Information Security Forum

ISF CONSULTANCY SERVICES

Addressing today's security challenges with confidence

Effective and agile 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. We help business leaders and information security professionals build and embed cyber resilience in their organisational structure, planning processes, information risk management and information security initiatives.

WHY CONSIDER ISF CONSULTANCY SERVICES?

Where organisations lack the time, resource or in-house expertise to deliver a business-essential project, ISF Consultancy Services can provide independent and objective guidance, support and training. Our consultancy services support organisations who need:

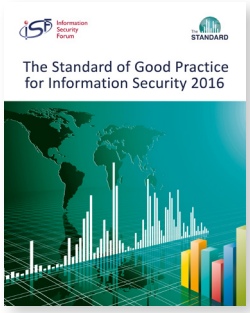
- interim CISO and senior staff who can build an effective cyber resilience programme
- independent evaluation and validation of security arrangements
- thorough assessment of information risk in critical environments
- objective, vendor-neutral and pragmatic security advice
- to translate security risks into effective board-level reporting
- internal training on using ISF tools and research
- to deliver a business-essential project securely and with confidence.

Our services are delivered by expert consultants using the ISF's powerful tools and research.

Organisations the world over trust the ISF to deliver in-depth knowledge, best practice and solutions that work.

Information Security Forum

ISF CONSULTANCY SERVICES

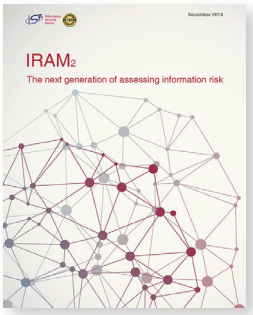


SECURITY GOVERNANCE, POLICIES, COMPLIANCE, STANDARDS AND CONTROL FRAMEWORK

The ISF's ***Standard of Good Practice for Information Security (the Standard)*** is the most comprehensive information security standard available. It provides complete coverage of the topics set out in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defense and Payment Card Industry Data Security Standard (PCI:DSS) version 3.1. It is used by many of the world's leading organisations as their primary reference to manage information risk and enable compliance. Our consultants will assist you in implementing ***the Standard***, thereby helping your organisation to:

- apply a robust framework for information security that provides consistent risk-based protection across the organisation and in your supply chain
- meet your regulatory and compliance requirements
- be agile and exploit new business opportunities – while ensuring that associated information risks are managed to acceptable levels
- respond to rapidly evolving threats
- update existing or develop new internal security policies.

Case Study: Following an external audit, a large multinational organisation was required to update and modernise its internal security policies. An ISF consultant helped the company to use ***the Standard*** as the basis for an updated set of policies, procedures and guidelines that met the requirements of the auditors and regulatory bodies.



RISK ASSESSMENT (IRAM2)

The ISF's ***Information Risk Assessment Methodology 2 (IRAM2)*** is a globally recognised approach that enables risk practitioners to perform end-to-end business-focused information risk assessments in a way that supports engagement with business stakeholders. Our consultants will help your organisation realise the full potential of ***IRAM2*** by:

- defining a risk appetite and supporting resources (for example, a Business Impact Reference Table) to reflect the risk posture of your management and nature of your business
- identifying your threat profile to highlight the threat actors, threat attributes and threat events that are relevant to your organisation
- assessing existing vulnerabilities
- helping you to develop pragmatic risk treatment plans.

ISF consultants can either train your own staff to perform ***IRAM2*** risk assessments, undertake full risk assessments for you, or deliver a combination of these approaches.

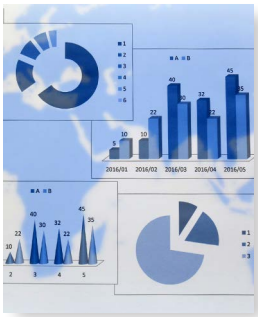
Case Study: ISF Consultants helped a large organisation from the Oil & Gas sector to carry out the *Scoping, Business Impact Assessment, Threat Profiling,* and *Vulnerability Assessment* phases of the ***IRAM2*** risk assessment methodology, culminating in a comprehensive plan to mitigate risk to a critical business system.

INFORMATION SECURITY ASSESSMENT, CONTROLS ASSURANCE AND ISO 27001/2 READINESS

The ***ISF Benchmark*** is an unrivalled tool that provides you with an in-depth and/or high-level assessment of your security arrangements. The ***Benchmark*** shows how your security arrangements stack up against ***the Standard***, and also against internationally recognised standards. In addition, the ***Benchmark*** enables you to demonstrate how your organisation's control status rates against that of other leading organisations around the world. Our ***Benchmark*** consultants will help you to:

- determine your organisation's readiness to achieve compliance with ISO 27001
- evaluate information security policy(ies) by identifying which areas require enhancement or fresh content
- assess security performance across a range of different environments in the organisation, and determine which business areas warrant most attention/investment
- build a plan for improvement where further action is recommended.

Case Study: ISF consultants helped a fast-moving consumer group company to assess the status of their global security operations and to establish policies that addressed the areas of weakness identified at departmental level across the business.



