SWIFT customer security program

What are your organization's obligations when it comes to the new SWIFT Customer Security Program? The answer isn't always obvious, particularly in the ever-changing, global environment in which we operate.

All organizations that use the Society for Worldwide Interbank Financial Telecommunication (SWIFT) interbank messaging network must comply with its new cybersecurity standards - as well as a related "assurance framework."

What is the impact?

While customers are responsible for protecting their own environments, SWIFT's Customer Security Program (CSP) was established to support customers in their fight against cyber-fraud. SWIFT released draft cybersecurity standards that will be finalized in March 2017, with inspections and enforcement beginning in January 2018. All organizations that use SWIFT, not just financial institutions, must attest that they comply with the standards, on an annual basis, or face being reported not just to regulators, but also other SWIFT members. The new SWIFT security assurance framework includes 16 mandatory controls as well as 11 optional "advisory controls". SWIFT customers and members may also be required to provide a more detailed proof of compliance.

What is your defensible position?

KPMG's cyber team will evaluate your readiness to meet the new SWIFT CSP Objectives, Principles and Controls, in preparation for the new rules. We will review your organization's defences around the SWIFT Payment and Wire Transfer processes and technologies using real world scenarios to more accurately gauge and address your readiness for the new SWIFT CSP rules and attestation requirements.

What is the SWIFT customer security program?

The SWIFT CSP requires each organization to define, document, implement and assess their payment processes and technologies against SWIFT's set of Objectives, Principles and Controls. KPMG's SWIFT Security approach is an industry leading assessment capability that seeks to align an organization's existing cyber security capabilities and controls against the new framework. As such, we offer a set of services that help enable our clients to bridge the gap between actions taken to protect its information assets from unauthorized access or disclosure and help to provide associated cyber defensibility in a legal or regulatory risk context.

We will work with you to identify the SWIFT CSP controls and activities that align against your existing investments in Payment Security, including NIST CSF, ISO27001 or PCI- DSS; our flexible, tailored approach means that all controls, or a subset, could be leveraged depending on the scope of SWIFT in your payment processes.

SWIFT customer security program

3 Objectives	8 Principles	27 Controls
Secure your environment	1. Restrict internet access 2. Segregate critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment	– Application to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure – Mapped against recognized international standards – NIST, PCI- DSS and ISO 27002 – Some controls are mandatory, some are advisory – Documentation and collateral will be available by end of October
Know and Limit Access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges	
Detect and respond	7. Detect anomalous activity to system or transaction records 8. Plan for incident response and information sharing	

Source: SWIFT

SWIFT gap assessment

KPMG's Cyber Team will work with you to perform a gap assessment of your SWIFT Payment and Wire Transfer processes, controls and governance against the SWIFT CSP Objectives, Principles and Controls. Our team can advise on the most efficient way to design and implement additional controls to help close any gaps with the new rules and provide insight on how SWIFT is interpreting the rules at other organizations.

Our approach is to identify the most efficient way to maintain a unified compliance posture between the new SWIFT requirements to help reduce duplication and overlap with existing payment processing compliance rules, including PCI-DSS.

SWIFT controls implementation

The team of professionals in the Canadian firm will provide post-assessment advice and implementation covering all areas of the SWIFT CSP controls, integrating the new controls into your organization's existing SWIFT Payment and Wire Transfer processes. This can include the design and development of processes, policies, procedures and technology architectures for the 3 SWIFT Customer Security Program Objectives:

- Secure Your Environment;
- Know and Limit Access; and
- Detect and Response

SWIFT attestation services

The SWIFT CSP has identified an assurance framework that will be deployed, requiring a detailed proof of compliance from each organization. KPMG can assist an organization in preparing for and performing the SWIFT CSP attestation, including:

- Self-Attestation
- Self-Inspection
- Third-Party Inspection

For organizations that are already completing a SOC 2, KPMG professionals can help you identify and realize efficiencies across your attestation portfolio by leveraging our knowledge of SOC 2 and the new SWIFT CSP Attestation requirements.

Have a cyber emergency? Contact our 24/7 Cyber response hotline.

1-844-KPMG-911
1 (844) 576-4911

The KPMG SWIFT security difference

KPMG's SWIFT Security Program has an established framework that:

- Anchors information technology controls as well as security and records management investment decisions;
- Aligns with the SWIFT CSP, including Objectives, Principles and Controls;
- Establishes an extensible foundation that serves as evidence of a baseline for a "defensible position" – allowing your organization to enable a single set of controls over your Payment and Wire Transfer processes;
- Enables assessment and identification of SWIFT CSP risk and compliance gaps and manages the relationship with SWIFT when interpreting the CSP requirements; and
- Supports the SWIFT Attestation and integrates into your overall attestation portfolio and SOC 2 approach.

KPMG SWIFT security key services

Highlights
Targeted information gathering workshops with key Payment and Wire Transfer Business, IT, Legal, Compliance, Security, Privacy and Risk Management stakeholders.
Readiness of existing controls against the SWIFT Customer Security Program Objectives, Principles and Controls.
Implementation of new controls and remediation of existing controls within the organization's Payment and Wire Transfer Processes.
Attestation services including Service Organization Control (SOC) reporting.

KPMG's Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

Jean-Francois Allard
Partner
T: 514 840 2645
E: jeanfrancoisallard@kpmg.ca

Yassir Bellout
Partner
T: 514-840-2546
E: ybellout@kpmg.ca

Erik Berg
Partner
T: 604-691-3245
E: erikberg@kpmg.ca

John Heaton
Partner
T: 416-476-2758
E: johnheaton@kpmg.ca

Adil Palsetia
Partner
T: 416-777-8958
E: apalsetia@kpmg.ca

Jeff Thomas
Partner
T: 403-691-8012
E: jwthomas@kpmg.ca