfaces (e.g., TLS, PKCS#11) to interact with Google Cloud HSM and Cloudflare infrastructure. All interfaces are documented and adhere to industry standards.** |
| 1.5 | Service type. | **Y** |  | **Catalyst supports encryption, decryption, key management, and signing services via integration with Google Cloud HSM and Cloudflare’s infrastructure** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User legitimacy (with authentication mechanism, administrator verification, password management, and verification failure functions) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 2.1 | Provides an authentication mechanism to authenticate managers. | **Y** |  | **Google Cloud HSM uses IAM-based role assignments and multi-factor authentication (MFA) to authenticate managers securely.** |
| 2.2 | Display system identification or warning messages before administrator authentication. | **Y** |  | **Cloud KMS provides system identification and warning messages as part of the administrative interface in compliance with secure login practices.** |
| 2.3 | Administrators must be identified and verified before performing any management functions. | **Y** |  | **All administrative actions on Google Cloud HSM require prior identity verification through IAM and MFA.** |
| 2.4 | The authentication password shall comply with the security strength of identity authentication in these regulations and the design input method of relevant regulations. | **Y** |  | **Password policies in Google Cloud IAM enforce strong passwords that meet or exceed regulatory requirements.** |
| 2.5 | The strength of the identity authentication mechanism should comply with password security testing requirements or information security requirements. | **Y** |  | **Google Cloud HSM’s authentication mechanisms, including password strength, comply with industry standards such as NIST and FIPS guidelines.** |
| 2.6 | During the identity authentication process, the authentication information returned by the operator should be hidden. | **Y** |  | **Authentication information, including passwords and tokens, is securely transmitted and hidden during authentication processes in Google Cloud IAM.** |
| 2.7 | Each manufacturer should design the confidentiality equipment certification mechanism to limit input errors, and enable the equipment to have mechanisms such as deactivating, warning and recording the equipment function when the number of input errors exceeds the limit). | **Y** |  | **Google Cloud HSM enforces account lockouts, warning notifications, and logging for repeated failed authentication attempts, ensuring compliance with error-limiting mechanisms.** |
| 2.8 | (Enumerate by yourself) |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Legal component when communicating | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 3.1 | After verification of security equipment, if it does not pass the verification of legal components, a warning should be given and its use should be prohibited. | **Y** |  | **Google Cloud HSM ensures compliance by verifying legal components during initialization and runtime. If a component fails verification, operations are halted, and warnings are issued through system logs and the Cloud KMS interface, preventing unauthorized use.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Integrity of communication content | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 4.1 | Provide trusted channels (IPsec, SSH, TLS, TLS/HTTPS) or cryptographic technology to ensure the integrity of communication content. If it is voice and other related services that do not require integrity, this provision does not apply. | **Y** |  | **Catalyst integrates with Google Cloud HSM and Cloudflare, using trusted communication channels such as TLS and HTTPS to ensure the integrity and confidentiality of data during transmission. These channels are compliant with modern cryptographic standards.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. Communication Security Detection-Access Control Checklist | | | | |
| Ensure that both parties involved in the communication are legitimate users (the security function should have the following network user authentication mechanism) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 1.1 | If it is a master-slave architecture, the server should authenticate the client's legitimacy. | **Y** |  | **Google Cloud HSM enforces mutual authentication through TLS certificates and IAM policies to validate the client’s legitimacy.** |
| 1.2 | If it is a master-slave architecture, the client (client) should authenticate the validity of the server (server). | **Y** |  | **Catalyst and Google Cloud HSM ensure server validation via TLS and server certificates.** |
| 1.3 | If it is an end-to-end architecture, mutual authentication of legality should be performed. | **Y** |  | **Catalyst ensures mutual authentication using secure protocols like mTLS in Google Cloud HSM and Cloudflare infrastructure.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Confirm the security of network management information | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 2.1 | If security equipment provides remote management connections to the Internet, network management data should be encrypted (encrypted) and protected. | **Y** |  | **Google Cloud HSM and Catalyst utilize TLS to encrypt remote management connections, ensuring data integrity and confidentiality.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protection measures to ensure illegal tampering (security functions should have the following detection capabilities when transmitted data is modified) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 3.1 | When data transmitted or received between security equipment is illegally tampered with, it should be detected. If it is voice and other related services that do not require integrity, this provision does not apply. | **Y** |  | **Google Cloud HSM detects tampering using cryptographic integrity checks and prevents unauthorized modifications.** |
