

# [News story: New Quality and Assurance framework open now](#)

Crown Commercial Service is helping the public sector to test the quality of IT services with a new framework agreement, developed in partnership with the Home Office.

Quality and Assurance Testing is [live now](#), and gives central government and the wider public sector access to pre-evaluated suppliers of IT testing services.

Of the 42 suppliers on the framework, 26 (62%) are small and medium-sized enterprises.

## **What is the framework for?**

If you're designing and/or building a digital requirement or cloud service integration, you may need independent, specialist quality assurance and/or testing before you go live to ensure a smooth implementation.

The new agreement complements other [digital agreements](#) such as:

- Digital Outcomes and Specialists (DOS)
- G-Cloud
- Cyber Security Services
- Crown Hosting

The services available will support testing functionality, usability and performance using independent specialist service expertise.

## **What is on offer?**

Buyers can choose from one of four flexible mini competition options, to select their supplier to deliver a wide range of testing and quality assurance services.

Services available under the new agreement are:

- Lot 1: Quality Assurance and Testing Specialists
- Lot 2: Automation, Agile and Development Opportunities
- Lot 3: Load and Performance Testing
- Lot 4: Functional Testing
- Lot 5: Infrastructure Testing and Environments
- Lot 6: Operational Acceptance Testing and Disaster Recovery
- Lot 7: Quality Assurance and Testing Management
- Lot 8: Strategic Quality Assurance Consultancy

## Buyer Confidence

Only Suppliers who have passed the Home Office's robust evaluation will be able to bid for work under the agreement, giving you an extra level of reassurance.

All Suppliers on this agreement have signed up to government terms and conditions, making tendering simple and effective.

## Want to know more?

[Complete the online form](#) to register your interest in the Quality Assurance and Testing for IT Systems agreement.

---

## [Press release: Jail term for Scunthorpe waste operator](#)

Yesterday, Nessa Anne Thompson, of Thompson Waste Recycling Ltd was sentenced at Hull Crown Court in relation to two charges relating to waste site operations in Scunthorpe. This followed as a result of the defendant pleading guilty to both offences.

Ms Thompson from Scotter Road, Scunthorpe was sentenced to a total of 6 months in custody. She was also disqualified from being a director for a period of 7 years.

The charges were brought by the Environment Agency contrary to section 33(1)(c) and section 157(1) of the Environmental Protection Act 1990 and one contrary to Regulation 12(1)(a) and Regulation 41(1) of the Environmental Permitting (England & Wales) Regulations 2010.

Ms Thompson operated an illegal waste operation for the company that had previously held a permit until it went into administration before liquidation. The permit at this point was formally disclaimed.

The site at Winterton Road in Scunthorpe continued to be used and waste was stored in large quantities and in such a manner that it presented a human health and fire risk.

When the site did catch fire on 6 May 2014, firefighters attending the scene were even advised not to re-use the firewater due to the risk of waterborne diseases linked to the number of rats on site.

As a result of inadequate fire breaks at the site efforts to prevent the spread of fire was hampered, causing a greater impact to the adjacent businesses and the wider community.

Speaking after the case, an Environment Agency officer involved with the investigation said:

This site posed a risk to property, the local environment, and people's health because our advice was ignored.

This prosecution demonstrates that we take cases such as this very seriously and will not hesitate to prosecute if necessary, to protect the environment and local communities.

In mitigation, the court heard that the defendant had pleaded guilty to both offences and she was given credit for that. It also heard that her partner was in poor health and that they were both suffering from significant financial hardship.

In passing sentence, the judge said there had been a deliberate flouting of environmental regulations by the defendant. He commented that as the Technically Competent Manager for the site, she would have been well aware that there was no permit in place at the site. He found that there had been attempts to conceal the illegal activity. The judge noted that Ms Thompson has previous convictions for breaches of environmental legislation, for which she was under investigation at the time the current offences were committed. He said that this amounted to a significant aggravating feature.

