January 2009

Governance IT Compliance Framework

A general introduction to Governance, Risk and Compliance in the context of the Governance IT compliant eMail Archiving Service

Key points

- **What is governance, risk and compliance?**
- **The benefits of compliance**
- **GRC in the context of Governance IT**

eCommunication Facts

21% of employee e-mail subpoenaed by courts & regulators.

13% of companies have battled lawsuits triggered by employee e-mail.

65% of companies lack e -mail retention policies.

94% of companies fail to retain & archive IM.

46% of companies offer employees NO e-mail policy training.

50% of workplace IM users send/receive in risky content including attachments, jokes, gossip, confidential info, porn.

Source: 2004 Workplace E-Mail and IM Survey from American Management Association

A Governance, Risk and Compliance framework for electronic communications

While the need for governance has always existed, corporate governance and particularly risk management has been given centre stage as a consequence of a number of high profile business collapses such as Enron, Arthur Andersen and WorldCom. Tightening economic prospects, both at a national and international level, will only raise the bar for good governance for companies of all sizes both in respect to customers and shareholders.

As a result, there is greater pressure from investors, stakeholders and the public for further transparency of financial reporting and internal controls, together with the broadening of directors' responsibilities to safeguard their interests in terms of ensuring that financial controls and systems are robust and defensible.

It is becoming common knowledge that national legislation and international standards such as Sarbanes-Oxley, Basel II, and requirements of the FSA in the financial sector, have made directors liable if they fail to ensure that accountable risk management frameworks are established and maintained in their organizations.

What is less understood is what is meant in practical terms by a risk management framework and how this relates to companies of all sizes. Furthermore how this should be addressed in a world where electronic communications is the de facto form of communication, knows no borders, easily accessible and where few – if any – controls are practiced.

This document looks at the critical role of how standards - such as ISO 27001 - can help form part of an organization's risk and compliance framework, to help towards providing and managing the operational risk profile of the organization and thereby contributing to an overall structure of corporate governance.

Corporate governance has taken centre stage in the management forum, and consequentially it has become a marketing factor for many organizations facing prospective clients and business partners.

Governance, Risk and Compliance as a service

Organizations wishing to manage information security and risk, require an organization to implement an information security management system (ISMS) - which is exactly why we chose the ISO 27001 framework.

The ISMS should include risk assessment, risk management, audit compliance and a management framework to ensure that true business benefits are realized from implementing ISO 27001, and the infrastructure to ensure its maintenance going forward.

The central design point for our ISMS services has therefore been to ameliorate the arduous task of defining a comprehensive and certifiable set of policies and procedures, hard-wire these in to a combined hardware, software and services offering.

Implementing the Governance IT services offering is therefore simply a matter of setting the baseline of company users. Cont. Pg. 2.

ISO271001—The Governance IT Compliance Back-bone

The primary goal of ISO 27001 within a corporate governance context is, via asset identification, valuation, business impact assessment and risk assessment to develop an intimate knowledge of the business activity under examination.

Without this risk identification and risk assessment there is a danger of being ill-informed and undiscovered risk 'blind spots'.

ISO 27001 is far broader than just IT: it encompasses an entire business function and its' supporting back office processes. It spans and affects every part of the organization (and those of trusted third parties) and can add to or subtract from an organization's bottom line. It can improve the way an entire department is operated, provide reassurance to senior managers, internal customers and external clients; put simply, it provides the assurance to stakeholders or shareholders that controls mandated under an organization's contractual, legislative and regulatory requirements are met.

ISO 27001 is the new "benchmark' for Information Security Management. It requires an organization to establish a risk management framework that can enable an organization to manage, review and improve the overall health of information security and risk under one management system or "information security management system" (ISMS).

Whatever your business requirement to demonstrate and manage information security and corporate governance, it all originates from one simple principle - good and effective risk management. .

It is for these reasons that the Governance IT Archiving services is based on and delivers on the promises of the ISO 27001 standard.

> **"In my experience … companies only do what is absolutely necessary and hope that the rest will not fall apart"**
>
> **Van Hauser of The Hacker's Choice - Heard on BBC World Service**

What are the Information Security Imperatives

An improved understanding of information and other assets, and of business processes themselves, across the organisation

Real tangible evidence of cost reduction through better risk management and reduction of impact caused by exploitation of threats

Better cost/benefit analysis to ensure return on investment when taking decisions on going forward with business initiatives

An easier process of monitoring the effectiveness of the ISMS (e.g. less labour intensive, for example, if using tools, and provides a means of self check.

