Information Security Forum

Information security governance

Raising the game

How many of the recent, high-profile data breaches at blue-chip companies could have been prevented with better governance? While corporate governance is common practice, often obligatory, in many aspects of business, governance is not always present in information security. Yet it plays a vital role in reducing risk and speeding response.

When the information security function adopts governance, it raises its game, engaging with senior management and other corporate governance functions. This not only minimises information risk and reputational damage, it also delivers continuing added value from information technology.

New technologies are constantly increasing the complexity of business information, while more sophisticated technology and processes are needed to manage it. Furthermore, that information is simultaneously more critical to the business and more susceptible to attack or abuse.

Information security governance enables the direction and oversight of information security-related activities across an enterprise, as an integrated part of corporate governance. It shows customers, business partners, shareholders and regulators that information is being protected according to industry best practice. It provides the agility to deal with incidents quickly and effectively, and enables better management of all of information security activities – decreasing the chances of headline-grabbing incidents.

The Information Security Forum's step-by-step, practical and comprehensive information security governance framework draws on the experience of ISF Members, new thinking and the ISF's own wide ranging research, reports, tools and workshops. The framework – which is aligned with, and expands on, current standards in the field – allows ISF Members to cut through the waffle and demonstrate how information security delivers value to stakeholders, achieves strategic goals and provides information risk assurance. In addition, the framework highlights the ISF tools and reports available to help Members strengthen the delivery and benefits of information security governance.

Building information security governance into your organisation

The rich library of deliverables produced by the ISF provides its Members with a practical and trusted toolset to raise their game by implementing an effective, relevant and value-adding information security governance framework.

INFORMATION SECURITY GOVERNANCE

A. DELIVER VALUE TO STAKEHOLDERS

A1. Improve effectiveness and efficiency

- ROSI – Return on security investment: Workshop report
- ROSI – Return on security investment tool
- Securing business applications
- Information security incident management: Establishing an information security incident management capability
- Benchmark

A2. Meet stakeholder requirements

- Managing a security function: Diagnostic version 1
- Role of information security in the enterprise: Workshop report
- Security function diagnostic tool

A3. Enable business initiatives

- Architectural responses to the disappearing network boundary
- Securing consumer devices
- Managing access in a changing world
- Threat Horizon (series of reports)

A4. Integrate with enterprise processes

- Risk convergence: Implications for information risk management
- Solving the data privacy puzzle: Achieving compliance
- Cyber citizenship in an enterprise environment

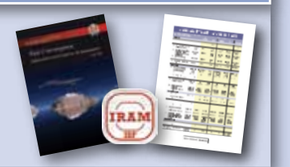
B. ACHIEVE STRATEGIC GOALS

B1. Execute strategic objectives

- Managing a security function: Diagnostic version 1
- Role of information security in the enterprise: Workshop report
- Information security strategy: Workshop report

B2. Set and refine information risk appetite

- Risk convergence: Implications for information risk management
- Information Risk Assessment Methodology (IRAM) (series of reports)
- IRAM: Business Impact Reference Table (BIRT)



B3. Sustain buy-in and commitment

- Protecting information in the end user environment
- Role of information security in the enterprise: Rich picture
- Role of information security in the enterprise: Workshop report

B4. Maintain security requirements

- Guidelines for information security
- Practical approaches to information classification: Workshop report
- The information lifecycle: A new way of looking at information risk

C. PROVIDE INFORMATION RISK ASSURANCE

C1. Oversee assurance programme

- Information security assurance: An overview for implementing an information security assurance programme
- The 2011 Standard of Good Practice for Information Security

C2. Implement risk assessment

- Information Risk Assessment Methodology (IRAM) tool
- IRAM Risk Analyst Workbench (RAW)
- Benchmark
- Device risk and control diagnostic tool
- Security Healthcheck

C3. Ensure compliance

- Monitoring compliance: Workshop report
- Security audit of business applications

C4. Manage supply chain risk

- Information security in third party relationship management
- Securing cloud computing: Addressing the seven deadly sins
- Information security for external suppliers: A common baseline
- External suppliers baseline maturity assessment tool
- Third party security assessment tool

C5. Monitor and report on assurance

- Reporting information risk
- ISF Briefing Paper: Key performance indicators for information security
- Information security metrics: SIG report

The ISF has developed a framework for information security governance which is designed to help you ensure that information security becomes a fully integrated part of your organisation in three key ways: **Delivering stakeholder value** (and not being seen purely as a cost centre); **being aligned to your organisation's overall strategy**; and **providing information risk assurance**.

The diagram above illustrates the information security governance activities that support these three top-line objectives.

Actions

Where next?

The full ***Information Security Governance*** report – available to Members from the Member Exchange (MX) system – provides a detailed overview of information security governance and how it relates to other governance initiatives. It outlines the key components you need to have in place for information security governance, provides pointers to the ISF materials and tools that will help you determine how your current governance framework measures up and check its level of maturity.

It outlines a model for linking management and activities to information security governance objectives and describes the security arrangements you need to have in place for information security governance, including: Information Security Management System, standards, guidelines, control framework, processes and procedures.

In the report, you will also find hints and tips for information security governance implementation and ongoing management and maintenance, including how to get organisational buy-in, run an implementation project, and review, revise and enhance information security governance on a regular basis.

As information security governance is an emerging concept, yet to be fully developed and implemented across most organisations, the report also offers pointers and recommendations for the next version of the ISF Standard of Good Practice and the ISO/IEC 27014 standard, to assist in the further development of information security governance.

About the ISF

Founded in 1989, the Information Security Forum is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in information security and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Contacts

For further information contact:
Steve Durbin
UK Tel: +44 (0)20 7213 1745
US Tel: +1 (347) 767 6772
Fax: +44(0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer