PassQueen
a.k.a dumpsqueen.com

Customer Security Programme Assessor Certification

Swift CSP-Assessor

Version Demo

Total Demo Questions: 15

Total Premium Questions: 151

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which statements correctly describe Alliance Gateway and Alliance Lite2 capabilities? (Select the two correct answers that apply)

A. Alliance Gateway acts as a single window to SWIFTNet messaging services by concentrating traffic flows.

B. Alliance Gateway is used to create and modify SWIFT messages in the same way as a messaging interface.

C. Alliance Lite2 requires a customer-operated HSM box as a key component.

D. Alliance Lite2 includes a web interface and can use AutoClient for automated exchange with local applications.

ANSWER: A D

Explanation:

Alliance Gateway acts as a central connectivity point by concentrating traffic flows to SWIFTNet messaging services. It is a connectivity and integration component, rather than a messaging interface used to create or modify SWIFT messages.

Alliance Lite2 provides a web interface for operational messaging activities and can use AutoClient to support automated exchange with a customer's local environment. A customer-operated HSM box is not a key Alliance Lite2 component in the same way as it is for certain on-premises SWIFT architectures.

QUESTION NO: 2

Swift requests assessment evidence from a CSP Certified Assessor as part of its quality assurance validation process. Which actions are appropriate? (Select the two correct answers that apply)

A. Refuse the request because assessment evidence is always confidential.

B. Provide the requested evidence in accordance with the certification programme obligations.

C. Use a secure method and limit the shared information to what is required for the validation.

D. Provide only the Assessment Completion Letter because Swift cannot request supporting evidence.

ANSWER: B C

Explanation:

A CSP Certified Assessor is expected to cooperate with Swift's quality assurance activities, including providing evidence relating to an assessment where requested. Quality assessment is an obligation associated with participation in the certification programme and supports consistent assessment quality.

Evidence must still be handled securely and limited to the information requested for the quality validation purpose. Confidentiality obligations require appropriate handling, but they do not automatically prevent the assessor from providing evidence to Swift for a valid programme quality review.

QUESTION NO: 3

When hesitant on the applicability of a CSCF control to a particular component? What steps should you take? (Choose all that apply.)

A. Call your Swift contact

B. Check appendix F of the CSCF

C. Check carefully the Introduction section of the CSCF

D. Open a case with Swift support via the case manager on swift com if further information or solution cannot be found in the documentation

ANSWER: B C D

Explanation:

“Check appendix F of the CSCF,” “Check carefully the Introduction section of the CSCF,” and “Open a case with Swift support via the case manager on swift com if further information or solution cannot be found in the documentation” reflect the appropriate escalation path for uncertainty about a Customer Security Controls Framework control’s applicability. The CSCF must first be interpreted in the context of the customer’s architecture, the component’s role, and the framework’s stated scope. The Introduction provides the foundational applicability principles, definitions, and implementation context needed to determine whether a component is in scope. Appendix F provides supporting applicability guidance and helps customers apply the framework consistently to particular environments and components.

If these authoritative framework sections do not resolve the question, submitting a case through Swift’s support channel is appropriate. This creates a documented request for clarification and allows Swift to provide guidance based on the customer’s specific circumstances. Using the documentation first, followed by Swift Support when necessary, supports a well-evidenced and defensible applicability decision during an independent assessment. Swift publishes the current framework and related customer-security materials through its Customer Security Controls Framework page; support requests are managed through the MySwift Support portal.

QUESTION NO: 4

An Internal Audit function performs the independent assessment of a Swift user's attested CSCF controls. The business team asks Internal Audit to submit the attestation in KYC-SA because the auditors know the assessed controls best. What should the assessor advise?

A. Internal Audit may submit the attestation if the CISO performs the final approval

B. Internal Audit may submit the attestation when it assessed all mandatory controls

C. Internal Audit must not submit or approve the user's attestation

D. Internal Audit may submit the attestation if the Head of Internal Audit authorises it

ANSWER: C

Explanation:

Internal Audit must retain its independence from the operational attestation activity. Submitting or approving the user's KYC-SA attestation is a customer governance responsibility, whereas Internal Audit may independently assess the controls and provide assurance over the reported posture. Combining these activities would compromise the required separation between control ownership, attestation, and independent review.