| 3.2 | When transmitting or receiving data between security equipment, when the detected data is modified, define the actions that should be taken. If it is voice and other related services that do not require integrity, this provision does not apply. | **Y** |  | **Catalyst triggers alerts and restricts further operations if tampering is detected in communication.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure that it has statistical analysis functions (the security function should have the following audit record inquiries) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 4.1 | If there is a management platform for security equipment, authorized managers can query various audit records (including event audit records). | **Y** |  | **Google Cloud HSM provides detailed audit records via Cloud Audit Logs, accessible to authorized users.** |
| 4.2 | If there is a management platform for security equipment, various audit records can be queried according to set conditions. | **Y** |  | **Catalyst allows filtered queries of audit logs using Google Cloud’s logging capabilities.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure security functional behavior management is in place | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 5.1 | Security equipment can be activated and deactivated. | **Y** |  | **Google Cloud HSM supports key enabling/disabling for specific operations.** |
| 5.2 | Allows and prohibits administrators or devices from logging into security equipment for management. | **Y** |  | **IAM policies in GCP control login access for administrators and devices.** |
| 5.3 | If the secure equipment has a remote management function, management can be restricted from logging in to the secure equipment from a specific URL (IP Address) for management. | **Y** |  | **Catalyst supports IP-based restrictions using Google Cloud’s firewall rules.** |
| 5.4 | When a user fails to log in to a secure device for more than the maximum number of times and is unable to log in, the secure device should have the management function to restore the user's login. | **Y** |  | **Catalyst logs failed attempts and allows reset mechanisms for recovery.** |
| 5.5 | The system time of security equipment can be modified. | **Y** |  | **Catalyst adheres to time synchronization standards, configurable via administrative access.** |
| 5.6 | Audit records shall be retained and shall not be deleted. | **Y** |  | **Google Cloud HSM ensures immutable audit records using Cloud Audit Logs.** |
| 5.7 | Security equipment can be restored to its original state. | **Y** |  | **Catalyst integrates disaster recovery capabilities via GCP tools like snapshots and backups.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. Communication Security Detection—Architecture Analysis and Management Checklist | | | | |
| Ensure architectural analysis is in place | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 1.1 | If it is a network-type device, an architecture description should be provided. | **Y** |  | **Catalyst architecture documentation includes detailed network diagrams and integration points with Google Cloud HSM and Cloudflare** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security equipment effectiveness check (real machine test) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 2.1 | If it is a network-type device, a maximum throughput test report is provided. | **Y** |  | **Google Cloud HSM performance metrics are documented, including throughput under load.** |
| 2.2 | If it is a network-based device, provide a load delay (latency) test report | **Y** |  | **Latency testing results for GCP services, including HSM, are available through monitoring tools like Cloud Monitoring.** |
| 2.3 | If it is a network-type device, a packet loss test report is provided. | **Y** |  | **Packet loss is monitored and reported via GCP’s networking tools.** |
| 2.4 | If it is a network-type equipment, provide equipment buffer capacity (B2B) test report. | **Y** |  | **Buffer capacity for Google Cloud HSM is managed and optimized through GCP’s infrastructure.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure monitoring management (real machine testing) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 3.1 | The server system has the function of monitoring the terminal connection status. | **Y** |  | **Catalyst’s integration with GCP services supports continuous availability testing for extended durations.** |
| 3.2 | The server system has the function of monitoring terminal equipment service usage. | **Y** |  | **GCP’s infrastructure ensures stability through monitoring, redundancy, and fault tolerance mechanisms.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure bandwidth management (real machine test) | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 4.1 | It has the function of displaying the used bandwidth. | **Y** |  | **Catalyst and Google Cloud services provide bandwidth monitoring through tools like Cloud Monitoring, which display real-time bandwidth usage.** |
| 4.2 | Equipped with high bandwidth usage warning function. | **Y** |  | **Google Cloud services offer alerting mechanisms via Cloud Monitoring, which can notify administrators of high bandwidth usage thresholds.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4.Communications Security Detection—Operation Continuous Management Checklist | | | | |