-ends-

Notes to Editors

Charges

Count 1

PERMITTING THE TREATING, KEEPING OR DISPOSING OF CONTROLLED WASTE IN A MANNER LIKELY TO CAUSE POLLUTION OF THE ENVIRONMENT OR HARM TO HUMAN HEALTH contrary to Section 33(1)(c) and Section 157(1) of the Environmental Protection Act 1990

NESSA ANNE THOMPSON as director of Thompson Waste Recycling Ltd, on or before 6 May 2014 Thompson Waste Recycling Ltd Thompson Yard, Winterton Road, Scunthorpe, North Lincolnshire, DN15 0DH, did treat, keep or dispose of controlled waste in a manner likely to cause pollution to the environment or harm to human health on land at Winterton Road, Scunthorpe, DN15 0DH, namely mixed waste that was being brought onto the site, processed and stored in a manner which posed a fire risk and which did result in two fires on site, and the said offence was committed with your consent, connivance, or attributable to your neglect, as director.

Count 2

PERMITTING THE OPERATION OF A REGULATED FACILITY WITHOUT AN ENVIRONMENTAL PERMIT contrary to Regulation 12(1)(a) and Regulation 38(1)(a) and Regulation

41(1)(a) and (b) of the Environmental Permitting Regulations 2010

NESSA ANNE THOMPSON, as director of Thompson Waste Recycling Ltd, between 18 March 2014 and 13 August 2014 Thompson Waste Recycling Ltd of Thompson Yard, Winterton Road, Scunthorpe, North Lincolnshire, DN15 0DH, operated a regulated facility, which was not authorised by a permit, namely a non-exempt waste operation, on land at Winterton Road, Scunthorpe, DN15 0DH, involving the deposit and processing of waste at the site and the said offence was committed with your consent, connivance, or attributable to your neglect, as director.

---

## **Press release: Harley Street dentist disqualified as a director for 7 years**

Dr Tapeswar Anand, the sole director of Q Healthcare Ltd, which traded as Q Clinic from premises in Harley Street, London, has signed an undertaking to be disqualified as a director for seven years after spending over £1 million of company money, received from patients for dental treatments, on a personally-owned property in Combloux, France.

The funds were spent between July 2009 and March 2013, resulting in the company falling into arrears with paying its liabilities to creditors.

At the date the company entered into administration, no value was listed against the expenditure as an asset, as the company had no legal interest in the overseas property, resulting in a deficiency as regards creditors of £1,080,093.

In agreeing a disqualification undertaking Mr Anand accepted that while a director of Q Healthcare Limited, he breached his fiduciary duties and failed to act in the best interests of the company and its creditors. Specifically, by causing the company to incur expenditure of at least £1,040,254 between July 2009 and March 2013 on an overseas property which he owned personally, and over which the company had no legal charge or security.

Commenting on the disqualification, Martin Gitner, Deputy Head of Investigations at the Insolvency Service, said:

It is clear that Dr Anand breached his duties as a director by using company funds to finance the refurbishment of a personally owned property, which means taxpayers and other creditors, lose out considerably.

This disqualification should serve as a warning that if directors behave in this way their conduct will be investigated fully by the

Insolvency Service and they will be removed from the business environment.

## Notes to editors

Dr Anand's date of birth is February 1974 and he currently resides in New Delhi, India.

Q Healthcare Ltd (CR0 No. 04369068) was incorporated on 7 February 2002 and latterly traded from 139 Harley Street, London W1G 6BG providing dental health treatment.

Dr Anand was a director from incorporation.

The Company went into Administration on 21 May 2013 with an estimated deficiency of £1,080,093.

On 20 March 2017, the Secretary of State accepted a Disqualification Undertaking from Tapeshwar Anand, effective from 10 April 2017, for 7 years.

At the time of the expenditure the company was insolvent on a balance sheet basis. The source of funds used to pay for the overseas property was monies received from patients for the provision of dental treatments.

A disqualification order has the effect that without specific permission of a court, a person with a disqualification cannot:

- act as a director of a company
- take part, directly or indirectly, in the promotion, formation or management of a company or limited liability partnership
- be a receiver of a company's property

Disqualification undertakings are the administrative equivalent of a disqualification order but do not involve court proceedings.

Between June 2010 and April 2013 at least 137 reminders, pressing letters and/or warnings of proposed legal actions were sent by suppliers.

By March 2011 the company was in arrears with paying its taxation liabilities to H M Revenue & Customs (HMRC) and by June 2012 HMRC took enforcement action in respect of unpaid tax liabilities totalling £124,970.

By May 2011 the company was in arrears with making payments to the key supplier of dental products; in 2012 the key supplier placed restrictions, and ultimately a stop, on the supply of further goods to the company as a result of the arrears.

By April 2013 winding up proceedings were being commenced against the company by two creditors: HMRC for tax liabilities of £87,449 and a credit finance provider for liabilities of £46,062.

The company went into Administration on 21 May 2013 owing unsecured

liabilities to unconnected parties totalling £431,518 (comprising £117,029 to patients for dental treatments not supplied; £180,569 to trade & expense suppliers; £113,691 to HMRC for tax; £20,229 to a bank) and unsecured liabilities to me totalling £836,684.

Further information about the work of the Insolvency Service, and how to complain about financial misconduct, is [available](#).

You can also follow the Insolvency Service on:

---

## **[Press release: £3 million to improve journeys and safety at Switch Island](#)**

Highways England has announced plans for major improvements to Switch Island in Merseyside, where the M57, M58 and 3 A roads all join together.

The scheme is being funded by the government's £220 million congestion relief programme, which was announced by Transport Secretary Chris Grayling last month.

Construction work at the junction, which is used by over 90,000 vehicles every day, is expected to start next year. The scheme is designed to improve the flow of traffic and enhance safety, following 49 collisions at the junction in the past 2 years.

New traffic lights will be installed at a height of over 5 metres – higher than HGVs and double-decker buses – so that drivers approaching the junction can clearly see when the lights are changing.

Other improvements will include changes to the road layout and lane markings, new barriers between carriageways, coloured high friction surfaces and better signs.

Bruce Parker, Asset Development Manager at Highways England, said:

We're delighted we've been able to secure funding from the government for this scheme, and can now carry out the detailed design and planning work before construction starts next year.

The improvements we're making at Switch Island will improve journeys and safety at the junction, benefitting the tens of thousands of drivers who travel through it every day.

Jerry McConkey, Transportation and Highway Infrastructure Service Manager at Sefton Council, said:

“We’ve been working with Highways England and Merseyside Police over the last 12 months to investigate the issues at Switch Island and to develop these improvement proposals.

It is great news that Highways England has secured this funding and we will continue working with them to improve the junction and make it safer for everyone using it.

Tony Jones, Chief Inspector of Roads Policing at Merseyside Police, said:

We welcome any improvements to the road infrastructure which assists drivers and makes the network safer for drivers and pedestrians.

Four congestion relief schemes, worth £6.4 million, have already been announced in the North West, with a further £21 million set aside for other schemes in the region, including the Switch Island upgrade.

The four schemes will see improvements made to two junctions where the A595 meets the A66 in Cumbria, at Norcross roundabout on the A585 near Thornton-Cleveleys in Lancashire, and at junction 3 of the M55 near Kirkham in Lancashire.

### **General enquiries**

Members of the public should contact the Highways England customer contact centre on 0300 123 5000.

### **Media enquiries**

Journalists should contact the Highways England press office on 0844 693 1448 and use the menu to speak to the most appropriate press officer.

---

## **[Speech: Countering online radicalisation and extremism: Baroness Shields’ speech](#)**

Good afternoon. I would like to thank Dr Vidino, Dean Knapp and the team here at George Washington University for convening this important gathering to discuss building a global partnership to combat extremism online in all its forms.