Appropriate portal credentials or approval from management do not resolve this independence conflict. The customer remains accountable for submitting and approving its own attestation through its authorised operational representatives.

QUESTION NO: 5

On which one of the following components must a Password/PIN Policy not be defined and implemented as per the CSCF? (Select the correct answer)

• Swift Customer Security Controls Policy

• Swift Customer Security Controls Framework v2025

• Independent Assessment Framework

• Independent Assessment Process for Assessors Guidelines

• Independent Assessment Framework - High-Level Test Plan Guidelines

• Outsourcing Agents - Security Requirements Baseline v2025

• CSP Architecture Type - Decision tree

• CSP_controls_matrix_and_high_test_plan_2025

• Assessment template for Mandatory controls

• Assessment template for Advisory controls

A. Operator PCs, (physical or virtual) systems running SWIFT-related components, network devices protecting the secure zone(s), bridging servers

B. Jump server(s), SWIFT-related components at application level

C. Personal tokens or mobile devices used as a possession factor

D. All equipment within the user environment

ANSWER: C

Explanation:

Personal tokens or mobile devices used as a possession factor is correct. The CSCF password/PIN-policy requirement is intended to ensure that passwords and PINs used to access in-scope SWIFT environment components are governed by documented rules. Those rules address matters such as credential strength, protection, change or reset processes, reuse, and account-access safeguards. Consequently, the policy must cover systems and devices on which users or administrators authenticate to operate, administer, protect, or access the SWIFT environment, including relevant endpoints, servers, network-security devices, jump hosts, and SWIFT application components.

A personal token or mobile device used solely as the possession element of multi-factor authentication has a different security role. It evidences something the user possesses, rather than being a target system for which the CSCF requires a Password/PIN Policy. The associated authentication process must still be securely designed and managed, but the device or token itself is outside the specific Password/PIN Policy scope described by this requirement. This distinction prevents the policy scope from being interpreted as every item a user may carry or use during authentication.

The applicable control requirements and CSP documentation are published through Swift's Customer Security Controls Framework. Swift also provides CSP context and security guidance at its Customer Security Programme page.

QUESTION NO: 6

Which ones are Alliance Lite2 key components? (Choose all that apply.)

A. A web interface

B. An AutoClient

C. A HSM box

D. A WebSphere MQ Server

ANSWER: A B

Explanation:

Alliance Lite2 provides a secure, browser-based connectivity solution for Swift users. "A web interface" is a key component because users access the Alliance Lite2 service through a web browser to perform operational activities, including creating, reviewing, authorising, and monitoring financial messages. This browser-based access model is central to the product's

design and supports institutions that require Swift connectivity without operating the larger on-premises infrastructure associated with other interfaces.

“An AutoClient” is also a key Alliance Lite2 component. The AutoClient supports automated exchange of files and messages between the institution’s local environment and Alliance Lite2, enabling integration with back-office applications and support for straight-through processing. Although an institution may use it according to its automation and integration needs, it is an Alliance Lite2 component provided for this purpose and is therefore correctly included in the component set.

Swift describes Alliance Lite2 as a secure, cloud-based connectivity offering that combines browser access with capabilities for integrating local applications. Product information is available from Swift’s Alliance Lite2 product page. The security obligations applicable to Swift users and their relevant architectures are set out through the Swift Customer Security Programme.

QUESTION NO: 7

A recipient receives a message protected with a digital signature created by the sender. Which key is used to verify that signature?

A. The receiver’s signing private key.

B. The sender’s signing private key.

C. The receiver’s encryption public key.

D. The sender’s signing public key.

ANSWER: D

Explanation:

The recipient verifies a digital signature using the sender’s signing public key. The sender created the signature using the corresponding signing private key. This asymmetric process enables the recipient to validate the origin and integrity of the signed data without access to the sender’s private key.

The receiver’s encryption private key is used for decryption of information encrypted for the receiver; it is not used to verify a sender’s signature.

QUESTION NO: 8

What are the conditions required to permit reliance on the compliance conclusion of a control assessed in the previous year? (Choose all that apply.)

