Repository of GRA features in ILC Newsletters 2021

Newsletter – 1 January 2021

1. The UK Treasury launched a consultation in December 2020 to seek comment on the UK's ***Overseas Framework*** for cross border financial services. In particular this exercise is to learn more of how the current legislative and regulatory regimes can continue to attract activity to the UK while supporting stability in the financial markets. The consultation document provides a wealth of information to better understand these processes, including areas of specific interest:

- the overseas persons exclusion (OPE),
- the Financial Promotion Order (FPO),
- recognised overseas investment exchanges (ROIE),
- overseas long-term insurers, and
- investment services equivalence (Title VIII) under the Markets in Financial Instruments Regulation (MiFIR).

Whether or not one participates in the consultation (closes 11 March 2021), the background context and information is useful to understand some of the activity the UK is considering in developing its post-Brexit posture https://www.gov.uk/government/publications/call-for-evidence-on-the-overseas-framework.

2. In the wake of the FireEye and Solar Winds incidents (https://www.ncsc.gov.uk/news/ncsc-statement-on-solarwinds-compromise), the UK National Cyber Security Centre reminds readers of its comprehensive ***Secure System Administration Guidance*** of September 2020 (https://www.ncsc.gov.uk/collection/secure-system-administration). It focuses on five design principles for Information Technology (IT) and Operational Technology (OT) systems to protect your most sensitive data: IT systems typically handle data, the way it moves around and is stored; OT systems typically manage physical processes and machinery.
This guidance is particularly useful for those responsible for remote management of system components, for budgeting secure system administration, and for assessing Third Party suppliers of such system administration.

3. A first for the National Cyber Security Centre (NCSC) is its ***Buying and Selling Second-Hand Devices Guidance***, with excellent tips including:

- what to do before erasing data on your device,
- how to erase data on your device;
- choosing a second-hand device, and
- things to know before using a second-hand device.

See https://www.ncsc.gov.uk/news/secure-second-hand-devices, published on 28 December 2020.

Newsletter – 15 January 2021

1. ILC Strategic Priorities – 2021: ILC is a Full Member of the Digital Policy Alliance (DPA) <https://www.dpalliance.org.uk>, an independent, cross-party not-for-profit policy forum informing Parliamentarians and policy-makers of the implications of online and digital technologies subject to legislation and regulatory review. The DPA is considering its work direction for this coming year, and to inform that, seeks three priorities or themes that its members have for 2021. It is that time of year when many organisations are contemplating similar exercises, and we welcome to hear from you to inform ILC activities and events as well.
To assist with developing your thoughts, some priorities and themes already suggested are:

- ***DevOps, accelerated cloud migration, AI governance, AI solutions leveraging the Cloud, and security and privacy of Augmented Reality (AR), Virtual Reality (VR) and Extended Reality (XR):*** as from ISACA blog https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/five-security- and-emerging-tech-insights-for-2021.
- ***Reform of the British audit market:*** the UK Department for Business, Energy and Industrial Strategy's (BEIS) Secretary Kwasi Kwarteng (newly appointed 8 January) is reported to prioritise audit reform, as arising from recommendations of the Kingman, UK Competition and Markets Authority (CMA) and Brydon Reviews. There is also the Redmond Review on local

authority financial reporting and external audit by the Ministry of Housing, Communities and Local Government. (GRA will be reporting further developments on these in due course).

- Other...

For ISACA Members willing to share their strategic thoughts and visions for 2021, please:

- reach out by email to the ILC GRA Team (by noon, Monday, 18 January);
- join the forthcoming ILC Young Member's Forum networking event (0800, Wednesday, 20 January) which is considering what one might expect for 2021.

2. The UK Telecommunications (Security) Bill amends the Communications Act 2003 by strengthening security duties of public telecoms providers, setting out specific security requirements and codes of practice, and providing Ofcom new tools and responsibilities to ensure industry compliance (https://www.gov.uk/government/collections/telecommunications-security-bill). The Bill takes into account findings of the July 2019 UK Telecom Supply Chain Review Report (by Department for Digital, Culture, Media & Sport) to review supply arrangements of the UK telecoms Critical National Infrastructure (https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference).
Since the Bill's Second Reading and motions of 30 November 2020, including debate on security aspects of Huawei components, the Bill is next undergoing scrutiny in the House of Commons Public Bill Committee from 14 January 2021. Bill stages can be followed at https://services.parliament.uk/Bills/2019-21/telecommunicationssecuritybill.html.

Newsletter – 3 and 4 February 2021

1.**Strategic Priorities 2021**: Early in the year, many organisations contemplate and develop their annual strategic priorities. This is a share of some related to ISACA:

- ***Five topics*** are noted in ISACA's trends blog: DevOps; accelerated cloud migration; AI governance; AI solutions leveraging the Cloud; and security and privacy of Augmented Reality (AR), Virtual Reality (VR) and Extended Reality (XR) (see https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/five-security- and-emerging-tech-insights-for-2021).
- ***Reform of the British audit market***: soon after his appointment on 8 January, the new Secretary of BEIS (Department for Business, Energy and Industrial Strategy), Kwasi Kwarteng, was reported to prioritise audit reform. This would be expected to take into account recommendations of the:

  - 2018 Kingman review of the Financial Reporting Council,
  - 2019 Competition and Markets Authority (CMA) Report,
  - 2019 Brydon Review (to which ISACA contributed).
  - A different area of government (the Ministry of Housing, Communities and Local Government) led on the 2019 Redmond Review on local authority financial reporting and external audit (to which ISACA contributed).

2. January 28th is an annual Data Protection Day marking the anniversary of the first binding international treaty to protect personal data: the 1981 ***Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)***. The Convention provided pillars for what is now the 2018 General Data Protection Regulation (GDPR). An *Amending Protocol* in 2018 (not yet in force) modernised the Convention to bring together privacy frameworks from around the world and to facilitate cross-border data flows while providing safeguards against abuse (https://www.coe.int/en/web/portal/-/data-protection-day-40-years-of-convention-108). For more information on issues and challenges to privacy addressed at 2021's Data Protection Day, see https://www.coe.int/en/web/data-protection/-/28-january-2021-celebrate-data-protection-day .
Members will find other related privacy topics in this ILC newsletter:

- the research feature drawing attention to the right to privacy from different perspectives around the globe,
- the ILC Member event on 16 February on protecting privacy in machine learning and data analytics.

3. Continuing in the House of Commons, the ***UK Telecommunications (Security) Bill*** is in the process of amending the Communications Act 2003. The Bill aims to strengthen security duties of public telecoms providers, set out specific security requirements and codes of practice, and provide regulator Ofcom new tools and responsibilities to ensure industry compliance (https://www.gov.uk/government/collections/telecommunications- security-bill).
Since the Bill's Second Reading and motions of 30 November 2020, including debate on security aspects of Huawei components, the Bill received scrutiny by the House of Commons Public Bill Committee from 14-29 January 2021. A date is to be set for the Report Stage and Third Reading in the House of Commons before going to the House of Lords and thereafter to Amendments and Royal Assent. Bill stages can be followed at https://services.parliament.uk/bills/2019-21/telecommunicationssecuritybill.html.

Newsletter 9 February 2021

1. The UK Government's ***COVID-19 Response*** on 22 February 2021, includes a roadmap to ease current lockdown in England (Devolved Administrations set out their respective roadmaps in Scotland, Wales and Northern Ireland). In the Roadmap (Step 4), there is mention of **COVID status certification**, referred to by some in the media as a vaccine passport (see https://www.gov.uk/government/publications/covid-19-response-spring-2021/covid-19-response-spring-2021). During Government review of the Response, a possible certification is to be assessed from various perspectives, including for:

- reduction of risk
- access to settings/venues or relaxation of COVID-Secure mitigations
- ethical, equalities, privacy and legal aspects
- operational aspects
- possible limits on use by organisations.

Among other countries and companies considering such certificates and technologies to create them, the **World Health Organisation (WHO)** opened a call in December 2020 for experts for a **Smart Vaccination Certificate consortium**. To date, "*yellow fever is the only disease expressly listed in the International Health Regulations [IHR 2005] for which countries can require proof of vaccination from travellers as a condition of entry into a country*." For further information on the Consortium's objectives, outputs and principles -- that might shape purpose and factors regarding a future digital (vs. paper) certificate -- see https://www.who.int/news-room/articles-detail/world-health-organization-open-call-for-nomination-of-experts-to-contribute-to-the-smart-vaccination-certificate-technical-specifications-and-standards-application-deadline-14-december-2020.

