

## CorreLog for King III Compliance

The King Code of Governance Principles (King III), effective March 1st, 2010, applies to all South African companies and entities. The principles contained in the King III Report promote effective governance within commercial (and other) institutions. *Failure to meet a recognised standard of governance may render a director or executive management member legally liable!*

In 1992 the King Committee was established with the specific aim of researching and making recommendations about corporate governance in South Africa. The first and second reports of this committee, published in 1994 and 2002, made specific and general recommendations dealing with corporate governance, and encouraging a series of “good practices” to promote responsible management.

Unlike previous reports, King III deals with IT governance in detail for the first time. According to the introduction of the report, “Information systems have now become pervasive in the sense that they are built into the strategy of the business. The risks involved in information technology (IT) governance have become significant”.

### **Question: What Does King III Require of IT Departments?**

Answer: King III, among its other provisions, asks entities to maintain audit logs and practice good security procedures for their enterprises. The board should ensure that an IT internal control framework is adopted and implemented, supporting good governance. The board should receive independent assurance on the effectiveness of the IT internal controls, and ensure that an IT security strategy is integrated with the company.

## King III Objectives for Information Technology

The King III report details specific goals that are to be met by South African IT departments, as of March 2010. The precepts of these goals are enumerated in various sections. Pertinent references to IT management are:

### **Section 5.1**

The board should ensure that an IT charter and policies are established and implemented, and should ensure promotion of an ethical IT culture and awareness. The board should ensure that an IT internal control framework is adopted and implemented, and should receive independent assurance of the effectiveness of the IT internal controls.

### **Section 5.2**

The IT infrastructure should be aligned with the performance and sustainability objectives of the company. The board should ensure that the IT strategy is integrated with the company's strategic and business processes.

### **Section 5.3**

The board should delegate to management the responsibility for the implementation of an IT governance framework. Management should be responsible for the implementation of the structure, processes and mechanism for the IT governance framework.

### **Section 5.4**

The board should monitor and evaluate significant IT investments and expenditures, should oversee the value delivery of IT and monitor the return on investment from significant IT projects. The board should ensure that private data in information systems are protected, and should obtain independent assurance on the IT governance and controls.

### **Section 5.5**

The IT management should form an integral part of the company's risk management. Management should regularly demonstrate to the board that the company has adequate business arrangements in place for disaster recovery. The board should ensure that the company complies with IT laws, standards and common practices.

### **Section 5.6**

The board should ensure that there are systems in place for the management of information, which should include information security, information privacy. The board should ensure that all personal information is treated by the company as an important business asset and is identified. The board should ensure that an Information Security Management system is developed and implemented.

### **Section 5.7**

A risk committee and audit committee should assist the board in carrying IT responsibility. The risk committee should ensure that IT risks are adequately addressed. The audit committee should consider the use of technology to improve audit coverage and efficiency.



## CorreLog Support for King III Requirements

### Question: How Does CorreLog Help Achieve King III Compliance?

Answer: CorreLog maintains security and audit controls for the enterprise by logging pertinent system activity. This establishes compliance to various security regulations, as well as creating demonstrable evidence to comply with the specific goals of King III.

#### **Establishment of IT Framework And Strategy**

CorreLog supports the objectives of Section 5.1 through 5.3 by providing an open, extensible, and standards based IT framework that leverages the existing framework elements of an enterprise. CorreLog does not impose proprietary methods on an organisation. CorreLog creates an open system that can be easily understood in the context of ISO (and other) standards. *CorreLog provides a highly interoperable framework that ensures long life cycle, flexibility, scalability, and functionality.*

#### **Establishment of Business Audit Trails**

CorreLog supports the objectives of Section 5.4 by establishing a method of independent verification of an organisation's governance (through the creation and maintenance of comprehensive logging of significant activities on the network.) This permits an entity to demonstrate its proactive compliance with the King III objectives. *This also provides a useful and comprehensive audit trail of management and worker activity.*

#### **Establishment of Security and Risk Management**

CorreLog supports the objectives of Section 5.5 through 5.7 by employing sophisticated security correlation rules that track user activity and system security. CorreLog detects attacks on the network, and furnishes real-time notifications of potential security threats and breaches. *In particular, CorreLog Security Correlation Server fully implements the requirements of King III, Section 5.6.1.*

#### **Demonstration of Good Return on Investment**

CorreLog supports the objectives of Sections 5.4 and 5.7, through its ease of deployment. CorreLog relies on the passive monitoring of log data within the enterprise, tapping into existing data stores to record and analyse the behavior of the network. *The CorreLog system provides a fast return on investment for entities by reducing installation effort and learning times.*

### CorreLog King III Highlights:

- ❖ Demonstrate compliance to the King III goals, and reinforce your good governance policies.
- ❖ Track user access; provide a history of governance suitable for investigation and auditing.
- ❖ Monitor system security, including servers, routers, and firewalls, in compliance with King III, Section 5.6.1
- ❖ Easy to deploy, scale and adapt. CorreLog reduces King III compliancy costs.



## CorreLog: Security Correlation Server

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.

CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog provides auditing and forensic capabilities for organisations concerned with meeting requirements set forth by King III and others.

*You can begin demonstrating immediate compliance to the King III objectives and goals through one simple download and installation. Visit our website for more information!*

## CorreLog, Inc.

<http://www.correlog.com>

Copyright © 2010