

N° de SOLPE: 14610	Gerencia usuaria: GERENCIA DE GESTIÓN HUMANA Y ADMINISTRACIÓN-DPTO TI
N° PAC (de ser el caso): 51	Centro de costo: 10110600 Fuente de Financiamiento: Recursos Propios ...X... De terceros ..... Rubro Servicio: Servicios prestados por terceros
Subcontratación Significativa: ¿El requerimiento podría ser desarrollado por COFIDE? Sí ..... No ...X.... Si contestó <u>Sí</u> a la pregunta anterior, llenar al final del presente formato los datos solicitados.	

## **TÉRMINOS DE REFERENCIA DE CUMPLIMIENTO MÍNIMO – SERVICIOS**

### **CONTRATACIÓN DEL SERVICIO DE CONSULTORIA Y AUDITORIA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD BASADOS EN CUSTOMER SECURITY CONTROLS FRAMEWORK (CSCF) DE SWIFT**

#### **1. OBJETO**

Contratar la Asesoría CSP, para facilitar la correcta implementación de los controles y recolección de evidencias para el cumplimiento de los lineamientos del programa CSP (Customer Security Programme) de SWIFT, aplicables a la arquitectura de servicio que tiene implementado COFIDE

Además, contratar la Auditoría SWIFT al Customer Security Control Framework, que permitirá a COFIDE cumplir con este requisito de SWIFT, que contrasta y valida la ejecución de la implementación de los controles CSP con la información registrada en el proceso de “attestation”.

#### **2. FINALIDAD PÚBLICA**

La presente contratación tiene como finalidad mantener la operatividad y modernización de nuestra infraestructura del Centro de Computo Principal (CCP), buscando elevar los niveles de eficiencia y continuidad del negocio y satisfacción de los usuarios internos y externos de COFIDE.

El servicio a contratar, ayudará a identificar las brechas existentes en seguridad de información de la plataforma SWIFT y permitirá habilitar controles obligatorios para establecer una línea base de seguridad, que permita una conexión segura a la comunidad SWIFT.

El presente servicio se alinea con los objetivos estratégicos de la corporación:

<b>Eje Estratégico 2</b>	<b>Objetivo Estratégico Institucional</b>
Organización Moderna y Sustentable	OEI6: Lograr la Excelencia Operativa

#### **3. PROCESO DE ESTANDARIZACIÓN**

No Aplica

#### **4. NÚMERO MÁXIMO DE CONSORCIADOS**

El número máximo de consorciados es de tres (03).

El porcentaje mínimo de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, es de 80%.

#### **5. EQUIPO DE TRABAJO**

El POSTOR deberá contar como el siguiente personal, cabe mencionar que este detalle no limita a la empresa a colocar mayor cantidad o calidad de personal, de acuerdo a la eficiencia para el cumplimiento del servicio:

Cada una de las certificaciones requeridas deberá ser oficial y vigente.

Cargo y Rol	Requerimiento mínimo
<b>Consultor</b>	<p><b>Carrera Profesional:</b> Ingeniería de Sistemas o Ingeniería de Computación e Informática o Ingeniería Industrial o carreras afines. Grado Académico: Titulado.</p> <p><b>Experiencia Profesional:</b> Contar con al menos 3 años de experiencia en los siguientes puntos:</p> <ul style="list-style-type: none"> <li>- Procesos de Implementación de Controles CSP en entidades del Sector Financiero, Corporativo o Service Bureau en los procesos de implementación de controles del Framework CSCF 2021.</li> <li>- Experiencia en gestión de proyectos o metodología PMP.</li> <li>- Experiencia en la operación SWIFT.</li> </ul> <p><b>Especialización:</b> Contar con certificación oficial en alguna de los siguientes puntos:</p> <ul style="list-style-type: none"> <li>- LEAD AUDITOR: ISO 27001:2013</li> <li>- CISA: Certified Information Security Auditor</li> <li>- CISSP: Certified Information System Security Professional</li> <li>- CISM: Certified Information Security Manager</li> <li>- QSA: Qualified Security Assessors - PCI</li> <li>- Al menos uno de los integrantes del equipo debe tener certificación como Swift certified specialist expert.</li> </ul>
<b>Auditor</b>	<p><b>Carrera Profesional:</b> Ingeniería de Sistemas o Ingeniería de Computación e Informática o Ingeniería Industrial o carreras afines. Grado Académico: Titulado.</p> <p><b>Experiencia Profesional:</b> Contar con al menos 3 años de experiencia en los siguientes puntos:</p> <ul style="list-style-type: none"> <li>- Procesos de Implementación de Controles CSP en entidades del Sector Financiero, Corporativo o Service Bureau en los procesos de implementación de controles del Framework CSCF 2021.</li> <li>- Experiencia en gestión de proyectos o metodología PMP.</li> <li>- Experiencia en la operación SWIFT.</li> </ul> <p><b>Especialización:</b> Contar con certificación oficial en alguna de los siguientes puntos:</p> <ul style="list-style-type: none"> <li>- LEAD AUDITOR: ISO 27001:2013</li> <li>- CISA: Certified Information Security Auditor</li> <li>- CISSP: Certified Information System Security Professional</li> <li>- CISM: Certified Information Security Manager</li> <li>- QSA: Qualified Security Assessors - PCI</li> <li>- Al menos uno de los integrantes del equipo debe tener certificación como Swift certified specialist expert.</li> <li>- Adicionalmente al menos uno de los integrantes del equipo debe tener certificación como Certified ISO 31000 Lead Risk Manager.</li> </ul>

