QUANN CONSULT

QUANN COMPLIANCE AND RISK ASSESSMENT

Crystallize and manage risk by assessing your security controls against best practices and standards

Today, the proliferation of channels ranging from web and mobile to social media provides us with new and exciting ways to engage with customers and presents new opportunities for business development. However, concerns over intellectual property protection, data privacy and regulatory compliance remain a major stumbling block. At the same time, hidden security gaps can expose an organisation to data and regulatory breaches, resulting in operational, reputational and financial damage.

QUANN COMPLIANCE AND RISK ASSESSMENT

QUANN Compliance and Risk Assessment services help organisations to crystallise and manage risk by making it visible through a combination of expertise, processes, methodologies and unique toolsets. Our IT consultants will evaluate your security controls against best practices and recognised security frameworks to determine how effectively those controls protect your organisation from cyberattacks and provide clear guidance and recommendations for improvement.

The journey towards compliance

- Carry out an in-depth evaluation of your business environment to identify weaknesses and vulnerabilities.

- Review security management controls including policies and compliance measures.

- Scan for security risks, and identify and prioritise them to help reduce exposure.

- Establish key risk and compliance metrics, implement continuous and consistent security management processes, and put in place effective security practices.

RISK ASSESSMENT SERVICES

ERP Assessment

- Proven methodologies and sophisticated Assure™ tools are used to help organisations assess the security of Enterprise Resource Planning (ERP) systems such as SAP and Oracle.

- Minimises risks such as data leakage, employee abuse and fraud without having to employ in-house audit or compliance professionals with ERP-specific knowledge.

ISMS Assessment

- Our independent Information Security Management System (ISMS) Assessment helps organisations analyse the efficiency and effectiveness of their information security and IT risk management.

- The assessment is carried out against international certification standards such as ISO 27001, the ISF Standard of Good Practice for Information Security, and NIST SP 800-53.

Application Controls Review

- An Application Controls Review provides a cost-effective way to enhance the security of applications before they are deployed into the production environment.

- It includes the evaluation of project management practices, design of control structures and security requirements, and audit of system interfaces and general controls.

Configuration Review

- Access controls, privilege levels and other significant variables in server and network device configuration are analysed and compared against established guidelines such as the Centre for Internet Security (CIS) Benchmarks and the product vendor's security best practices.

- This enables organisations to identify and correct oversights and missteps, which could be exploited by threat agents.

Security Posture Assessment

- A Security Posture Assessment provides organisations with a clearer picture of their risks and security vulnerabilities.

- It includes vulnerability scanning, penetration testing, configuration reviews and security audits using various international standards.

Cloud/Virtualisation Assessment

- We analyse the security of an organisation's cloud system from two perspectives. The external perspective involves vulnerability assessment and penetration testing against external-facing applications and services.

- The internal perspective covers both governance (such as compliance with internal security policies and data security) and the operational domains (such as remote administration and virtualisation security).

Wireless Assessment

- Various wireless assessment and penetration tools and techniques are used to measure vulnerabilities and exposure.

- The service includes mapping out the wireless access points, identifying rogue access, reviewing the wireless configuration and analysing the security of various devices and hosts connected to the network.

Social Engineering Assessment

- Cybercriminals are targeting contractors or employees with privileged access by using social engineering techniques to gain their trust.

- They harvest personal and organisational data on the public Internet to engineer these attacks.

- Our Social Engineering Assessment service helps organisations to address this by evaluating the risks, increasing employee awareness and strengthening technical measures such as identity management and authentication.

COMPLIANCE ASSESSMENT SERVICES

We provide independent assessment of the security controls implemented across your organisation against industry standards and regulatory requirements such as:

(a) **The Payment Card Industry Data Security Standard (PCI DSS)**, a proprietary information security standard for organisations handling credit cards,

(b) **The Internet Banking Technology Risk Management (IBTRM)** guidelines published by the Monetary Authority of Singapore,

(c) **The International Standards Organisation (ISO) 27001 standard** which provides a framework of policies and procedures for information risk management, and

(d) **The Instruction Manual 8 - Data Management (IM8F)** which provides the data protection policy framework for the Singapore public sector.

BENEFITS

Quann uses cyber threat intelligence to provide predictive, continuous and responsive protection to enterprises and governments worldwide.

established standards to assess the risk exposure and possible implications such as reputational damage and direct loss.

Provides an in-depth understanding of your organisation's risk profile

Our certified consultants and research teams will provide you with a thorough assessment of your security posture. We adopt a business-driven approach and measure risk and compliance against

Ensures that security is aligned with your business needs and best practices

We provide recommendations for effective security practices that are aligned with your business needs. We will also help ensure that your risk management approach meets compliance requirements and standards for your industry.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE