

Effective security?

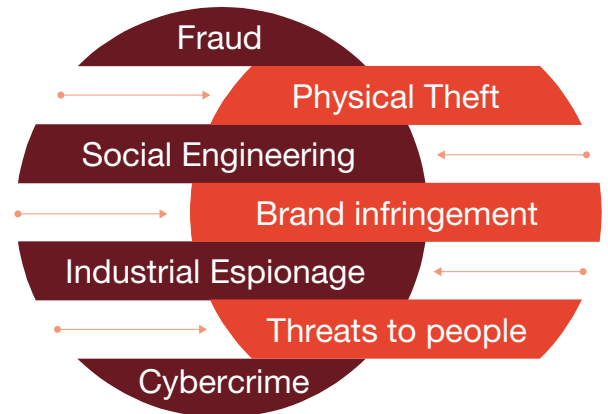
From risk management to real business advantage



Understanding the ‘convergence’ of risk issue

The risks faced by a typical organisation have never been more significant, or more complex, and as threats have proliferated, it's no surprise that many security departments are struggling to keep pace. Safeguarding people, process and technology has got much harder. At the same time the whole concept of ‘security’ has expanded way beyond this traditional remit into areas like brand and IP protection, loss prevention, anti-counterfeiting, cyber-terrorism, parallel trading, online and traditional fraud. Many security departments are so busy fighting day-to-day fires that they're missing less obvious but equally important threats, as well as failing to address the wider issue of converged risk – converged risks are risks that could seriously jeopardise the organisation's long-term profitability, damage its brand or even its very existence.

Figure 1. Convergence of Risk

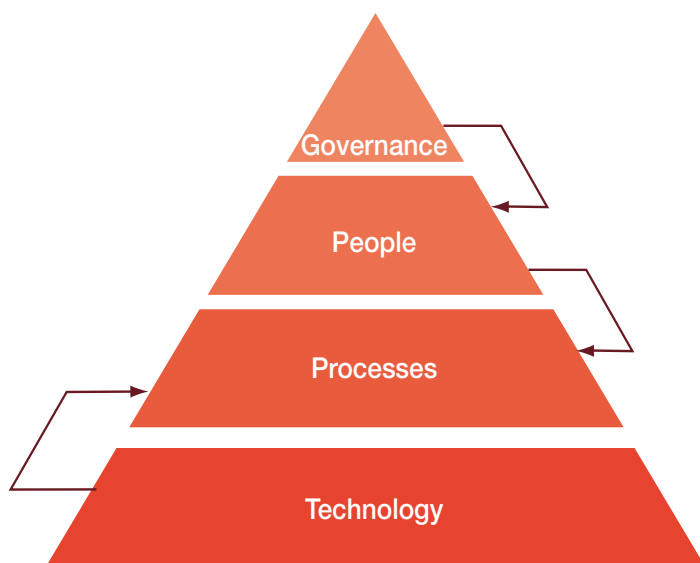


This figure depicts how the multiple and complex merging of risk is causing senior risk officers to rethink their risk and security strategy.

A false sense of security

According to 2008 BERR Report most major UK businesses are devoting between 5-7% of their IT operating budgets to security. That's a huge proportion of money, but is it enough?

Figure 2. Top down – bottom up approach



It's all too easy to spend and focus on the wrong things. Most large organisations have well-established strategies in place to deal with easily definable security risks like fraud, IT security protection, business continuity or physical security, where there are clear lines of responsibility that in some cases go right up to Board level. This can often lull senior executives into a false sense of security. As traditional risks converge with new risks, even some of the world's largest organisations have dangerous security and risk gaps that no-one in the organisation is actually managing, principally because they are operating in silos and focusing on ensuring their area of responsibility is secure or protected, the ‘not in my back-yard’ mentality or because they are unaware of such risks. This leaves organisations open to potentially damaging security-related risks, as no-one is aware that these converged risks, this issue is not being adequately addressed.

