Advisory

SWIFT CSP Assistance

SWIFT client duty

Yearly assessment to be performed by an internal/external, **certified, independent assessor**.
Risk to your organization's security and image if this is not carried out or you are non-compliant.
Non-compliance might be reported to the CSSF.

Why EBRC?

EBRC is referenced on the SWIFT directory of cyber security service providers.
Risk based approach.
EBRC is part of the SWIFT partnership program.

Business Benefits

SWIFT CSP compliance assessment and action plan to cover gaps. Remediation work can be carried out on customer request, based on a RISK analysis approach.

Deliverables

Detailed review of security measures.
Risk Analysis report.
Action Plan.
Final report.

Solution Overview

The SWIFT Customer Security Program (CSP) has been introduced to support customers in their fight against cyber fraud. The CSP establishes a common set of **security controls designed to help customers** secure their local environments and to foster a more highly protected financial ecosystem.
The SWIFT Customer Security Controls Framework (CSCF) describes a set of mandatory and advisory security controls for SWIFT users. This framework is **upgraded** and shall be reassessed **on a yearly basis**.
With its cybersecurity and cyber risk assessment experience, EBRC has carried out these assessments for banking clients since the creation of this program, we have joined the SWIFT Partner Program.
This partnership allows EBRC to benefit from all necessary documentation and training for our consultants. The result is we can offer a risk-based approach action plan in full compliance with this framework.
Since 2021, an independent assessor is required to review and certify the accuracy of the assessment.
Thanks to our extensive experience, expertise and engagement with the SWFT CSP program, EBRC is able to assume the role of Independent Assessor.

Key Features

Use of **EGERIE Risk Manager** with pre-defined scenarios.

ebrc