2. The UK National Cyber Security Centre (NCSC) along with similar authorities in Australia, New Zealand, Singapore, and the United States issued on 24 February 2021, a joint advisory to mitigate cyber attacks on the **Accellion File Transfer Appliance (FTA)**. The FTA, reaching end-of-life on 30 April 2021, was targeted in December. The advisory contains more information and mitigation about the incident affecting this product's file sharing with Third Parties (https://www.ncsc.gov.uk/news/ncsc-advisory-on-accellion-file-transfer-appliance-customers).

3. The Cabinet Office (CO) is consulting on widening the powers of the **National Fraud Initiative (NFI)** on data matching exercises, and updating the NFI Code governing this matching including data protection legislation. The NFI compares sets of data electronically, eg, payroll or benefit records of primarily public sector bodies in England, against other records held by the same or another body. After completed investigations of inconsistencies or similarities, a body can take appropriate action, eg, prosecute cases of fraud, address over and underpayments, update records as well as identify system weaknesses and review controls. This consultation can be seen in the context of the CO's role to ensure efficient spending and cost saving innovation when COVID-19 has increased financial pressures across the public sector.

The current **Local Audit and Accountability Act 2014** embeds the NFI data matching power for the one purpose of fraud prevention and detection, with four supplementary ones available to be added by an affirmative Statutory Instrument (SI) adopted by Parliament. The consultation seeks views to amend the 2014 Act by way of an SI, to become Regulations 2021 comprising the five powers to *assist in the:*

- *prevention and detection of fraud,*
- *prevention and detection of crime (other than fraud),*
- *apprehension and prosecution of offenders,*
- *prevention and detection of errors and inaccuracies,*
- *recovery of debt owing to public bodies.*

Members interested to submit views by 10 March 2021, or to learn more about factors and compliance issues when processing public sector data, please see the consultation and related documents at https://www.gov.uk/government/consultations/consultation-on-the-expansion-of-the-national-fraud-initiative-nfi-data-matching-powers-and-the-new-code-of-data-matching-practice.

Newsletter – 19 and 23 February 2021

1.This year's **Safer Internet Day** (https://www.saferinternet.org.uk/safer-internet-day/2021) provided tips and resources for online reliability all year round. This 9 February was also notable for government announcing the set up of the **UK Cyber Security Council**, a new independent body to develop cyber security as a profession, with the setting of standards and career opportunities (https://www.gov.uk/government/news/new-uk-cyber-security-council-to-be-official-governing-body-on-training-and-standards).
The work in creating the Council arose from the five-year National Cyber Security Strategy (https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021). That involved a consultation in 2018 by the Department for Digital, Culture, Media & Sport (DCMS), and the commissioning of a consortium – the Cyber Security Alliance – led by the Institution of Engineering and Technology to form the Council. ISACA is part of that formation Alliance: see https://www.isaca.org/why-isaca/the-uk-cyber-security-council. Trustees are appointed and the formal launch is 31 March 2021.

2.On 11 February 2021, the UK Department for Digital, Culture, Media & Sport (DCMS) published a pre-legislation **policy document on digital identities** for which it seeks public feedback by 11 March (https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework). The proposed policy lays out a new 'trust framework' of rules for organisations to produce or use digital identity products and services. The government is not providing solutions or actual products and services, and instead sets out principles, policies, procedures and standards for business and industry innovation to do so. The framework areas include:

- handling and protecting people's data,
- indicating security and encryption standards to be followed,
- managing user accounts,
- protecting against fraud and misuse.

3.The Competition and Markets Authority (CMA) published on 19 January 2021 new research on ***Algorithms: How they can reduce competition and harm consumers*** arising from their deliberate or unintended misuse (https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers). Algorithms are processes or rules to perform a computation or solve a problem, and enable efficient online activities and markets. Their misuse, however, can have negative impact, eg, reduce choice or artificially change consumers' perceptions, change product rankings on websites, and aid business collusion to sustain higher prices for products and services.
The CMA also seeks evidence on specific issues that it can consider for its future work in digital

markets, including analysing algorithms and operating its new regulatory regime and regulator – the Digital Markets Unit (DMU) (https://www.gov.uk/government/news/cma-lifts-the-lid-on-impact-of-algorithms). Members interested in answering eight questions to contribute to that evidence gathering, by 18 March 2021, please see https://www.gov.uk/government/consultations/algorithms-competition-and-consumer-harm-call-for-information.