**NOTA IMPORTANTE:**

El postor deberá entregar la documentación correspondiente al perfil requerido, manifestando sus habilidades correspondientes al servicio ofertado, antes de la firma de la orden de servicio.

Para sustentar la formación académica del personal propuesto se deberá presentar copia simple de sus diplomas y/o títulos y/o constancia de estudios realizados.

Para sustentar la experiencia profesional se deberá presentar las certificaciones o constancias de trabajo o contrato y su respectiva conformidad, donde se indique claramente la vigencia del servicio, nombres y apellidos, y nombre del proyecto o actividades realizadas.

El personal propuesto solo podrá ser reemplazado por causas justificables aceptadas por la Corporación, y siempre que medie un aviso previo de 15 días de anticipación. El reemplazante deberá cumplir con igual o mejor perfil que el personal sustituido.

## **6. DESCRIPCIÓN DEL SERVICIO**

### **6.1 Antecedentes**

A partir del 2017 y con el objetivo de promover y mejorar la seguridad de los usuarios de la comunidad SWIFT y de la red de comunicaciones financieras, Swift inició el programa de seguridad conocido como Customer Security Program - CSP, de obligatorio cumplimiento por todas las entidades que forman parte del sistema.

El Programa y sus requisitos están consignados en la documentación provista por SWIFT y son de especial aplicación para el objeto de esta solicitud de servicios los siguientes:

- Customer Security Controls Framework (CSCF) v2023
- Independent Assessment Framework (IAF)
- Políticas del Customer Security Program (CSP)
- Términos y Condiciones del Customer Security Program

Para la versión 2023 del Programa están definidos 32 controles, de los cuales 24 son de obligatorio cumplimiento y 8 son recomendados, quedando a discreción de la entidad su implementación.

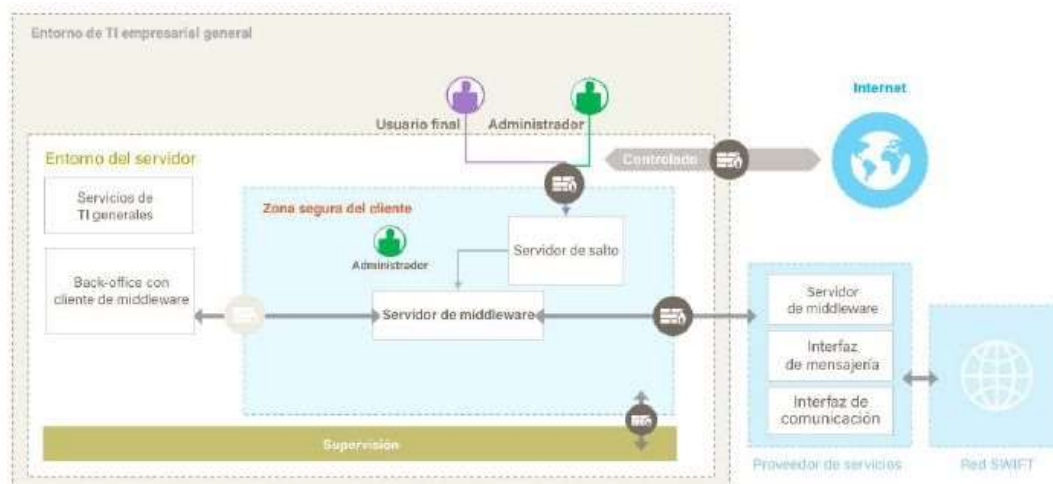
Adicionalmente, a partir del 2021 será obligatorio certificar como mínimo el cumplimiento de los controles obligatorios con una auditoría independiente, según está definido en el Independent Assessment Framework (IAF).