Proactive measuring tools can prevent problems arising at a later date (e.g. network bottlenecks, disk clutter, development of poor human practices)

Reduction of security incidents and better understanding of their root causes

Greater staff security awareness, motivating staff to support when senior management set security and risk management targets

Tangible evidence to auditors, and assurance to senior management that you are in control.

Governance, Risk and Compliance as a service—continued

- An ISO 27001 certificated ISMS based solution will provide an important foundation for any overall certification process the company choose to implement.
- The Governance IT certified policies and processes tells existing and potential customers, as well as regulators, that you have defined and put in place effective information security processes, thereby helping to create a trusting relationship
- A pre-tailored ISO 27001 certification will cost a fraction of a full audit and demonstrates the existence of a best-practice based information security infrastructure
- The certification process also helps the organization focus on continuously improving its information security processes
- ISO 27001 can be easily mapped and contribute towards an ITIL environment and COBIT effective IT control framework, thus provide transparency of services and greater management.
- ISO 27001 is also an effective response to information risks identified in any COSO-type enterprise risk management framework.

The Information Systems Audit and Control Association (www.isaca.org) has reported that a number of recently issued documents are the result of continuing efforts to define, assess, report on, and improve internal control.

What are the challenges to corporate good governance?

The United Kingdom has in many ways acted as a leading exponent of governance, risk and compliance within the European context. Revised Turnbull Guidelines on Internal Control Oct 2005 requires UK listed companies and organizations to establish a security management framework, which is similar to the definition of an Information Security Management System (ISMS) defined within ISO/IEC 27001:2005 (“ISO 27001”).

This Standard discusses and mandates risk assessment and risk management, and requires organizations to ensure they can demonstrate the relationship between controls implemented to mitigate or reduce risks, and how they must manage and accept risks.

This means that:

- The corporate governance framework should be developed with a view to its impact on overall economic performance, market integrity and the incentives it creates for market participants and the promotion of transparent and efficient markets

- The legal and regulatory requirements that affect corporate governance practices in a jurisdiction should be consistent with the rule of law, transparent and enforceable

- The division of responsibilities among different authorities in a jurisdiction should be clearly articulated and ensure that the public interest is served

- Supervisory, regulatory and enforcement authorities should have the authority, integrity and resources to fulfil their duties in a professional and objective manner.

Source: OECD Principles of Corporate Governance 2004

IBM Data Governance Best Practices

According to findings by the IBM Data Governance Council, the top governance challenges today are:

• Inconsistent data governance, which can cause a disconnect between business goals and IT programs.

• Governance policies are not linked to structured requirements gathering and reporting.

• Risks are not addressed from a lifecycle perspective with common data repositories, policies, standards and calculation processes.

• Metadata and business glossaries are not used to bridge semantic differences in global enterprises.

• Few technologies exist today to assess data asset values that link security, privacy and compliance.

• Controls and architecture are deployed before long-term consequences are modelled.

In the general context of Compliance Frameworks

In the context of good governance it is important to recognize other existing supporting management frameworks that currently support corporate governance.

Control Objectives for Information and related Technology (COBIT) can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by IT governance to generically suit every organization.

COBIT adapted its definition of control from COSO, i.e. the policies, procedures, practices, and organizational structures should be designed to provide reasonable assurance that business objectives will be achieved; and that undesired events will be prevented or detected and corrected.

There is also a need for detailed, standardized processes. Specific practices and standards, such as ITIL and ISO 27001 also cover specific areas that can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials. In addition, each of the 34 IT processes and high-level control objectives can be specifically mapped to sections within ISO 27001. COBIT and ISO 27001 can work together as a framework, for providing assurance.

COSO defines internal control as: a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

COSO emphasizes that the internal control system is a tool of, but not a substitute for, management and that controls should be built into, rather than built onto, operating activities. Although it defines internal control as a process, it recommends evaluating the effectiveness of internal control as at point in time, similar to that now found in the Clauses of ISO 27001 - See Clause 4.2.2 - measuring the effectiveness of controls selected.

From this, you can see that COBIT, COSO and SAC allows greater alignment with other supporting standards (i.e. ISO 27001, ISO 9000, ISO 20000, ISO 18000) to help ensure any audit and compliance framework can potentially benefit from managing, and subsequently auditing, one management system.

The introduction of the Sarbanes-Oxley Act also places strict requirements on directors and financial officers to ensure their systems have acceptable controls in place when signing off on accounts (SOX only affects companies if they, or their subsidiaries, are listed on the USA stock market).

