Information Security Forum

ABOUT THE ISF

What's included in our Membership?

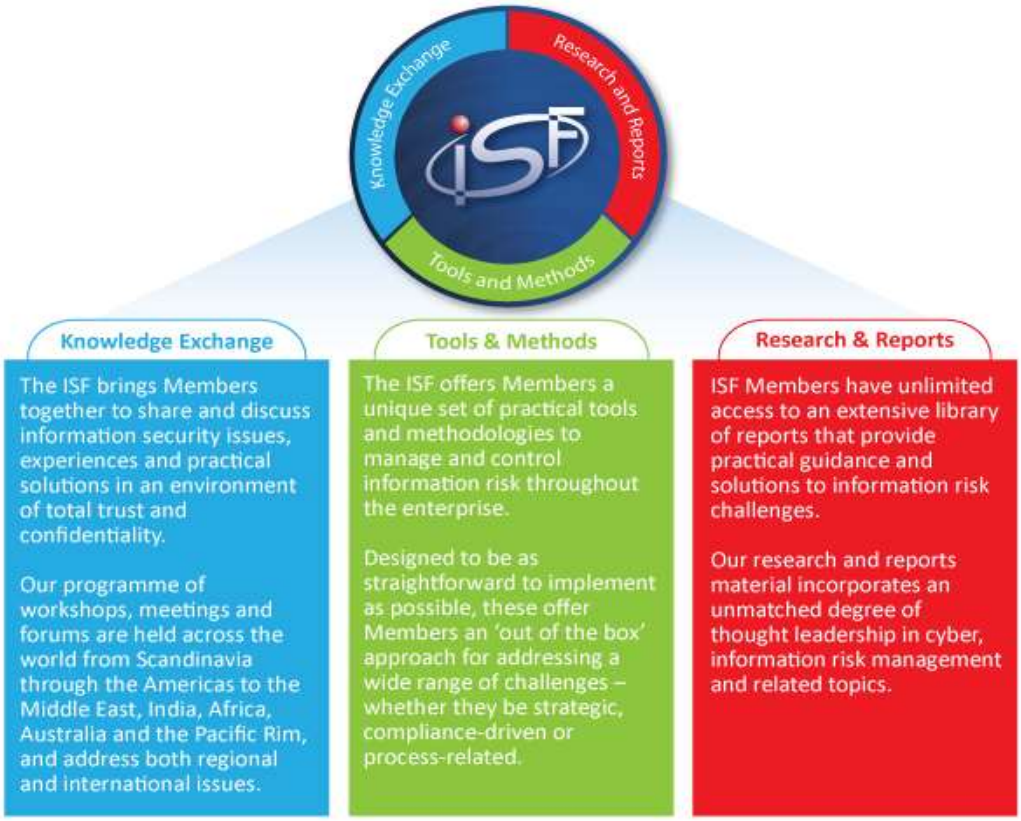
Background

The ISF is an independent, not-for-profit organisation that is driven and owned by its Members.

Formed in 1989, the ISF is an international association of over 400 leading organisations from around the world and from a wide range of sectors, including government, finance, manufacturing, pharmaceuticals and transport. The ISF's core aims are to:

- address key issues in information risk management through research and collaboration
- develop practical implementable tools and guidance
- facilitate networking within its Membership.

Access to all ISF services and deliverables is available from https://www.isflive.org. The three core elements of the ISF Membership service are shown in the graphic below and explained over the following pages. ISF imposes NO restriction on the number of individuals in your organisation that can use the service (including physical Chapter meetings and project events) – so please start using it!



1. ISF Tools and methods

ISF's Standard of Good Practice for Information Security

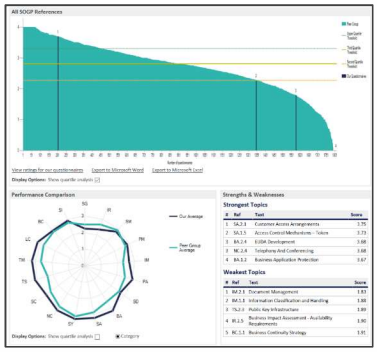
Available at https://www.isflive.org/community/compliance/standard-of-good-practice-for-information-security, the ISF's Standard of Good Practice is:

- the foremost authority on information security and key deliverable from the ISF's extensive work programme
- the basis for assessment using the ISF's Security Healthcheck and Benchmark
- developed using a proven methodology to produce the international benchmark for information security
- provides key objectives and a clear overview of the practical measures and activities that need to be carried out to keep information risks under control
- adopted by many organisations across the ISF Membership.

