Guidelines

Assessing Cybersecurity Counterparty Risk

A Getting Started Guide

Contents

Qualifications and limiting conditions

This document provides general and non-binding guidance for SWIFT users on how to use and interpret cybersecurity data from counterparties within the financial services ecosystem. It provides suggestions on the recommended approach to governance, and on processes for sharing and integrating cybersecurity risk data into an institution's existing risk management framework.

It does not address user-specific issues or requirements.

The information in this document is not exhaustive, nor does it replace sound judgment or compliance with best practices.

Users are solely and exclusively responsible for any actions taken or decisions made as a consequence of the guidelines or recommendations, and for any interpretation of the data set forth in this document. SWIFT disclaims any and all liability in respect of the contents of this document, or of any actions taken or decisions made based or in connection with the contents of this document or their consequences. Nothing in this document shall be interpreted or construed as constituting any obligation, representation or warranty on the part of SWIFT.

SWIFT supplies this document for information purposes only. The information in this document may change over time. Users must always refer to the latest available version.

Voice of the Customer

What are the key challenges you encounter in cyber risk management applied to your counterparties?

"A key challenge that we encounter is accessing the cyber controls that exist with our counterparties. The lack of knowledge of the level of controls at each counterparty makes cyber risk management challenging. You are only as strong as your weakest link. This is the reason why performing counterparty cybersecurity due diligence reviews is so important.

Key issues include:

- Finding a consistent standard used by all counterparties that can be leveraged for benchmarking
- Getting counterparties to share information about their security controls or lack thereof
- Validating the accuracy of the information provided by the counterparties
- Consuming and processing the data in a way that provides valuable risk information to the business in a manner they can understand and make appropriate business decisions on
- Following up on any issues to ensure they get remediated and closed out and to agree on implementing compensating controls in the interim"

Executive Summary

Given that cybersecurity remains a top issue within an evolving threat landscape, this guideline looks at how an organisation within the banking and payments ecosystem could approach the assessment of cybersecurity risk posed by counterparties that they transact with on a daily basis.

The guideline covers four areas that each institution should look to address: establish a governance model; establish a cybersecurity risk management framework; adopt cybersecurity risk countermeasures and incorporate cybersecurity 'attestation' data from counterparties.

Cybersecurity risks, including those brought by counterparties, need to be managed together with other types of risk - operational, financial and regulatory. Many institutions are working to integrate cyber risk assessment into their existing counterparty risk processes.

The oversight of this process - the **governance** – needs to be crafted to ensure that the right people with the right responsibilities have decision-making ability, and that the processes are strong and repeatable. With a solid governance structure in place, institutions can approach the implementation of a cybersecurity risk **management framework**. This includes the risk assessment of counterparties, by:

- Collecting the necessary data to support risk-driven decisions;
- Processing this data and transforming it into a weighted, risk-based assessment, typically shown as a numeric score or a red-amber-green indicator;
- Adopting suitable countermeasures to mitigate or 'treat' the risks.

Institutions may have varying risk appetites, but example cybersecurity risk mitigation countermeasures may include:

- Implementing additional levels of scrutiny on transactions from the counterparty;
- Limiting the type of transactions conducted with the counterparty;
- Requesting the counterparty implements additional controls or fraud detection measures;
- Requesting the counterparty substantiates their information through an independent assessment;
- Reassessing counterparty agreements and contracts.

Within this governance model and risk management framework, an institution should also consider incorporating the **attestation data** from its counterparties that use the SWIFT network. These are available as a result of the SWIFT's Customer Security Programme (CSP) and its associated set of security controls.

CSP provides a tool that allows an organisations' compliance level per control to be published to its counterparties. Within the tool, this attestation data can be viewed and exported, either counterparty-by-counterparty or bulked across all counterparties, to allow an organisation to '**consume**' the data by integrating it into their risk-based decision framework (i.e. process the data, assess the risk and assign countermeasures) to help manage the risk posed by the counterparty.

CSP attempts to create a level of standardisation and transparency in information that is shared, which can then be used by SWIFT users. This attestation data is rich in information and a unique source of cybersecurity counterparty risk data for SWIFT users.

