TÜV UK achieves UK Government required Cyber Essentials (CE) and Cyber Essentials plus (CE+) certification

To sell advice to certain UK government agencies in secret nuclear matters, TÜV UK's Nuclear Division had to achieve certification allowing it to work on government owned data. After many months of extensive and expensive work by TÜV IT, funded by Division, both certifications were achieved within a week of each other ending 19th June 2019. CE+ certification is similar to, but not identical to ISO27001, meaning that TÜV UK's IT infrastructure is now very close to being ISO27001 certified. This is something we have asked TÜV IT to work on as a next step, as it is also required by other customers of our division, as well as an enabling step to allow TÜV UK Systems Certification to gain accreditation for ISO27001 delivery.

Description extracted from the internet:
"Cyber Essentials is a UK government information assurance scheme operated by the National Cyber Security Centre (NCSC) that encourages organisations to adopt good practice in information security. It includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

It was developed in collaboration with industry partners, including the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI), and is endorsed by the UK Government. It was launched in 2014 by the Department for Business, Innovation and Skills.

Organisations can earn two levels of certification, or badges:
Cyber Essentials: Organisations self-assess their systems, and this assessment is independently verified.

Cyber Essentials Plus: Systems are independently tested, and Cyber Essentials is integrated into the organisation's information risk management.

Annual recertification is recommended. Certifying Bodies are, in turn, licensed by Accreditation Bodies, which have been appointed by UK government.

As with ISO/IEC 27001, organisations may choose to limit the scope of certification to a certain subset of their business.

The five main technical controls are:
1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

Cyber Essentials guidance breaks these down into finer details. These controls can be mapped against the controls required by ISO/IEC 27001, the Standard of Good Practice and IASME Governance, although Cyber Essentials has a narrower focus, emphasising technical controls rather than governance, risk, and policy.

The Cyber Essentials scheme was launched on 5 June 2014. Several organisations were quickly certified by the end of June. Since October 2014, Cyber Essentials certification has been required for suppliers to central UK government who handle certain kinds of sensitive and personal information. This is intended to encourage adoption by businesses wishing to bid for government contracts. Insurers have suggested that certified bodies may attract lower insurance premiums. Over 6,000 Cyber Essentials certificates have been awarded so far to businesses and organisations. “

Contact:
John Falch
VP Nuclear , TÜV UK Ltd
jfalch@tuv-nord.com