Third party assurance

Prepared by:

David Rowan, Managing Security Consultant

Agwu Nwoke, Managing Consultant

Table of contents

1. Introduction

Third parties provide an invaluable resource and service to enterprises. Who else do you turn to if you do not have the capacity, capability or competency to provide agreed and expected deliverables? Third parties can provide the experience, skillset and efficiency that might otherwise be missing. But, how do you ensure that the same third party is trustworthy? It is, after all, your reputation and future business at stake here.

It is a sound generalisation that we only hear of third party assurance failures when there hasn’t been enough assurance; the food not labelled correctly or the missile test that shot off in the wrong direction.

But, how far should an organisation go when validating the service of a third party? What does the third party need to be validated against? How can you be confident that the validation process is effective? Is the validating process detrimental to the aspirations and requirements of the organisation or the effectiveness of the third party?

The objective of any third party assurance is twofold:

1. To provide verification that the purchased/contracted services, goods or products from the third party meets the requirements and values of the purchasing organisation.
2. To minimise the level of risk of resultant issues, penalties, fines and the like as a consequence of utilising that third party.

Therefore, it is imperative that appropriate assessments must be performed on the third party and their practices.

This paper explores the concept behind third party assurance and the extent to which such assurance is deemed satisfactory or detrimental.

2. What are third parties?

What exactly is a third party? Loosely speaking, it is an individual or entity that is involved in a transaction or service but is not one of the principle agents. It may have a lesser interest or stake in the value of that transaction or service. Essentially, it is an entity external to the purchasing organisation that provides a product or service for or on behalf of that organisation. Use of third parties happens in every industry and sector.

A simple example of a third party could be when an organisation asks a third party to provide desktop support for their IT environment. In this simple example, the organisation engages the third party and that service will almost certainly be invisible to the customers of the purchasing organisation and have little or no impact on the customer at all. In a more complex example, the third party could be asked to provide logistics and move stock on behalf of an organisation or even create and produce entire products and services with the purchasing organisation’s branding. In these examples, the third party is critical to the delivery of products and services of the purchasing organisation.

3. Why are third parties used?

The main reasons a purchasing organisation will use a third party: they cannot do everything themselves or they do not want to do everything themselves. These hide a multitude of refined reasons. A third party may have greater expertise in producing widgets; having an additional supplier may provide resilience in manufacturing; a third party may focus on a service which isn't core to the purchasing organisation, but still needs to be carried out; outsourcing may free up internal resources to be used on a different project or a third party may be able to offer a service more quickly as it already has skills or equipment in place.

Whatever the reason for using a third party, trust is placed in them to provide the services that are contracted. However, no matter how beneficial and innocuous these strategic arrangements might seem, a third party can make or break an organisation's operations, reputation and security.

As an end consumer we can generally trust that a product is as described. If not, it can be returned, complained about, or we can live with minor inconvenience if it is not as described.

For an organisation, it is different. The organisation should verify that the products and services they receive are as expected and that there are no unintended consequences. Once a third party has access to an organisation's network or a critical part of the infrastructure, they also have access to confidential company, customer and employee information, processes and operations. If the third party's network and other parts of its infrastructure are not secure, they put the purchasing organisation at risk. The organisation is ultimately responsible for whatever happens to their resources, services and products.

> "The organisation is ultimately responsible for whatever happens to their resources, services and products."

4. Third parties - The good & the bad

It is the case that many organisations need to perform vendor assessments to gain assurance. At NCC Group, we often find that organisations are not properly equipped to perform these assessments and do not have the capability to answer key questions about how third parties could adversely impact them.

Assuming that an assurance process that assesses the use of a third party is actually in place, to what extent must that process be executed? Let us consider some contributing factors. The one thing that is rarely given up is brand. We see the brand identity in supermarket, transport logistics, road repairs and education – but all these sectors use third parties while retaining their brand as the mast head of the product or service being delivered.

Brand identity has the benefit and drawback of keeping the purchasing organisation in the spotlight. If the third party does a great job then we can call this successful outsourcing while taking the credit as the purchasing organisation. If the third party does a bad job then who delivered the service is forgotten and the purchasing organisation will take the brunt of the impact in the news and from consumers. Additionally, any consumer recourse is with the provider of the service and not with the third party partner. Consequently, the purchasing organisation will have to pay compensation in a more visible manner.