### **6.2 Plataforma Actual**

COFIDE cuenta con una plataforma Full Service Bureau certificado por SWIFT, montada sobre una infraestructura de terceros, permitiendo la conectividad hacia los servidores Swift, a través de una Aplicación o Plataforma de acceso Web segura.

Nuestra plataforma de servicio cuenta con una Arquitectura tipo A4 (Figura N°1), la cual nos permite enviar mensajería y transacciones interbancarias al exterior, cumpliendo con los estándares de seguridad exigidos por el Customer Security Programme (CSP) de SWIFT, asegurando la vigencia y cumplimiento de programas futuros.

**Diagrama 13b: Ejemplo de zona segura para la Arquitectura A4**  
**Servidor de middleware como conector del cliente**



**Figura N°1**

### 6.3 Alcance del servicio

COFIDE requiere el servicio de una consultoría que nos ayude a identificar las brechas de seguridad, con respecto a los 32 controles exigidos por SWIFT (Ver Anexo A). Así mismo este servicio ayudará en la recolección de evidencias, para el cumplimiento de los lineamientos del Customer Security Control Framework (CSCF) de SWIFT.

Adicionalmente a partir del 2021, debido a las exigencias de SWIFT se requiere contar con una entidad independiente, que cumpla con lo establecido en el Independent Assessment Framework (IAF), que verifique los controles implementados y recolectar las evidencias necesarias según el Customer Security Controls Framework (CSCF). Para ello, es necesario el servicio de Auditoría SWIFT, el cual nos permitirá cumplir con este nuevo requisito, el mismo que contrasta y valida la ejecución de la implementación de los controles del Customer Security Controls Framework (CSCF) con la información registrada en el proceso de “attestation” del KYC SA (Know your Customer Self Assessment).

El servicio a contratar está conformado por los siguientes rubros:

- Consultoría CSP
- Auditoría CSCF

En resumen, la consultoría y auditoría especializada, debe incluir como mínimo lo siguiente:

- Realizar el análisis de la arquitectura SWIFT de producción y contingencia.
- Realizar diagnóstico de los controles existentes en la organización frente a los objetivos, principios, controles y directrices del Customer Security Controls Framework (CSCF) aplicables a la arquitectura SWIFT de la organización.
- Presentar informe con el diagnóstico y las recomendaciones para el debido cumplimiento de estos controles, basados en los hallazgos que pudieran encontrarse.
- Realizar el acompañamiento a la implementación de las recomendaciones consignadas en el informe.
- Realizar auditoría del Customer Security Controls Framework (CSCF) 2023 en los términos definidos en el Independent Assessment Framework (IAF) de Swift y metodologías aplicables a esta actividad.

- Presentar los informes y documentos recomendados por SWIFT como soporte de la evaluación, tanto para la consultoría como para la auditoría.
- Acompañar en la presentación de la Atestiguación, a solicitud de la entidad.

## **7. CONDICIONES DEL SERVICIO**

Todos los servicios a los que está obligado a realizar el POSTOR para cumplir con lo indicado en los numerales siguientes están incluidos en el servicio requerido y no representa costo adicional para COFIDE.

### **7.1 De COFIDE:**

- Proporcionar acceso a los ambientes necesarios durante el periodo de levantamiento de información.
- Brindar oportunamente toda la información y/o documentación necesaria para que el postor realice la ejecución del servicio.

### **7.2 Del POSTOR:**

- El postor debe demostrar experiencia en plataformas SWIFT acreditado por SWIFT.
- El postor debe contar con experiencia en la prestación de consultorías y auditorías del Customer Security Program (CSP) y Customer Security Controls Framework (CSCF).
- El postor debe estar registrado ante SWIFT para prestar los servicios de Evaluación del CSP (CSP Assessment)
- El postor debe certificar que cuenta con una metodología para la prestación de los servicios de consultoría y auditoría del CSCF
- El servicio debe prestarse para los ambientes de Producción y Contingencia.
- El Proveedor debe prestar los servicios con personal de habla hispana.
- El Proveedor debe contar con el personal necesario para prestar los servicios y que estos cumplan con la experiencia y requisitos establecidos en el Independent Assessment Framework - IAF.
- El Proveedor deberá asignar a un responsable principal, el cual será el único punto de contacto con COFIDE, el mismo que estará a cargo de todas las coordinaciones y será el responsable del cumplimiento de lo solicitado en el Punto ALCANCE DEL SERVICIO.
- Es responsabilidad del Proveedor, coordinar con el staff del proyecto las fechas de las reuniones y/o entrevistas para el levantamiento de la información.