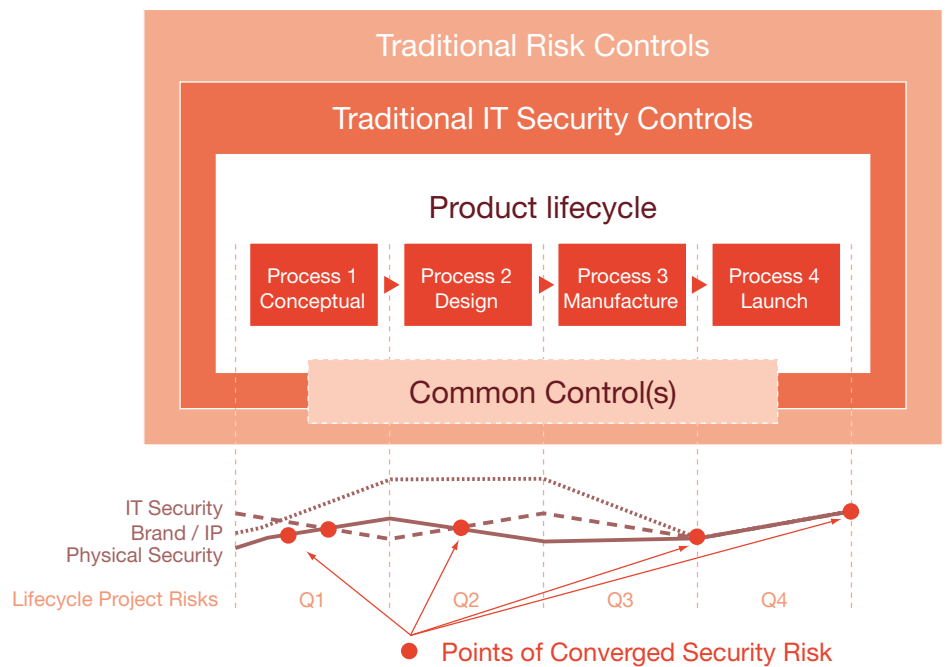
This is why it can also be useful to look at your security profile in terms of actual and potential converged security risks, rather than specific risks to a single asset, person, process, department, company or business application. The advantage of this approach is that it picks up potential issues that might involve more than one process, person or system, or cut across existing departmental lines of responsibility. Taking a more top down and bottom up approach can also help identify possible weaknesses that might not immediately present themselves as conventional ‘risks’. (See figure 2.)

According to an Information Security Survey report from the Ponemon Institute, fraud is costing UK industry at least £6.7 billion in lost revenue and insurance payouts annually. The indirect impact could be as high as £17 billion a year. Is this because we are so focused on ‘traditional’ risks, that no one is looking at the converged risk angle to discover where fraud and security risks are merging?

A good example of converged security risk would be where a new product or service is being taken from concept to formal development and finally sales. In the weeks and months before launching the new product or service, the risk profile changes, ranging from physical risks, supply chain risks, IT security risks, to people theft of intellectual property. Some of these are obvious, some less so, but they can all pose substantial security challenges if not addressed in a holistic strategic or tactical risk perspective. (See figure 3.)

The complexity and ever-changing threat landscape means that security and risk departments around the world need to realign their thinking to address the issue of converged Risk.

