



# WINNING THE INFORMATION SECURITY COMPLIANCE BATTLE

**Toby Scott-Jackson, Head of Compliance Services, at SureCloud Limited, gives his tips on how to achieve GCSx CoCo and PCI DSS compliance**

**A LARGE NUMBER OF LOCAL AUTHORITIES** have been placed in the unenviable position of having to comply with multiple security standards; two of which have been imposed by external bodies, namely the PCI SSC and Government Connects. What's more neither standard represents a small undertaking, and consequently IT management must carefully manage constraints along the dimensions of resource, budget and time. However, on the plus side it's important to recognise that these standards do improve organisational security – to date we are not aware of a breach to a PCI DSS compliant organisation; in all cases of breaches known to us, the compromised organisation was deemed to be non compliant at the time of the breach.

Organisations that endorse these standards will undoubtedly be more secure – the trick is to effectively manage the constraints mentioned above. There will always be an element of overlap between PCI DSS and GCSx CoCo, although this will vary from one organisation to the next. For example both require some form of gap analysis, a network schematic, penetration testing and vulnerability scanning – so you have the opportunity to avoid duplication of effort if you plan carefully. In addition, each standard is open to an element of interpretation, which can lead to the potential for confusion and in some cases, incorrect choices. For example CoCo requires an organisation to minimise service obfuscation, but doesn't state what measures need to be taken nor to what degree – so seeking advice early can avoid costly mistakes.

**A METHODOICAL APPROACH**

In our experience the most effective way of achieving compliance is to adopt a methodical approach. For example, we take a pragmatic workshop based approach, which allows us to engage key stake holders, assess the current situation, and provide an action plan to achieve compliance, in a very short period of time. Our approach broadly covers the following:

- Current Situation Assessment, facilitated by a security and networking expert, ensuring that the standards are fully understood. This requires a detailed understanding of each control and the test required to determine its compliance status; PCI 1.2 (issued Oct 2008) is much clearer regarding these control tests, so it is worth re-visiting the standard if you haven't already done so
- Security Test your systems and processes, to

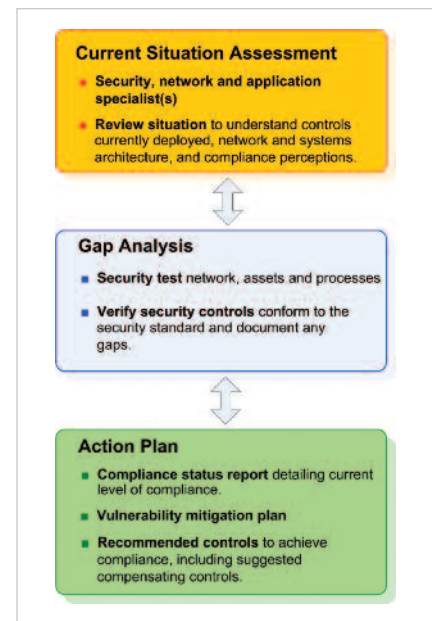
determine the gap between the existing environment and the standard. The most economic way to achieve this is to get your security testing provider to perform this as part of the broader vulnerability assessment – this will also give you a tick in the box, as both standards require annual penetration testing (IT Health Checks). However, it is essential that your chosen test provider understands: a.) the necessary tests to verify each control against the standard; and b) the test scope associated with the standard – for example, CoCo security assessments are very broad ranging from physical security (such as locks on doors) through to server and service configuration. It's also important to recognise that contact with the PCI SSC and Government Connects representatives can be difficult and many documents must be referenced if the controls are to be fully understood – so taking into account the time constraints, particularly with CoCo, it is vital that you enlist the services of a provider who is registered with the relevant body and has successfully helped organisations achieve compliance status.

- Produce an Action Plan, clearly stating areas of compliance and non-compliance. For non-compliance detail the technologies and processes to be implemented and any compensating controls that can be submitted for you to achieve compliance.

**POINTS OF INTEREST**

During my engagements assisting organisations with their compliance needs, a number of issues have garnered more interest than others. The remainder of this article will focus on some of these items – I hope you will find the insight and suggestions helpful:

- Network segregation can provide an effective approach to compliance scope reduction – for example the cost of providing GCSx connectivity to a remote office may significantly outweigh any benefit, so it is quite justifiable to restrict access.
- Patching systems to the latest update will lead to a more secure environment, but can result in disruption to services, so carefully consider the trade-offs when implementing patching procedures particularly where critical systems are concerned – mirroring devices/services to be patched for testing can help identify compatibility issues.
- Legacy systems that are no longer supported by the manufacturer will not comply, so



analyse their function and replace with a different method of achieving the same goal.

- Mobile workers will require two factor authentication, which can be a very costly technology. One method of avoiding these costs is to fully isolate mobile workers from GCSx network segments or fully isolate the GCSx connection from the entire network. Finally, here are three often overlooked issues that may lead to PCI DSS non compliance:

- VoIP systems transmit credit card information in digital format – this information can be captured using ARP Spoofing or other man-in-the-middle techniques – so ensure RTP traffic is encrypted (SRTP) when transmitted and encrypted when stored (with voice recorders).
- Staff may record credit card information on paper, due to system deficiencies (such as speed or ease of access) – ensure policies and staff education prevent this.
- The practice of repeating credit card information out loud, particularly in quiet open plan offices, means information can potentially be passed on to unattended recipients – again policies and procedures should be implemented to avoid this.

**FOR MORE INFORMATION**

**Tel: +44 (0)1189 637999**  
**E-mail: [gt@surecloud.com](mailto:gt@surecloud.com)**  
**Web: [www.surecloud.com/gt](http://www.surecloud.com/gt)**