### **7.3 Etapas del Servicio:**

Cada uno de los rubros que conforman el servicio se dan de manera independiente con sus plazos y entregables:

#### **7.3.1 Proceso de Consultoría CSP**

A continuación, se detalla la duración de cada etapa del proceso.

**a. Etapa 1 - Planeación:** Análisis de la arquitectura SWIFT (A1, A2, A3, **A4** y B) que tenga COFIDE implementada, al momento de la contratación del servicio.

✓ Duración: **01 Semana**, después de la firma del acta de inicio de servicio.

**b. Etapa 2 - Ejecución:**

- Validación e identificación de los controles aplicables a su infraestructura (obligatorios – opcionales).

- Validación de los riesgos y controles aplicables a la arquitectura del cliente, acorde a la versión del CSP Programme vigente al momento de la contratación de la asesoría.

✓ Duración: **02 Semanas**, después de culminada la etapa1.

**c. Etapa3 – GAP y Análisis:** Informe con las recomendaciones, planes de acción definidos con cada uno de los responsables

Informe incluye: Descripción y diagnóstico del hallazgo, los riesgos asociados y las recomendaciones para solucionar los hallazgos encontrados. El plan de acción a seguir quedará a potestad de COFIDE.

✓ Duración: **02 Semanas**, después de culminada la etapa2.

**d. Etapa4 – Cierre:** Entrega del informe final y acompañamiento a la atestiguación preliminar en la herramienta provista por SWIFT, a decisión de COFIDE.

✓ Duración: **01 Semana**, después de culminada la etapa3.

**e. Etapa5 – Seguimiento:** Seguimiento a demanda a los planes de acción definidos.

El proveedor otorgará a COFIDE el plazo necesario, para subsanar los hallazgos encontrados aplicando las recomendaciones otorgadas, previo al inicio del servicio de auditoría CSCF. El plazo otorgado, no deberá afectar el normal desenvolvimiento de la auditoría CSCF.

### 7.3.2 Proceso de Auditoría CSCF

**a. Etapa 1 - Planeación:**

- Sesión virtual de acercamiento.
- Términos de Referencia: Establecimiento de los criterios, alcance y objetivos de la auditoría.
- Generación de Acuerdo de Confidencialidad.
- Análisis de la arquitectura SWIFT (A1, A2, A3, **A4** y B) de producción y contingencia implementada, al momento de la contratación del servicio.
- Solicitud de documentos soporte para la auditoría (basado en lista de Chequeo).
- Análisis de los documentos recibidos.
- Definición y establecimiento del Equipo de Trabajo.
- Elaboración del plan de auditoría según el archivo: CSCF Assessment Template for Mandatory and Advisory Controls (en la versión vigente para la fecha de contratación) y equipo de trabajo que atenderá los controles. Cronograma de la Inspección.

✓ Duración: **01 Semana**, después de firmada el acta de **Inicio del Servicio de Auditoría CSCF**.

**b. Etapa 2 - Inspección: (Sesiones Virtuales Remotas)**

- Sesión virtual de inicio de auditoría con dueños de los controles CSP. (Meet, Go to Meeting, Zoom, MS Teams o Webex), programado por el Auditor Líder.

- Desarrollo de la inspección: verificación a través de entrevistas, observación u otros medios, según el plan de auditoría diseñado y documento CSCF Assessment Template for Mandatory and Advisory Controls (en la versión vigente para la fecha de contratación). Estas sesiones se realizan de forma virtual en donde el responsable o designado de la ejecución del control sustentará y mostrará evidencias en vivo de la eficacia de los controles. (Por ejemplo, el responsable de la administración de los Firewalls relacionados con la infraestructura SWIFT, ingresará a su consola en vivo y en directo para mostrar al Auditor las políticas de seguridad operativas a la infraestructura evaluada).
- Recolección de evidencias para cada control del ambiente productivo y contingencia. Durante la sesión, se deben tomar pantallazos o capturas de información como sustento de la efectividad de los controles. Estos deben ser entregados al Auditor según las características de identificación que acuerden.
- Declaración de hallazgos u observaciones de auditoría durante el proceso de inspección virtual sobre el cumplimiento CSCF.
- Pre-Informe: Respuestas de la administración a cada punto. Definición de las fechas de cierre. (Este preinforme se incluye únicamente cuando se adquiere con la opción de un punto de chequeo posterior).