Context

Cybersecurity and fraud remain top global threats. The sophistication of threat actors is increasing, massive data breeches are common place and with Advance Persistent Threat (APT) cyber-attacks, virtually anybody could be a target and with 'Internet of Things' ubiquitous 'smart' devices could be used as a DDoS weapon.

Within financial services, these threat actors pose a threat from sophisticated cybersecurity attacks where the primary motivation from the victim is **asset theft**.

But, of course, organisations within in the banking and payments ecosystem do not operate in a vacuum - they interact and transact with their numerous counterparties on a daily basis. The risk is real, as the cyberattacks on SWIFT customers from a small number of sophisticated and well-funded threat actors continue. **How should an organisation view and treat the possible risk that they may be transacting with an unwitting victim of a cyber-attack?** If the risk is not managed, and funds are lost, the financial exposure may be significant.

This guideline looks at how an organisation could approach the assessment of cybersecurity risk posed by their counterparties and covers four key areas:

- Establish a governance model for cybersecurity risk management;
- Establish a cybersecurity risk management framework;
- Adopt cybersecurity risk mitigating countermeasures;
- Incorporate cybersecurity attestation data from SWIFT counterparties.

The remainder of this document discusses these four topics.

Voice of the Customer

Has cybersecurity attestation data helped you with addressing one or some of these challenges, and if so, how?

"SWIFT's customer security attestation process has complemented our overall member management programme to help address those challenges. Through the receipt of the attestation data, we now have the ability to understand the level of counterparty controls implemented. Understanding the type and level of controls implemented at each counterparty, we are better suited to perform cyber risk management.

SWIFT CSP has provided us with a consistent set of responses used by all counterparties that can be leveraged for benchmarking. It is for us what the SAT test is for college admissions teams. The attestation tool is very easy to use requesting and granting access to counterparties. The SWIFT CSP program assists in the level of confidence we have in the counterparty responses by providing a means for counterparties to get their responses validated by internal and/or external audit. We developed a quantitative model to consume the data from the attestation tool and generate reports and charts."

Establish a Governance Model for Cybersecurity Risk Management

Cybersecurity risks, including those represented by counterparties, need to be managed together with other types of risk - operational, financial and regulatory.

The oversight of this risk management process - the governance - should be crafted to ensure that the right people with the right responsibilities have decision-making ability, that the processes are strong and repeatable and that exceptions can be managed.

Senior Committee Structure

Cybersecurity risk governance should be considered as a holistic function. This means it should be overseen centrally by those with a responsibility for the business as a whole, rather than being confined to an isolated back-office function in IT or operations. In practice, counterparty risk management should be part of (or subset of) a **senior committee structure, such as the Risk Committee,** with its own mandate and sufficient resources.

Within this cross-disciplinary governance, consideration should also be given to align responsibilities across the '3 Lines of Defence'. In practice this means that the day-to-day operational risk decisions should be taken in the first line (e.g. business, operations, IT/cyber) as they are responsible for executing internal controls and operational procedures. Exceptions and escalations should be managed in the second line of defence (e.g. compliance, risk) as they have a degree of operational independence. Assurance should be overseen by the third line of defence (e.g. internal audit) as they are independent.

Business Driven Stakeholders

The governance functions should be carried out by individuals with adequate levels of seniority which have the authority to take impactful decisions across the right internal stakeholder groups.

Arguably, many of the day-to-day operational risk decisions for counterparty management should be driven by **business people** rather than solely technical or cybersecurity people.