It is indeed ironic that one of humanity's most liberating innovations, the internet, is being misused in this way – as a vessel for violence and hatred.

Over the past few years, I have spoken at many symposiums about the escalating threat posed by the abuse of internet platforms and applications by terrorists and extremist groups. I have called for united action and spoken about the urgent need for governments, civil society groups and the private sector to come together to apply new technologies, share information and develop best practice solutions. But today we are at an impasse.

It is no longer a matter of speculation that terrorists and extremists use internet platforms and applications to inspire violence, spread extremist ideology and to plan and execute attacks. Each tragic incident reconfirms it.

We come together this week following yet another horrific attack. This one in London around the Houses of Parliament; my home and my place of work. Five people tragically lost their lives, 50 were injured and 30 hospitalised. The victims were from 12 different countries. And within 24 hours, Daesh claimed responsibility.

We know how extremists manipulate information and sow the seeds of discord in society. We know how they use propaganda to reinforce grievance and instigate hatred. And we know how they convince people to give up their lives and join 'the fight'. They target those who feel vulnerable, marginalised and invisible. But today the pool is expanding exponentially, as billions connect to social networks – fertile platforms for enticing and enlisting recruits.

Yet unlike the physical world where national governments can take clear and firm actions to keep people safe and secure in their homes and communities, the virtual space is the domain of commercial companies and we must rely on their cooperation and support to keep people from harm.

If we are to protect human life in this ever more connected world, we need a new model of shared responsibility and this is the conversation I want to have with you today. I would like to challenge our thinking and ask how we move from reacting to crisis, to prevention and a full acceptance of responsibility on all sides.

In western societies we hold sacred our democratic values: freedom of speech, the right to privacy, the rule of law, safety and security. These values apply to the internet as well, which we believe must be free, open and accessible by all. But there is growing public sentiment that not enough is being done to tackle terrorist misuse of the internet. And when it comes to the question of what to do about it, we are at an impasse.

But the voices of consumers and brands are loud and clear and the recent exodus of top advertisers from social media platforms sends the strongest possible message that their products and services must not be promoted next to deplorable extremist content.

Recently, Germany proposed legislation that sets out binding standards for how social network companies should delete criminal content. However, the



challenge with this approach is that regulation creates a new set of national rules for these businesses that are by definition global and borderless. And there is significant complexity around any regime that governs online activity not least keeping any such obligation current given the speed and evolution of technology and extraterritorial jurisdiction that applies.

So, we are at a critical moment, when united action to tackle this threat is the only way forward. Governments and experts can provide extensive knowledge and a rigorous understanding of the threat but industry is best placed to innovate on technical solutions that address this threat specifically for their own commercial platforms. They must innovate and automate their response to identifying and removing this vile, hateful material so that together we can ensure that everything possible is done to stop it infiltrating and poisoning a global audience.

And increasingly we see a potent 'cycle of hate' across multiple groups and ideologies as all sides of the extremist spectrum feed off each other, escalating tensions. We saw this post the London attack when this image appeared. The photographer who took this picture said he posted it because it showed the young woman wearing a hijab was traumatised by the events around her. But this was not how she was portrayed. The image was wildly misappropriated by right wing groups as representing her as insensitive and indifferent to the carnage that was unfolding.

The growing audacity of all types of extremist groups is perpetuating this vicious cycle. The far-right asserts that Islam represents an existential threat to the West, stating that all Muslims are supportive of terrorism. We have seen terms like 'rapefugees' used in social media, stigmatising those fleeing the atrocities in the Middle East. The far-right is using groups like Daesh as an opportunity to frighten, sow division in communities, and make their extremist narratives more palatable.

Social networks algorithmically connect like-minded individuals and amplify their passions. That is the core of the online advertising business model. But these connections can channel people into echo chambers where highly emotive and passionate content, amplified by these algorithms, reinforces extremist messaging. This creates an illusion of strength in numbers when these views are in fact fringe views.

