

You ask the question, we find the answer

The how, who and why of criminal record checks, dealing with cyber attacks and registering as a TCSP are addressed in this month's trio of questions

Q: DO I NEED TO DO CRIMINAL RECORD CHECKS FOR ALL THE PRINCIPALS IN MY FIRM?

A: The short answer is yes. The requirement comes from Regulation 26 in The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17). It sets out certain responsibilities and requirements on supervised firms as well as supervisory authorities.

Firstly, as a Supervisory Authority, ICAEW must approve all beneficial owners, officers and managers (BOOMs) in the firms they supervise, and secondly, all supervised firms must take reasonable care to ensure no one is appointed, or continues to act, as a BOOM without approval.

Regulation 26 also states that ICAEW, as a supervisory authority, can only approve a BOOM if that individual has no relevant unspent criminal convictions. To prove that an individual has no relevant unspent criminal convictions, we require all BOOMs to obtain criminal record checks.

HM Treasury has confirmed that we are not able to accept self-declarations as proof. They have also confirmed that a basic DBS check is sufficient.

ICAEW will ask to see the original DBS check certificate during our onsite Practice Assurance monitoring visits. We have also written to a sample of firms to ask them to submit the original DBS certificate for all the BOOMs in the firm. The sample is based on risk factors agreed by the accountancy sector AML supervisory authorities, as informed by the National Risk Assessment.

These include whether there are higher risk factors present in a firm's service or client portfolio, the structure of the firm, the geographical reach of the firm or the firm's channels of engagements. We use information you provide on your annual return to identify these high risk factors.

You can find further information on criminal record checks at icaew.com/criminalchecks

Michelle Giddings, senior manager, Professional Standards, ICAEW

Q: WHAT IS HMRC'S TRUST OR COMPANY SERVICE PROVIDERS REGISTER, AND CAN WE GET ON IT?

A: HMRC holds a register of all trust or company service providers (TCSPs). Anyone providing such services is required to be on HMRC's TCSP register.

MLR17 defines a TCSP in regulation 12(2). A firm will be a TCSP where any of the following services are provided by way of business: forming companies or other legal persons; acting, or arranging for another person to act, as a director or secretary of a company, as a partner of a partnership, or in a similar capacity in relation to other legal persons; providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or other legal person or legal arrangement; acting, or arranging for another person to act, as a trustee of an express trust or similar legal arrangement, or a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

Where ICAEW is your firm's money laundering supervisor, you won't need to register separately with HMRC. If you told ICAEW (in your last annual return) that you provide such services, your firm will have already been added to the register by ICAEW and this will have been confirmed by email to you. If you have not told ICAEW that you perform TCSP work but want to be included on the register, email AMLR@icaew.com with your firm details and a request to be added. Firms should also check the guidance available on the ICAEW webpage on the HMRC TSCP register (icaew.com/technical/legal-and-regulatory/hmrc-tcsp-register).

Further guidance on your specific circumstances is available to members from the ICAEW Anti-Money Laundering Helpline on +44 (0)1908 248 250.

Chris Turner, professional consultant for ICAEW's Technical Advisory Service

There are many forces shaping accountancy practices, from regulation and skills to technological advancement and economic change. If you have a question or need advice about any of these things and more, please email us at economia@icaew.com and we'll find the answer for you

Q: HOW DO WE DEAL WITH LOSING CLIENT PERSONAL DATA IN A CYBER ATTACK?

A: It depends on what you have in place, and the nature of the attack. The disruption caused can be minimised by discussing, creating, documenting, publishing and regularly testing and reviewing a business resiliency plan (BRP).

Before an attack or data breach takes place: create and test a BRP. Allocate responsibilities - who will do what if an attack takes place? Revise, update and test the BRP in line with changing technology and client and business needs.

