KAON SecurITy

IT Security Services

OUR BACKGROUND

Kaon SecurITy specialise in the human factors side of information security and provide services to Local Government, Central Government and commercial enterprises in New Zealand and Australia.

Kaon SecurITy is acknowledged for its regional leadership in IT Policy deployment and technical security auditing services. Its SecurITy IT Policy System is used by more than 100 organisations worldwide.

Established in 2004, Kaon SecurITy is the professional services division of MPA New Zealand Ltd.

TECHNICAL SECURITY AUDIT

Security threats can manifest in a variety of ways involving human and non-human intervention. A typical security audit involves an in-depth examination of servers, network components, the physical environment, operational procedures and an intrusion test.

The Kaon SecurITy audit process is a hands-on test of how your systems operate and how they are being managed. The level of protection is assessed against the amount of risk to the organisation. Procedures, overall management and other mitigating factors are also scrutinised to establish that these are effectively being implemented. A comprehensive report is produced for the client highlighting the major areas of concern.

Risk management is becoming a big issue for large organisations and the Government sector. Auditing completes the compliance loop by highlighting the areas where you are most at risk. In some cases you may already have policies that mitigate the risks, but are not complying with them and in other cases you may need to develop policy, procedures, processes and controls to ensure that gaps are closed for the future. Audits can be customised to target specific areas of concern should a client suspect that anomalies exist within their IT environment.

All technical security audit work is scheduled following agreement with the client and is carried out on the basis of a fixed-price quote; generally this involves two days on site. A full report is provided detailing vulnerabilities observed and offering recommendations for remediation.

POLICY COMPLIANCE AUDIT

Implementing policy is the first step on the road to information security maturity. From that first step the development of procedures, processes and controls provide the means of ensuring that policy is being complied with.

A Kaon SecurITy IT Policy Compliance Audit is a comprehensive review of how well your organisation is complying with your own documented policies and provides the organisation with an assurance that policy is being effectively implemented, that the appropriate procedures, processes and controls are in place; and that these are operational.

This audit also provides a base for those organisations seeking an ISO27001 or PCIDSS assessment from a qualified assessor at a later date and allows the organisation to take remedial action prior to their formal assessment.

An assessment report is provided detailing policy compliance and making recommendations for remedial action. Where ISO27001 or PCIDSS assessment is being sought a summary of compliance to those standards will also be provided. A Policy Compliance Audit is an extensive engagement and is quoted based on the organisation's specific requirements.

WEBSITE VULNERABILITY TESTING

Websites are developed with a variety of purposes in mind and this is reflected in the complexity of the design, but should the website be compromised the effects may not only damage the reputation of the organisation but may affect sales, loss of customers, legal actions and even reparation. If the website seems to function well or even good-enough, it is not easy to tell if the code has been written well or is substandard. But how well your website has been developed will have a huge impact on how easy it is to gain unauthorised access to the site.

Kaon SecurITy has the tools and the expertise to provide an independent assessment of websites in order to determine vulnerabilities and weaknesses. Clients receive a comprehensive report and test results, highlighting areas susceptible to attack and offering guidance on how to remediate the vulnerabilities.

During the vulnerability testing process we perform a thorough investigation of the site, exploring it for coding and installation vulnerabilities that may be present as a result of default installation or introduced during the development process.

BUSINESS CONTINUITY – DISASTER RECOVERY

Business Continuity (BC) and Disaster Recover (DR) – businesses are dependent on technology to function properly and to conduct trade or provide service. However, if the technology you rely on is disabled or destroyed due to an unforeseen disastrous event e.g cyber attack, fire, flood, power outage - what plans have you got in place to ensure you have full Disaster Recovery and Business Continuity?

The same applies for your people, processes, environment and market which can also be impacted due to an unforeseen event.

Consider some of the following examples.

In the event of a disaster -

- What would be your organisational priorities?
- What key risks do you need to consider?
- Does your organisation have an emergency recovery process?
- The technology continuity plan is?
- Roles and responsibilities are?
- What is the communication plan?

Kaon SecurITy can help your organisation develop BC and DR plans and documentation - or can review your existing plans to ensure they are current and will be effective if put into practice.

vCISO

Increasingly company boards and senior executives need to have cyber security on their agenda and integrated into their existing risk management programmes. The role of Chief Information Security Officer (CISO) is key to making sure that the crown jewels of an organisation are adequately protected and that the executive team identify and address the risks associated with the mission critical information and technology assets that form the foundation of their business units. Many organisations do not need to have the CISO function on a full time permanent basis and they do not have the ability to identify and recruit a person with the relevant experience to perform this role.

The Kaon Security professional services team includes personnel that have the seniority and business understanding to provide this expertise and fulfil the CISO role on a part time basis for commercial and public sector organisations. Balancing risk exposure versus investment in security improvement is a challenge that all boards face and so being able to draw upon external expertise to weigh up and strike the right balance is essential.

vITSM

Our vITSM Service addresses the growing demand for experienced IT Security Managers that can provide expertise to organisations to ensure they are managing security controls effectively to drive operational improvements that reduce security incident risks. This requires IT security experience across many domains including mobile, desktop, server and network infrastructure. Kaon Security can provide this expertise on a project by project basis or on contract for a fixed term.

MPA New Zealand Ltd, Level 1, 4 Waipuna Road, Po Box 62049, Mt Wellington, Auckland 1644, New Zealand
t. NZ +64 9 570 2233 | t. VIC +61 3 9913 3248 | t. QLD +61 7 3194 3664 | t. NSW +61 2 9098 8206 | f. +64 9 570 2355 | e. sales@kaonsecurity.co.nz