A consequence of using a third party is the surrender of influence. Depending on the product or service being commissioned and the relative sizes of the organisations involved, influence may be diminished to simply picking from a menu of services with no customisation and no say on how the service is delivered. That lack of influence can lead to undesirable or unethical manufacturing practices being used in products that are then sold as the purchasing organisation’s own. This is not ideal for any organisation and almost certainly against their own corporate policies on corporate social responsibility and the like. Such consequence is not just restricted to manufacturing; this lack of influence can also happen when a third party platform, such as Facebook or Twitter, is used for customer service: it is difficult, perhaps impossible, to control the ads served next to your brand when there is no payment for the service being provided.

> “A consequence of using a third party is the surrender of influence.”

5. When Third Party utilisation goes wrong

Third party failures hit the news fairly regularly. Here we look at three examples of what went wrong and, importantly, what lessons can be learnt from each failure.

5.1 The Horsemeat scandal

This failure of third party assurance comes from a well-known case in 2012 when horsemeat was found in the human food chain across Europe incorrectly labelled as beef. This led to product recalls, government enquiries, people unknowingly betraying their religious beliefs and jail time for the perpetrators. Here, consumers were choosing food from a retailer who had chosen products from a third party manufacturer.

Even in retrospect, it was difficult to know how many and which third parties were involved in the production of even one of the ingredients (the "beef"). This example, was found to be the result of criminal activity, but shows some of the difficulties of a third party assurance programme and consequences of it failing. [1]

What can be learnt?

If supply chain assurance checks are to be undertaken, we must be able to have confidence in the results. That means the tests being appropriate to the risks of using a third party and those tests being carried out in an effective manner independently of those with vested interests – i.e. not by the processor themselves. In the official report into the horsemeat scandal, there is a call for proper unannounced audits of the food supply chain to ensure that everything being produced is as it should be. This sort of unannounced inspection will provide an effective control against some risks but not all.

To make sure we have the right checks to cover relevant risks, we must first identify the risks; this means taking an aggressive approach to identifying what could go wrong and then creating suitable checks to identify if those risks are being realised. Each check must be based on the risk impact and likelihood.

5.2 Factory conditions

In another well publicised scandal, a number of clothing brands were found to be using a supplier in India where workers were in unsafe conditions to the point of a factory collapsing with the loss of more than 1,000 lives. In this case, there weren't any lengthy supply chains; the factory was directly contracted to a number of clothing brands.

While this is an extreme example, it is not an isolated incident and it is not uncommon to hear of conditions in factories which do not align with safety or ethical standards that could easily be assumed as in place. [2]

What can be learnt?

[1] https://www.gov.uk/government/publications/elliott-review-into-the-integrity-and-assurance-of-food-supply-networks-interim-report

[2] https://www.nytimes.com/2013/05/14/business/global/hm-agrees-to-bangladesh-safety-plan.html

The search for cheaper suppliers led some brands to India where costs are lower partly because of cheaper labour costs and partly because of a less stringent regulatory environment. In this case, when the lower regulations led to deaths, the firms found that their outsourcing strategy didn't align with their values as businesses and employers or with the values of their customers. Impact to the reputation was just one adverse effect for the companies involved.

A third party assurance programme would have to be particularly detailed and well-funded to detect building defects in a third party's factory; but to suggest in contracts that safe working conditions should be provided would not be unreasonable and these could then be inspected prior to commencement. More widely, it is prudent to take a general look at an organisation that is being proposed as a third party in order to determine if the general values of that organisation align with the purchasing organisation. If there is alignment, there is a lower likelihood of incidents that will adversely impact the purchasing organisation.

5.3 Reaction wheels

Satellites are made up of many components. As with lots of complex machinery, there is no single manufacturer but a complex supply chain. The Kepler space telescope used reaction wheels to keep it stable enough to take sharp images of far-away galaxies. They were made by an external company and supplied to NASA for installation in the space telescope.

The wheels were cheap compared with the overall cost of the telescope comprising of just 0.1 per cent of the overall cost. Yet, with four on board – three in use and one spare – the failure of these components has made the telescope unable to fulfil its primary mission of finding Earth-like planets in other parts of the galaxy.

This isn't the only satellite where such wheels from the same manufacturer have failed. NASA undertook additional checks on the components prior to their inclusion but that didn't stop them failing on Kepler before the mission was completed.[3]

What can be learnt?