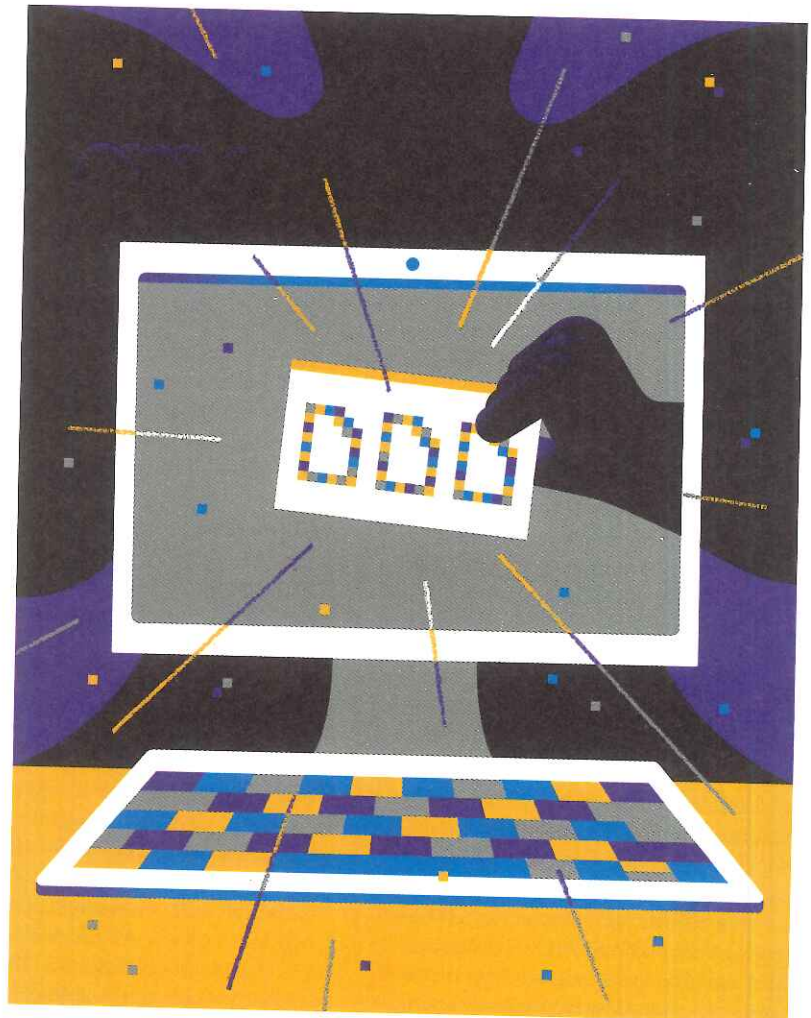
If a cyber attack has taken place: understand the issue: has data been lost? What do you need to tell your clients or regulators? Preserve the system log and files as these could be used by those investigating the cyber attack. Contain the damage, and identify which systems need to be shut down or isolated. Eradicate the cause of the issue - this may involve outside IT specialists. Do not rush to come back online. Be confident you can operate normally.

ICAEW will be producing a Tech Essential Guide to Cyber Recovery early in the new year. In addition, our example password policy (tinyurl.com/ICAEW-passwordpolicy) could help you reduce the likelihood of a cyber attack being successful.

Mark Taylor, technical manager - technical innovation, IT Faculty, ICAEW

“If a cyber attack has taken place, preserve the system and log files, as these could be used by those investigating the attack”

Mark Taylor, technical manager - technical innovation, IT Faculty



Five in brief

01

IFRS 16, Leases

The new standard on leases prescribes a single lessee accounting model requiring the recognition of asset and corresponding liability for all leases with terms over 12 months, unless the underlying asset is of low value.

icaew.com/ifrs16

02

FRS 102

The key changes to FRS 102 cover directors' loans to small entities, investment properties and intangible assets acquired in business combinations. Read *IFRS 102 Triennial Review 2017 Amendments - What Are the Changes?*

icaew.com/ukgaapfaqs

03

Corporate governance rules

The Companies (Miscellaneous Reporting) Regulations 2018 requires large companies to include an s172 statement in their strategic reports and ensure PIEs explain what corporate governance code they have adopted and if they haven't, why not.

frc.org.uk

04

Piloting MTD for VAT

HMRC has extended its pilot scheme to around half a million businesses whose affairs are up to date and straightforward, and will be opening up for most other business types over the coming months. Check if you can use the pilot to make sure you're ready before it is mandatory.

icaew.com/MTD

05

Contractor loans

Finance Act (No 2) 2017 introduced a new charge on outstanding disguised remuneration loans, known as the 2019 loan charge. This will apply to all loans made since 6 April 1999 if they are still outstanding on 5 April 2019.

icaew.com/tax

ILLUSTRATION BY ANDREA MANZATI