



IT security and compliance: they *can* live happily ever after

## Contents

1	Pitfalls, misconceptions and mistakes	2
2	It's not all doom and gloom	3
3	Take the right steps towards compliance and IT security harmony	3
4	Base security programs on security principles	5
5	Try to change your perspective	5
6	About the author	6

IT security and compliance are two terms frequently used in conjunction with each other, yet few terms are more likely to have CIOs around the globe, sink their head into their hands. It's not that organisations don't understand the importance of ensuring that data is treated with confidentiality, integrity and prescribed availability; the vast majority of organisations understand this completely. Besides a market crash or natural disaster, few things can damage a business more than a well-publicised security breach. It's rather that security management now feel that they have the additional responsibility of ensuring IT regulatory compliance, and are obliged to spend valuable human and financial resources on fulfilling auditor requirements that they may, or may not, agree with. Rather than being kept separate, compliance management has a habit of moving into the IT department's jurisdiction, where it becomes yet another item on the plate of an already stretched team. The pure volume of requirements, with their multiple standards, on multiple domains, has IT managers around the world often chasing their tails.

## ① Pitfalls, misconceptions and mistakes

Executive management has a dangerous habit of assuming that by meeting a myriad of compliance requirements they are, by default, secure. This is a common misconception in the relationship between compliance and security, but one is not a given result of the other. You can have secure data, but if you're found to be non-compliant it will, without exception, impact on your business. Additionally, compliance legislation can be quite broad and seemingly open to interpretation; you can have the best of intentions and yet still be found non-compliant.

IT security and compliance are two terms frequently used in conjunction with each other, yet few terms are more likely to have CIOs, around the globe, sink their head into their hands.

There are a number of examples where companies have successfully cleared a compliance audit, only to suffer a security breach shortly afterwards. In terms of PR and customer confidence, it really can be the material of nightmares. Consequently, it's crucial to understand that compliance is not a guarantee against failure or compromise, and that vigilance and continuous control mechanisms have to be built in.

Organisations find themselves distracted in the quest for compliance. This can result in a loss of focus, where short term, quick fix decisions prevail over a structured and strategic long term approach. But whilst security and compliance horror stories often prove motivation enough for change, organisations should be equally motivated by a sense of responsibility to clients, shareholders and employees. It's a case of demonstrating proper management and corporate governance, and taking your security responsibilities seriously.

## ② It's not all doom and gloom

Organisations should look at security and compliance as an opportunity and not just a necessity of little business value. Of course non-compliance can be a threat to your organisation, but if handled properly it's a valuable opportunity which can be leveraged to embed IT security throughout the entire organisation. Compliance objectives should, therefore, involve senior management in the issue of IT security; it's no longer an IT problem but a company initiative, and serves as a perfect spring board to greater alliance and cooperation across management.

Management must be advised that security spending decisions should not only extend to fulfilling compliance requirements, but should also take account of the threats to the organisation, and be aligned with corporate objectives. IT security should be given the attention and response that organisations would give any other threat to their operations, and security spending decisions should not only extend to fulfilling compliance requirements, but also take account of the threats to the organisation, and be aligned with corporate objectives. What's more, the market is demanding best practices and this is an opportunity for organisations to evaluate their existing practices, define new projects, raise their bar and develop long term strategies.



## ③ Take the right steps towards compliance and IT security harmony

There are logical, and achievable steps that companies can employ in working towards a more harmonious approach to IT security and compliance. IT security can be seen as an enabler of, and closely linked to, the corporate strategy and business objectives. Compliance should be accounted for in the organisations' structure with the assignment of a compliance project team. The team's objectives would be to identify requirements and map these to the current situation, to develop a compliance matrix or scorecard from which actions can be identified and non-compliance anticipated, in order to both manage risk and the remediation process. This team should include all stakeholders.

It's exactly this systematic approach that will help organisations make sense of the requirements expected of them, and enable them to address these requirements in a methodical, consistent manner. Enterprises should take comfort in the fact that there are a series of tried and tested actions that can alleviate unnecessary security and compliance challenges.