However, overall governance should be holistic and include representatives from:

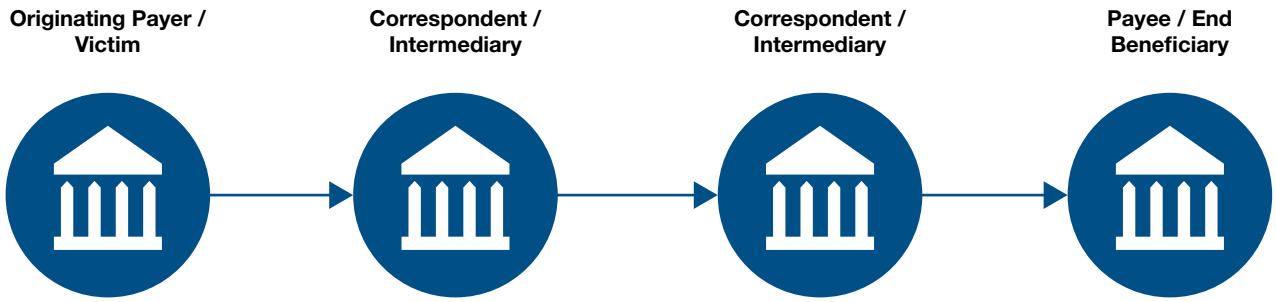
- **Business** and counterparty relationship management, in order to assess market and counterparty exposure and to liaise with the counterparty;
- **Payments operations,** in order to implement operational controls, adjust limits and intervene in normal processing operations;
- **Technical,** e.g. IT / information security / cybersecurity, in order to request the implementation of additional technical controls or specific fraud detection measures;
- **Risk, compliance, and audit,** in order to manage exceptions and undertake independent assurance.

Due to the sensitivity of the data and the potential impact of security compromises, oversight of this process should be undertaken by a senior executive and this senior executive should help drive the risk assessment and escalation process and oversee the resultant countermeasure decisions.

Clear Mandate

The senior committee with counterparty risk oversight should have a clearly articulated mandate, or Terms of Reference, that describes the longer-term strategy as well as the day-to-day operating model including roles and responsibilities.
This mandate should also include the need for regular briefings to the board and to senior management on the counterparty risk landscape, specific incidents and evolution and trends.

Framework for Assessing Cybersecurity Counterparty Risk



This guide is intended for:

- **Small to medium sized enterprises** that receive instructions from the originating payer. These SMEs' would have a limited number of counterparties, compared to larger institutions which would have multiple counterparty relationships and complex internal structures.
- **Correspondent banks** (irrespective of their size) that act as intermediaries of the transaction between originating payer and the end-beneficiary.

Voice of the Customer

Can you describe how you use cybersecurity attestation data concretely beyond simply submitting your self-attestation in the tool; more specifically, how you use them in the context of security risk management for your counterparties?

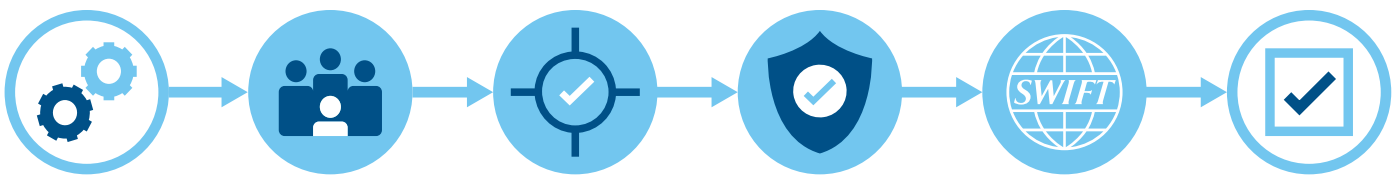
"The attestation tool provides consistent responses, so we are able to evaluate each attestation and apply a numeric value based on the responses. This has allowed us to apply repeatable quantitative and qualitative measurements to each attestation. Previously we relied solely on questionnaires that in many instances inconsistent responses."

Establish a Cybersecurity Risk Management Framework

With a solid governance structure in place, institutions will typically approach cybersecurity from a risk perspective. This means that they assess the level of risk and invest budget where it is most needed and accept risks where they are below a set threshold or appetite. This cybersecurity risk management process, or framework, comprises several steps:

1. **Collect the necessary counterparty risk data;**
2. **Assess the level of the risk by processing the data. This is typically done by assigning an overall score and then considering it against the level of company risk appetite;**
3. **Based on the risk score, implement suitable measures to manage or 'treat' the risks.**

Framework for Assessing Cybersecurity Counterparty Risk



Establish a **governance** model for cybersecurity risk management

Establish a cybersecurity **risk management** framework

Adopt cybersecurity risk mitigating **countermeasures**

Incorporate cybersecurity **attestation data** from SWIFT counterparties

Counterparty Risk Data

Institutions collect and process a variety of data in order to help determine the risk profile of counterparties from a cybersecurity perspective.