Figure 3. Changing Risk Profile



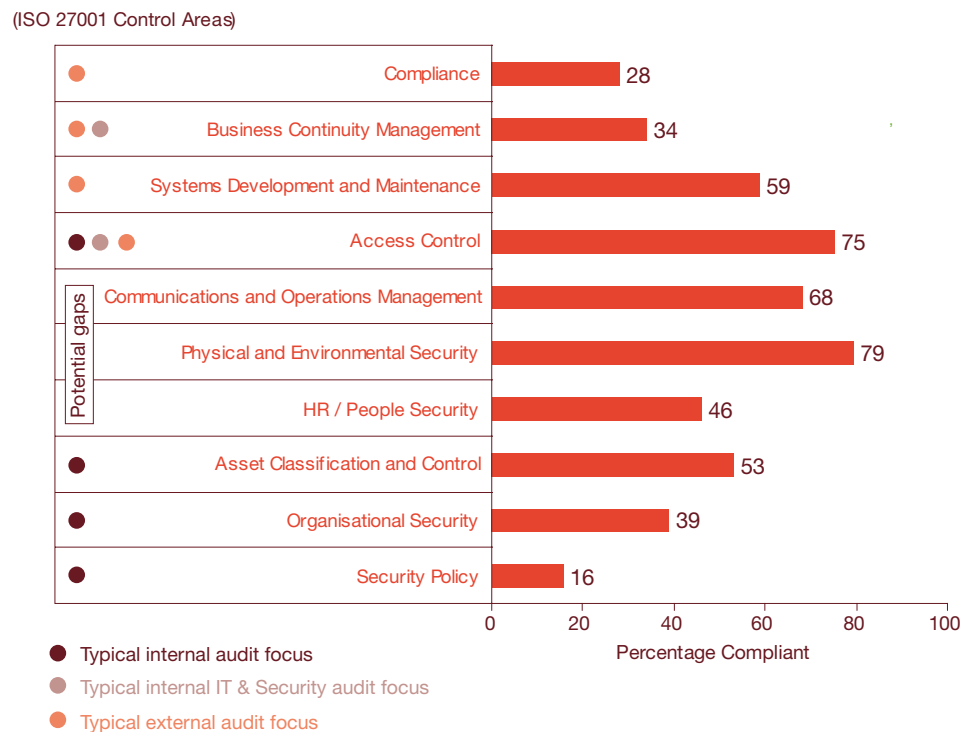
Mind the gaps

Even organisations that have audited their security and risk procedures may find that they're not as well protected as they'd assumed. In our experience, most auditors will focus only on specific aspects of a security programme, with Internal Audit tending to concentrate on procedural details like access control and role segregation, while external auditors taking a wider view that includes these and also emphasises issues like compliance and governance. Yet again, we can see from figure 4 that 'Potential Gaps' in the security and risk audit programme can leave an organisation wide open to converged security risks.

Security Best Practice domains (ISO 27002)

A common misconception is that different aspects of security are being reviewed by internal and external audit. Unfortunately, this can create gaps in auditing schedules and little is realised until a breach or loss occurs.

Figure 4. Potential Audit Gaps?



So how can you protect and prevent and how can PwC help?

What can be done?

Figure 5. Root Cause Analysis



You need to assess whether you have the sort of cross-functional framework in place that can handle all your different risks effectively on an individual basis, as well as being able to make the crucial links between them all (Root Cause Analysis). This will also involve reviewing the roles and responsibilities of all your risk owners and security staff, and examining whether current processes are providing you with the right information at the right time, so you can take pre-emptive action quickly if you need to, and spot potential problems before they happen. This can also help you develop a comprehensive risk review process, so that you can take account of new threats as they arise and over time, this will also help you to avoid the danger of stagnation and complacency or, larger gaps appearing within your audit schedules.

Equally important, if not more so, is having the right culture and understanding of converged risk, and the right way of thinking about security risks. Everyone in

the business needs to understand why security and risk is so important, and how their own behaviour contributes to making the organisation a safer, or more dangerous place to be or do business.

The answer doesn't lie in a silver bullet, but in a more cooperative and cohesive approach to understand converged risk – irrespective of department, process, asset or people involved. Start by modelling your business environment by people, process and technology and then identify the risks that become blurred or invisible due to operational, technology or departmental constraints. By then conducting a more detailed root cause analysis, this will allow you the opportunity to understand and map the risk profile within your business model (people, process and technology) and hopefully identify where the converged risk hotspots or vulnerabilities may lie – you can then begin the successful journey of security risk treatment or mitigation.

Root Cause Analysis can help you identify crucial factors where converged risk may be addressed from a people, processes and technology perspective.

