ISACA

ISACA Vision Paper

A Manifesto for Bridging the UK's Digital Skills Gap and Improving Cyber Resilience

About ISACA

ISACA is a global not-for-profit association that provides industry-leading training and certifications for cybersecurity, IT audit, assurance, risk and privacy professionals, as well as frameworks and models to business technology professionals and their enterprises.

ISACA has more than 0.5M engaged professionals and 180,000 members across 225 Chapters in 188 countries around the world. In the UK, ISACA has more than 10,000 members, brought together by five local Chapters: the London Chapter, the largest ISACA Chapter in the world; the Central UK Chapter; the Northern England Chapter; the Scottish Chapter and the Winchester Chapter.

Globally, ISACA has…

180,000+ MEMBERS across **225 CHAPTERS** in **188 COUNTRIES**

Through its more than 50 years of history, ISACA's mission is the pursuit of digital trust. This means, foremost, empowering individuals with knowledge and skills in IT audit, governance, risk, privacy and cybersecurity, to progress their careers and transform their organisations.

In alignment with its mission, and with the support of a strong UK membership, ISACA provides expert feedback to the UK Government on a range of digital and cyber policy initiatives, including key issues such as: the enhancement of digital skills and the upskilling of UK professionals, provision of AI literacy, and training for emerging technologies and mitigation of cyber risks for the UK's public and private sectors.

ISACA is a founding member and was heavily involved in the formation of the UK's Cyber Security Council. The bulk of ISACA's UK advocacy work centres on advising the Cyber Resilience Directorate at DSIT and their counterparts at the National Cyber Security Centre.

Introduction

All over the world, the digital threat landscape is changing. Despite commendable efforts from UK policymakers to update specific cyber policies and strategies, high-profile events highlight that a more concerted, renewed effort is necessary to protect individuals and organisations. This manifesto provides our analysis of where the UK should look to augment its policies over the next parliamentary term.

From a national security perspective, it considers the importance of reevaluating the scope of regulation of critical sectors in the UK economy and addressing the threat posed by critical third parties (CTPs). Ensuring the resilience of our critical national infrastructure (CNI) against cyber threats is imperative, as demonstrated by incidents like the ransomware attack on Synnovis, which disrupted vital services in NHS hospitals across London. By expanding the coverage of cyber resilience regulations to encompass more supplier relationships, we can better protect our most vital assets.

From a business security and growth perspective, our manifesto explores how government guidance can support and incentivise the adoption of robust cybersecurity strategies. The implementation of the government's draft Cyber Governance Code of Practice and its accompanying security codes will help businesses integrate cyber risk management into all aspects of their operations. Encouraging widespread adoption of these codes will foster a more resilient business environment, enabling firms to achieve critical operational resilience and protect themselves from cyber-attacks.

From a workforce perspective, this manifesto addresses how the UK can tackle digital and cyber skills gaps and meet the growing demand for skilled professionals. The CyberFirst programme has successfully sparked interest in cybersecurity among UK students, but expanding and upscaling this initiative in partnership with industry is crucial. By providing clear pathways into emerging critical sectors such as AI, quantum, and data science, we can ensure a steady supply of talent to meet future demands. Additionally, promoting and supporting bodies that provide leading industry certification and upskilling programmes will help connect aspiring cyber professionals with the opportunities they need to thrive.

This manifesto sets out our analysis alongside a series of practical steps the UK Government can adopt to meet national objectives. ISACA looks forward to working with policymakers to improve the UK's cyber resilience and invites them to rely on the wealth of expertise in the UK's cyber profession for the design and implementation of future cyber policies. Together, we can build a secure and resilient digital future for the UK.