Over the past year, we have seen new developments such as the use of social media live during attacks that complicate disruption efforts. Terrorists document their unspeakable actions and bask in a nihilistic personal moment of fame and notoriety. Furthermore the footage is later released and used in instructional videos to inspire and incite more violence, perpetuating a vicious cycle.

The precedent for the real-time sharing was tragically set in 2016 in the broadcast of the murder of a French policeman and his wife on social media while their little boy looked on in horror. We saw this used again a few weeks ago during the horrific attack in Kabul on a military hospital, where the attackers posted live photos as the event was unfolding.

Terrorists' use of the internet as a sphere of influence will continue to evolve and adapt, and we need new methods to quickly identify and remove terrorist and violent content, and to deliver more effective strategic communications to counter these deadly narratives. And we must be evidence based; too often we are reactionary and do not adequately deal with the complexities faced.

Daesh in particular produces material designed to capitalise on community tensions and hostility towards Muslims in the West. This further isolates groups away from mainstream society. Their message is that every Muslim has a duty to fight – that 'jihad' is a fight that is local, as well as global and that if they are unable to travel, there are legitimate targets in their home countries.

Following the attack on Berlin's Christmas market, Daesh released a statement on Telegram in Arabic, French and English encouraging their supporters to carry out lone actor attacks in the West and Europe during the holiday period, specifically advising supporters to target 'celebrations, clubs, hospitals, markets and movie theatres'. Tragically, foretelling the Reina nightclub attack in Istanbul on New Year's Eve.

We have seen this call to arms before. Last year, the then spokesperson Abu Muhammad al-Adnani, called for the group's supporters to carry out terrorist attacks during Ramadan. At the time, analysts regarded this call as less persuasive than his previous fatwas. But in fact it proved deadly. It was the bloodiest Ramadan this century.

Other emergent narrative themes in Daesh propaganda include the total rejection of LGBTQ communities and a hatred of nationalism and secularism were cited as motivation for the attack on the Pulse nightclub in Orlando and the lorry attack in Nice on Bastille Day.

This directional shift is reflected in Daesh's official online publications as well. The image on the left of the screen shows its Dabiq magazine which encouraged supporters to embrace the Caliphate and build a new state, the second shows its newer publication, Rumiya which calls on its followers to carry out acts of terrorism wherever they live and wherever they can, reflecting the new reality and its survival as an ideology.

Let me illustrate some of the atrocities that Rumiya has inspired, as each edition contains graphic instructional videos. The second edition called for lone actor attacks using knives with a full demonstration on a frightened hostage, which was replicated in the heinous murder of the French priest in Normandy and attacks in the Minnesota shopping mall last year. The third edition, advised its supporters to carry out vehicle-based lone actor attacks, praising the Bastille Day Nice attack replicated in Berlin and here in the US at Ohio State University.

Recently, a scene showing how to build a shrapnel-filled IED in a kitchen was disseminated. More than 100 links to this video were posted across 29 platforms within an hour. This was organised on Telegram, distributed on Twitter and the video was hosted on YouTube, Archive, Send Vid and Google

Drive, part of the terrorist 'ecosystem' used by Daesh to ensure their propaganda has maximum impact. Twenty-four hours after the video's release, despite best efforts, half of these links were still active.

Although their ability to produce and distribute propaganda has declined, their ability to reach a global audience has not. According to research the UK government has undertaken, as Daesh have been degraded and defeated, and their infrastructure compromised on the ground, its 'unofficial' brand ambassadors are prominent distributors of propaganda. These devotees critically create their own material which they promote and discuss across networks. Idolisation of lone-actor terrorists as martyrs for the cause feeds an increasing audacity in attacks and offers members the chance to gain fame, status and glory.

We now see other terrorist groups mimicking Daesh online tactics with devastating consequences. In fact we see an escalating competitive dynamic amongst terrorist groups – a savage game of one-upmanship.

In the past few weeks we have seen the Syrian al-Qa'ida linked franchise Hayat Tahrir al-Sham (HTS) launch al-Ebaa, a professional media brand for its online communiques and videos. In mid-March they released their first English language statement, rebuking the US for its 'selfish' policy on Syria.