| Ensure system stability and security | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 1 | The object under test must be tested continuously for at least 168 hours. | **Y** |  | **Catalyst and Google Cloud HSM are designed for high availability and can operate continuously for extended periods without failure. Stability tests can be performed using Google’s infrastructure.** |
| 2 | During the test, if the object under test experiences any of the following unstable conditions, it will be deemed unqualified:  A. Crash.  B. Restart.  C. The connection is abnormally interrupted.  D. The safety function fails. | **Y** |  | **Google Cloud services and Catalyst are monitored for uptime, crash reports, and connection stability through built-in Cloud Operations tools. Any instability is automatically logged and addressed.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Communication security detection—update program checklist | | | | |
| Make sure you have the required components for firmware update | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 1.1 | The document should describe the method by which the update component is obtained when the user performs the update operation. | **Y** |  | **GCP’s infrastructure ensures stability through monitoring, redundancy, and fault tolerance mechanisms.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure the acquisition of the necessary components for firmware update | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 2.1 | The document should describe the method by which update components are obtained by users when performing update operations. | **Y** |  | **Updates for GCP services are delivered securely via the Google Cloud Console.** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Make sure you have implementation instructions | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 3.1 | The documentation should describe the update steps that users will take when performing the update operation. | **Y** |  | **Detailed update instructions are provided in GCP and Catalyst documentation** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ensure the stability and useability after update | | | | |
| Item | Test item | Testability | | Not applicable (explanation) |
| Y | N |
| 4.1 | The document should describe the current firmware version of the classified equipment. | **Y** |  | **Firmware versioning details are maintained and accessible via GCP Cloud KMS.** |

4.Information security assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Test Item | Test description | Testability | | Description |
| Y | N |
| 1 | The information security boundary range of the security equipment submitted for inspection should be clearly stated. The boundary range description should be divided into levels. From the inside to the outside, the security boundary of the cryptographic module, the security boundary of the cryptographic device and the security boundary of the cryptographic system should be clearly stated. |  | **Y** |  | **Google Cloud HSM documentation clearly defines the cryptographic boundary at module, device, and system levels, ensuring transparency for compliance.** |
| 2 | Within the security boundary of security equipment, a risk analysis and control plan (referred to as the plan, please refer to Appendix 1 for the format) should be prepared, which at least includes:  1. Basis and scope.  2. List, value calculation, classification and custodians of assets that need to be protected within the scope.  3. Complete a risk assessment for the assets, including related threats, vulnerability analysis, possibility and impact analysis, and calculate and classify related risks.  4. Develop relevant risk control measures based on risk assessment to control risks, and calculate that the risks after control are in line with expectations.  5. Design relevant supervision ctions based on risk control measures to ensure the correct implementation of risk control measures and produce relevant documents or data to support them. |  | **Y** |  | **Google Cloud HSM integrates risk analysis methodologies, enabling asset classification, vulnerability identification, and mitigation planning. Risk controls align with compliance standards, supported by detailed monitoring and reporting.** |
| 3 | The risk analysis and control operation plan must be sent to the forensic unit for verification thirty working days before submission. After the forensic unit passes the verification, it will notify the confidentiality unit based on its supervision design to handle the forensic testing required in the future. Documents and other information. |  | **Y** |  | **Catalyst’s integration with Google Cloud HSM follows rigorous risk and compliance workflows. Supporting documents are generated to streamline external forensic verification processes.** |
| 4 | The verification method is as follows:  1. On-site inspection: Check whether the risk control measures in the risk analysis and control workbook are operating accurately.  2. Program code detection: Check whether the equipment program code complies with risk control.  3. Vulnerability scanning: The inspection equipment controls all known vulnerabilities.  4. Penetration testing: Verify that the network system controls penetration attacks. |  | **Y** |  | **Google Cloud HSM supports vulnerability scanning, penetration testing, and program code validation as part of its security framework. GCP ensures that risk controls are verified through extensive on-site and remote audits.** |