Even with what from the outside appear limitless resources, the checks that NASA was able to carry out on the procured products were not enough to ensure that they were fit for the job – even with redundancy in the design. It may be that the low relative cost of the component meant fewer checks were carried out. It may be that it was the best product available at the time the design was completed and NASA had no choice but to go for a component with known design flaws. Either way, we can learn lessons:

- Consider the potential impact of the outsourcing engagement rather than the cost as a means to determine the rigour or breadth of checks that should be undertaken, and;
- Ensure the critical features of the component or service are fully known and understood.

Without this knowledge, it's not possible to determine if the outsourcer is able to fulfil the contract or even if the right product is being procured.

Little things can have a big impact. The supply chain must check critical items – lots of things can be critical!

[3] https://news.yahoo.com/planet-hunting-kepler-spacecraft-suffers-major-failure-nasa-203147459.html

6. What do regulations say?

Regulations and standards are very aware of the use of third parties in delivering services and products. We see this in security standards such as ISO27001, the Payment Card Industry Data Security Standard (PCI DSS) and in the General Data Privacy Regulation (GDPR).

ISO 27001:13 suggest that third party relationships should be:

- Bound by policy
- Address security requirements in the contract
- Monitored and reviewed
- Managed to ensure changes to the supply chain are know

While the PCI DSS agrees that third party relationships should be:

- Recorded (all service providers known, 12.8.1)
- Documented in a contract (12.8.2)
- Have due diligence prior to engagement (12.8.3)
- Able to maintain compliance with the standard (12.8.4)
- Have the split of responsibilities known (12.8.5)

GDPR sets out relationships whereby:

- The Controller is responsible for all actions taken by the processor within contract
- The Controller's DPO is responsible for ensuring that the processor is continually in compliance with GDPR i.e. that they are using the data only for the stated purposes and in a secure manner

NIST CSF scores against the following for supplier assurance:

- That there are processes for identifying, establishing, assessing, managing and agreeing the cyber supply chain risk management by organisational stakeholders
- Suppliers and partners of critical information systems, components and services are identified, prioritised and assessed using a cyber-supply chain risk assessment process
- Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan
- Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted
- Response and recovery planning and testing are conducted with critical suppliers/providers

The common themes across these standards are that controls must be:

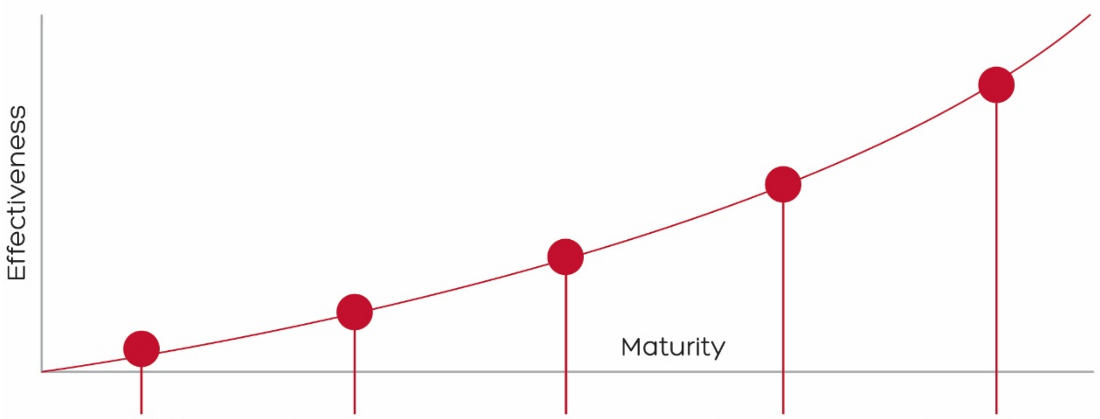
1. Documented so they are known and understood by both parties
2. Put in place before the third party starts providing services
3. Reviewed during the course of the contract

There is broad agreement across these regulations that the responsibility lies with a purchasing organisation to make sure that its third parties are doing the right things. It shouldn’t be left to the third party to be an honest provider, there should be verification of the services provided. So how do we best make sure this happens?

The regulatory requirements for the purchasing organisation should be taken into consideration when assessing third parties. All third parties should either be compliant, enable compliance or help the purchasing organisation maintain compliance with the applicable regulations.

7. What really happens in organisations?

Across the work that NCC Group carries out, we see a wide range of approaches to third party assurance approaches and maturity.



No controls and no ideas
Dispirate lists of third parties. No contacts, no SLA or contractual controls. No single register of third parties. No central contact list. No idea who is responsible for any relationships. In an incident scenario access is shut off to see who screams as it's the only way to identify services. Resources for third party management are an aspiration only. Any control is based purely on what the third party offers as standard.

Some ideas but no control
The purchasing organisation has a register of third parties but does nothing more than keep track of who they are and the services they provide. Knowledge that third parties should be controlled but little resource or skill to be effective. Registers are created but aren't kept up-to-date. Not reviewing risk based or compliance driven requirements. All details become inaccurate and controls ineffective. A first step but doesn't provide any effective control or risk mitigation.

Pre-engagement checks, no in-contract controls. There are pre-engagement or due diligence checks on each third party as they are engaged but no furher checks through the lifetime of the contract. Pre-engagement checks pass prior to being allowed access to their network. Infrequent insistence on further controls and driven only by compliance, not risk. Lack of resources in the third party management team prevent further checks. Third party details amnd controls quickly age and suspicious activity cannot be detected or reviewed.

Pre-engagement checks and some in-contract controls
Pre-engagement due diligence and SLA in a contractor or supporting document. However these aren't referred to unless there is a problem detected by some other means. Excellent pre-engagement checks and bespoke technical controls on systems assessed. The resources available don't stretch to active monitoring of the actions each third party took so nefarious activity or changes to control effectiveness not pro-actively detected.

Pre-engagement checks with in-contract controls and monitoring and reviews
The gold standard. Not only are there due diligence checks prior to contract signing but the contract sets out what is expected in a measurable way. The SLAs are agreed monitored and reported on regularly in reviews with the third party. Team dedicated to third parties management. Quantified review criteria with multi-disciplinary abilities. Engagement with procurement from the start. Identify security requirements based on the service required. Audit, review and follow up. Regular scheduled checks and engagement in service review meetings. Automated security controls and monitoring.

8. Can third parties help assess third parties?

The key factors so far listed can all be performed by a third party; one that specialises in performing the due diligence and assurance assessment on third parties to the purchasing organisation. The irony of this is not lost. Where a third party is used to help assess a purchasing organisation's third party risk, it too must be managed. The advantage though of using a third party to carry out assessments is that, if properly engaged, they will have the proper time, resources, expertise and the capability to provide as in-depth as an assessment as required. The onus of ensuring that what is done, is done properly, will always falls to the purchasing organisation.

In line with using a third party to carry out external assessments, a factor that should not be forgotten is external certifications, regulations or other legal constraints on a supplier. In the world of card payments, for example, there is often a cry of "but they are PCI compliant" (or any other standard) as if this means that all other checks are irrelevant.

It is true that a relevant certification can be a shortcut to validating some controls but it must also be verified to ensure:

- The certification is valid
- The certification applies to the product or service being supplied
- It is appropriate to control for the risks identified to your organisation
- It is backed up with regular checks to ensure that there isn't any "certification cramming"

In short, an external certification is a single piece of assurance evidence but not the full risk picture.

9. What should be considered for a third party assurance scheme?

What can be achieved with the resources available? Focus on the third parties and risks that could have the biggest impact on your organisation. This could be based on contract value, access to the network, provision of intellectual property, visibility of the service. Metrics will need to be built that allow the focusing of effort on the areas most in need of improvement. Time is a key factor here as most other relevant resources are not measured by monetary value. Enough time must be spent on the assurance process to allow for a satisfactory result – whatever that result is. How much time is enough time? That is dependent on the assurance requirements of the purchasing organisation which should be written into the assurance plan and statement of requirements.

All third parties are not equal. The risk profile of each third party should be measured and continually assessed. To gain an understanding of the risk to the purchasing organisation in engaging with the third party, an assessment must be made against a risk management framework. With the external and internal risk levers known, the third party can be monitored for changes for or against the purchasing organisation. This will help provide a further level of confidence in any decision taken.

Looking at risk in a different context, the risks posed by different third parties will differ and will require a different type and depth of checks to ensure that those risks are managed. Focus should be given to those third parties to whom the riskiest activities are outsourced. That risk level should be calculated based on a risk assessment methodology that may consider contract value, systems access, information sharing or any other element that impacts the risk to the purchasing organisation.

Once the risk is understood, the assurance team should be just as bold in removing controls that aren't necessary as they are in the adding controls that are.