Nota: Es obligatorio mostrar en vivo y en directo durante las sesiones virtuales, la implementación de los controles evaluados.

✓ Duración: **02 Semanas**, después de culminada la etapa 1.

**c. Etapa 3 – (Cierre e Informe)**

- Sesión virtual para el cierre de la auditoría con los aspectos relevantes. Esta reunión se realiza el último día del proceso de inspección en compañía de los responsables de los controles.
- Entrega informe de observaciones de auditoría (8 días hábiles después). Aunque el servicio termina con la entrega del informe de auditoría, el cliente puede solicitar la realización de sesiones "Checkpoint" para la validación de cierres de hallazgos. La carta firmada por nuestro Lead Auditor ISO 27001 - SWIFT Certificate Expert, así como los Templates SWIFT, deberán ser subidos a la página por parte del cliente. Esta labor puede ser apoyada por nuestro personal.

**8. GESTIÓN DEL PERSONAL**

No aplica.

**9. OTRAS PENALIDADES**

No aplica.

**10. ENTREGABLES**

El POSTOR está obligado a presentar la siguiente documentación, en el proceso en que corresponda.

**10.1 Proceso de Consultoría CSP**

Etapas del Servicio	Entregable	Plazo de entrega
Etapas 1	<ul style="list-style-type: none"> <li>• Acta de Inicio del Servicio Consultoría CSP</li> <li>• Informe de Levantamiento de Información.</li> <li>• Cronograma y Plan de Trabajo Detallado</li> </ul>	Hasta 1 semana posterior a la fecha indicada en el acta de inicio de



		servicio de consultoría CSP
Etapa 2, Etapa 3, Etapa 4, Etapa 5	<ul style="list-style-type: none"> <li>Resumen ejecutivo.</li> <li>Informe de diagnóstico de la situación respecto del CSP 2023 y recomendaciones para la remediación de los hallazgos encontrados.</li> </ul>	Hasta 6 semanas posterior a la fecha indicada en el acta de inicio del servicio

Luego de finalizada la consultoría, tanto el PROVEEDOR como COFIDE acordarán el plazo necesario, para subsanar los hallazgos encontrados, sin que esto afecte el normal desarrollo del cronograma del servicio de auditoría exigida por SWIFT. Para dar inicio del proceso de auditoría CSCF, el proveedor entregará los informes de reuniones de avance del plan de implementación de las recomendaciones.

## 10.2 Proceso de Auditoría CSCF

Etapa del Servicio	Entregable	Plazo de entrega
Etapa 1	<ul style="list-style-type: none"> <li>Acta de Inicio del Servicio Auditoría CSCF</li> <li>Informe de análisis del alcance de los objetivos a evaluar.</li> <li>Durante esta etapa se debe aprobar el Plan de Auditoría a firmar entre el proveedor y COFIDE.</li> </ul>	Hasta 1 semana posterior a la fecha indicada en el acta de inicio del servicio de auditoría CSCF
Etapa 2 Etapa 3	<ul style="list-style-type: none"> <li>Resumen ejecutivo e informe de la auditoría realizada.</li> <li>Certificación expedida en los términos estipulados en el Independent Assessment Framework - IAF.</li> <li>Formatos con detalle del cumplimiento de los controles obligatorios y recomendados, en los términos estipulados en el Independent Assessment Framework - IAF.</li> </ul>	Hasta 4 semanas posterior a la fecha indicada en el acta de inicio del servicio de auditoría CSCF

Los entregables serán remitidos al Departamento de Tecnologías de la información en formato digital (PDF), vía correo electrónico a los siguientes emails:

- [mesadepartes@cofide.com.pe](mailto:mesadepartes@cofide.com.pe)
- [entregablesti@cofide.com.pe](mailto:entregablesti@cofide.com.pe)

## 11. PLAZO DEL SERVICIO

El plazo total del servicio es de siete (07) semanas para el proceso de Consultoría CSP y cinco (05) semanas para el proceso de la Auditoría CSCF y se iniciará a partir de la fecha indicada en el **Acta de inicio del servicio** de cada proceso.

