



# The Standard of Good Practice for Information Security 2018

**The definitive guide for responding to rapidly evolving threats, technology and compliance.**

*The Standard of Good Practice for Information Security 2018 (the Standard)* provides comprehensive controls and guidance on current and emerging information security topics enabling organisations to respond to the rapid pace at which threats, technology and risks evolve. Implementing *the Standard* helps organisations to:

- be agile and exploit new opportunities, while ensuring that associated information risks are managed within acceptable levels
- respond to rapidly evolving threats, including sophisticated cyber security attacks, using threat intelligence to increase cyber resilience
- identify how regulatory and compliance requirements can be best met.

The latest edition of *the Standard* includes enhanced coverage of the following hot topics: Agile system development, alignment of information risk with operational risk, collaboration platforms, industrial control systems, information privacy and threat intelligence.

*The Standard*, along with the *ISF Benchmark*; a comprehensive security control assessment tool, provide complete coverage of the topics set out in ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS and COBIT 5 for Information Security.

# THE STANDARD AS AN ENABLER FOR IMPROVING INFORMATION SECURITY

## RESILIENCE

*The Standard* provides a ready-made framework that can help an organisation to prepare for, manage and respond to major incidents that may have a significant impact on business.

*The Standard* provides extensive coverage of information security topics including those associated with security strategy, incident management, business continuity, cyber resilience and crisis management.

## RISK ASSESSMENT

*The Standard's* current and comprehensive content, when combined with the *ISF Information Risk Assessment Methodology 2 (IRAM2)*, can underpin an organisation's risk assessment process of identifying business impacts, assessing key threats and vulnerabilities, and treating information risks.

With this set of controls, an organisation can gain efficiency savings and deliver consistent protection in line with their organisational risk appetite.

## SUPPLY CHAIN MANAGEMENT

*The Standard* offers an easy-to-implement solution to ensure that an organisation's supply chain incorporates a risk-based approach to information security. It can also be used as the basis for understanding and assessing the level of information security implemented by external suppliers, including cloud services providers.

Used in combination with the *ISF Supply Chain Assurance Framework (SCAF)*, the *ISF Supply Chain Information Risk Assurance Process (SCIRAP)* and the *ISF Benchmark*, *the Standard* enables an organisation to implement protection that is fully aligned with ISO/IEC 27036-3:2013 (covering supplier relationships).

The *ISF Standard of Good Practice for Information Security 2018* is the leading authority on information security. Its practical and trusted guidance helps organisations to extract relevant good practice to underpin any new initiative in your information security programme.

*The Standard* provides complete coverage of the topics set out in ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS and COBIT 5 for Information Security.

### ISF RESEARCH

An extensive research programme into hot topics in information security. Latest research reports include:

-  Threat Horizon 2020: Foundations start to shake
-  Industrial Control Systems: Securing the systems that protect physical environments
-  Embedding Security into Agile Development: Ten principles for rapid improvement
-  IRAM2: The next generation of assessing information risk
-  Preparing for the General Data Protection Regulation
-  Threat Intelligence: React and prepare
-  Securing Collaboration Platforms – briefing paper
-  Aligning IRM with ORM – briefing paper
-  Protecting the Crown Jewels: How to protect your mission-critical information assets

### BENCHMARK RESULTS

The results of the *ISF Benchmark*, which provide valuable insights into how information security is applied 'on the ground' in Member organisations.



### EXTERNAL DEVELOPMENTS

Analysis and coverage of information security-related standards and frameworks, for example:

- NIST Cybersecurity Framework
- ISO/IEC 27001/2:2013
- CIS Top 20
- COBIT 5 for Information Security



plus legal and regulatory changes, for example:

- European Union General Data Protection Regulation 2016/679 (GDPR)
- PCI DSS



## The STANDARD

### MEMBER INPUT

Input from ISF Members, including workshops, online collaboration on *ISF Live*, face-to-face meetings, interviews and academy sessions at the *ISF Annual World Congress*.



## COMPLIANCE

*The Standard* is an ideal tool to help prepare for ISO/IEC 27001:2013 certification, and achieve compliance with other relevant standards (e.g. PCI DSS). It is aligned with key information security standards in the ISO/IEC 27000 suite including security governance and supplier relationships.

*The Standard* covers hot topics not found in ISO/IEC 27002 including cyber attack protection, system decommission, enterprise mobility management and industrial control systems.

## AWARENESS

Adopting *the Standard* reduces the need to develop security awareness content from scratch. *The Standard* covers topics that can be used to improve security awareness and achieve expected security behaviour amongst many different audiences across an organisation, including business users, technical specialists, senior management, systems developers and IT service providers.

It also addresses how information security should be applied in local business environments that typically require tailored awareness activities.

## INFORMATION SECURITY ASSESSMENT

*The Standard* is integrated with the *ISF Benchmark*, providing detailed, mid-level and high-level assessments of the strength of information security controls – either across an organisation, locally or against your peers (e.g. organisations in the same sector or geographic region).

Using *the Standard* and the *ISF Benchmark* in conjunction provides meaningful and objective analysis of the true level of security across an organisation that can be reported to executive management and stakeholders.

## SECURITY ARRANGEMENTS

*The Standard* is a complete and up-to-date reference guide for developing new security arrangements or improving existing ones as circumstances change (e.g. as a result of increasing cyber threats, use of cloud computing or reliance on mobile devices in the workplace). Its straightforward and intuitive security topics enable the extraction of relevant good practice to underpin any new initiative in an information security programme.

*The Standard* can help an organisation to respond to changing circumstances by accelerating information security initiatives and avoiding potentially costly incidents, operational impact and damage to brand and reputation.

## POLICIES, STANDARDS AND PROCEDURES

*The Standard* can be adopted directly as the basis of a new or existing information security policy. It is an effective tool for identifying gaps and reduces the time and effort required to produce information security policies, standards and procedures.

The harmonisation of internal policies throughout an organisation helps deliver a consistent and balanced level of information protection.

# WHERE NEXT?

*The Standard of Good Practice for Information Security 2018 (the Standard)* is the most comprehensive and current source of information security controls. *The Standard* is updated on a biennial basis to reflect the evolving international landscape of information security-related legislation and standards.

These updates include the latest findings from the ISF's research programme, input from our Member organisations, trends from the *ISF Benchmark* and major external developments including new legislation, changes in regulation and the releases of other information security-related standards.

Good practice described in *the Standard* will typically be incorporated into an organisation's business processes, information security policy, risk management and compliance arrangements. Consequently, *the Standard* is valuable to a range of key individuals or external parties, including Chief Information Security Officers (or equivalent), information security managers, risk management specialists, business managers, IT managers and technical specialists, internal and external auditors, IT service providers and procurement and vendor management teams.

The ISF encourages collaboration on its research and tools. Members are invited to join **The Standard of Good Practice for Information Security** community on *ISF Live* to share their experience and discuss the findings and recommendations presented in this report.

Consultancy services from the ISF provide Members and non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

The report is available free of charge to ISF Members, and can be downloaded from the ISF Member website [www.isflive.org](http://www.isflive.org). Non-Members interested in purchasing the report should contact Steve Durbin at [steve.durbin@securityforum.org](mailto:steve.durbin@securityforum.org).

## CONTACT

For further information contact:

**Steve Durbin, Managing Director**

**US:** +1 (347) 767 6772

**UK:** +44 (0)20 3289 5884

**UK Mobile:** +44 (0)7785 953 800

[steve.durbin@securityforum.org](mailto:steve.durbin@securityforum.org)

[securityforum.org](http://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.