ISACA's Top 3 Asks to Government

Chapter 1: Improving digital skills in the UK workforce

Meeting the growing demand for skilled professionals is essential to seizing the opportunities presented by digital innovation. Government-sponsored education and training programmes are crucial to achieving this goal. A successful example is the CyberFirst programme, which has developed effective pathways into the cybersecurity profession through industry partnerships. **Government-industry partnerships** such as this, **and the provision of incentives for industry, will be essential to develop strong pipelines and a steady flow of talent into emerging critical sectors such as AI, quantum computing, and data science.**

Chapter 2: Delivering enterprise resilience through government guidance

To empower businesses to achieve critical operational resilience and protect themselves from cyber-attacks, **it is essential to establish the final UK Cyber Governance Code of Practice and its accompanying technology-specific codes.** These codes should be implemented as central pillars of government guidance and best practice. Encouraging businesses to adopt these codes will help integrate cyber risk management into all aspects of their operations, fostering a more resilient business environment

Chapter 3: Enhance UK CNI's resilience through targeted regulations

Given the increasing reliance on digital infrastructure and the growing threat of cyber-attacks on the UK's CNI, **it is crucial to reevaluate the regulatory framework governing critical sectors.** This includes expanding the coverage of cyber resilience regulations to encompass critical third parties (CTPs) working with CNI organisations. Strengthening the regulatory framework will ensure that these third parties adhere to robust cybersecurity and operational resilience standards, thereby enhancing the overall security of the UK's most vital assets

Chapter 1: Improving digital skills in the UK workforce

Where are we?

The state of digital skills development in the UK workforce is a pressing concern, highlighted by the Department for Education's latest annual Consumer Digital Index compiled by Lloyds Bank. According to the index, approximately 13 million people in the UK, or about 25% of the population, possess the lowest level of digital capability, meaning they struggle to interact with online services. Furthermore, UK employers report that only 48% of individuals leave full-time education with advanced digital skills.

According to research carried out by ISACA amongst its membership in Europe in 2023, 62% of respondents reported that their cybersecurity team was understaffed. Looking specifically at AI, further research amongst ISACA's European members from earlier this year revealed that 40% of organisations offered no AI training to staff and a further 30% only offered AI training to those working in tech-related positions.

62%
of respondents reported that their **cybersecurity team** was **understaffed**

40%
of organisations offered **no AI training** to staff

30%
only offered AI training to those working in **tech-related positions**

This skills gap significantly hampers national productivity, costing the UK an estimated £63 billion annually in lost potential GDP. With the advent of new technologies, particularly AI, this gap is expected to widen, posing a substantial threat to the UK's growth prospects. However, addressing this deficit presents a significant opportunity to unlock the economic potential of both businesses and individuals.

To tackle this issue, the previous Conservative administration launched the Digital Skills Council in June 2022 to investigate the root causes inhibiting skills provision in the digital economy. The Council found that individuals often lacked encouragement and perceived digital courses or careers as "not for people like me." This perception was compounded by a lack of awareness regarding training options and the potential value of digital courses.

Despite positive policy interventions such as increased funding for local government-run Skills Bootcamps, the CyberFirst scheme, new digital-specific T Levels, and the Statutory Digital Entitlement for adults with low digital skills, more needs to be done to change cultural attitudes towards digital skills.

The CyberFirst programme stands out among these initiatives. Since its launch in 2015, it has reached over 260,000 students in 2,500 schools, improving interest in computer science and challenging gender stereotypes about the subject. In May, DSIT announced it was inviting views on creating a new industry-funded organisation to run the programme in partnership with the government, aiming to increase its reach and adapt its scope to include pipelines into wider tech sectors such as AI, quantum, and data science. While this presents opportunities, transferring stewardship to the private sector also brings uncertainties and risks.

Where do we need to go?

Meeting the UK's skills gaps and workforce demands will be contingent on continued and renewed investment in carving out and offering the professionals of tomorrow a clear thread of opportunity and pathways into employment, starting at school level. Simultaneously, businesses will need to be provided with more information and financial incentives to incubate their employees' expertise through upskilling and training programmes.

How do we get there?

- **Offer businesses renewed incentives to invest in digital training for their workforce and ensure reforms to the Apprenticeship Levy increase pathways into the digital economy**

  The introduction of financial incentives is crucial for encouraging UK businesses to invest in digital upskilling training for their employees at the necessary pace. Investment in skills related to nationally strategic technologies has been shown to yield strong economic returns in the long run. ISACA has found that matched funding initiatives, where the government matches business investments in key digital skills training, have significantly increased private investment. To ensure fair competition, such a scheme should be complemented by specific grants for SMEs to support their digital skills training efforts. Additionally, to enhance the diversity and availability of pathways into the digital economy, future reforms to the Apprenticeship Levy should prioritise funding and accreditable courses that open new career opportunities in the digital sector.

- **Introduce AI literacy schemes and quantifiable targets for secondary schools**

  Mandate the inclusion of AI literacy and ethical AI use in the national curriculum for secondary schools and set quantifiable targets to improve student knowledge at the end of their education. Changes to the curriculum should cover the basics of AI technology, its applications, and the ethical considerations surrounding its use. In tandem, we urgently need to develop and fund comprehensive teacher training programmes focused on AI literacy, ensuring educators are well-equipped to teach AI concepts effectively.

- **Launch AI literacy schemes for board-level business leaders**

  Launch government-sponsored AI literacy training programmes for business leaders with accompanying certifications, focused on governance, ethical considerations, and risks of AI integration in business. Provide financial incentives, such as tax credits or grants, for companies that ensure their executives complete accredited AI literacy courses.

- **Deliver an expanded CyberFirst programme in partnership with industry**

  The government should ensure that it offers the necessary incentives to industry partners to deliver an upscaled and expanded iteration of the CyberFirst programme, that builds on the initiative's success in recent years. If delivered correctly, the programme has the potential to carve out new professional pathways into emerging critical sectors and improve the diversity and appeal of the cyber profession to a wider audience.

- **Promote industry certification and training programmes**

  The government should work with industry-leading certification providers and trade associations to facilitate new structures and dialogues with both employers and educational institutions, using relevant initiatives and bodies as vectors to connect supply and demand.

Chapter 2: Delivering enterprise resilience through government guidance

Where are we now?

In 2014, the UK government launched Cyber Essentials, its central guidance scheme outlining the controls that organisations need to implement to improve their cybersecurity standards. Businesses require a Cyber Essentials certification to bid for central government contracts handling sensitive information. Under this scheme, the National Cyber Security Centre (NCSC) also created a five-step Small Business Guide to cater to the size and capacity of different organisations implementing cybersecurity standards.

SOURCE: https://www.ncsc.gov.uk/images/cyberEssentials.png

In addition, the NCSC's Cyber Security Toolkit for Boards facilitates embedding cyber resilience and risk management measures within an organisation's systems, processes, and technologies. Through these tools, the NCSC has made a concerted effort to comprehensively address the dissemination of cybersecurity best practice within the business landscape. The recent addition of cyber as a material risk in the UK Corporate Governance Code, which sets principles of good governance in UK company law, also underscores the government's greater focus on cybersecurity.

A decade after the launch of Cyber Essentials, the UK government is now working towards delivering more comprehensive cyber governance guidance measures to keep pace with evolving cyber threats. Earlier this year, DSIT launched a draft Cyber Governance Code of Practice for public consultation. This draft guidance contains proposals on cyber governance for small-to-medium-large sized organisations with suggested actions to improve internal cyber policy. In addition to the overarching Cyber Governance Code, DSIT has released four accompanying codes of practice for specific technology types, to create a system that allows organisations to select codes most relevant to their operations.

Among these, the previous administration launched a draft code specific to ensuring security across the lifecycle of AI systems—across design, development, deployment and maintenance—for public consultation, with the ambition of agreeing a final version that could be shared with fellow constituents of the European Telecommunications Standards Institute (ETSI). The proposed AI code would support existing government AI adoption guidance, such as the Responsible Technology Adoption Unit (a directorate within DSIT, formerly known as the CDEI)'s portfolio of AI assurance techniques for businesses. The portfolio sets out real world, best practice examples of deploying or procuring AI-enabled systems. The proposed AI code, along with the NTAU's portfolio, are steps in the right direction to provide businesses with the information they need to safely adopt AI systems, but the landscape of guidance in the UK remains confusing to navigate, especially for small to mid-sized firms.