## 12. FORMA DE PAGO

La forma de pago será del 100% al inicio del servicio por ser una condición de la contratación al ser un proveedor no domiciliado.





**COFIDE**

EL BANCO DE DESARROLLO DEL PERÚ

**13. GARANTÍA**

No Aplica

**14. DEPENDENCIA ENCARGADA DE DAR LA CONFORMIDAD DEL SERVICIO**

La conformidad del servicio será otorgada por el Subgerente de Tecnologías de Información.

**15. REQUISITOS DE CALIFICACIÓN DE POSTORES**

No aplica.

**16. SUB CONTRATACIÓN SIGNIFICATIVA**

Si contestó Sí a la consulta: ¿El requerimiento podría ser desarrollado por COFIDE?, responder lo siguiente:

- a. En caso de falla o suspensión del servicio, ¿Podría verse afectada la Corporación respecto a:  
Ingresos: Sí ..... No ...x.... Solvencia: Sí ..... No ...x....  
Continuidad Operativa: Sí ..... No ...x....
- b. Identificar y marcar el proceso de la Corporación que esté relacionado con el contrato del servicio solicitado:

P01	P02	P03	P04	P05	P06	P07	P08	P09	<del>P10</del>	P11
-----	-----	-----	-----	-----	-----	-----	-----	-----	----------------	-----

P01= Captación

P02= Colocación

P03= Invers. y Gestión de Tesorería

P04= Fideic. y Comis. de Confianza

P05= Cartera Cedida

P06= Desarrollo de Nuevos Productos

P07= Apoyo al Desarrollo Económico

P08= Dirigir el Negocio

P09= Servicios Financieros

P10= Proveer Recursos Corporativos

P11= Registro y Control Operacional

## ANEXO -Security Controls Summary Table

Mandatory and Advisory Security Controls	Architecture Type				
	A1	A2	A3	A4	B
<b>1 Restrict Internet Access and Protect Critical Systems from General IT Environment</b>					
1.1 SWIFT Environment Protection	•	•	•		
1.2 Operating System Privileged Account Control	•	•	•	•	•
1.3 Virtualisation Platform Protection	•	•	•	•	
1.4 Restriction of Internet Access	•	•	•	•	•
1.5 Customer Environment Protection				•	
<b>2 Reduce Attack Surface and Vulnerabilities</b>					
2.1 Internal Data Flow Security	•	•	•		
2.2 Security Updates	•	•	•	•	•
2.3 System Hardening	•	•	•	•	•
2.4A Back Office Data Flow Security	•	•	•	•	•
2.5A External Transmission Data Protection	•	•	•	•	
2.6 Operator Session Confidentiality and Integrity	•	•	•	•	•
2.7 Vulnerability Scanning	•	•	•	•	•
2.8A Critical Activity Outsourcing	•	•	•	•	•
2.9 Transaction Business Controls	•	•	•	•	•
2.10 Application Hardening	•	•	•		
2.11A RMA Business Controls	•	•	•	•	•
<b>3 Physically Secure the Environment</b>					
3.1 Physical Security	•	•	•	•	•
<b>4 Prevent Compromise of Credentials</b>					
4.1 Password Policy	•	•	•	•	•
4.2 Multi-Factor Authentication	•	•	•	•	•
<b>5 Manage Identities and Separate Privileges</b>					
5.1 Logical Access Control	•	•	•	•	•
5.2 Token Management	•	•	•	•	•
5.3A Staff Screening Process	•	•	•	•	•
5.4 Physical and Logical Password Storage	•	•	•	•	•
<b>6 Detect Anomalous Activity to Systems or Transaction Records</b>					
6.1 Malware Protection	•	•	•	•	•
6.2 Software Integrity	•	•	•	•	
6.3 Database Integrity	•	•		•	
6.4 Logging and Monitoring	•	•	•	•	•
6.5A Intrusion Detection	•	•	•	•	
<b>7 Plan for Incident Response and Information Sharing</b>					
7.1 Cyber Incident Response Planning	•	•	•	•	•
7.2 Security Training and Awareness	•	•	•	•	•
7.3A Penetration Testing	•	•	•	•	•
7.4A Scenario Risk Assessment	•	•	•	•	•