The risk data broadly fits into three categories; data related to the external environment in which the counterparty operates, data that describes the business relationship with the counterparty and data that is transactional:

1. Risks related to external environment in which the counterparty operates

- **Country/region of operation** – Could serve as a measure for the level of cybersecurity, regulation and crime/fraud in the jurisdiction in which the counterparty operates. This can be assessed using publically available sources, such as the Basel AML risk report;
- **Industry type** - Could be correlated against the likelihood of being attacked, as some sectors suffer from cybersecurity attacks and data breaches more frequently than others;
- **Degree of regulatory oversight** over the counterparty and the extent that the local overseer is imposing cybersecurity regulation or policy.

2. Risks related to the business relationship with the counterparty

- **Depth / length of the counterparty relationship** – Newer relationships could potentially have a higher risk than a long-standing, deep and trusted relationship;
- **Size / ownership structure of the counterparty** – Could be correlated against the availability of budget, skilled resources and tools to combat threats, especially if part of a larger group, e.g. Global Systemically Important Banks (GSIB);
- **Known cyber or security incidents** or other available news, information or due diligence materials;
- **Existing risk assessments for the counterparty,** e.g. operational, financial or regulatory.

3. Risks related to transactions

- **Types of transaction** – Limiting the type of transactions conducted with the counterparty as certain transaction types are inherently more vulnerable than others, for example payments versus statements;
- **Transaction value** – Serves as a representation of credit risk exposure;
- **Transaction frequency** – The greater the volume of transaction per period, the greater the potential attack surface.

Once this counterparty data has been gathered, the risk assessment process can be applied.

Risk Assessment Process

Once counterparty data has been collected, institutions process and transform it into a risk-based assessment. This assessment methodology can vary from institution to institution, but generally follows one of three approaches:

- **Expert-based** – where the assessment is driven by expert judgement and a qualitative evaluation of risks by specialists;
- **Rule-based** – where the assessment is made via a decision tree using simple rules on how the counterparty scores against each risk factor;
- **Model-based** – where the assessment is derived analytically based on how the counterparty scores against each weighted risk factor.

Regardless of the approach taken, the counterparty is usually assigned an overall score, which is typically represented as a red, amber or green indicator.

Risk mitigation countermeasures would depend on this score compared to the internal risk appetite. For example, counterparties with a low, or green, score may be classified as not requiring additional scrutiny, but counterparties with a high, or red, score, may be selected for risk mitigation countermeasures.

Adopt Cybersecurity Risk-Mitigating Countermeasures

The risk management framework can allow an institution to assess and classify the degree of security risk associated with a counterparty. The institution can then make a decision to either accept the risks, or consider risk mitigating countermeasures.

Cybersecurity risk mitigation countermeasures may include:

1. Countermeasures related to the business relationship with the counterparty

- Proactive **outreach to senior management** to strengthen the relationship and provide overall reassurance;
- Requests for the counterparty to **substantiate their information** through an internal or third party/external independent assessment, or through providing technical specification documentation or test results;
- Requests for the counterparty to implement **additional controls** or **fraud detection** measures;
- Reassess counterparty **agreements and contracts**, including the possibility of 'de-risking' the counterparty and changing or terminating the contract.

2. Countermeasures related to stricter transactional governance with the counterparty

- Flag for review transactions that breach **pre-defined thresholds**. These can include transaction type, transaction value, transaction currency, or profile of the end beneficiary;
- For all flagged transactions, implement **additional scrutiny**, for instance manual four-eyes oversight and/or bilateral verification of the transaction with the counterparty.

The above list of countermeasures is not intended to be exhaustive and institutions may have other controls and tools that they can deploy to help manage the risk.

