

## ***REDUCE TECHNOLOGY RELATED RISK WITH PRE-RISK VULNERABILITY ASSESSMENTS FROM ASM***

Reduce technology related risk with Pre-Risk Vulnerability Assessments from ASM

In the current economic climate organizations must make difficult decisions regarding how to develop their businesses whilst also reducing the risk of doing business in an interconnected and online world. This has meant that technology related risks are evolving as quickly as the business models of the companies at the forefront of these changes.

The problem; There are business risks associated with storing and processing corporate and customer data which could cause damage to the reputation of your organization. Can you rely on the effectiveness of your IT Security controls if the effectiveness of these measures have not been validated and are you in a position to adequately protect and manage against potential threats?

Particularly where new technologies are involved such as Cloud services and “Bring Your Own Device” (BYOD) the real risk to your business may not be apparent to your stakeholders.

Key questions to be asking are “what is our risk appetite?” and “can we safely accept these risks?”

These questions highlight how many companies make decisions regarding risk management without fully understanding their risk profile and actual exposure or what sensitive information they need to protect to what degree.

Is your level of protection adequate for the nature of data that you are protecting? Will improving certain security measures reduce your real exposure? This is where the Pre-Risk vulnerability assessment is designed to provide these answers. This will arm you with the knowledge to decide whether your controls are adequate, and whether improvements in specific areas will reduce your exposure to acceptable levels.

We can provide tailored security assessments of your IT Security posture prior to you binding the risk. We will provide you with a clear and concise report of cyber exposure based on IT Security Management standards such as ISO27001 ensuring that your business fully understands the potential outcomes if the exposure is not treated. Our industry leading experts are leaders in their field utilizing commercial and open source software to provide fully exhaustive security assessments, as well as moving beyond one dimensional testing towards the Data-centric view of IT Security that is required to protect against modern threats such as Cyber Espionage.

Our industry leading experts are the best in their field utilizing customized open source software to provide fully exhaustive security assessments. Understanding cyber-crime risk modelling is paramount, let us help you to gain a competitive advantage through improved risk management.

Our standard services are offered in three levels of engagement:

## **Bronze**

At bronze standard we provide you or your client with the tools required to perform a self-assessment of your cyber security stance. This encompasses a questionnaire style approach.

One of our assessors will visit your staff or your client and walk them through filling in the questionnaire the first time. After this you will continue to self-assess at a period suggested by our CERT (Cyber Security Emergency Response Team).

At periods agreed between you and the CERT you will be audited and assessed to provide a management level report about the effectiveness of your current solution. The audit will involve spot checks of criteria specified as "required" in the self-assessment report.

## **Silver**

The ASM Silver cyber security service includes all the benefits of the Bronze service plus...

At silver standard you will be initially assessed with a full external penetration test. After the publication of a report there will be second penetration test this time from the inside. This event may be coupled with an internal training event for your IT staff in cyber defense and awareness. A ASM consultant will assess the effectiveness of your Cyber Security Policy document including your corporate user acceptable use policy.

The ASM CERT will perform 2 subsequent external penetration tests and audits with the intention of assessing the gap between the policy and the reality.

The ASM emergency response team is constantly on call and available to support you in case of a cyber-security event. 3 calls are included in the service. Others are chargeable.

## **Gold**

The ASM Gold cyber security service includes all aspects of the Silver service plus...

At Gold standard ASM becomes your Cyber Security partner. We will help you refine and or create your enterprise wide security policy. Penetration tests will be provided and performed as directed in consultation with the ASM head of emergency response team.

The ASM consultants will assist you in implementing a continuous improvement model for your cyber protection of all your assets on a cradle to grave basis.

The ASM CERT is at your disposal for an agreed number of calls and responses.

The ASM emergency response team is constantly on call and available to support you in case of a cyber-security event. 2 calls are included in the Gold service.