Accordingly, Sarbanes-Oxley, COBIT and COSO all provide a similar framework for organizations to meet regulatory requirements. By implementing control procedures using COSO directives, COBIT business and IT governance objectives - corporate governance can be satisfied.

Once these control procedures are functioning correctly, directors and corporate boards will be able to sign off financial reports as required under s302 and s404 of Sarbanes-Oxley Act with the knowledge that they are in compliance.

Governance IT®

Islandsbrygge 43

DK 2300 København

Tel: +45 7026 0350

We deliver…..
Good Governance
Risk Management
Automated Compliance,

Visit our website

www.governance-it.com

Governance IT A/S is a company founded with the goal of delivering a comprehensive and certified Information Management Security System (ISMS) specific to eMails and other eCommunications.

Our service is an IBM Express Advantage Solution which includes IBM hardware, software, content and education—all of which is supported by our service desk.

This is why we are able to deliver Governance, Risk and Compliance as a service.

The Governance IT services provide out of the box policies and procedures for the implementation of a comprehensive Information Management Security System (ISMS) based on the ISO 27001 standard.

If you would like to find out more about how we can help you manage your eMail and reduce risk in your organization, visit our website or contact us directly for a free trial and evaluation.

The Governance IT Compliance Framework

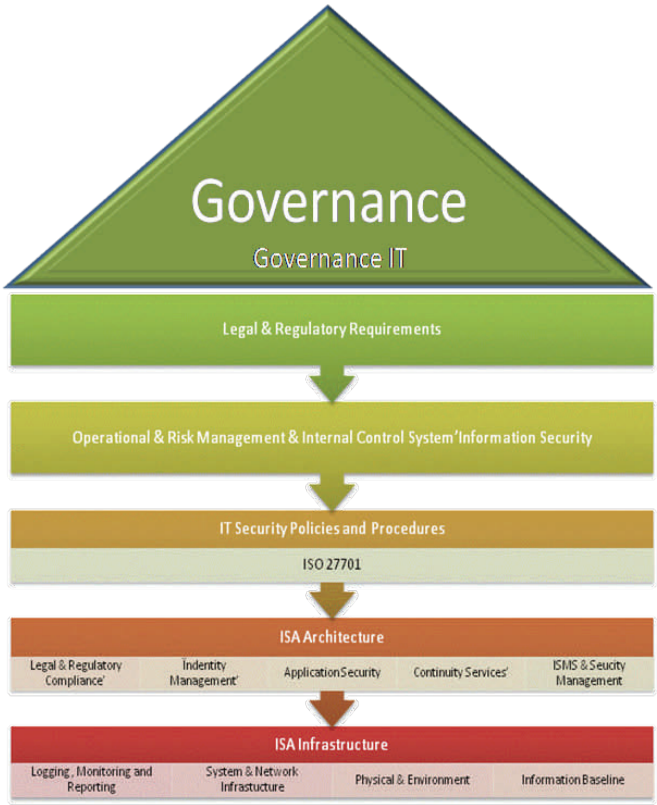
Industry and leading standards bodies, such as the ISACA, International Security Forum, International Standards Organisation and British Standards Institute, are all working to get a grip on the topic of eMail information security.

Using existing management systems to achieve corporate governance and identifying synergies between COSO, COBIT, ISO 20000 (ITIL), ISO 9001, and ISO 27001 are rapidly becoming board room agenda items.

At Governance IT we have created a systematic and holistic framework for implementing an Information Security Management solution – especially targeted at mid-sized to large companies who are looking for good governance assurance but do not have the infrastructure or financial means to implement a traditional solution.

The Governance IT solution takes its' starting point in the context of the issues facing all modern businesses in addressing the benefits and associated issues of eCommunications.

The Governance IT Governance, Risk and Compliance framework is built upon the best practices and management frameworks as defined by COSO, COBIT, ISO 20000 (ITIL), IBM Data Governance Model and ISO 27001.


Governance
Governance IT
Legal & Regulatory Requirements
Operational & Risk Management & Internal Control System'Information Security
IT Security Policies and Procedures
ISO 27701
ISA Architecture
Legal & Regulatory Compliance'
Indentity Management'
Application Security
Continuity Services'
ISMS & Seucity Management
ISA Infrastructure
Logging, Monitoring and Reporting
System & Network Infrastucture
Physical & Environment
Information Baseline

Information Security Assurance (ISA) Model