Applying countermeasures for higher-risk counterparties

For higher-risk counterparties, institutions may wish to apply any combination of the above countermeasures. Typically, an institution will want to apply additional scrutiny and monitor payment instructions over a predetermined value or volume threshold. The institution should have the ability to adjust thresholds, and also the tools and capacity to deal with an increased number of alerts plus the additional effort to manually process the transaction, including needing up-to-date counterparty contact information.

This state of increased scrutiny does not necessarily need to be permanent. As soon as the counterparty manages to be re-classified into the 'low' risk category, for example because they comply with additional countermeasures, thresholds can be altered or removed.

Beyond any decision to implement mitigation countermeasures, each institution remains solely and exclusively responsible for altering, suspending or terminating, in whole or in part, the relationship with the counterparty.

Once the cybersecurity risk management process is in place, it is prudent for the governance structure to undertake periodic reviews of the counterparty to assess whether its risk profile has changed.

Voice of the Customer

How does cybersecurity attestation data feed into cyber risk management, and what are the governance bodies that are organized around this?

"Weekly reports are provided to our Chief Risk officer, along with other risk departments. We track the number of granted attestations in comparison to the number of pending request. For the granted attestations we risk score each attestation then apply each scored attestation at qualitative profile. Our risk departments have begun to incorporate the profile results with in their disciplines."

Appendix A: Incorporate Attestation Data from SWIFT Counterparties

Launched in May 2016, SWIFT's Customer Security Programme (CSP) supports all SWIFT user segments in reinforcing the security of their local SWIFT-related infrastructure.

The SWIFT Customer Security Controls Policy (CSCP) defines the user attestation process and related principles, roles and responsibilities. SWIFT also developed a Customer Security Control Framework (CSCF), which establishes a security baseline of mandatory and advisory controls for the entire user community.

The CSCP Policy requires users to self-attest compliance against a set of **mandatory security controls**, and encourages them to also self-attest compliance against a set of advisory controls. They attest their level of compliance, and their **attestation** is published and managed through the KYC-Security Attestation (KYC-SA) application provided by SWIFT.

A key function available in the KYC-SA tool is the ability for institutions to exchange attestation data with their counterparties by mutual agreement through **'requesting' and 'granting' access**. In doing so, this allows institutions to assess counterparty risk, and then make counterparty risk decisions based on the attested compliance levels. This attestation data is rich in information and a unique source of cybersecurity counterparty risk data.

As institutions begin to integrate CSP attestation data into their counterparty risk frameworks, a number of factors should be taken into consideration:

- Considerations for the governance model;
- Considerations for the risk management framework;
- Further options for mitigation countermeasures.

These three areas of consideration are discussed below within the overall context of the KYC-SA tool.

It is important to stress that attesting users are solely responsible for and SWIFT does not validate the correctness of user attestations. The CSP is designed to create a level of **standardisation** and **transparency** in security information that is shared, which can then be used by SWIFT users.

Note that Appendix B contains links to the CSCF Framework and CSCP Policy documentation.

Appendix B also contains links the KYC-SA User Guidelines that give step-by-step details of how to request / grant access to the attestation data and how to export attestation data as an excel file. The attestation data can be exported on a counterparty-by-counterparty basis, or as a bulk export across all relevant counterparties by the organisation's Security Officer. However, these guidelines do not go to the extent of describing how an organisation should consume the data, i.e. assign governance, process the data, assess the risk and assign countermeasures. These are outlined below.

Voice of the Customer

What is the governance around granting counterparties access to your attestation data? Is this a shared responsibility (e.g. between Risk, Compliance, Legal et cetera)?

"The governance process for granting counterparty access to our attestations data requires multiple teams' participation. To ensure that there is transparency with granting access to our attestations. We have an internal workflow approval process. Once approved internally, the administration team performs the granting of access with in the attestation tool."

Considerations for the Governance Model

Before deciding to share attestation data, or requesting others to share theirs, the overall process for consuming counterparty attestation data should be defined. In particular, this needs to include how sharing will take place, and who should perform which role.

While SWIFT provides the technical platform, the institution's governance model also needs to be adapted to support the assessment of counterparty security attestation data. Appropriate representatives from the breadth of the institution should be considered for 'granting' or 'requesting' access to attestation data, and the data should be viewed as an additional element within the institution's existing counterparty risk management framework.

Granting (or rejecting) access to counterparties

In order to grant access to a requesting counterparty, the governance model needs to clearly identify the business owner managing the 'yes' or 'no' approval decision process. Without a clear 'granter', incoming attestation requests will be left queued and unanswered.

The approval decision criteria used to grant incoming requests should, typically, be signed off by a senior committee structure such as the Risk Committee, or by executive management such as the CISO, General Counsel, or Chief Compliance Officer.

Example decision criteria used by the 'Granter' for granting counterparties access

- Attestation data will be shared with Global Transaction Banks, regardless of their geography
- Attestation data will be shared with counterparties in the same geography with oversight from the same regulator
- Attestation data will be shared once we can report our 'Attestation Type' as supported by an external assessment or audit
- Attestation data will be shared with all requesting counterparties with whom we have an active messaging relationship
- Attestation data will be shared with requesting counterparties who also share their attestation data with our institution
- Attestation data will be shared with all requesting counterparties

The senior committee structure or executive management should sign off the decision criteria. When this is done, middle management can apply them to incoming requests and provide technical operators with a decision to either grant or reject access.

Exceptions should be escalated to the senior committee structure or to executive management.

At an operational level, the operators (or "granters") should report a summary of the received requests, and actions taken, to management on a regular (e.g. weekly) basis.

Example process flow for granting access

1. Assign 'granter' role to an operator
2. Operator receives an access request from a counterparty
3. Operator reviews the request against approval criteria and recommends a positive or negative response
4. Middle management reviews the recommendation and either provides permission to execute, provides alternative decision or escalates to executive management
5. Operator 'grants' or 'rejects' the counterparty request. In cases of rejecting access, operator should be in a position to provide a reason for rejection. This might include not having a relationship with the counterparty or not being prepared to share attestation data at this time
6. Operator reports summary of status requests and actions on a regular basis, e.g. weekly

The attestation tool also provides the facility to create a 'whitelist' of counterparty BICs that meet the criteria as defined by executive management. This would allow for the automated granting of access to such counterparties upon request, thereby avoiding manual review and approval flows. This feature is known as "Auto-Grant".

Requesting Access from Counterparties

The senior committee structure or executive management should sign off on criteria for granting access to counterparties. The criteria for requesting counterparty attestation data should be decided at a similar level.

Example decision criteria used by 'Requester' for requesting access to counterparty data

- We will request attestation data from all of our counterparties
- We will request attestation data only from counterparties with whom we do not regularly interact
- We will request attestation data only from counterparties that reside in a high risk area
- We will request attestation data only from counterparties already considered high risk

Once the decision criteria have been defined by executive management, attestation requests would be executed in the attestation tool by an operator ("requester").

The status of requests to access counterparty attestation data should be reported to management on a regular basis (e.g. weekly) – similar to status reporting on granting access to counterparties.

Example process flow for requesting access

1. Assign 'requester' role to an operator
2. Executive management defines decision criteria for requesting access to counterparty attestation data
3. Operator sends the request to counterparty via the attestation tool
4. Counterparty 'grants' or 'rejects' access request. In cases where a request has been rejected, executive management should consider further engagement with the counterparty and re-request access after the reason for rejection has been mitigated
5. Operator reports summary of status requests and actions on a regular basis, e.g. weekly

Voice of the Customer

In being granted access to counterparties' attestation data, has there been any information you received that triggered you to take a significant cybersecurity decision? If yes, can you elaborate?

"Once we are granted access to a counter-party attestation data we review the responses to the controls. Although we have not made cybersecurity decisions based on a counter-party attestation. Counterparty responses have driven our internal conversations around the cyber contagion."

Considerations for the Risk Management Framework

Organisations which have been granted access to a counterparty's attestation data may use the tool to 'consume' the data. This attestation data, which includes compliance levels per control, should be integrated into the organisations' risk-based decision framework to help manage the risk posed by the counterparty.

Institutions wishing to embed cybersecurity attestation data into their existing risk management process may wish to apply weightings and scores based on that information.

Example approach to weightings and scores

- If the counterparty has not attested, it should be scored
- If the counterparty has not responded to KYC-SA access requests, it should be scored
- Compliance levels for each CSCF control should be scored: e.g. compliance per the guidelines, compliance by alternative means, lack of compliance, or future compliance by given date
- Each specific control, mandatory or advisory, may be assigned a different weighting
- Other attestation variables may be given a specific weighting, such as:
  - **Infrastructure type**
  - **Infrastructure components** – is the counterparty using a certified interface?
  - **Service Provider** - is the counterparty connecting through a service provider and what is the certification or compliance status of that provider?
  - **Assessment type** - has the counterparty engaged internal or an external third party for advice, or has their attestation been substantiated by an internal or external independent assessment? See below

Assigning meaningful weightings and scores is a detailed exercise for which institutions should ensure collaboration between internal stakeholders, such as those from information security, operations, technology, risk, compliance, business and legal.

Interpreting 'Assessment Type'

This field in the self-attestation captures the extent that the counterparty has used independent reviewers to substantiate their attested level of compliance

– **Third-Party Independent Assessment (which can include audit by external auditor)** – the institution has validated control compliance through the use of an independent external assessor. Its name must be declared by the attesting institution. – **Internal Independent Assessment (which can including audit by internal audit)** – the institution has validated control compliance through the use of the internal assessor function.	May allow a higher degree of reasonable assurance that the compliance status assigned to each control has been independently verified. May imply a higher trust level for counterparties that can provide this level of assurance. Allows scrutiny of the name of the external assessor.
– **Advisory review by external firm** – the institution has engaged a third party for advisory services in their compliance assessment. The name of the third party must be declared by the attesting institution. – **Advisory review by internal independent teams** – the institution has engaged an independent internal party for advisory services in their compliance assessment.	May give some degree of confidence in the independent verification of the listed control status. Advisory assessments are not executed in a fixed, pre-defined framework. Confidence may be stronger if a full assessment report is undertaken and made available. Could be supplemented with a targeted assessment or a sample check.
– **Self-assessment** – the institution has self-assessed its input, e.g. through sign-off by the CISO, the CRO, or other executive roles.	May establish a minimum degree of confidence that the counterparty has thoroughly assessed its compliance with the CSCF controls.

Additional Risk Mitigation Countermeasures

Beyond the generic countermeasures outlined in Section 4, consideration could be extended to include a number of additional options specific to the use of SWIFT, as outlined below.

Request compliance against advisory controls

Aside from the existing obligation to self-attest against the set of mandatory controls, institutions may wish to request that some counterparties should also self-attest against some, or all, of the advisory controls.

Counterparty utilisation of fraud detection measures

SWIFT users may wish to request that some counterparties should implement fraud detection capabilities that look for anomalies or outliers that do not represent the normal pattern of behaviour. This is currently defined as an Advisory Control in CSCF v2019.

Example: SWIFT Daily Validation Report (DVR)

As part of the CSP programme, SWIFT has expanded its financial crime compliance portfolio by adding a transaction pattern detection tool. This is designed to mitigate the risk associated with payment fraud.

The Daily Validation Report (DVR) makes it easy for institutions to validate payment transaction activity, highlight potential risks, and respond quickly if fraud incidents occur.

DVR provides information on the previous day's payments activities. Each day's transaction value and volume totals are compared to the user's daily value and volume averages over the previous 24 months, allowing any significant change in activity to be quickly identified and understood.

Two key areas are covered:

- Activity Reporting allows users to see their aggregated daily activity - Aggregated daily activity is provided by message type, currency, country and counterparty. Daily value and volume totals are provided as well as details of the largest transactions.
- Risk Reporting is designed to highlight large or unusual message flows that may be indicative of fraud risks. It helps users select the largest single transaction(s) and largest aggregated transaction flows seen with their counterparties for inbound and outbound payments. Comparisons to previous average daily value and volume totals allow users to assess changes in activity. Risk Reporting also highlights any new combinations of direct and indirect counterparties from transactions during that day.