Moreover, the wider government-issued cybersecurity guidance landscape for businesses is, by all accounts, ineffective. It suffers from low adoption and recognition. ISACA's members reported that, in the absence of legal or regulatory obligations, firms are fertile to cultural poor cyber awareness, with boards frequently viewing cybersecurity as a technical issue and an additional, non-critical cost.

FRAUD IN THE UK HAS INCREASED **25%** SINCE THE PANDEMIC

COSTING ORGANISATIONS **£137** **PER YEAR**

To underline the need for an improved government offering to businesses, since the COVID-19 pandemic, the UK has experienced a 25% increase in fraud, with 80% of these incidents being cyber-enabled, costing UK organisations an estimated £137 billion per year. The Cyber Security Breaches Survey 2024, conducted by DSIT in partnership with the Home Office, highlighted that cybersecurity breaches and attacks remained a common threat for 50% of UK businesses in the last year. The study also found 75% of these businesses reported cybersecurity was a high priority for their senior management.

ISACA's own research carried out amongst its European membership earlier this year found that 20% of respondents' organisations are experiencing an increase in cybersecurity attacks compared to the previous year. A further 23% are experiencing the same number of attacks.

Where do we need to go?

The simple end goal of government guidance to businesses is to empower firms to achieve critical operational resilience and protect themselves from cyberattacks. For this, cyber governance codes need to attract industry attention and uptake to eventually yield a business domain where cyber risk is considered by an organisation in the entirety of its operational model (instead of as an isolated vertical).

How do we get there?

- **Establish the UK Cyber Governance Code of Practice**

  The primary task at hand is to establish the UK Cyber Governance Code of Practice as a central tenet of government cyber guidance and best practice and encourage its implementation among businesses. This will support businesses to achieve critical operational resilience, providing the directions to develop personalised cyber-strategies, as well as clear instructions to demarcate cyber in their investment plans.

- **Incentivise uptake of the UK Governance Code of Practice through 'trustmarks' and collaboration with trade associations**

  To increase uptake of both the overarching Cyber Governance Code and its accompanying technology-specific codes, government must collaborate with trade associations to build awareness of the Code, while simultaneously introducing an external assurance 'trustmarking' mechanism, issuing 'badges' (or 'trustmarks') to companies who adopt the code to provide an additional incentive for firms to adopt them.

- **Encouraging the process-driven adoption of AI systems**

  Consumer and business assurance of AI relies on how explainable these decisions are, especially for companies with personnel and resource constraints. For this assurance to take place, the government's AI security code and CDEI's portfolio of AI assurance techniques are promising first steps. Building on these measures, the government should encourage the use of implementation and maturity assessment toolkits for firms to understand the role and effect of AI within an organisation and how to deliver explanations for decisions to employees and customers. Specifically, these stakeholders should be issued easily accessible guidance on the degree of risk systems can carry, the professional expertise required to adopt and safely operate AI systems tailored to the size of the organisation.

- **Launching a Cyber Charter**

  The launch of a Charter for intelligence-sharing purposes between larger businesses and their third-party critical suppliers could have a positive impact on the supply chain resilience in the UK.

Chapter 3: Enhance UK CNI's resilience through targeted regulations

Where are we?

Critical national infrastructure (CNI) consists of the most important systems in the UK today. From the facilities which provide people with safe and clean drinking water, to the networks which help keep the country connected, the UK's 13 CNI sectors are vital to the functioning of everyday life and the wider economy. Not only does damage to this infrastructure impact the availability, integrity or delivery of essential services, it can have major knock-on effects for the UK economy and national security.

Cyberattacks perpetrated by hostile nation states or state-sponsored groups are becoming increasingly frequent and more sophisticated. Ransomware remains the most acute cyber threat facing the vast majority of UK organisations today. As much of the UK's CNI is underpinned by digital infrastructure, malicious actors are becoming increasingly adept at exploiting the vulnerabilities of digital technologies and can effectively deploy tactics to access personal details and threaten to publish this data online or block access to it unless a ransom is paid.

