Descrição do Serviço

Consultoria Geral de PCI PIN

Sumário

Consultoria Geral de PCI PIN

A SecureTrust™ é uma divisão da Trustwave Holdings, Inc.

DESCRIÇÃO DO SERVIÇO

A Consultoria Geral em Números de Identificação Pessoal do Setor de Cartões De Pagamento (PCI PIN – Payment Card Industry Personal Identification Number) da SecureTrust (o "**Serviço**") é uma consultoria para design de soluções, design de aplicativos, políticas, procedimentos e práticas empregadas ou de uso pretendido para organizações visando conformidade com os requisitos de segurança PCI PIN e o Guia do Programa do Avaliador de PIN qualificado (QPA – Qualified PIN Assessor), conforme estabelecido pelo Conselho de Padrões de Segurança do PCI (o "Padrão").

Os termos em maiúsculas usados nesta descrição de serviço, mas não definidos aqui, têm seus significados indicados no Contrato Principal de Serviços da Trustwave localizado em https://www.trustwave.com/en-us/legal-documents/contract-documents/ ou em um contrato similar assinado entre a SecureTrust e o Cliente.

RECURSOS DO SERVIÇO BÁSICO

O Serviço inclui os seguintes recursos padrão:

Portal SecureTrust

Os recursos do Portal SecureTrust consistem, entre outros, em um aplicativo de Gerenciamento de conformidade para administrar o processo de engajamento, bem como para coletar e armazenar com segurança evidências, documentação e produtos finais.

Serviços Globais de Conformidade e Risco

A equipe de Serviços Globais de Conformidade e Risco (GCRS — Global Compliance and Risk Services) é composta, entre outras, pelas seguintes pessoas e funções de destaque:

Avaliador de PIN qualificado (QPA – Qualified PIN Assessor) – Um QPA é o recurso principal para a execução do Serviço, responsável pelo agendamento e pela condução das atividades de consultoria.

Consultor gerencial (MC – Managing Consultant) – Um MC fornece orientação, supervisão de projeto e garantia de qualidade de relatórios ao QPA, além de servir como ponto de contato secundário do Cliente para escalamentos e consultas.

Conselho de Revisão de Conformidade (CRB – Compliance Review Board) – O CRB serve como ponto final para a interpretação dos Requisitos de segurança da versão 3 do PCI PIN ou para a solução de questões complicadas de conformidade, fornecendo consistência e continuidade ao longo das avaliações da SecureTrust. O CRB também é o ponto final de escalamento para a solução de problemas relativos a status de conformidade contra os requisitos do Padrão ou a revisão de um controle de compensação.

Consultoria geral de PCI PIN – Um QPA da SecureTrust oferece ao Cliente consultoria geral na interpretação de requisitos, desafios de conformidade, projeto de solução ou aplicativo, políticas,

procedimentos e outros assuntos relacionados ao Padrão. O QPA pode auxiliar na análise das operações e salvaguardas de segurança de PCI PIN existentes ou planejadas do Cliente por meio de consultoria remota ou no local.

ENTREGA E IMPLEMENTAÇÃO

Início do projeto

A equipe de GCRS da SecureTrust inicia o Serviço agendando e conduzindo uma reunião de abertura remota para definir e chegar a um acordo sobre um plano de projeto de alto nível que consiste em datas de marcos importantes, etapas principais, estimativas de duração, requisitos de recursos e procedimentos de escalamento.

A SecureTrust solicitará informações iniciais e agendará reuniões futuras. O Cliente fornecerá uma visão geral preliminar do ambiente de PCI PIN do Cliente.

Fase I: Coleta de informações

A SecureTrust e o Cliente trabalharão para coletar e analisar informações sobre o ambiente de PCI PIN do Cliente.

A SecureTrust examinará a documentação de projeto aplicável para compreender a funcionalidade do ambiente de PCI PIN do Cliente, os processos de manipulação de dados e os parâmetros de projeto.

Os tópicos para coleta de informações podem incluir, entre outros:

- Determinar ativos críticos.
- Examinar processos de negócios.
- Identificar processos de gerenciamento de segurança e conformidade vigentes e revisar a documentação de conformidade ou avaliação prévia.

Fase II: Consultoria geral de PCI PIN

O Serviço pode ocorrer no local das instalações do Cliente, ou pode ser fornecido remotamente, a critério da SecureTrust. Um QPA da SecureTrust trabalhará junto com o Cliente para determinar as áreas do Padrão em que é necessário se concentrar.

A SecureTrust fornecerá consultoria sobre áreas acordadas entre o Cliente e a SecureTrust relativas ao ambiente de PCI PIN do Cliente. A consultoria será fornecida de acordo com o Padrão, discutindo requisitos de teste e sua aplicabilidade ao ambiente do Cliente.

