Managing Information Risk the ISF way

To manage risk you need to plan for it – identify, assess, protect

Effective management of information risk has never been as critical as it is today, particularly if organisations are to stay resilient while in pursuit of strategic goals.

The role of cyber and information risk management is a board issue and must be given the same level of attention afforded to operational risk management and other established risk management practices. The insatiable appetite for speed and agility, the growing importance of the full supply chain (upstream and downstream) and the mounting dependence on diverse technologies (such as cloud computing and Bring Your Own (BYOx)) are just some of the challenges organisations are facing today.

Designed to be as straightforward to implement as possible, ISF tools offer organisations an 'out of the box' approach for addressing a wide range of challenges – whether they be strategic, compliance-driven or process-related.

They can be used individually, or together as a suite, to complement an organisation's existing approaches.

This guide presents the ISF's most powerful, business focused Tools, it shows their relationship with the ISF Research Programme and shares some of the key benefits realised by Members who use them.

Using the ISF Tools to Manage Information Risk

The Standard of Good Practice for Information Security

The ISF's ***Standard of Good Practice for Information Security (the Standard)*** is the most comprehensive and current source of information security controls available, enabling organisations to adopt good practice in response to evolving threats and changing business requirements. Updated annually to reflect the latest findings from the ISF's ***Research Programme***, input from our global Member organisations, trends from the ISF ***Benchmark*** and major external developments including new legislation and other requirements, ***the Standard*** is used by many organisations as their primary reference for information security.

Implementing ***the Standard*** helps organisations to:

- increase executive management confidence in implementing a globally accepted approach to managing information security
- provide assurance that applied information security practices have been developed, tested and validated by the world's leading organisations
- be agile and exploit new opportunities – while ensuring that associated information risks are managed to acceptable levels by applying good practice
- respond to rapidly evolving threats, using up-to-date techniques to increase cyber resilience
- establish a more harmonised and streamlined approach to legislative and regulatory compliance activities
- reduce times and costs in developing an Information Security Management System (ISMS) and achieving certification (eg against ISO/IEC 27001).

Information Risk Analysis Methodology (IRAM)

The ISF's ***Information Risk Analysis Methodology (IRAM)*** provides organisations with an easy to use, flexible and thorough approach for analysing business information risk and selecting effective approaches for treating these risks. ***IRAM*** is used by blue-chip companies and public sector organisations across the globe. Complementary materials and tools are available to implement ***IRAM*** including the browser-based multi-user ***Risk Analyst Workbench (RAW)*** and stand-alone spreadsheet based tools for each of the three phases of the methodology.

Implementing ***IRAM*** helps organisations to:

- focus information security resources in areas where it is most needed
- increase the level of trust from customers and organisations
- reduce the frequency and magnitude of incidents
- reduce the time taken to perform information risk analysis
- reduce costs associated with managing information risk
- meet legal and regulatory requirements.

The ISF is currently enhancing ***IRAM*** to move it from its current position as a leading system focussed risk analysis methodology to include more detailed risk treatment and monitoring. The enhanced ***IRAM*** will help organisations: perform business process focussed risk assessments, make more informed decisions about information risk, integrate information risk management into the organisation's broader risk management approach, balance risk with reward and incorporate the organisation's risk appetite into information risk management activities

How the ISF's tools and research help Members manage information risk

Research Programme and ISF Accelerator Tools

The ISF's extensive ***Research Programme***, which is driven by the Members, covers a broad range of essential information security topics. Output from research projects is typically in the form of a report and is often supported by an accelerator tool, such as the ***Supplier Security Evaluation Tool (SSET)***, to help organisations efficiently implement recommendations in the report.

Output from the ***Research Programme*** informs the continuous update and development of the ISF's Tools, including ***the Standard, Benchmark*** and ***IRAM***. In particular, the 2013 release of ***the Standard*** incorporates the key findings and recommendations from the previous 12 months of research reports, including: ***Managing BYOD Risk, Engaging With The Board, Data Privacy in the Cloud, Securing the Supply Chain, You Could Be Next*** and ***The Modern CISO*** briefing paper. These updates will form the basis of changes to the ***Benchmark*** in 2014.

Research projects that are currently underway and that will inform ISF Tools over the next 12 months include: ***Information Security Strategy, Best Practice in Management Reporting and Status/KPIs, Security awareness – instilling a security culture?, Assessing Information Security Maturity as a Driver of Strategy Planning, Threat Horizon 2016, Applying Lean and Agile to Information Security*** and ***Risk Appetite***.

Benchmark

The ISF's ***Benchmark*** is an unrivalled online tool that provides organisations with an in-depth assessment of information security arrangements. Taking part in this confidential initiative allows organisations to compare security performance against similar anonymised organisations around the world, as well as against ***the Standard***, ISO/IEC 27002 and COBIT 5 for Information Security.

Implementing ***Benchmark*** helps organisations to:

- identify areas of control weakness
- drive down information risk
- achieve better implementation of security controls
- reduce the number and impact of major security incidents
- support the business case for information security investment
- target spending where it will provide most benefit
- justify introduction of new security policies, standards and controls
- improve enterprise-wide security awareness.

Organisations are welcome to participate in the ***Benchmark*** at any time, and as often as they wish. The flexibility of the healthcheck template and the detailed questionnaire template enables organisations to assess a variety of environments at a high level, or concentrate on performing deep-dive assessments on specific areas of concern.

"I use the ISF Standard of Good Practice and Benchmark to demonstrate the importance of good information risk management practice to the board"

"IRAM is easy to use... flexible and adaptable"

Action

Where next?

The ISF's Tools present organisations with a way to help manage the associated information risk. They can be used individually, or together as a suite, to complement an organisation's existing approaches.

The ISF's most powerful and popular tools are:

- The ***Standard of Good Practice for Information Security (the Standard)***, includes extensive coverage of topics on security governance, risk management, security assurance, security monitoring and improvement, and supporting material to help engage with executive management, such as the Guidelines for Information Security and the Categories and Topics List.
- The ***Information Risk Analysis Methodology (IRAM)***, includes a three phase process for performing information risk analysis and provides supporting material to help support each phase, such as the ISF Business Impact Reference Table (BIRT), ISF Threat List and reference tables to help determine likelihood and risk ratings.
- The ***Benchmark***, includes the ability to assess the organisation's controls at a high-level or detailed level, provide a powerful reporting dashboard, understand the organisation's approach to information security and technologies such as cloud computing and BYOD (using additional questionnaires), and view results in the Standard, ISO/IEC 27002 and COBIT 5 for Information Security formats.
- The ISF ***Research Programme*** covers a broad range of essential cyber and information security risk management topics, which are often supported by an accelerator tool.

Non-Members can purchase ISF reports by visiting the ISF Store at https//www.securityforum.org/research or by contacting Steve Durbin at steve.durbin@securityforum.org

About the ISF

Founded in 1989, the Information Security Forum (ISF) 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 cyber, information security and risk management by 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 programme. 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.

Contact

For further information contact:
Steve Durbin, Global Vice President
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.