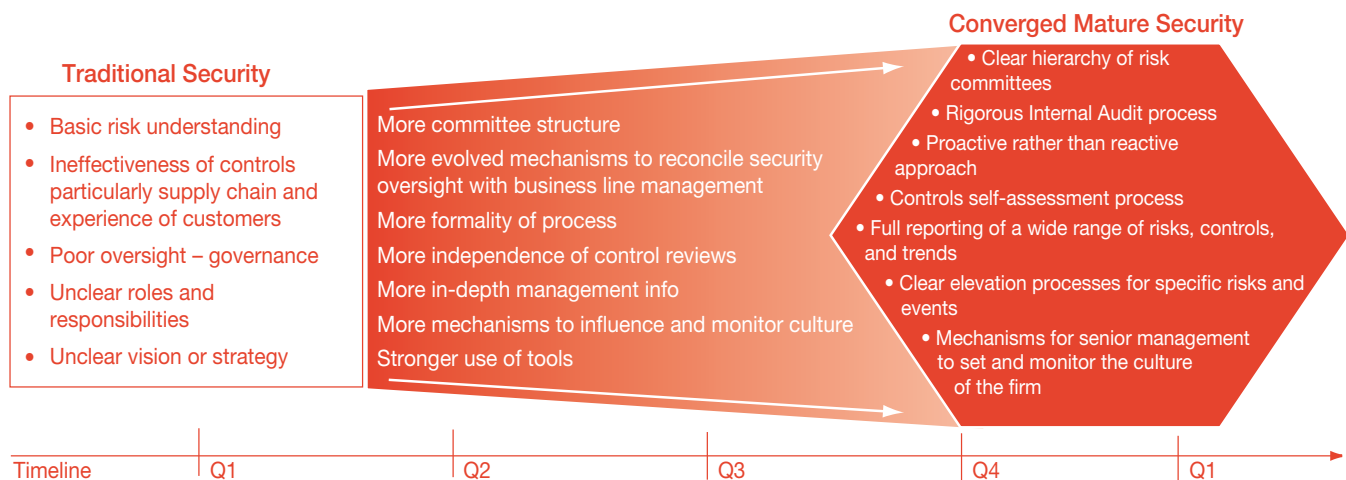
Recognising it's a journey

The process involved to mature your organisations security and risk posture is often slow and arduous, but having a clear strategy and defined goals will ensure processes and procedures can mature to ensure a more holistic business protection strategy across your people, processes and technology.

Other organisations have developed particular expertise in wider security issues, either because they operate in challenging markets (like the oil majors) or in challenging sectors, like the tobacco and drinks companies, where counterfeiting is an endemic problem. Businesses from a broad range of industries have invested heavily in security, and have large teams and a sophisticated understanding of the risks they face, including the potential costs of getting it wrong. Some organisations have gone even further by publishing their security policies on the internet. This clearly demonstrates forward thinking, as communication is integral to a successful security position and they openly publish their attitudes towards convergence of risk through these policies.

There's a lot to be learned from the decisions these organisations have made surrounding converged risk, and scope for others in many different sectors to follow their lead in turning security expertise into tangible business advantage. The common message that can be learnt from some of these organisations is recognising it's a journey, and not a race and that effective security can be turned into real business advantage.

Figure 6. Maturing your security position



A recent Gartner Survey identified consumer 'confidence as key'. There are three basic steps involved here: you need to be able to accurately identify potential problems before they happen, prevent them if possible, and deal with them effectively if they do occur – so that the business can recover as quickly as possible. In our experience most organisations are good at the first, less good at the second, and poor at the third.

The 2008 BERR Report also shows that 55% of businesses have a documented security policy, but again we've found that very few have the sort of coherent and coordinated management structure that can manage the full range of potential converged security issues. According to the PwC Global State of Information Security 2008, only 59% of the 7000 respondents surveyed across the world had a security strategy in place, and only 56% had either a Head of Security, or Chief Security Officer (CSO) responsible for security. This a worrying statistic given the number of well published 'security incidents'.