Newsletter 2 March 2021 No.1

1. The UK Government's ***COVID-19 Response*** on 22 February 2021, includes a roadmap to ease current lockdown in England (Devolved Administrations set out their respective roadmaps in Scotland, Wales and Northern Ireland). In the Roadmap (Step 4), there is mention of **COVID status certification**, referred to by some in the media as a vaccine passport (see https://www.gov.uk/government/publications/covid-19-response-spring-2021/covid-19-response-spring-2021). During Government review of the Response, a possible certification is to be assessed from various perspectives, including for:

- reduction of risk
- access to settings/venues or relaxation of COVID-Secure mitigations
- ethical, equalities, privacy and legal aspects
- operational aspects
- possible limits on use by organisations.

Among other countries and companies considering such certificates and technologies to create them, the **World Health Organisation (WHO)** opened a call in December 2020 for experts for a **Smart Vaccination Certificate consortium**. To date, "*yellow fever is the only disease expressly listed in the International Health Regulations [IHR 2005] for which countries can require proof of vaccination from travellers as a condition of entry into a country*." For further information on the Consortium's objectives, outputs and principles -- that might shape purpose and factors regarding a future digital (vs. paper) certificate -- see https://www.who.int/news-room/articles-detail/world-health-organization-open-call-for-nomination-of-experts-to-contribute-to-the-smart-vaccination-certificate-technical-specifications-and-standards-application-deadline-14-december-2020.

2. The UK National Cyber Security Centre (NCSC) along with similar authorities in Australia, New Zealand, Singapore, and the United States issued on 24 February 2021, a joint advisory to mitigate cyber attacks on the **Accellion File Transfer Appliance (FTA)**. The FTA, reaching end-of-life on 30 April 2021, was targeted in December. The advisory contains more information and mitigation about the incident affecting this product's file sharing with Third Parties (https://www.ncsc.gov.uk/news/ncsc-advisory-on-accellion-file-transfer-appliance-customers).

3. The Cabinet Office (CO) is consulting on widening the powers of the **National Fraud Initiative (NFI)** on data matching exercises, and updating the NFI Code governing this matching including data protection legislation. The NFI compares sets of data electronically, eg, payroll or benefit records of primarily public sector bodies in England, against other records held by the same or another body. After completed investigations of inconsistencies or similarities, a body can take appropriate action, eg, prosecute cases of fraud, address over and underpayments, update records as well as identify system weaknesses and review controls. This consultation can be seen in the context of the CO's role to ensure efficient spending and cost saving innovation when COVID-19 has increased financial pressures across the public sector.
The current **Local Audit and Accountability Act 2014** embeds the NFI data matching power for the one purpose of fraud prevention and detection, with four supplementary ones available to be added by an affirmative Statutory Instrument (SI) adopted by Parliament. The consultation seeks views to amend the 2014 Act by way of an SI, to become Regulations 2021 comprising the five powers to *assist in the:*

- *prevention and detection of fraud,*
- *prevention and detection of crime (other than fraud),*

- *apprehension and prosecution of offenders,*
- *prevention and detection of errors and inaccuracies,*
- *recovery of debt owing to public bodies.*

Members interested to submit views by 10 March 2021, or to learn more about factors and compliance issues when processing public sector data, please see the consultation and related documents at https://www.gov.uk/government/consultations/consultation-on-the-expansion-of-the-national-fraud-initiative-nfi-data-matching-powers-and-the-new-code-of-data-matching-practice.

Newsletter 15 March 2021 No.2

1. The UK Competition and Markets Authority (CMA) published on 5 March 2021 a **consultation for views on features of oversight for open banking**. The CMA's investigation and 2016 report into the UK retail banking market concluded that older and larger banks do not compete enough for customer business; CMA established Open Banking Ltd to enable innovation and competition of UK financial services. Open Banking is to deliver application programming interfaces (APIs), data structures and security architectures so customers can share securely their financial records to compare bank and Third-Party deals. See consultation documentation and roadmap with factors being considered including enforcement, monitoring and compliance; submissions are due 29 March (https://www.gov.uk/government/consultations/future-oversight-of-the-cmas-open-banking-remedies/the-future-oversight-of-the-cmas-open-banking-remedies).

2. The UK National Cyber Security Centre (NCSC) launched on 26 February 2021 a new **Cyber Security Self-Assessment Tool** aimed primarily to help sole traders and micro businesses to keep safe online in the face of increased cyber threats since Covid-19 (https://www.ncsc.gov.uk/news/cyber-aware-action-plan). Complementing the tool is the small business guide https://www.ncsc.gov.uk/collection/small-business-guide. These NCSC awareness efforts are part of the cross-government **Cyber Aware Campaign** https://www.ncsc.gov.uk/cyberaware/.

