Information Security Forum

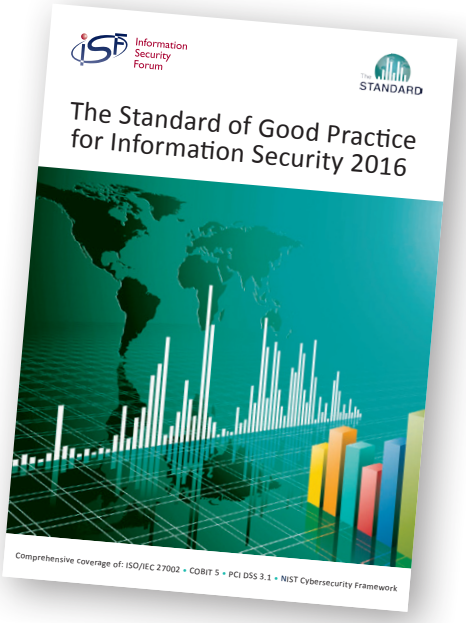
Press Release | **27 July 2016**

Information Security Forum releases the Standard of Good Practice for Information Security 2016

All-in-one guide used by global organizations as their primary reference for information security best practices.

The Information Security Forum (ISF) has published a major update to its ***Standard of Good Practice for Information Security (the Standard)*** for IT security professionals, the industry's most business-focused, all-in-one guide to information security assurance, presenting business-orientated information security topics with practical and trusted guidance. ***The Standard*** enables organizations to meet the control objectives set out in the NIST Cybersecurity Framework and extends well beyond the topics defined in the framework to include coverage of essential and emerging topics such as information security governance, supply chain management (SCM), data privacy, cloud security, information security audit and mobile device security.

"The increasing pace of change, shifting global threat levels, growing reliance on the supply chain and greater demand for efficacy from stakeholders represent some of the numerous challenges organizations are facing today," said Steve Durbin, Managing Director, ISF. "***The Standard*** is used widely across the ISF Membership which consists of many of the leading Fortune and Forbes global companies. It provides extensive coverage of information security topics including those associated with security strategy, incident management, business continuity, resilience and crisis management. These topics present practical advice that enables organizations to improve their resilience against a wide-ranging array of threats and low probability, high-impact events that can threaten the success, and sometimes even the existence, of the organization."



The 2016 version of ***the Standard*** has been restructured into 17 main categories for ease of use and improved alignment with ISF Member approaches to managing information security – while still retaining the same look and feel of previous versions. The revised design approach of the 2016 ***Standard*** has enabled systematic coverage of four new or enhanced life cycles that often require a great deal of information security protection.

These include:

- **Employment life cycle:** recruitment, induction, development, retention of employees and termination of their employment
- **Information life cycle:** creation, processing, transmission, storage and destruction of all types of information (electronic, printed or spoken), including confidential or mission-critical information
- **Hardware life cycle:** acquisition (purchase or lease), maintenance and disposal of physical equipment and devices
- **System development life cycle:** mainly focused on the design and development of critical business applications, but applicable to all types of system development (e.g., for IT infrastructure)

Updated annually to reflect the latest findings from the ISF's research program, input from global ISF Member organizations, trends from the ***ISF Benchmark*** and major external developments including new legislation and other requirements, ***the Standard*** is business-friendly and used by many global organizations as their primary reference for information security. ***The Standard*** addresses the rapid pace at which threats and risks evolve and an organizations' need to respond to escalating security threats from activities such as cybercrime, 'hacktivism', insider threats and espionage. As a result, ***the Standard*** helps the ISF, and its Members, maintain their position at the leading edge of best practices in information security.

"Effective implementation depends on strong information risk assessment, so that controls described in ***the Standard*** are applied in line with risk," continued Durbin. "The best practices defined in ***the Standard*** will normally be incorporated into an organization's information security policy, business processes, environments and applications, and should be of great interest and relevance to a range of individuals within the organization as well as external stakeholders."

Businesses today require the latest, practical guidance on the fast changing legislative landscape, particularly with how this impacts the gathering, use, storage and sharing of critical information assets. This includes legislation such as the EU General Data Protection Regulation (GDPR), which will take effect in May 2018, impacting every organization that holds personal information on EU citizens, as well as the EU Network and Information Security (NIS) directive, which aims to protect critical infrastructure and sets common cyber security standards and reporting requirements for applicable organizations.

"Transparent governance and clear lines of responsibility are essential in this day and age," continued Durbin. "Organizations will be required to identify the steps they have taken to protect data – its gathering, access, storage and disposal – and also to explain the rationale behind their decisions. ***The Standard*** has been developed for organizations of all sizes that recognize information security as a key business enabler, providing comprehensive controls and practical guidance on current and emerging information security topics."

The Standard helps ISF Members deliver up-to-date, best practices that can be integrated with their business processes, information security policy, risk management and compliance arrangements. Available at no cost to ISF Member companies, ***the Standard*** can also be purchased by non-Members. For more information on ***the Standard*** or any aspect of the ISF, please visit **www.securityforum.org**.

MEDIA CONTACT

NORTH AMERICA
John Kreuzer
Gutenberg Communications
Tel: +1 (408) 896 3307
Email: jkreuzer@gutenbergpr.com

Information Security Forum (ISF)

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organizations from around the world. The organization 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 organizations and developed through an extensive research and work program. 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 and provide ISF Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

For more information on ISF Membership, please visit **www.securityforum.org**