SWIFT Payment Systems Review (CSP)

Company Overview

World Informatix Cyber Security provides comprehensive cyber security solutions to commercial and federal Industries to help organizations minimize the risk of cyber-attack.

Our services are a culmination of years of industry experience and expertise through performing cyber security assessments for global institutions. We provide a full spectrum of cost-effective regulatory support, security assessments, vulnerability assessment and penetration testing which produce threat-based results.

In 2016, **World Informatix Cyber Security** was chosen to respond to the largest cyber-heist in history at the Central Bank of Bangladesh with $101 million stolen. The experience launched our flagship service, the SWIFT payment system review, which has been used at global organizations such as the United Nations and Central Banks around the world.

World Informatix Cyber Security

Overview

Our SWIFT Payment System Review is a comprehensive risk assessment which provides assurance of the highest level of cyber security assurance for banks, financial institutions and users of the SWIFT Payment System. Our service goes beyond compliance and provides 3rd party attestation to SWIFT Customer Security Programme (CSP).

With deep industry knowledge and understanding of financial platforms, our certified engineers perform a gap assessment of security controls along with a vulnerability assessment on all SWIFT related surfaces. WICS uses a proprietary SWIFT checklist with over 300 detailed controls. The result is a series of technical and executive reports which aid remediation efforts.

WICS - Competitive Advantage

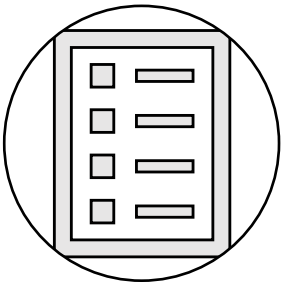
1. **World Informatix Cyber Security is a global leader in SWIFT Payment Systems Reviews, trusted by the United Nations, Governments, & Fortune 500 companies worldwide.**
2. **Primary investigator in the 2016 Central Bank of Bangladesh Heist, which caused a global shift in financial industry cybersecurity and prompted SWIFT to create its CSP programme.**
3. **Listed in the SWIFT 3rd party directory of Cybersecurity & CSP assessors*.**
4. **Cost-effective services using including 100% remote delivery.**
5. **Professional cyber security engineers and ethical hackers with relevant certifications (CEH, CISSP, OSCP, CHFI)**
6. **Proprietary Indicators of Compromise (IoC) search tools to look for evidence of compromise typically found in financial institution SWIFT-related attacks.**

"SWIFT does not certify, warrant, endorse or recommend any listed Provider; it remains the SWIFT customer's responsibility to determine whether the Provider satisfies all necessary criteria to properly assist them in being compliant towards the CSP Controls."

SWIFT
Payment System Review

WICS SWIFT payment system review uses a detailed and tested methodology developed from our extensive experience dealing with financial system cyber-attacks. The review is used to help organizations assess a broad set of controls to ensure highest level of cyber-security for payment systems and associated infrastructure. The Payment System Review provides annual 3rd party assurance and attestation to SWIFT's mandatory Customer Security Programme (CSP) guidelines by providing threat-based technical & executive vulnerability reports aimed at providing top-to-bottom remediation plans.

Service Overview

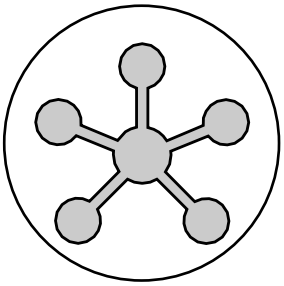


SWIFT Security Checklist

-Assess security controls against SWIFTs 31 mandatory and advisory controls in CSCF v2021.

-Proprietary checklist seperated into 300+ detailed controls.

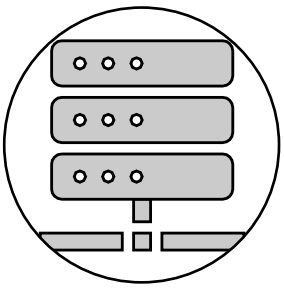
-Provide compliance to regulatory requirements.



Develop Custom Threat Models

-Review internal documents, policy and procedures.

-Create custom threat-model based for payment system environment using industry leading Threat-Risk modelling.



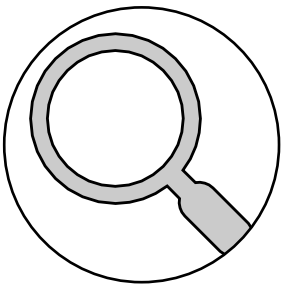
Vulnerability Assessments & Penetration Testing (VAPT) on SWIFT Infrastructure

-VAPT for networks, servers & endpoints

-Application Hardening

-Patch configuration & management

-Weak Cipher checks



Threat hunting for Indicators of Compromise (IoC)

-Search for Known IoC's using custom scripts and proprietary tools

-Detect evidence of Malware used in global SWIFT hacks using binary search strings.

A Closer Look

SWIFT Security Checklist

Our proprietary checklist has been divided into 8 functional security domains. Each domain is further divided with a total of 300+ detailed security controls.

1) Restrict internet access and segregate critical systems from general IT environment.
2) Reduce attack surface and vulnerabilities.
3) Physically secure the environment.
4) Prevent compromise of credentials.
5) Manage identities and segregate user privileges.
6) Detect anomalous activity to systems or transaction records.
7) Plan for incident response and information sharing.
8) Check for known Indicators of Compromise (IoC).