There's immense value in having a single point of ownership for every aspect of your organisation's security. A CSO can take responsibility for both physical and intangible assets, as well as the increasingly complex area of compliance. A dotted line to the audit and risk committees is vital, and a direct reporting line to the Chief Operating Officer (COO) can ensure that the issues raised are understood and addressed at the highest level. Most of the leading organisations in this field are starting to go this way, but for those that haven't, then in the short-term, it's important to ensure that the Board and the business have a complete picture of the risks the organisation really faces, and plans in place to deal with them.

It's both surprising and alarming to find that a large proportion of companies don't even know how many security breaches they have. According to the PwC Global State of Information Security survey, 35% of the 7,000+ respondents weren't aware how many incidents had occurred in their businesses in the last year, and 44% didn't know what type these incidents were (See figure 7). And while companies are more dependent on their systems than ever before, 28% of respondents did not have any sort of IT disaster recovery plan,

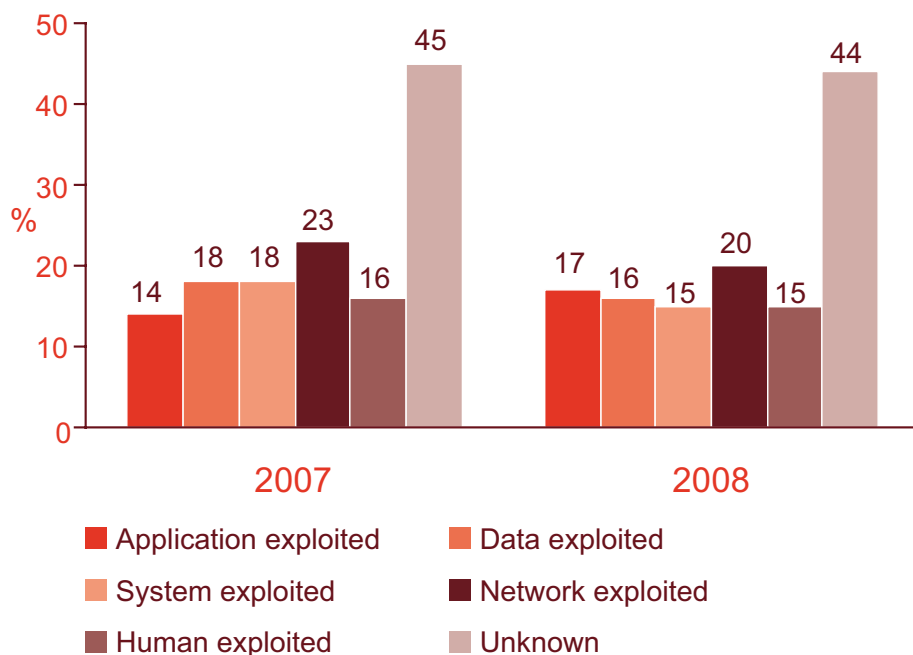
and of those that did, 48% had not carried out a test in the last year.

Organisations with an online presence also face particular challenges in areas like data protection and identity theft, and the nature of their business means they're often on the security front-line for other reasons such as consumer trust and confidence. According to a recent Annual UK Online Fraud Report, as many as 66% of respondents are concerned about the safety of shopping online.

Higher rates of staff turnover, as well as higher proportions of temporary or call-centre workers result in lower levels of employee loyalty, and in some cases – disgruntled employees. All of which make these businesses far more vulnerable to fraud or theft, including the theft of valuable data such as credit-card data.

But it's not all bad news. Our work with some of the world's most sophisticated players has shown that there's a lot more that the majority of organisations could be doing, not only to improve the way they protect what's important to them, but to turn their in-house security know-how into a real business and a potential competitive differentiator.