Supply chains can get long. Assessing the third party itself is generally the norm but consideration should be given to the whole supply chain. The supply chain to the third party must be considered for evaluation as security is only as strong as the weakest link; this is just as applicable to fourth, fifth and subsequent parties.

Be multi-disciplinary. In line with spending adequate time on the assurance process, the right skill set is imperative for assessing a third party. When engaging a third party, there will be consideration from many areas: commercial, operational, regulatory, security and continuity to name but a few. No one team has all the skills and no one team has the entire visibility needed to ensure all the correct controls are in place. Having the breadth of manpower to effectively assess these third parties ensures that the resources are not overwhelmed and can therefore pay particular attention to the areas of concern. Having the correct skill sets will draw out any gaps to be addressed or at least identify the short comings of that third party effectively helping the purchasing organisation to make the correct decision around them.

Be relevant. To make sure we have the right checks to cover relevant risks, we must first identify the risks. This means taking an aggressive approach to identifying what could go wrong and then creating suitable checks to identify if those risks are being realised. Provisions such as the Internet of Things (IoT), cloud technologies and 3D printing all lend themselves to different types of checks. This means that the likelihood of each risk must be evaluated to provide information on the frequency and nature of the checks. Consider the product, service or process that is being outsourced and make sure that the checks being undertaken are relevant to the risks posed by that activity.

Respond to changes. Things change. Regulations, customer preference, contract performance, even organisational ownership. Whatever changes, be ready react and to change the assurance programme if it is necessary. This could be making relationship meetings more or less regular, focussing on different items or keeping an eye on the environment for changing threats. Monitoring of the third party post the initial assessment is a key and essential process which must be continual. The maturity of the third party can change as can the risk profile. Keeping metrics and KPIs updated as well as knowing performance against defined SLAs is vital. Purchasing organisations need to be aware of any fluctuations that can harm their operations and have to be ready to react and respond accordingly.

For any gaps that have been identified a decision must be made. There are always gaps as no two organisations share the same risk appetite; the onus falls on the purchasing organisation to decide what to do:

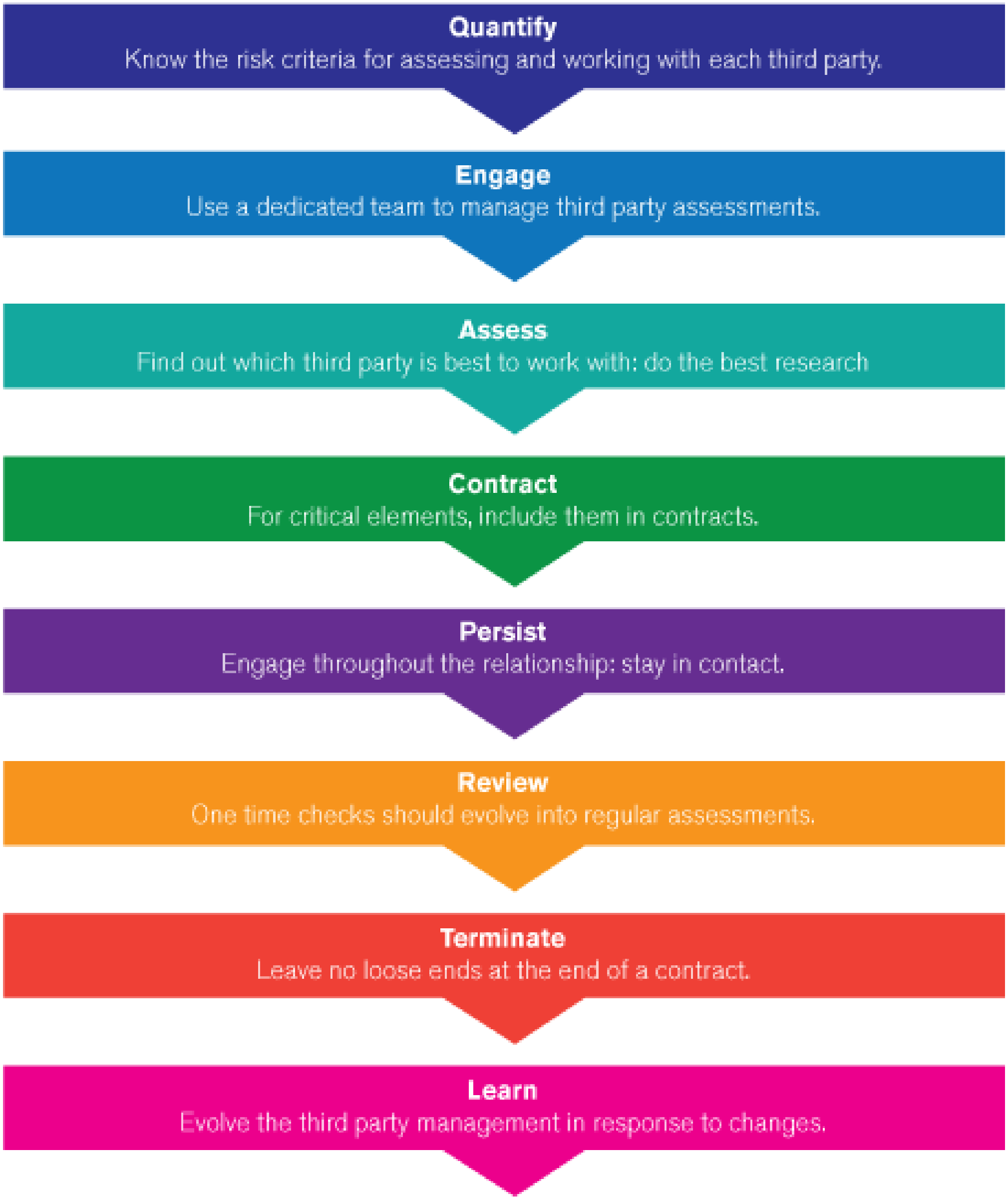
- accept the risk;