One of the most high-profile cases was the ransomware attack on Synnovis, a third-party supplier of pathology services to several NHS hospitals in London. The attack affected all Synnovis IT systems, compromising patient and clinician confidential data, with significant impacts on the delivery of services at several hospitals and primary care services in London.

St Thomas Hospital, London

Attacks of this nature highlight how critical services often rely on complex supply chains to function and demonstrate the need to think more holistically about our critical infrastructure and the types of defences that can be deployed to protect them.

The inclusion of a new Cyber Security and Resilience Bill in this year's King's Speech is therefore significant and sends an important signal that recent cyberattacks on the UK's most important institutions and public bodies have not flown under the radar, and that 'swift action' to strengthen the UK's cyber defences and address vulnerabilities in the delivery of essential services, is high on the agenda of this Government.

In line with the National Cyber Strategy 2022, the Conservative administration introduced plans in December 2023 to build a stronger risk management framework to mitigate against the risks posed by third-party data centres. Similarly, the risk that critical third parties (CTPs) pose to the UK financial system was a key driver in the decision of the UK's financial regulators in December 2023 to propose new requirements on CTPs to ensure the resilience of any technology that delivers a material service, including by having technology and cyber risk management and operational resilience measures in place.

This Government's commitment to legislate to expand the remit of the existing regulatory framework to protect more digital services and supply chains is a welcome step that will help to fill gaps in the UK's regulatory approach and improve the resilience of the broader CNI ecosystem.

Where do we need to go?

The NCSC made a stark assessment in 2023, stating that it's 'highly likely the cyber threat to UK CNI has heightened in the last year [2022]'. It adds that while progress has been made to build resilience in the most critical sectors, the UK still isn't where it needs to be. The inevitability of a rapidly changing threat landscape and proliferation of emerging technologies highlights the need to increase the pace of action to ensure the security and resilience of the UK's most critical assets.

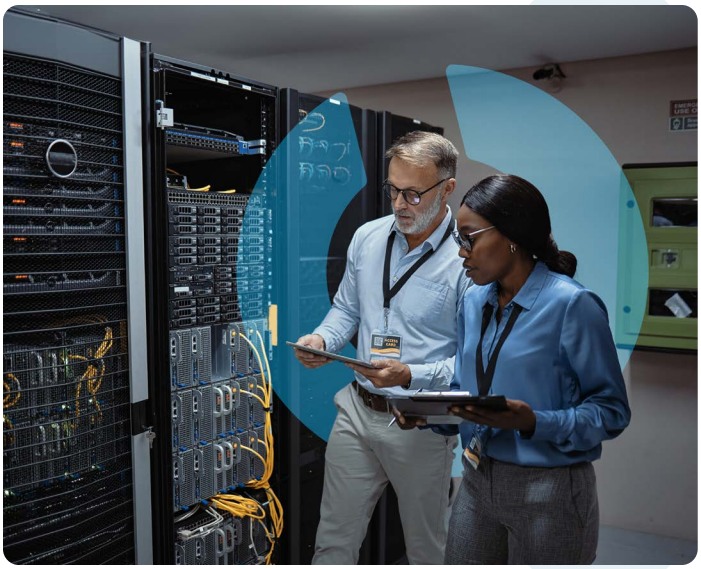
The Government should not hesitate to bring forward the Cyber Security and Resilience Bill and consider how legislation can best strengthen the UK's cyber defences and ensure that critical infrastructure and the digital services that companies rely on are secure. As part of this, consideration should be given to how the remit of existing regulation should be expanded to cover critical supply chains, bringing new sectors and CTPs into scope.