A. The control compliance conclusion must have already been relied on the past two years

B. The previous assessment was performed on the (correct) CSCF version of the previous year

C. The control definition has not changed

D. The control-design and implementation are the same

ANSWER: B C D

Explanation:

Reliance on a prior-year compliance conclusion is permitted only where that conclusion remains applicable to the control being attested in the current assessment cycle. The previous assessment must have been performed against the correct CSCF version for the previous year. This establishes that the conclusion was reached using the framework requirements that governed that earlier assessment and provides a valid baseline for considering reliance.

The control definition must also not have changed. A conclusion can be carried forward only when it relates to the same control requirement, including its objective and the elements that the assessor is required to evaluate. In addition, the control

design and implementation must be the same. This confirms that the architecture, processes, technical configuration, and operating arrangements on which the earlier conclusion was based continue to apply. Together, these conditions allow an assessor to determine that the earlier conclusion is still relevant, while retaining responsibility for validating that no material changes affect compliance. Swift describes the Customer Security Controls Framework and assessment approach within its Customer Security Programme resources: Swift Customer Security Programme and Customer Security Controls Framework.

QUESTION NO: 9

Can an assessor re-use an ISAE 3000 report dating back 2 years to support an independent assessment?

A. No, that is too old, the maximum is 18 months

B. Yes, there is no time limit for an iSAE 3000 report

C. No, the SAE 3000 report is no validsurrogateas a rule

D. Yes, provided there is no change to the Swift user's infrastructure

ANSWER: A

Explanation:

No, that is too old, the maximum is 18 months. Under the SWIFT Customer Security Programme assessment approach, an ISAE 3000 assurance report may support an independent assessment when its scope and assurance work provide suitable evidence for the relevant SWIFT Customer Security Controls Framework requirements. However, its age is expressly limited: the report must not be more than 18 months old at the time it is used for the CSP assessment. A report issued two years earlier exceeds this permitted evidence-reuse window and therefore cannot be relied upon as the supporting ISAE 3000 report for the current independent assessment. The 18-month limit helps ensure that the assessment evidence remains sufficiently current and reflects the user’s security-control environment during the applicable CSP assessment cycle. The assessor should obtain more recent independent assurance evidence, or perform the necessary assessment procedures, so that the CSP attestation is based on evidence within the accepted timeframe. SWIFT describes the CSP and its assessment expectations at SWIFT Customer Security Programme and provides programme resources through the CSP Assessment Framework.

QUESTION NO: 10

Is the restriction of Internet access only relevant when having SWIFT-related components in a secure zone?

• Swift Customer Security Controls Policy

• Swift Customer Security Controls Framework v2025

• Independent Assessment Framework

• Independent Assessment Process for Assessors Guidelines

• Independent Assessment Framework - High-Level Test Plan Guidelines

• Outsourcing Agents - Security Requirements Baseline v2025

• CSP Architecture Type - Decision tree

• CSP_controls_matrix_and_high_test_plan_2025

• Assessment template for Mandatory controls

• Assessment template for Advisory controls

A. Yes, because if there is no secure zone, then the internet connectivity does not need to be restricted

B. No, because there can be in-scope general operator PCs used to access a SWIFT-related application hosted at a service provider

ANSWER: B

Explanation:

No, because there can be in-scope general operator PCs used to access a SWIFT-related application hosted at a service provider. The applicability of Internet-access restrictions is determined by whether a component is within the SWIFT environment and performs a relevant SWIFT function, rather than solely by the presence of customer-operated SWIFT infrastructure in a secure zone. For example, where a SWIFT-related application is hosted by a service provider, the customer's general-purpose operator PCs may still be used to access that application, process SWIFT-related information, or use credentials that enable SWIFT activity. These endpoints are therefore relevant to the CSP assessment scope and require appropriate protection against Internet-borne threats.

The Customer Security Controls Framework uses a risk-based architectural scope: outsourced or hosted deployment does not remove the customer's responsibility for securing its own in-scope access points. Restricting unnecessary Internet connectivity on operator PCs reduces exposure to malware, credential theft, malicious downloads, and browser-based compromise that could affect SWIFT operations. The assessor should consequently establish whether such operator PCs are in scope and verify that Internet access is restricted or otherwise controlled in line with the applicable control objectives and documented architecture. Swift's CSP resources and framework information are available at Swift Customer Security Programme and Customer Security Controls Framework.

