Security Assessment from CWSI

In the mobile world, mobile app updates, new apps, data roaming and VPN technologies are needed every day to be "mobile first". We understand the inherent risks that mobile technology can bring and how a threat or data breach can adversely affect your reputation. Mobile security issues do occur. There have been many examples of this recently in the news, throughout the world, with devastating consequences.

Improving regulatory standards arriving in 2018 such as the **European General Data Protection Regulation** (GDPR), **Directive on Security of Network and Information Systems** (NIS Directive), and **Markets in Financial Instruments Directive** (MIFID II) will all drive organisations to improve data protection, information security, and privacy standards. This is all good news in the long term as it will massively improve standards on how data is handled, secured and processed as well as helping protect critical infrastructure from external and internal threats. However, there is a lot of work involved in getting there across all levels of organisations.

CWSI Security Assessment leverages our experienced in-house security expertise in enterprise mobile security to help organisations ensure that the security controls for mobile devices meet the organisations requirements.

We will work with you to ensure your relevant security requirements for enterprise mobility are captured and prioritised. We will then use them to evaluate your existing capabilities and provide you with the intelligence required to help protect your business.

To find out more

For more information on arranging a Security Assessment from CWSI for your organisation, please contact your account manager or call us on:
+353 (0)1 293 2500 or visit **www.cwsi.ie**
+44 (0) 2036 515 392 or visit **www.cwsi.co.uk**

Examples of what CWSI Security Assessment will review

- Security controls related to mobile
  - Internal Audit
  - External compliance standards – ISO, PCI

- Enterprise Mobile Management tool:
  - AirWatch
  - MobileIron
  - Blackberry/Good
  - Microsoft InTune
  - MaaS360

- Any related EMM technologies for example App Risk or malware scanners

Typical Engagement process

1 **Customer engagement and preparation**
CWSI will work with your organisation to identify the relevant stakeholders responsible or who should have input to the security requirements and set a date for the workshop in stage two.

2 **Security Assessment Workshop**
Workshop Day 1
Elicit client's security requirements including any relevant compliance standards that may apply (PCI, ISO27001)

Workshop Day 2
EMM technology review and mapping of security requirements from Day 1 to technical controls. Recommendations will take into account change control requirements such as User impact, testing and rollback.

In the event that no technical controls can be implemented to manage or mitigate a specific risk or security requirement CWSI will call this out and suggest a suitable procedural or "soft" control based on our experience in similar engagements and industry best practice.

Pricing Model

The CWSI Security Assessment is typically a fixed price consultancy engagement. We charge €3000/£3000 for a standard engagement. For very large programmes where it may not be possible to complete the engagement within two workshop days we will work with the client to scope a suitable pricing model.

To find out more

For more information on arranging a Security Assessment from CWSI for your organisation, please contact your account manager or call us on:
+353 (0)1 293 2500 or visit **www.cwsi.ie**
+44 (0) 2036 515 392 or visit **www.cwsi.co.uk**

Why CWSI?

CWSI have vast experience in the Enterprise Mobility space. This is literally all that we do and is the core of our value proposition. Through our vast direct experience with leading vendors, as well as our deep knowledge of the core fundamentals of mobile technologies, mobile use cases, and mobile security we have developed a number of advisory products to assist organisations with the challenges of developing and maintaining Enterprise Mobility programmes.