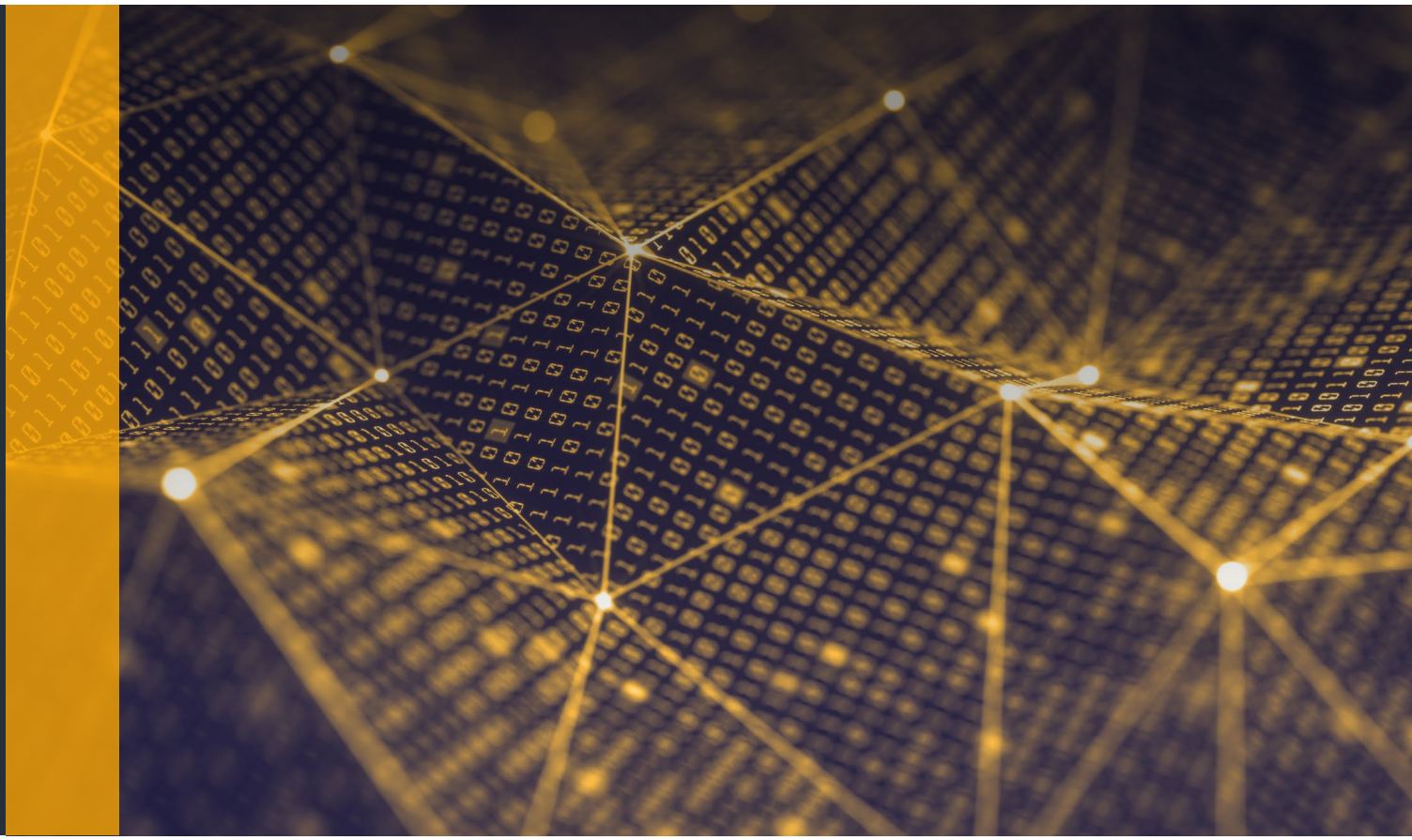

Standard of Good Practice for Information Security 2020

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

The ***Standard of Good Practice for Information Security 2020 (SOGP 2020)*** 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 ***SOGP 2020*** 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 ***SOGP 2020*** includes enhanced coverage of the following hot topics: securing cloud services, running a Security Operations Centre, protecting mobile devices, security assurance programmes, asset management and managing suppliers.