  or
- make sure it is reduced.

Reduction strategies could include mandating that the third party sign up to the purchasing organisation's policies and standards, implement new technical controls or restricting data and systems access. The purchasing organisation should always ensure that the risks of using the third party is within their risk appetite. It is a way of obtaining an expected level of assurance and also of increasing the level of confidence in the relationship between the purchasing organisation and the third party.

10. Best practice

When looking around at various organisations and combining all of the best practices that NCC Group sees, the following is a good indication of what current best practice looks like:



Quantify
Know the risk criteria for assessing and working with each third party.

Engage
Use a dedicated team to manage third party assessments.

Assess
Find out which third party is best to work with: do the best research

Contract
For critical elements, include them in contracts.

Persist
Engage throughout the relationship: stay in contact.

Review
One time checks should evolve into regular assessments.

Terminate
Leave no loose ends at the end of a contract.

Learn
Evolve the third party management in response to changes.

Third party assurance is a crucial element in any sustainable business. This should sit inside a wider risk framework that encompasses the entire organisation. Using a framework enables consistency, commonality, accountability, transparency and highlights critical differences between organisations. It improves the understanding and applicability of risk management. It enhances accountability and reduces the cost and complexity of the assurance process. It also reduces the compliance monitoring burden by the use of such a standardised approach. In short, using a framework for third party assurance is the easiest way to ensure that risks are known, understood and either mitigated or accepted in a structured manner.

11. Summary & conclusions

There's no getting away from the fact that each organisation needs to individually consider each of their third parties and the services they deliver. How this decision is reached though should be based on the risk posed by each third party, the risk appetite and values of the purchasing organisation against a consistent and common approach and framework for assurance. By implementing a flexible framework for third party assurance, a purchasing organisation can react to circumstances and flex up or down in the level of assurance without fundamentally changing the approach.

While automation can certainly be of use, more fundamental is to get the right framework process in place and have staff who are skilled and empowered to make the right decisions to keep the assurance programme on-track and effective. This means a cooperative environment within the purchasing organisation and within the third party. There needs to be cooperation between the two organisations. Communication, collaboration and cooperation within and between all parties is essential.

> "Communication, collaboration and cooperation within and between all parties is essential."

The risks of using a third party must always be balanced against the benefits. By implementing a flexible framework of assurance, each organisation can tailor the programme to suit their risk appetite while showing that they have gone far enough, but not too far, in managing the risks related to third party assurance.

As the business landscape changes from the traditional sectors to new technology areas such as virtualisation, "anything-as-a-service" and cloud technologies, there should not be a hard stop to the depth of assessment. Rather a considered view as to the number, quality, importance and intrinsic value of the provision of the service or product and the level of assurance that is required around it.

> "The risks of using a third party must always be balanced against the benefits."