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 today. The insatiable appetite for speed and agility, the growing importance of an organisation’s supply chain, the mounting dependence on technology and the ever-evolving regulatory environment are just some of the challenges organisations are facing today.

Designed to be as straightforward to implement as possible, ISF research and tools offer organisations a ‘think outside the box’ approach for addressing a wide range of challenges – whether they be strategic, compliance-driven or process approaches.

ISF tools can be used individually, or together as a suite, to complement an organisation’s existing approach. This guide presents the ISF’s most powerful, business-focused tools and Research Programme and shares some of the key benefits realised by Members who use them.
Using the ISF’s tools to manage information risk

RESEARCH PROGRAMME

The ISF’s extensive Research Programme, which is driven by the Members, covers a broad range of essential information security topics and includes our annual Threat Horizon series. 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.

Findings from the Research Programme informs the continuous update and development of ISF tools, including the Standard, Benchmark and IRAM2. In particular, the 2016 release of the Standard incorporates the key findings and recommendations from the previous 24 months of research reports, including: Threat Intelligence, Protecting the Crown Jewels, Security Architecture, Preparing for the General Data Protection Regulation and Managing the Insider Threat – briefing paper.

Research projects that are currently underway and that will inform ISF tools over the next 12 months include: Emerging Quantitive Techniques in Information Risk Management, Building Tomorrow’s Security Workforce, Mobile Application Security and Securing Industrial Controls Systems.

THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY

The ISF 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 every two years 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 (e.g. against ISO/IEC 27001: 2013).

“I use the ISF Standard of Good Practice and Benchmark to demonstrate the importance of good information risk management practice to the board”
**ISF BENCHMARK**

The ISF Benchmark is an unrivalled strategic tool that organisations are using to improve their 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, COBIT 5 for Information Security, PCI DSS v3.2, CIS Top 20 CSC and the NIST Cybersecurity Framework.

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.

The Benchmark enables organisations to evaluate their security performance at three different analysis levels ranging from a high-level questionnaire designed to provide an assessment at speed, a modular mid-level questionnaire which provides a fast and simple overview, through to a deep-dive investigative questionnaire that can be tailored to focus on areas of concern.

**INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)**

As information risks and cyber security threats increase, organisations need to move away from reacting to incidents towards predicting and preventing them. The ISF Information Risk Assessment Methodology 2 (IRAM2) is an end-to-end approach to presenting a business-focused view of information risk.

Implementing IRAM2 helps information risk practitioners, as well as other risk, business and technology leaders to:
- apply a simple, practical, yet rigorous approach
- focus on the business perspective
- obtain a greater coverage of risks
- focus on the most significant risks
- speak a common language
- engage with key stakeholders.

IRAM2 is set out in six phases. Each phase details the steps and key activities required to achieve the phase objectives, as well as identifying the key information risk factors and outputs.

This robust yet easy-to-use methodology is supported by four IRAM2 Assistants, each accompanied by a practitioner guide.

“IRAM2 is easy to use... flexible and adaptable”
WHERE NEXT?

The ISF’s research and 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:

- The ISF’s Research Programme covers a broad range of essential cyber and information security risk management topics, which are often supported by an accelerator tool.

- 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 Benchmark, includes the ability to: compare security performance against peers, assess the organisation’s controls at various levels and view results in a series of formats, including the Standard and ISO/IEC 27002.

- The Information Risk Assessment Methodology 2 (IRAM2), includes a six phase process and supporting material for performing information risk assessments. The report is supported by four IRAM2 Assistants, each accompanied by a practitioner guide.

ISF Consultancy Services

The ISF provides Members and non-Members with a full range of consultancy services to assist in the implementation of ISF research, tools and methodologies, addressing issues relating to governance, risk and compliance.

Non-Members can gain access to ISF’s research and tools by contacting steve.durbin@securityforum.org

CONTACT

For further information contact:

Steve Durbin, Managing Director
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

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.

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.

Reference: ISF17 ISF Tools Marketing | Copyright © 2017 Information Security Forum Limited | Classification: Public, no restrictions