Risk Solutions

Fraud Prevention Self Assessment

Helping organisations to manage payment-related fraud risk

Authorities such as UK Finance report increasing levels of payment fraud, with many hundreds of £millions lost every year. Attackers have become specialists in their target sectors by building a thorough knowledge of operating methods, technologies, and suppliers, along with sector-specific vulnerabilities, including those in the legal, financial, medical, and public sectors, to name a few.

Whilst no business is immune, we know that professional and scientific organisations are being targeted for other purposes alongside fraud. The large sums held in client accounts, high number of transactions, and the intellectual property and personal data held increases the threat of extortion from releasing data or preventing system access, and if actualised, can result in significant interruption and reputational damage.

Prevent fraud loss and improve your risk profile

As fraudsters leverage new technologies such as Artificial Intelligence, businesses need to ensure their fraud prevention and cyber security controls remain robust against current and emerging attack methods. Many of the frauds experienced by organisations take advantage of poor payment procedures, the blind trust that individuals place in IT, and their natural vulnerability to being socially engineered.

We have developed our fraud prevention risk assessment and the associated guidance, checklists, and template resources, to help you determine your ability to manage fraud risk, specifically in relation to payees and payments. Addressing any recommended risk improvements can improve your risk profile and demonstrate to stakeholders your commitment to preventing fraud.

About the Fraud Prevention Self Assessment

The self assessment evaluates risk controls in four vital areas:

> **Fraud prevention policy and awareness training:** focusing on reducing the opportunity for fraud through effective leadership, governance, training, and education.

> **Security of your payment systems and processes:** addressing specific payment controls, user access security, recruitment processes and online identity management.

> **Security best practice with your bank:** dealing with identity theft and banking fraud.

> **Compliance and cyber security:** covering incident reporting processes, and controls to protect data and limit technology-related crime.

Adding value to your insurance policies

In addition to minimising fraud risk for your business, extra value can be gained if you:

> claim CPD for time spent on learning through the self-assessment process

> access the QRisk Knowledge Centre and apply the wealth of practical guidance available

> use the easily adaptable templates to address any development areas identified

> build resilience further by using the wide range of other self assessments available – from risk culture or governance effectiveness, to mental health and wellbeing

> engage with eLearning providers and other Solution Panel members at discounted rates.

Where appropriate, assessments can be delivered as a facilitated review by a QBE Senior Risk Manager. Qualification for this depends on service level agreed, longevity of our relationship, and/or premium paid. Just ask your usual QBE or broker contact for details or email us on rs@uk.qbe.com

Easy to access and use

Access to our self assessments and supporting content is through our dedicated online customer portal, QRisk. Here you can complete your self assessments, download your reports, and update your risk improvements using the range of templates and practical guides to help implement any changes needed.

So head to the QRisk portal and log in using your work email and QBE policy number, or visit the QRisk webpage for more information.

QBE European Operations
30 Fenchurch Street
London EC3M 3BD
+44 (0)20 7105 4000
QBEeurope.com

792204/2412