QUESTION NO: 11

Who can connect to SWIFT? (Select all answers that apply)

•Connectivity

•Generic

•Products Cloud

•Products OnPrem

•Security

A. Financial institutions, such as banks and securities broker-dealers

B. Individuals who use online banking for international transfers

C. Market infrastructures that provide financial institutions with centralized transaction processing

D. Corporates that work with multiple banking partners

ANSWER: A C D

Explanation:

Financial institutions, such as banks and securities broker-dealers, can connect to SWIFT because SWIFT's services support regulated institutions in exchanging financial messages and using related services across payments, securities, treasury, and trade workflows. These institutions form the core community that uses SWIFT connectivity directly or through an appropriate service arrangement. SWIFT describes its community as including banks and other financial institutions that rely on its secure communication and messaging capabilities.

Market infrastructures that provide financial institutions with centralized transaction processing can also connect. Financial market infrastructures—including payment systems, clearing entities, and securities market infrastructures—use SWIFT services to support interoperable, resilient communication with their participants and counterparties. Their role in centralized processing makes them established users of financial-network connectivity.

Corporates that work with multiple banking partners can connect through SWIFT's corporate connectivity offerings. SWIFT for Corporates is designed to help corporates standardize and centralize their bank communication, including payment and reporting flows, across multiple banking relationships. This enables a corporate treasury function to communicate with its banks using SWIFT services rather than being limited to separate proprietary bank channels.

These user groups are reflected in SWIFT's descriptions of its global community and its corporate solutions. See SWIFT overview and SWIFT for Corporates.

QUESTION NO: 12

As a SWIFT CSP Certified Assessor, my external cybersecurity certification (example: CISA) has expired. Am I still allowed to work as a certified assessor?

• Swift Customer Security Controls Policy

• Swift Customer Security Controls Framework v2025

• Independent Assessment Framework

• Independent Assessment Process for Assessors Guidelines

• Independent Assessment Framework - High-Level Test Plan Guidelines

• Outsourcing Agents - Security Requirements Baseline v2025

• CSP Architecture Type - Decision tree

• CSP_controls_matrix_and_high_test_plan_2025

• Assessment template for Mandatory controls

• Assessment template for Advisory controls

• CSCF Assessment Completion Letter

• Swift_CSP_Assessment_Report_Template

A. No, a valid external cybersecurity certification is mandatory to keep the CSP Certified Assessor certification

B. Yes, if the SWIFT CSP Assessor certification is still valid

ANSWER: A

Explanation:

No, a valid external cybersecurity certification is mandatory to keep the CSP Certified Assessor certification. Swift's independent-assessment arrangements are designed to ensure that assessors remain demonstrably qualified throughout the period in which they perform Customer Security Controls Framework assessments. A current, recognised external professional cybersecurity qualification—such as CISA—is an eligibility condition, not merely evidence supplied when first applying for Swift assessor certification. Consequently, when that underlying certification expires, the assessor no longer meets the qualification requirement for acting as a Swift CSP Certified Assessor until the external credential is renewed and the assessor's eligibility is restored in accordance with Swift's process.

This continuing-validity requirement supports the reliability and independence of CSP assessments: assessors are expected to maintain current professional standing, including any continuing-professional-education and renewal obligations associated with their external certification. The customer and Swift must be able to rely on the assessor's credentials at the time an assessment is conducted and reported, rather than solely on the expiry date of a previously issued Swift credential. Swift describes the independent assessment model and assessor-related resources within its Customer Security Programme at Swift Customer Security Programme. The programme's control and assessment documentation is available through MySwift CSP resources.

QUESTION NO: 13

Which authentication methods are possible on the Alliance Interfaces? (Choose all that apply.)

A. Password

B. LDAP Authentication

C. Radius One-time password

D. Password and TOTP

ANSWER: A B C D

Explanation:

Alliance Interfaces support several configurable authentication mechanisms so that institutions can align operator access with their local identity-management architecture and security policy. **Password** is available for locally managed user authentication. **LDAP Authentication** enables the interface to use an organisation's directory service for centralised credential validation and user administration. **Radius One-time password** is also possible where a RADIUS infrastructure provides an OTP challenge, supporting a second authentication factor through an external authentication service. **Password and TOTP** provides a password-based sign-in combined with a time-based one-time password, giving a multi-factor authentication method for the interface. These alternatives are relevant to the Customer Security Controls Framework requirement to protect access to Swift-related systems and to apply multi-factor authentication where required, particularly for privileged or sensitive access. The exact method selected should be deployed, administered, and monitored in accordance with the institution's risk assessment and the applicable Alliance Interface release documentation. Swift describes the control objectives and security expectations in its Customer Security Controls Framework. Product and implementation information is available through Swift's Alliance Access product information.

QUESTION NO: 14

Is the restriction of Internet access only relevant when having Swift-related components in a secure zone?

A. Yes, because if there is no secure zone then the internet connectivity does not need to be restricted

B. No, because there can be in-scope general operator PCs used to access a Swift-related application hosted at a service provider

ANSWER: B

Explanation:

"No, because there can be in-scope general operator PCs used to access a Swift-related application hosted at a service provider" is correct. The Customer Security Programme's security requirements are determined by the systems, users, and access paths that are within the Swift environment's scope; they are not limited solely to infrastructure physically or logically located in an institution's secure zone. When a customer uses a service provider to host a Swift-related application, operator workstations in the customer's general IT environment may still be in scope if they are used to connect to, administer, or operate that application. Those endpoints represent a potential path to the Swift service and therefore require appropriate protection, including restricting Internet access as required by the applicable control. This approach reduces exposure to Internet-borne threats, such as malicious downloads, phishing-led compromise, and unauthorised remote connectivity, that could affect operator credentials or the integrity of payment-processing activity. Assessors should evaluate the actual end-to-end architecture and operational access model, including service-provider arrangements and operator PCs, rather than treating the presence or absence of an on-premises secure zone as the sole deciding factor. Swift describes the programme and its scope-based security expectations at Swift Customer Security Programme and provides control-framework resources through CSP Controls.

QUESTION NO: 15

The control SWIFT Environment Protection supports several objectives. (Select the one that does not apply)

•Swift Customer Security Controls Policy

•Swift Customer Security Controls Framework v2025

•Independent Assessment Framework

•Independent Assessment Process for Assessors Guidelines

•Independent Assessment Framework - High-Level Test Plan Guidelines

•Outsourcing Agents - Security Requirements Baseline v2025

•CSP Architecture Type - Decision tree

•CSP_controls_matrix_and_high_test_plan_2025

•Assessment template for Mandatory controls

•Assessment template for Advisory controls

•CSCF Assessment Completion Letter

•Swift_CSP_Assessment_Report_Template

A. Restrict malicious access from external sources

B. Forbids any interactive sessions towards the SWIFT infrastructure

C. Limit risks of privileged accounts compromise

D. Limit risks of lateral movement

ANSWER: B

Explanation:

“Forbids any interactive sessions towards the SWIFT infrastructure” is the statement that does not apply. SWIFT Environment Protection is intended to protect the local SWIFT environment through appropriate isolation, segmentation, and restrictions on connectivity. Its security outcomes include reducing exposure to malicious external access, helping contain lateral movement within the customer environment, and reducing opportunities for compromise of privileged access used to administer SWIFT-related components.

The control does not require an absolute ban on every interactive session. Customers may need controlled administrative access to operate, maintain, troubleshoot, and recover the SWIFT infrastructure. Such access must be tightly governed and protected: it should be limited to authorized administrators, use secure and managed access paths, apply strong authentication and least privilege, and be monitored in accordance with the applicable CSCF requirements and the customer’s architecture. The relevant distinction is therefore between unrestricted or insecure interactive access and necessary, controlled administrative access—not a categorical prohibition of all interaction with the infrastructure.

SWIFT publishes the Customer Security Controls Framework and supporting programme materials through its Customer Security Programme page. The current controls documentation is available from the Customer Security Controls Framework page.