As atividades do Serviço podem incluir, entre outras:

- Revisão de políticas e procedimentos.
- Avaliação das configurações do sistema.
- Entrevistas.
- Observação de processos e procedimentos realizados, de acordo com a documentação coletada durante a fase de Coleta de informações.
- Inspeção física das instalações e dos equipamentos.
- Identificação e revisão de alto nível de terceiros usados no apoio do ambiente de PCI PIN do Cliente e consultoria sobre requisitos específicos de PCI PIN.

A SecureTrust trabalhará com o Cliente para resolver as dúvidas de avaliação do Cliente. A SecureTrust também fornecerá ao cliente assistência razoável na interpretação do Cliente dos Padrões e de suas respostas. A SecureTrust pode solicitar revisão adicional do ambiente de PCI PIN do Cliente, documentação ou processos e procedimentos de manipulação de dados.

O Serviço não tem a intenção de se concentrar em nenhum controle específico, a menos que explicitamente acordado entre a SecureTrust e o Cliente. O propósito do Serviço é o de auxiliar o Cliente na determinação do melhor curso de ação para as áreas de concentração de PCI PIN e auxiliar o Cliente a fazer uma determinação de suas capacidades para realizar uma avaliação de segurança de PCI PIN, e, quando possível, identificar áreas prioritárias para correções.

Fase III: Relatórios

O Serviço não inclui nenhum produto de relatório, pois é um serviço de consultoria por hora.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente.

RESPONSABILIDADES DA SECURETRUST

- Estabelecer contato e permanecer disponível para comunicações com o Cliente.
- Estabelecer comunicação e planos de escalamento.
- Criar uma conta do Cliente no Portal SecureTrust.
- Definir o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração e requisitos de recursos.
- Agendar e conduzir reuniões de abertura, status periódico e fechamento.
- Entrevistar o pessoal apropriado da organização e coletar informações dessas pessoas.
- Fornecer ao Cliente feedback sobre observações identificadas durante o Serviço que possam exigir correção.

RESPONSABILIDADES DO CLIENTE

- Estabelecer contato e permanecer disponível para comunicações com a SecureTrust.
- Estabelecer comunicação e planos de escalamento.
- Concordar com o plano de projeto de alto nível, consistindo em datas de marcos importantes, etapas principais, estimativas de duração e requisitos de recursos.
- Fornecer com precisão todas as informações necessárias, incluindo principais partes interessadas, informações aplicáveis sobre o ambiente do Cliente e requisitos de configuração.
- Informar à SecureTrust sobre todas as atividades de manutenção do ambiente do Cliente e sobre mudanças que podem impactar o fornecimento do Serviço.
- Responder com precisão às solicitações das equipes da SecureTrust ao estabelecer contato e na coleta das informações necessárias.
- Fornecer detalhes completos e precisos sobre o ambiente relevante e outras informações sobre as operações de negócios.
- Tornar disponíveis recursos capazes de participar das atividades do Serviço.
- Participar de e compreender os materiais explicados durante as chamadas, reuniões, entrevistas, discussões, inspeções de instalações e análises de controles.
- Aceites do cliente:
    - Todas as atualizações de segurança e recursos do Portal SecureTrust serão incluídas em atualizações de versões principais.

- O Serviço usa os requisitos e procedimentos de teste do Padrão atual aplicável na ocasião da data de início do Serviço.
- O Serviço não inclui nenhum produto de relatório, pois é um serviço de consultoria por hora.
- Os Serviços não incluem testagem ou revisão profunda das configurações do sistema, definições ou a observação de processos e procedimentos implementados.
- O Serviço não inclui visitas a terceiros usados para apoio ao ambiente de PCI PIN do Cliente.
- O Serviço pode consistir em atividades de avaliação remota e no local.
- A SecureTrust poderá solicitar evidências dos sistemas e processos do Cliente conforme necessário para comprovar a conformidade com quaisquer requisitos específicos. O Cliente concorda em fornecer todas essas evidências o mais breve possível.
- Todos os serviços de PCI PIN selecionados para um único SOW ou Formulário de pedido devem ser por uma vigência idêntica. A SecureTrust não é responsável por definir sistemas em escopo nem pela exatidão das informações fornecidas pelo Cliente.
- A SecureTrust reserva-se o direito de rejeitar ou aceitar comentários do Cliente baseados nos fatos e circunstâncias do Serviço.
- A SecureTrust desempenhará o Serviço no idioma inglês.
- A SecureTrust não fornecerá serviços corretivos como parte do Serviço.
- A SecureTrust não oferecerá nenhuma orientação ou aconselhamento legal.
- A qualidade e a precisão do Serviço dependem do fornecimento pelo Cliente de informações precisas e acesso aos sistemas e recursos do Cliente para a SecureTrust.