As the Standard provides comprehensive coverage of other recognised standards such as ISO 27001/2, COBIT version 5 for Information Security, the NIST Cyber Security Framework, PCI DSS 3.0 and the EU Directive on GDPR, it can play an important role in harmonising compliance activity.

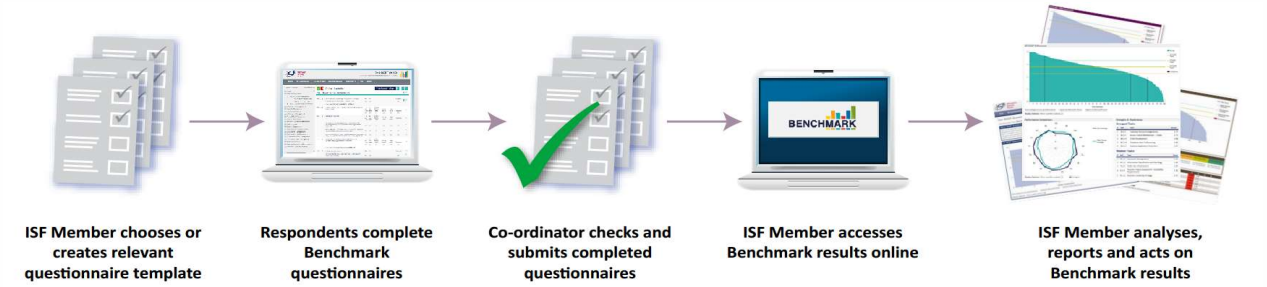
The Benchmark services

The Benchmark service is tightly aligned with the Standard of Good Practice and enables ISF Members to assess the extent to which the Standard has been applied. In particular, the Benchmark:



- creates a picture of information security status across the organisation
- allows assessments at varying levels of detail
- compares performance with other leading organisations
- shows the extent of ISO 27002 and/or COBIT version 5 compliance (PCI DSS 3.0 and NIST Cyber Security Framework results views will be made available shortly)
- identifies areas of weakness for further investigation
- supports the business case for improvement
- helps improve security awareness among staff.

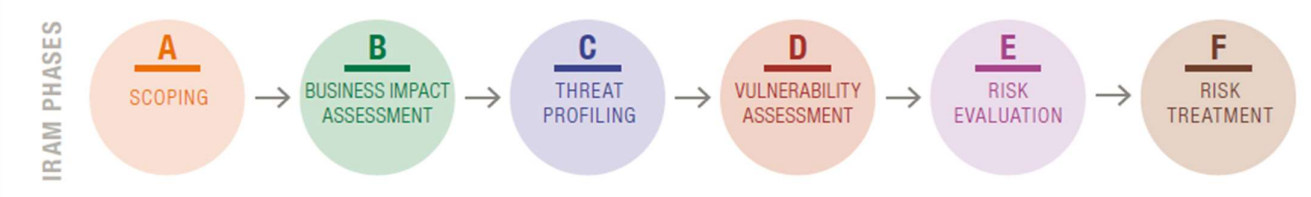
The benchmark is conducted using secure online tools. The overall process is outlined below.



More information about the Benchmark service is available here: https://www.isflive.org/community/compliance/benchmark

Information Risk Assessment Methodology (IRAM2)

The ISF's Information Risk Assessment Methodology provides a robust process for assessing information risk and for selecting appropriate controls in line with the risk identified. Released in October 2014, version 2 of IRAM applies significant new thinking to reflect different types of threat actor; a more rigorous calculation for risk likelihood; and latest concepts in risk mitigation/treatment. The phases of IRAM2 are shown below.



The full IRAM2 methodology Guides and assistants are available here: https://www.isflive.org/community/risk/iram2

Quantitative Techniques in Information Risk Analysis

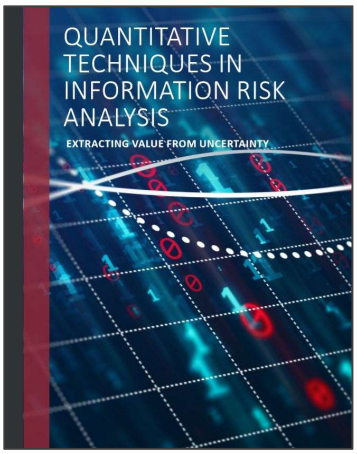
This report enables organizations to gain value from using quantitative techniques in information risk analysis by:

THE ISF APPROACH

– providing three techniques that are essential for understanding and undertaking quantitative information risk analysis.