As the quality and quantity of Daesh output fluctuates, we must not lose sight of other extremist groups seeking to increase their online presence. In the UK, the neo-Nazi group National Action were proscribed for glorifying terrorism, having built up a fan base through the use of explicitly youth-orientated material to reach new recruits. The ability for other terrorist groups' propaganda to incite violent attacks is no longer theoretical as the brutal murder of Jo Cox, a UK Member of Parliament, last summer demonstrates.

The threat we face continues grow. We must develop and rapidly deliver an ever-stronger response at pace and scale. Some progress has already been made.

In the UK, we have developed a world leading approach for tackling terrorist and violent extremist use of the internet focuses on 2 areas of work:

1. Working with industry to voluntarily remove extremist content online through the counter terrorism internet referral unit.
2. Bringing communication experts and civil society groups together to develop and run targeted and effective counter messaging campaigns that provide compelling alternative voices to extremist rhetoric.

Working together with industry in 2016, the UK's counter terrorism internet referral unit, run by our metropolitan police department, secured the removal of over 120,000 pieces of terrorist and extremist content. We supported the setting up of this model in the EU, and their unit was launched in July 2015 to secure the removal of content in a wider range of languages. The unit has

reported that 90% of their referrals to industry have been removed.

Following the Paris attacks, Telegram acted swiftly to suspend the accounts of 78 public channels used by Daesh and supporters in 12 languages. Telegram recently to the UK request to remove English language Daesh propaganda. And last year, we saw leading internet companies come together in December in a proposal to build a shared hash database of terrorist content at the EU Internet Forum.

So this looks like progress, right? Yes, but it is still too little too late. By the time we react, the terrorists have already reached their audience. Research conducted by the UK government shows that the majority of links to terrorist content are shared within 2 hours of first release. They anticipate take-downs and suspensions by instructing their supporters to return to the open net time and time again.

This must change. We need a new approach, a new partnership. Governments across the world are agitating, looking at legislation to force the more timely removal of content by social media companies; reinforced by fines and other sanctions. I do not believe this approach alone will succeed.

It is incumbent upon industry to drive this change. They must build new capacity that is holistic, targeted and dynamic to address these threats and reclaim their platforms from those who exploit them, incite violence and push dogma and repression.

Finally, if the terms and conditions that govern these sites are based on corporate philosophies, values and beliefs, then surely the goal posts can be moved.

While violent extremist groups seek to undermine the very ideals and values that the internet was established to advance, we must reinforce its capacity to be the answer to hatred and intolerance, rather than the vehicle for it.

We must understand the influence of terror groups online and deploy the use of strong data analytics to recognise how terrorists amplify their messages and to decipher the patterns of their deadly actions.

And in terms of technology, we need to improve solutions that classify the language of extremism, automate the identification and removal of dangerous content at scale, and create tools that better tackle automated bots and other techniques that support these propaganda machines. In essence we must take a stance of solidarity against terrorism. Solidarity across governments, industries and peoples around our world.

The internet is universal and it is imperative that developers consider these dangers alongside other internet harms. We need companies to champion and support projects that build digital resilience – programmes that help young people think critically about what they see and read online so they can make informed and safe choices. Together with online safety charities we can help increase awareness, confidence and capabilities.

We must empower the global community with better tools to report and respond

to harmful content; to speak out and take action. Every person has the ability to recognise bias, hatred, and intolerance and to say, no, not on my profile, not in my name.

We can't let the world retreat to a dark place of ignorance and prejudice. We must stand up for what we believe in. Freedom. Peace. Democracy. Understanding. Inclusivity. A world in which knowledge, debate and discussion bring people closer together and make them feel a part of something greater than themselves.

To close, I will leave you with this quote from Prime Minister Theresa May the day following the London attack:

Yesterday we saw the worst of humanity, but we will remember the best.