- ▲ Establish a Compliance Project Team that understands the business the organisation is in, and that can then effectively create and communicate policies for implementation.
- ▲ Identify current, and anticipate future, compliance requirements.
- ▲ Complete a Risk Assessment on the requirements and environment in question.
- ▲ Develop or modify existing organisational policies into procedures, guides and standards.
- ▲ Implement technical and non-technical procedural controls. Re-use existing controls. Don't assume new compliance mandates require new technologies.
- ▲ Communicate policies. Make IT security part of an approach that enables, not restricts, business.
- ▲ Take heart in the fact that there are existing frameworks that assist in measuring and enforcing compliance. These include:
  - Technical Policy Management
    - Patch Management
    - Vulnerability Management
    - Change Management
  - Security Information / Event Management

Organisations should **look at security and compliance as an opportunity** and not just a necessity of little business value.





#### ④ Base security programs on security principles

Once a security and compliance program is structured around a framework and associated controls, organisations will find that they're able to map them to current and even future regulations, and adjustments can then be made accordingly. If a program is based purely on compliance mandates it will need to be updated or changed every time a new regulation rears its head. Similarly, while one regulation might address a certain risk it might neglect other, equally important, corporate threats. This is why it is crucial for security programs to be based on security principles rather than a dogged adherence to regulatory mandates. It's also important to distinguish between security spending and compliance spending. Traditionally IT security has been responsible for achieving compliance objectives, and it's not uncommon for senior management to lump both IT security and compliance into one budget. Effective security programs should be malleable enough to deal with changes in both security threats and compliance regulations. In a landscape of increasingly complex security attacks, enterprises must be able to adapt accordingly. It is precisely for these reasons that security and compliance should be approached on a corporate level, and not as a departmental issue.

#### ⑤ Try to change your perspective

As discussed, ad hoc or short-term compliance will not necessarily make you secure in the long run. Security entails constant evaluation, not least because attacks are becoming more and more complex in both nature and execution. You need to look at what is in place at the moment, what areas you have covered, and have a risk assessment performed. Map out what you have today and then map out what you need for tomorrow. If senior management remains convinced that compliance equals security then you'll find that IT initiatives won't be supported. Security is never a done deal, and to think it is will set you up for a serious failure. But similarly don't panic and dive in without proper assessment first - rather take a strategic and forward thinking approach. A well organised and driven compliance initiative will result in a higher level of security. It's about approach; the identification of risks, the mapping out of requirements and the implementation of adequate control mechanisms. If IT security is managed according to basic commonly accepted best practices in Information Security and Operations, then compliance does not have to be an issue. Shift your perspective, and turn a threat into an opportunity.

## ⑥ About the author

### Kevin Vanhaelen

Kevin is Practice Lead for Dimension Data's Surveyor for Security range of services, which focus on Security Compliance and Risk Assessment. He initiated the local development of this range of services in 2002 and is responsible for business development and service delivery. Kevin has been involved in large assessment projects for major organisations around the globe and has built up invaluable experience in interacting with clients on both a technical and management level.



His expertise lies in auditing, penetration testing and vulnerability assessment and prevention in different markets and complex and sensitive environments. This experience in security is backed by strong academic and professional credentials, including: A Bachelor Degree in Informatics (with distinction), CISSP, CISA, PCI QSA, Qualys, CheckPoint. Other training includes SANS Auditing Networks, Perimeters and Systems, Sensepost Applied Hacking Techniques and regular seminars organised by for example BlackHat, ISSA, and ISACA.



#### Regional Head Office Contact Details

##### **Americas**

One Penn Plaza  
Suite 1600  
New York, NY 10119  
Tel +1 212 613 1220  
Fax +1 212 563 7279

##### **Asia\***

6 Temasek Boulevard, #26-01/ 05  
Suntec Tower Four  
Singapore 038986  
Tel +65 6322 6688  
Fax +65 6323 7933

##### **Australia**

121-127 Harrington Street  
The Rocks, NSW 2000  
Australia  
Tel +61 (0) 2 8249 5000  
Fax +61 (0) 2 8249 5369

##### **Europe**

Dimension Data House  
Building 2, Waterfront Business Park  
Fleet Road, Fleet  
Hampshire GU51 3QT  
United Kingdom  
Tel +44(0)1252 779000  
Fax +44(0)1252 779010

##### **Middle East & Africa**

The Campus  
57 Sloane Street  
Bryanston Sandton, 2191  
South Africa  
Tel +27 (0)11 575 0000  
Fax +27 (0)11 576 0000

\*trading as Datacraft Asia Ltd

[www.dimensiondata.com](http://www.dimensiondata.com)