Figure 7. Quantity and type of incidents



One way of understanding your current security risk position is to re-examine your Security Risk Governance Framework. Such a framework should include policies and processes that are in place to manage the protection of all tangible and intangible assets. This framework should address the convergence of risk issue and recognise the ever-changing threat landscape most organisations face. It is also prudent to analyse your risks in terms of a number of other categories such as financial risk, operational risk (all of which can be significant, especially if you operate in politically volatile markets), brand risk (from IP to counterfeiting), reputation risks, and governance and compliance risks (see next page for examples).

Examples where PwC has helped in the past

Financial risk

One of our long-term clients is a global pharmaceutical business. Some time ago one of their warehouses reported duplicate invoices on the sales system, and within hours the same problem was occurring all over Europe. This was not only a serious commercial issue, given the risk of over-shipments, but there was a real danger that the organisation's sales would be overstated in its management numbers, which could potentially have resulted in misleading financial reports being issued to the market. There was no alternative but to shut down the European system while the fault was traced, as it turned out, to an Indian IT subcontractor. As this suggests, the whole episode was hugely costly and disruptive, so how did it come about and how could the organisation ensure it didn't happen again?

We started by working with the organisation to trace and reverse the duplicate transactions, before moving onto the larger question of how the whole system should be managed, monitored, and controlled. We helped them to identify their 'critical transactions' for the first time, and establish proper access processes – especially important given that this had been the cause of the original problem. And finally we helped them set in place a more effective control framework overall, which has significantly improved their corporate security.

Operational risk

Keeping your business operational is becoming ever more complex and challenging as the number of potential threats multiplies. Business continuity management is increasingly recognised to enable businesses to improve their resilience, response and recovery capability. We've used our own experience of setting up a comprehensive business continuity programme across PwCs 40 sites in the UK to help a range of organisations in both the public and private sectors.

This sort of work involves identifying critical activities, applications, services, and establishing how quickly they need to be restored after a disruptive event. It may involve setting up 'incident management teams' who can take responsibility at local sites, as well as part of a scalable framework to cope with major incidents that could have a national impact. As we've found in our own case, the detailed planning involved in effective business continuity management doesn't just prepare you for incidents but helps you focus your efforts and resources on the most crucial aspects of your business, which in turn helps make them more resilient to day-to-day demands of operational risk.

Governance and compliance risk

All the risks we've looked at so far present both a cost and a very real threat to your organisation. Governance and compliance risk adds a new dimension that no Board can afford to ignore the threat of prosecution. The protection of price-sensitive information is only one obvious example of the vital role security can play here, but any organisation that handles other people's data has a legal duty of care to handle that information confidentially. As several businesses have found to their cost, the Information Commissioners Office (ICO) has the power to impose serious legal sanctions when these standards are breached.

We've worked extensively on all aspects of compliance, and can help you ensure that you have robust governance processes that take account of all your possible vulnerabilities. This sort of review will often have the additional benefit of identifying overlaps and duplication, which can result in significant cost savings.

Brand risk

'In recent years brands have become the most valuable assets on most companies' balance sheets, far outstripping the value of more tangible items like plant, machinery, or even property. Protecting an intangible asset presents its own challenges, from dealing with the potential impact of product recall, to ensuring that poor customer service or product safety issues do not compromise the trust consumers place in your brand.

One area where PwC have particular expertise is anti-counterfeiting. This has been a problem for premium and luxury good manufacturers for many years, but it's becoming more of a threat as new technology makes it ever easier for the counterfeiters to produce convincing fakes. PwC have a wide range of experience with global businesses, and can help you develop a joined-up approach that brings together every aspect of your operations, from country managers, to security, to risk management and brand protection.

Reputation risk

The most enduring collateral damage of a major data loss can be the impact on your corporate reputation. The credibility of a number of government departments has been particularly damaged by recent high-profile incidents.

We've worked with a range of prominent international companies in the aftermath of a significant data breach, from major insurance and financial services businesses, to household-name retailers. We've helped them to minimise the public fall-out, and sometimes contain it altogether. In those cases where the story had already reached the public domain many clients found that calling us in actually helped to reassure their customers that appropriate and rigorous action was being taken, and lessons would be learned. In our experience the key is to take action quickly, and to have a detailed crisis plan already in place that includes how you will manage the press, the bigger and more well-known you are, the more of a media circus there will be.