CISO AS A SERVICE

ISF can provide you with an interim CISO. We can also help CISOs present the value of information security to the business at board level and deliver the benefits of good cyber resilience and security awareness across the enterprise. We use ISF resources and best practices to provide security expertise to drive your organisation's security programme in the right direction. Our consultants can help organisations and teams who:

- require an interim CISO, e.g., whilst recruiting for a permanent role, have no CISO or security leadership role but need immediate advice
- are recovering from a significant incident and require immediate direction and coordination of activities
- want to implement an effective security governance programme
- need to confidently deliver presentations or reporting to the board or shareholders.

Case Study: The ISF placed an interim CISO at a large financial services company. The CISO used ***the Standard*** and ***Benchmark*** to understand the current security posture of the organisation and the ISF's ***Engaging with the Board*** approach to recommend an improvements programme aligned with business objectives.

CRITICAL ASSET MANAGEMENT AND PROTECTION

Can you be sure that you know exactly where your organisation's most critical information assets are, and that they are being protected in line with their importance to the business? Building on our expertise in key disciplines such as information classification and information risk assessment, ISF consultants will help you implement an approach to critical asset management and protection that enables your organisation to:

- identify its critical information assets based on their true value to the business
- reflect the latest information risk assessment techniques to identify the threat profile of critical assets
- provide protection to critical information assets that reflects their threat profile and importance to the business, whilst using resources as efficiently as possible (by avoiding 'over protection')
- maintain a consistent approach that addresses each stage of the information life cycle, allowing for factors that may change over time (such as the value of an information asset to the business, risk profile, or adequacy of current controls).

Case Study: ISF Consultants assisted a financial organisation to establish a critical asset protection programme, which involved: a comprehensive, enterprise-wide discovery exercise; detailed profiling of key threats (using the ISF's Cyber Attack Chain); and the deployment of specialised protection to counter sophisticated, targeted attacks against these assets.

SUPPLY CHAIN / THIRD PARTY ASSESSMENT

Recent high-profile security breaches have highlighted that information-related incidents in the supply chain can be just as damaging, if not more so, than those occurring within the organisation. The ISF's ***Supply Chain Risk*** tools help organisations to identify information risk exposure in their supply chains and manage this risk in line with business appetite. Our consultants will apply the ISF's ***Supply Chain Information Risk Assurance Process*** and ***Supply Chain Assurance Framework*** to help your organisation:

- identify instances of information risk exposure in existing supplier and third-party relationships
- rank suppliers by the level of information risk identified, and prioritise risk mitigation activity
- identify enhancements to your ongoing vendor management processes to ensure that the information security controls required of every supplier are effective and in proportion to potential information risk exposure
- implement processes for initial and periodic supplier controls assessments.

Case Study: An ISF Consultant worked with a major industrial conglomerate to validate the organisation's existing approach to managing supply chain risk against the ISF's ***Supply Chain Assurance Framework***. This resulted in a set of pragmatic recommendations for improvement that were linked clearly to business risk, along with a supporting roadmap for implementation

---

THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

The EU's General Data Protection Regulation (GDPR) will take effect by May 2018 – and any organisation that operates within the EU, does business with organisations in the EU, or stores data in the EU, will need to comply. The GDPR strengthens the rights of citizens with respect to access, portability and protection of personal data. In particular, it increases responsibility and accountability for those processing personal data, and places an emphasis on key areas such as risk assessments and the role of data protection officers. Compliance with the GDPR will require a focus on how privacy and data protection are addressed in handling information, but also on related areas such as awareness, incident management and achieving 'data protection by design'. Our consultants will leverage the ISF's expertise in building standards, benchmarking and risk assessment to:

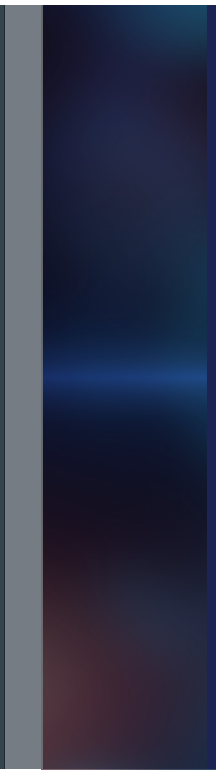
- determine the extent to which your organisation is 'GDPR ready'
- identify likely areas of non-compliance
- help you develop a roadmap for full GDPR readiness.

WHERE NEXT?

ISF Consultancy Services provide organisations with a variety of business solutions which are tailored to meet your immediate business requirements. Our consultants provide customised, professional support and training to strengthen your organisation's cyber resilience and information risk management arrangements, while equipping you to respond to rapidly evolving threats.

Benefits of ISF Consultancy Services:

- Independent and objective guidance, support and training.
- Help your organisation to embed consistent, capable, objective information risk best practice across the business.
- Can be used to demonstrate transparency, get the budget you require, align with your business strategy and shine the spotlight on key risk areas within the business.
- Provide real-world expertise that reflects proven practices from the world's leading organisations.
- Deliver high-impact services at speed.



CONTACT

For more information on the ISF's Consultancy Services, please 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