Ticking The Box... and Missing The Point

There are significant differences between the needs of 'compliance' and 'security'. There's also a vast difference between ensuring that the organisation operates in a legally correct, ethical and morally correct manner. Angus Darroch-Warren explains why, without an ongoing understanding of the host organisation's security posture, audits – no matter how rigorous – will only miss the point of what they're actually trying to achieve

Angus Darroch-Warren BA (Hons) MSc PSP CSyP FSyI: Group Director of Linx International

There are sets of laws, regulations, rules and standards by which we run our lives on a daily basis. Common law, criminal law and a myriad of Parliamentary Acts and regulations ultimately govern how we behave as individuals as well as groups. This plethora of 'red tape' is overseen by the courts, local Government, central Government, international agreements and – dare it be said in a post-Brexit vote Britain – regional assemblies such as the European Parliament.

In the security and risk workplace environment (and across businesses in general), we're continually required to meet, adhere to, follow or take a passing interest in a variety of laws, regulations, standards, specifications and other useful pieces of information that shape today's organisational world. Deciding which ones are mandatory, which are relevant and those that make for coffee break reading falls within the remit of senior managers and the compliance function.

Compliance describes the behaviour of an organisation to meet and comply with the various laws and regulations that cover how it behaves towards its staff, customers and stakeholders and the way in which the business is managed. To borrow from the Register of Chartered Security Professionals, security covers protecting people and property from threats posed by crime, terrorism or malpractice and dealing with the risks by responding to them.

From Sarbanes-Oxley to Health and Safety, the International Standards Organisation to the British Standards Institution or from CTPAT to CFATS, organisations are increasingly required to demonstrate adherence to regulations emanating from home and abroad. While these standards are of value, they're not unlike a Disclosure and Barring Service (DBS) check on an individual in the workplace. In other words, they only provide a snapshot of the organisation at any given point in time.

Having a DBS clearance shows that, on the day in question, the individual didn't have any adverse information recorded on file. Similarly, audits demonstrate that, at any given point in time, the company was able to show that it met the requirements of a particular set of criteria.

Preparing for audit

On many occasions, I've visited clients preparing for a compliance audit and it's almost comical to see the frantic search for policies and procedures or evidence to show that the organisation meets its requirements. Whether it's Quality Management Systems (in relation to ISO 9001), Information Security (via ISO 27001) or Authorised Economic Operator (AEO), the fear of failure and potential 'non-compliance' is palpable. Reputations and jobs may be on the line. It's a serious issue.

A recent example serves to illustrate the point. We were consulting for a well-known national organisation requiring AEO status such that the company could develop its international business. The transport manager took on this project and declined technical input from both the security manager and myself. The rationale was that, due to the value of the product being shipped and the highly overt and documented layered security measures already in place, meeting the security criteria would be a breeze.

The assessor duly arrived, passed through various checkpoints and started their work. All was going well. Building security, access control, cargo units, incoming/outgoing goods and storage processes all passed with flying colours. Boxes were being ticked with gusto and the end of the audit was near.

Completing some final checklists, the auditor was discussing minor issues with members of the Despatch Team when the top of a head appeared at the office window. The window was then slid back and a package dropped through, promptly landing on the desk below.

The assessor was quite taken aback and asked the Despatch Team if this was normal procedure, to which one clever soul duly responded: "They always drop them through the window. It's quicker than going through all of the security checks".

On the back of this episode the company failed the assessment, but may well have passed if the package had been dropped in either two minutes earlier or later.

Falling into the trap

In the security world, we're sometimes guilty of falling into the same compliance trap. An example is the management of security teams.

All-too-often, we rely on quantitative security metrics in Service Level Agreements or KPIs to judge how well a team is doing. The client strives to ensure that the security officers maintain the required number of patrols, that the exact percentage of personnel and vehicle are searched, that the number of First Aid boxes and break glass are checked and that the telephones are answered with haste.

Once upon a time, I was working with an FMCG client experiencing losses in one of its packing warehouses. When speaking with the contracted security manager and the client manager in the HR Department, they were both flummoxed as to why they were unable to work out how the losses were occurring.

The workforce was primarily agency staff and the security manager was conducting regular searches of personnel, vehicles and lockers, but hadn't managed to catch anyone in the act. He was exasperated as the search regime was "at double what we should be doing" and had resorted to bringing in extra security officers to help with the search procedures.

Pretty quickly it became apparent that the security manager had missed what was staring him in the face – the product was going out in the recycling waste and being collected outside the site by an entrepreneurial group of full-time employees. Suffice to say, the manager was replaced, vehicles were no longer allowed on site and regular searches of refuse and recycling bins were initiated, in turn leading to a negligible loss rate.

Quality over volume

What's absolutely essential when 'doing security' isn't the volume, but rather the quality of the work that's provided as an output. The tick-box exercise involving questions such as 'Do you have a security policy? – Yes' 'Do you have assignment instructions? – Yes' 'Do you have documented access control processes? – Yes' 'Are intrusion detection alarms installed across the facility? – Yes' 'Are the premises adequately illuminated (eg continuous light, movement sensors)? – Yes' does little to prove that security provision is either effective or offers scope for improvement.

When compliance requirements are put in place, this tends to establish a baseline for security which can quickly become the 'be all and end all' of a security programme. The overriding desire to meet targets often supersedes the need to effectively carry out the required task and provide the appropriate response to defined security issues.

Surely the point of any compliance check must be to ensure that operational activity continually exceeds requirements rather than doing so only on a specific date, in turn providing the desired safeguards to protect organisational assets? Indeed, what's far more impressive is to see a gradual reduction in incidents and a diminishing need for patrolling or conducting searches. This indicates that the security programme is effective and that a positive security culture has been created.

What would be far more relevant is to ensure that effective threat, vulnerability and risk assessments are conducted and that the mitigation options put in place both reduce risk to a level the organisation can tolerate and actually surpass the basic requirements of compliance standards.

The use of tools such as the Operational Requirement process will ensure that all relevant stakeholders are engaged in developing security strategy. The requirements of whichever standard, be it a national or international 'must have', can be incorporated into the planning process. In this way, systems and processes alike may be progressively monitored to ensure they continue to deliver the appropriate mitigation for the developing threat landscape.

When the inevitable tick-box exercise commences, the security team can be confident knowing that not only will they pass the audit or compliance check but, if faced with more probing questions, they can also justify and demonstrate security provision that's based on careful research and consideration of the threats facing the organisation.

"Surely the point of any compliance check must be to ensure that operational activity continually exceeds requirements rather than doing so only on a specific date, in turn providing the desired safeguards to protect assets?"