Entities using **Microsoft (MS) Exchange Servers** are advised to urgently patch MS updates, released ahead of schedule, to fix vulnerabilities exploited in recently publicised 'Hafnium' attacks. See further information in the **NCSC advisory** published 3 March 2021 https://www.ncsc.gov.uk/news/advice-following-microsoft-vulnerabilities-exploitation.

3. The UK HM Revenue and Customs published on 3 March 2021 a policy document on **Reporting Rules of Digital Platforms**. It introduces a new power to create regulation for UK digital platforms to collect and report income of sellers of services (eg, taxi, short-term lettings, freelance) using the platform (https://www.gov.uk/government/publications/reporting-rules-for-digital-platforms).

This new power enables the UK to implement the **OECD Model Rules for Reporting by Platform Operators with respect to Sellers in the Sharing and Gig Economy**, July 2020 (https://www.oecd.org/tax/exchange-of-tax-information/model-rules-for-reporting-by-platform-operators-with-respect-to-sellers-in-the-sharing-and-gig-economy.htm). This would enable HMRC to exchange information internationally with other tax authorities about digital platform services income in a more standardised approach to replace patchwork of local reporting requirements.

Newsletter – 23 March 2021 No.3

1.The UK is committed to make open, safe and secure use of the Internet. The UK's Department for Digital, Culture, Media and Sport (DCMS) and Home Office published on 15 December 2021 the ***Online Harms White Paper*** – an update on the outcome of a 2019consultation. It includes joint ministerial plans for clear accountability and oversight for technology companies to provide a secure digital economy (https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper). The scope includes technology companies of all sizes ranging from social media platforms, file hosting sites, public discussion forums, messaging services and search engines. The plans go beyond self-regulatory efforts to create a new independent regulatory body and framework for

online safety. Additionally, the ambitious plans aim to improve messaging and resources covering online media literacy, including further work with parents, and addressing sharing of disinformation, catfishing (ie, fictional online persona luring someone into a relationship), online harassment and attacks, and differing needs of people with disabilities when navigating information. Next steps legislative efforts are to be undertaken in line with the parliamentary schedule.

2.Complementary efforts to above are:

- the DCMS ***Safety Tech 2021*** Expo on 24 March 2021 is showcasing technologies to support safer online communities (https://cogx.live/events/safety-tech-2021).
- National Cyber Security Centre (NCSC) published 15 March 2021 its first ever ***Guidance for Early Years practitioners***, offering education and childcare settings practical tips to keep data and devices secure for children and their families (https://www.ncsc.gov.uk/news/early-years-providers-helped-to-take-first-steps-with-cyber-security).

3.On 19 March 2021, a Statement was issued on a ***Memorandum of Understanding on the Role of the ICO in relation to new UK adequacy assessments*** signed between the Department for Digital, Culture, Media and Sport (DCMS)'s Secretary of State and the Information Commissioner (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding). With the UK departure from the EU, the Secretary of State now holds powers to make independent UK data adequacy arrangements with new partners around the world, to facilitate international data transfers. This statutory process of assessing the adequacy requires consultation with the Information Commissioner's Office. The MoU is at: https://ico.org.uk/media/about-the-ico/mou/2619468/uk-adequacy-assessments-ico-dcms-memorandum-of-understanding.pdf.

Newsletter – 7 April 2021 No. 1 and 27 April No. 2

1. In the ILC February 2021 Newsletter 1, the GRA section mentioned that the new Secretary Kwasi Kwarteng of the Department for Business, Energy & Industrial Strategy (BEIS) was reported to prioritise **UK audit reform**. On 18 March 2021, BEIS brought this priority to light with major reforms proposed in a Policy Paper and consultation on ***Restoring trust in audit and corporate governance*** (https://www.gov.uk/government/news/business-secretary-launches-major-overhaul-of-uks-audit-regime-in-wake-of-big-name-company-collapses). The reforms come in the wake of large-scale company failures such as Carillion, Thomas Cook and BHS and subsequent job losses and taxpayer costs. The Paper's proposed reforms aim to restore public trust in how large UK companies are run and to ensure responsible governance of these companies, as well as to provide investors and stakeholders access to information on company performance in addition to finance, and to keep the UK in the lead of related international good practice.
The proposed reforms take into account most of the recommendations of three major reviews commissioned during 2018-19:

- the ***Kingman Review of the Financial Reporting Council*** (FRC), recommending replacement of the FRC with a new independent statutory regulator https://www.gov.uk/government/news/independent-review-of-the-financial-reporting-council-frc-launches-report,
- the ***Competition and Markets Authority (CMA) study of the audit services market*** https://www.gov.uk/government/consultations/statutory-audit-services-initial-consultation-on-the-competition-and-markets-authority-recommendations, and
- the ***Brydon Review on the quality and effectiveness of audit*** https://www.gov.uk/government/publications/the-quality-and-effectiveness-of-audit-independent-review. (ISACA contributed to the Brydon Review).

The BEIS Policy Paper (https://www.gov.uk/government/publications/restoring-trust-in-audit-

and-corporate-governance) proposes how companies should report on their governance and finances, how their reports should be audited, and how the audit and audit market should change and be overseen by a new statutory regulator – **The Audit, Reporting and Governance Authority (ARGA).** Responses to the **open consultation** on the reform proposals are due by 8 July 2021: see https://www.gov.uk/government/consultations/restoring-trust-in-audit-and-corporate-governance-proposals-on-reforms.

2. In the context of the BEIS consultation on *Restoring trust in audit and corporate governance*, the **Financial Reporting Council (FRC)** announced on 25 March 2021, its new report ***Our Approach to Audit Supervision*** (https://frc.org.uk/news/march-2021/frc-approach-to-audit-supervision). While the FRC is currently responsible for regulating the UK statutory auditors and audit firms and for monitoring audit market developments, it is to transition to the **ARGA** in line with the BEIS proposals, Kingman Review and CMA. In the meantime, the FRC is already facilitating reforms for the transition: this paper states it has 'revamped' its supervisory approach to the largest audit firms with the creation of three teams (Audit Firm Supervision, Audit Market Supervision, Audit Quality Review). The new paper is serving two purposes, to:

- aid accountability (by describing audit supervision goals and process), and
- communicate requirements and practices expected from firms conducting statutory audits of public interest entities (PIEs), eg, entities listed fully on the London Stock Exchange, credit institutions (eg, banks and building societies), insurance undertakings authorised by the Bank of England.

This paper is to be updated when the FRC audit supervision approach changes again, for example, after planned changes for the FRC to register firms auditing PIEs, and when the FRC transitions to ARGA.

3. Parallel to UK and World Health Organization (WHO) efforts on what popularly is called a vaccine passport (see ILC March 2021 Newsletter 1), the European Commission reported on 17 March 2021, its **Proposal** to create a **Digital Green Certificate** for safe travel inside the EU during the COVID-19 pandemic (https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181). This Certificate is to be proof of a person's vaccination, testing or recovery regarding COVID-19. In paper or digital form, the proposed certificate would contain a QR Code with key information to be digitally signed for authentication, and would be verified across the EU by a Commission-built gateway. EU Member States in the meanwhile are to implement the ***trust framework*** and technical standards for the certificates as agreed in the eHealth network (https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf). The Commission Proposal is for a Regulation to be adopted by the European Parliament and the European Council (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130). The Digital Green Certificate is to be a temporary measure until the WHO declares the end of the COVID-19 international health emergency.

News letter – 11 May 2021 No. 1

1. The **UK Home Office** launched on 11 May 2021, a **Call for Information** to identify activity causing harm that is not already covered in the current offences of the **Computer Misuse Act 1990**. This Act is the main UK legislation relating to **cyber-dependent crime:** offences or attacks (eg, hacking, denial of service) against, and conducted by, information and communications technology (ICT) systems and devices (https://www.legislation.gov.uk/ukpga/1990/18/contents). Cyber-dependant crime is set out by the National Cyber Security Strategy 2016-2021 as distinct from *cyber-enabled crime*, eg, traditional crimes that are enhanced in scope and reach by computers and other ICTs. The cyber-enabled crime category (*not* covered by this Call for Information) includes fraud, data theft, cyber bullying, malicious and offensive communications sent via social media, child sexual offences, extreme pornography. By way of background, explanations of these and other cybercrime categories can be found on the Crown Prosecution Service site https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.
Relevant entities interested to submit information to the Call, by 8 June 2021, please see https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information.

2. In advance of the UK government preparing a new National Cyber Security Strategy, the Department for Digital, Culture, Media and Sport (DCMS) has published on 17 May 2021 a Policy paper and Call for Views on **Cyber security in supply chains and managed service providers**. Views are sought in two areas:

- how organisations manage supply chain cyber risk and what additional government
- intervention could assist in that effort,
- a proposed framework and its implementation for Managed Service Provider security that
- manages risks associated with such providers.

Further information for submissions due 11 July 2021 is at: https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security/call-for-views-on-cyber-security-in-supply-chains-and-managed-service-providers.

3. On 21 April 2021, the **European Commission** proposed new rules and actions for Europe to become the global hub for trustworthy **Artificial Intelligence** (AI). These efforts combine:

- the first ever *AI Regulation* (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence),
- a *Coordinated Plan with Member States* on policy changes and investment for safety, innovation and development of human-centric AI (https://digital-strategy.ec.europa.eu/news-redirect/709091),
- new rules on *Machinery* to address safety risks of AI systems, and the safe integration of AI
- systems into overall machinery (https://ec.europa.eu/docsroom/documents/45508).

This site https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 has a wealth of documentation on these and related developments, including a risk-based approach on AI rules, developments and products; and the creation of a *European Artificial Intelligence Board* to facilitate new rules and standards for AI.

4. Members are reminded of the opportunity to participate in ISACA's submission by 8 July 2021 to the **BEIS consultation** on UK audit reform – ***Restoring trust in audit and corporate governance: proposals on reforms***. Members can contact <gra@isaca-london.org> expressing your interest and possible areas of contribution. Further information on the proposals and questions for views is at: https://www.gov.uk/government/consultations/restoring-trust-in-audit-and-corporate- governance-proposals-on-reforms.

Newsletter – 24 May 2021 No. 2

1. The **UK Home Office** launched on 11 May 2021, a **Call for Information** to identify activity causing harm that is not already covered in the current offences of the **Computer Misuse Act 1990**. This Act is the main UK legislation relating to **cyber-dependent crime:** offences or attacks (eg, hacking, denial of service) against, and conducted by, information and communications technology (ICT) systems and devices (https://www.legislation.gov.uk/ukpga/1990/18/contents). Cyber-dependant crime is set out by the National Cyber Security Strategy 2016-2021 as distinct from *cyber-enabled crime*, eg, traditional crimes that are enhanced in scope and reach by computers and other ICTs. The cyber-enabled crime category (*not* covered by this Call for Information) includes fraud, data theft, cyber bullying, malicious and offensive communications sent via social media, child sexual offences, extreme pornography. By way of background, explanations of these and other cybercrime categories can be found on the Crown Prosecution Service site https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Relevant entities interested to submit information to the Call, by 8 June 2021, please see https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information.

2. In advance of the UK government preparing a new National Cyber Security Strategy, the Department for Digital, Culture, Media and Sport (DCMS) has published on 17 May 2021 a Policy paper and Call for Views on **Cyber security in supply chains and managed service providers**. Views are sought in two areas:

- how organisations manage supply chain cyber risk and what additional government intervention could assist in that effort,
- a proposed framework and its implementation for Managed Service Provider security that manages risks associated with such providers.

Further information for submissions due 11 July 2021 is at: https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security/call-for-views-on-cyber-security-in-supply-chains-and-managed-service-providers.

3. On 21 April 2021, the **European Commission** proposed new rules and actions for Europe to become the global hub for trustworthy **Artificial Intelligence** (AI). These efforts combine:

- the first ever *AI Regulation* (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence),
- a *Coordinated Plan with Member States* on policy changes and investment for safety, innovation and development of human-centric AI (https://digital-strategy.ec.europa.eu/news-redirect/709091),
- new rules on *Machinery* to address safety risks of AI systems, and the safe integration of AI systems into overall machinery (https://ec.europa.eu/docsroom/documents/45508).

This site https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 has a wealth of documentation on these and related developments, including a risk-based approach on AI rules, developments and products; and the creation of a *European Artificial Intelligence Board* to facilitate new rules and standards for AI.

4. Members are reminded of the opportunity to participate in ISACA's submission by 8 July 2021 to the **BEIS consultation** on UK audit reform – ***Restoring trust in audit and corporate governance: proposals on reforms***. Members can contact <gra@isaca-london.org> expressing your interest and possible areas of contribution. Further information on the proposals and questions for views is at: https://www.gov.uk/government/consultations/restoring-trust-in-audit-and-corporate- governance-proposals-on-reforms.