Information is aggregated for the following key SWIFT message types: MT 103, MT 202, MT 202COV, MT 205 and MT 205COV. DVR was launched in 2016.

Example: SWIFT Payment Controls Service (PCS)

Payment Controls Service (PCS) specifically focuses on helping SWIFT users to detect in-flight anomalous activity. PCS performs in-flight real-time detection of payments that are out of policy for a counterparty, or which are uncharacteristic and indicative of fraud risk. It is performed out of band, i.e. away from user premises. This implies that even if the institution is compromised, data remains trustworthy.

PCS works in one of two real-time operating modes using policy rules defined by the subscriber:

- Message copy and alert, or
- Message hold and alert

At its core, PCS allows users to configure the policy rules across a number of parameters:

- Business calendars, non-business days and normal business hours
- Currency whitelist / blacklists, single and aggregate payment limits
- Country whitelist / blacklists, single and aggregate payment limits
- Thresholds for country, currency, single entity or group combinations
- New institutions: Identify payments with new participants or chains, based upon historical message flows
- Badly formed messages: Identify and stop messages where preceded by repetitive NAKs to the same recipient
- Suspicious accounts: Verify end customer account numbers against an institution black list of account numbers believed to be high risk

PCS was launched in October 2018.

Note that before an institution implements receiver fraud controls or before an institution requests a counterparty to implement sender fraud controls, the Terms and Conditions as well as other legal considerations should be reviewed.

Refine the relationship and enforce with RMA

Relationships that were founded several years ago may have changed over time and not be aligned with business patterns today. In addition to controlling who can send messages with the Relationship Management Application (RMA), SWIFT users can restrict the types of messages with RMA+. For example, a user can agree to receive treasury or trade messages but not payment messages.

Example: SWIFT RMA and RMA Plus

Relationship Management Application (RMA) is the key exchange and authorisation process between two financial institutions and enables institutions to define which counterparties can send them FIN messages. Any unwanted traffic is blocked at the sender level, reducing the operational risks associated with handling unwanted messages.

RMA Plus, the more granular version of RMA, goes one step further by letting institutions specify which message type(s) they want to send to, and receive from each of their counterparties. For example, an institution might only wish to receive letters of credit from a particular correspondent.

Institutions need to grant RMA or RMA Plus authorisation to their counterparties in order to receive messages from those counterparties and RMA functionality is built into the Alliance Access and Alliance Entry SWIFT interfaces

Over time, many institutions have opened many RMA relationships with many counterparties. However, the list of RMA authorisations may not always have been updated when business relationships change or are terminated. Institutions may therefore have a large number of inactive RMAs in place – and may not even be aware of them.

By rationalising and revoking dormant or inactive RMAs, institutions can minimise the time and cost associated with such activities, as well as reducing risks.

Institutions can undertake this rationalisation task themselves. Alternatively, SWIFT offers the ‘clean up’ of RMA and RMA Plus authorisations as a service.

RMA was launched in 2009

Appendix B: Glossary

Term	Acronym	Description
SWIFT Customer Security Programme	CSP	**Click here for more info**
Customer Security Control Framework	CSCF	**Click here for more info**
Customer Security Control Policy	CSCP	**Click here for more info**
Know Your Customer – Security Attestation (application)	KYC-SA	Baseline: **Click here for more info** User Guide: **Click here for more info**
Relationship Management Application	RMA	**Click here for more info**
Daily Validation Report	DVR	**Click here for more info**
Payment Controls Service	PCS	**Click here for more info**
Shared Infrastructure Provider	SIP	**Click here for more info**
Business Identifier Code	BIC	**Click here for more info**
Chief Information Security Officer	CISO	Common denomination used for the most senior executive accountable for information security in a firm.

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

For more information visit www.swift.com, or contact your Account Manager, or email weareswift@swift.com.

57397 – April 2019