Thinking about UK CNI in more holistic ways means regulation must consider the broader ecosystems within which supplier organisations operate and the role and function they serve in supply chains and ensuring they manage risk appropriately. However, there should be no stick without a carrot, and financial or regulatory incentives must be made available to encourage a broader field of organisations to take steps to proactively mature their resilience. To further support implementation, steps should be taken to ensure CNI operators can secure the right resources and draw from a workforce who have the skills necessary to conduct audits against the NCSC's Cyber Assessment Framework (CAF).

How do we get there?

- **Urgently introduce the Cyber Security and Resilience Bill to protect the UK's CNI**

  As the threat of cyberattacks on the UK's most critical assets continues to increase and evolve, the Government must urgently introduce the Cyber Security and Resilience Bill that was announced in the King's Speech. As part of this, consideration should be given to whether to designate more sectors as CNI and bring critical private sector third parties, working with UK CNI, into scope of cyber regulations. In developing this legislation, the Government should consider establishing a new statutory framework focused on third-party data centres, as well as create an oversight regime for services provided by CTPs to firms in the UK financial sector. This should be followed by wider cross-sector criticality reviews to map dependencies within CNI and its supply chains to ensure new and emerging risks are accounted for.



- **Consider a tiered system of incentives to support implementation**

  In its recent consultation on the resilience of UK data infrastructure, DSIT suggests that commercial drivers are not currently sufficient to drive the level of security and resilience that is necessary to protect the UK's national security. In competitive environments, businesses are faced with conflicting interests, and investment in cybersecurity can be deprioritised to cut costs. To ensure regulations are robust, fair and promote a culture of continuous improvement across CNI sectors, the UK should develop a tiered system of 'trustmarks' which clearly delineates the cybersecurity practices government expects of organisations depending on the sensitivity of the information they are handling. Companies should required to show they can meet particular levels of resilience as a condition to contract awards and conduct certain activities. However, to ensure non-designated companies- such as smaller entities, market newcomers, or those operating within a particular niche - also have incentives to adopt best practices, we believe it is essential the UK's framework of 'trustmarks' is open to everyone. Alongside government recognition, for these companies there should be forms of regulatory relief attached to achieving certain resilience levels and demonstrating their commitment to improvement and regularly publishing evidence of their security protocols.

- **Conduct an urgent review of NIS regulations**

  We would like the government to urgently conduct a review of the impact and effectiveness of the NIS regulations to ensure they remain effective in boosting the security of systems that are critical for the provision of digital and essential services. ISACA responded to the Government's consultation in 2022 on proposals to strengthen the NIS regulations, including campaigning for managed service providers (MSPs) to be brought into scope of the regulations to keep digital supply chains secure.

- **Implement the Procurement Act 2023**

  The government should explore the full range of levers to support CNI operators' management of supply chain risk, including by implementing the Procurement Act 2023 to introduce mandates for CNI contracts to include cyber capability assessment and reporting requirements.

- **Ensure CNI operators can secure the right resources and skills**

  Plans to extend the remit of existing regulations to cover more CNI supply chains need to be accompanied by further work to ensure that they can be implemented effectively. To support implementation, steps should be taken to ensure CNI operators can secure the right resources and draw from a workforce who have the skills necessary to conduct audits against the NCSC's Cyber Assessment Framework (CAF).

For more information

Please contact Sergio Tringali at **stringali@isaca.org**

ISACA

For more information:

AI Resources
www.isaca.org/resources/artificial-intelligence

Digital Trust Resources
www.isaca.org/digital-trust

About ISACA

ISACA® is a global leader with more than 50 years of experience offering knowledge, certifications, community, advocacy, and education in cybersecurity, information systems audit, governance of digital technology, risk and privacy. We have a worldwide network of 180,000 members in 188 countries, with a new European office in Ireland as well as 44 European chapters. ISACA offers globally recognized professional certifications, which are considered the gold standard in the aforementioned domains, as well as solutions to help businesses train and build quality teams to ensure their ICT ecosystem is trusted. This makes ISACA a one-stop shop with services marked by reliability, efficiency and excellence. ISACA is committed to using its deep expertise to support policymakers as they work to make Europe more secure and competitive.