The 2008 PwC Corporate Security survey

During October and November 2008 the PwC OneSecurity team in the UK conducted an in-depth survey of the corporate security practices of ten leading multi-nationals, including Diageo, BAT, and Unilever. This was the first time that corporate security (as distinct from information security) has ever been benchmarked in this degree of detail, and the subjects covered included governance, people management, physical and equipment security, incident investigation and crisis management, anti-counterfeiting and supply chain, and monitoring.

These issues were measured according to three key criteria, which in our view are the most important measures of the success of any effective Corporate Security function. These are

- **Business Insight:** this is a key objective for Security, because the function will only create value if it collaborates successfully with the business.
- **Compliance and Control:** this means developing robust, efficient processes, so that risks are identified in advance, and effective action taken.
- **Efficiency:** this assessed the day-to-day running of the function, and how well it is performing key tasks.

There were also some interesting overall conclusions to be drawn;

1. There needs to be far greater collaboration with external parties and a deeper understanding of the risks these partnerships represent
2. People security and media security are areas of particular weakness
3. Investigation and intelligence gathering needs to be improved, given the convergence of a wide variety of risks
4. Most companies could do more to prepare for potential crises, especially when it comes to disaster recovery
5. There's scope for better co-operation with Internal Audit, as well as improved monitoring
6. Effective measurement is still an issue. Senior executives want more and better information about the value Corporate Security is contributing
7. Challenging economic times are likely to lead to higher levels of crime

Steve Wright, Senior Manager responsible for leading the engagement commented:

“We found there were considerable differences between the highest and the average scores in each of the three areas. This means there were clear opportunities for all the companies to improve at least one aspect of their corporate security strategy”.



Business Insight	<ul style="list-style-type: none"> • Management Commitment • Strategy & Planning • Risk Management • Internal Organisation • Contact & Cooperation with Supporting Bodies & External Agencies • Intelligence Gathering
-------------------------	--

Compliance & Control	<ul style="list-style-type: none"> • Monitor & Review • Supporting External Parties • Internal Audits • Management Review of inputs • Management Review of outputs • Corrective & Preventive Actions
---------------------------------	--

Efficiency	<ul style="list-style-type: none"> • Implement & Operate • Maintain & Improve • Training & Competence • Physical, Environmental, Equipment & Media Security • Management of Security Incidents, Investigations & Crisis • Anti-Counterfeiting
-------------------	---

For more information on the survey email Steve.Wright@uk.pwc.com Tel: 07841 568 865.

PwC OneSecurity

The PricewaterhouseCoopers OneSecurity team has over 30 years' experience in all aspects of security, from data loss protection to governance risks. Our globally based team understands and speaks business language, we know when and how best to involve experts in legal, IT, business continuity, disaster recovery, crisis management, fraud, forensic and human resources expertise. This wide range of know-how means we can help your organisation to devise a dynamic and forward-thinking security strategy that identifies all the converged risks you face, and offers practical and effective ways of addressing them that won't just save you money, but could even end up making you money.



William Beer

Director

William is a Director in the Risk Assurance Services group and has over 20 years of broad international experience at multinational IT companies. He has worked extensively in IT services, security environments and with security technologies. Additionally William has focused on Information security including security intelligence services, managed security services, data compromise and computer crime. Other areas that he specialises in include information security incident management, security architecture, security governance and risk management.

William provides specialised quality assurance work and is the chair of the OneSecurity leadership team.



Steve Wright

Senior Manager

Steve has worked for the last 15 years in a Professional Service environment as a CISO and in Head of Security Management. This included working in many different sectors such as financial services, public sector, utilities, and FTSE organisations.

Steve provides direction and leadership for major transformation and security integration projects. This includes practical experience of implementing global Information Security Management and Governance framework in new and acquired businesses throughout the UK, Europe and Americas.

Steve is also a representative at the OneSecurity leadership team.