The ***ISF SOGP***, 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.

ISF STANDARD OF GOOD PRACTICE FOR

AN INFORMATION SECURITY ENABLER

1 | RESILIENCE

The ***SOGP*** provides a ready-made framework that can help an organisation improve their resilience by preparing for, managing and responding to major incidents that may have a significant impact on business.

To achieve this, ***SOGP*** provides extensive coverage of information security topics including those associated with security strategy, incident management, business continuity, cyber resilience and crisis management.

2 | RISK ASSESSMENT

The ***SOGP's*** current and comprehensive content, when combined with the ***ISF Information Risk Assessment Methodology 2 (IRAM2)***, can underpin an organisation's risk assessment activities, including identifying business impacts, profiling key threats and assessing vulnerabilities.

Any risks identified can then be treated using controls from the ***SOGP***, enabling an organisation to gain efficiency savings and deliver consistent protection in line with their organisational risk appetite.

3 | SUPPLY CHAIN MANAGEMENT

The ***SOGP*** 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 ISF Supply Chain accelerator tools and the ***Benchmark***, the ***SOGP*** 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 Secur***
Its practical and trusted guidance helps organisations to e
initiative in your information security programme.

The ***SOGP*** provides complete coverage of the topics set out
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 2022:
Digital and physical worlds collide


Using Cloud Service Securely:
Harnessing Core Controls


Demystifying Artificial Intelligence in Information Security
Briefing Paper


Human-Centred Security:
Addressing psychological vulnerabilities
Briefing Paper


Securing the IoT:
Taming the connected world
Briefing Paper


Building a Successful SOC:
Detect earlier, respond faster


Establishing a Business-Focused Security Assurance Programme:
Confidence in controls


Blockchain and Security:
Safety in numbers
Briefing Paper


Building Tomorrow's Security Workforce
Briefing Paper


Delivering an Effective Cyber Security Exercise

BENCHMARK RESU

The results of the ***ISF***
which provide valuab
how information secu
'on the ground' in Me
organisations.

STAN
OF GOOD

MEMBER INPUT

Input from ISF Memb
workshops, online co
ISF Live, face-to-face
and academy session
at the ***ISF Annual World Congress***.

4 | COMPLIANCE

The ***SOGP*** 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 ***SOGP*** covers hot topics not found in ISO/IEC 27002 including securing cloud services, running a Security Operations Centre or protecting mobile devices.

INFORMATION SECURITY 2020

rity 2020 is the leading authority on information security. extract relevant good practice to underpin any new

in ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS

ULTS
Benchmark,
le insights into
urity is applied
ember

BENCHMARK

DARD
PRACTICE

ers, including
llaboration on
meetings, interviews
s

ISF LIVE

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

ISO

COBIT 5
AN ISACA® FRAMEWORK

CIS Center for Internet Security®

NIST

plus legal and regulatory changes, for example:

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

PCI Security Standards Council™

8 | INFORMATION SECURITY ASSESSMENT

The ***SOGP*** is integrated with the ***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 ***SOGP*** in conjunction with the ***Benchmark*** provides meaningful and objective analysis of the true level of security across an organisation that can be reported to executive management and stakeholders.

7 | SECURITY ARRANGEMENTS

The ***SOGP*** 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 services 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 ***SOGP*** 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.

5 | POLICIES, STANDARDS AND PROCEDURES

The ***SOGP*** 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.

6 | AWARENESS

Adopting the ***SOGP*** reduces the need to develop security awareness content from scratch. The ***SOGP*** 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.

WHERE NEXT?

The ***Standard of Good Practice for Information Security 2020 (SOGP 2020)*** is the most comprehensive and current source of information security controls. The ***SOGP*** 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 ***SOGP*** will typically be incorporated into an organisation's business processes, information security policy, risk management and compliance arrangements. Consequently, the ***SOGP*** 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.

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. Non-Members interested in purchasing the report should contact Steve Durbin at 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
securityforum.org

INFORMATION SECURITY FORUM (ISF)

Founded in 1989, the ISF is an independent, not-for-profit association of leading organisations from around the world. The organisation is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management 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 programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

DISCLAIMER

REFERENCE: ISF 20 03 10 | **CLASSIFICATION:** Public, no restrictions