– demonstrating how quantitative information risk analysis can be conducted to provide accurate and informative results.

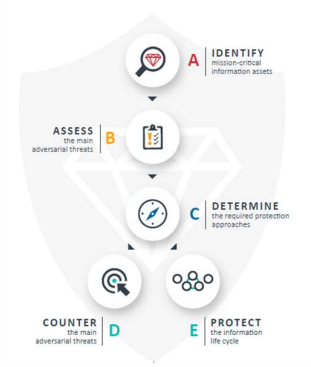
– presenting ways in which the results of quantitative information risk analysis can be communicated to support decision making .

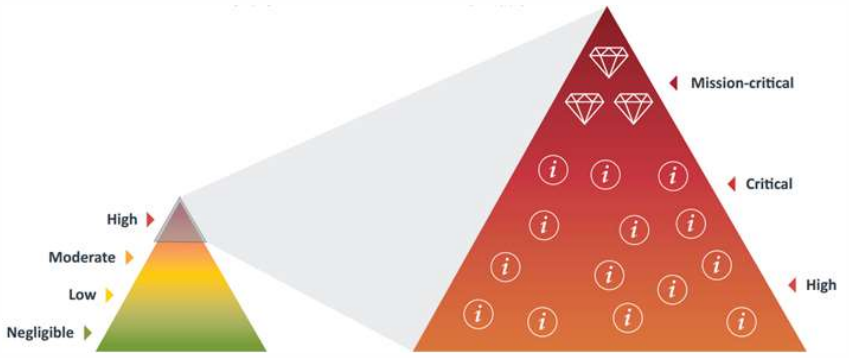


Executive Summary
+
Report

Protecting the Crown Jewels

The Crown Jewels approach builds upon the concepts in IRAM2 with a focus on Mission-Critical Information Assets which require protection by specialised controls, above and beyond the baseline controls that are applied to all information assets.





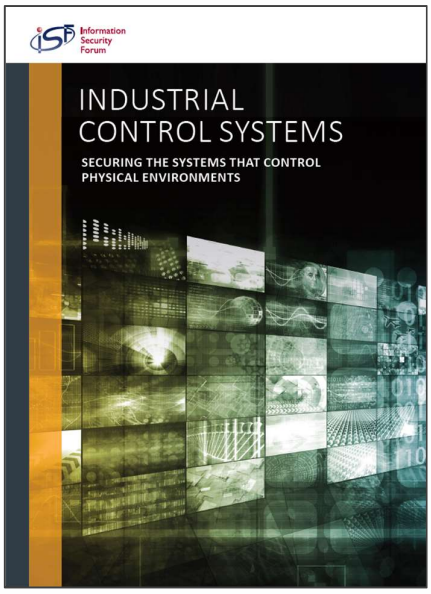
Preparing for the General Data Protection Regulation

The GDPR strengthens the requirements for protecting personal data. It affords individuals new and enhanced rights and freedoms and holds organisations responsible for enabling them. It promises to penalise organisations unable to uphold these rights and freedoms – a risk best managed by establishing an enterprise-wide GDPR compliance programme.

The European Union's General Data Protection Regulation (the GDPR) brings data protection legislation into line with new, previously unforeseen ways in which information is used today. The GDPR applies to most organisations handling European personal data and supersedes the 1995 European Union (EU) Directive on Data Protection; unifying data protection law for EU Member States. This regulation holds organisations responsible for enabling the new and enhanced rights and freedoms of data subjects

Industrial Control Systems: Securing the systems that control physical environments

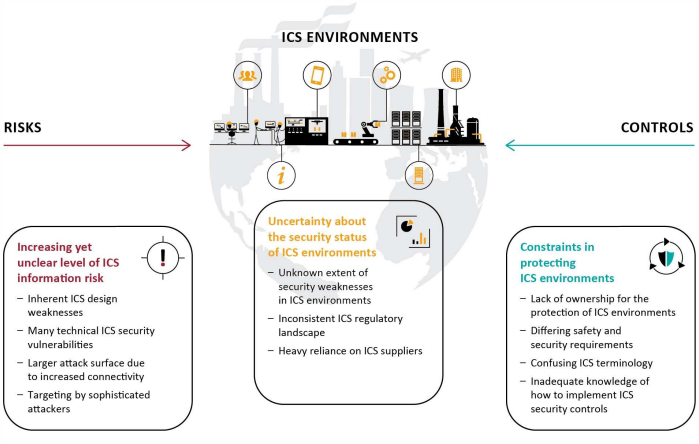
The digital revolution that transformed both commercial organisations and governments is now affecting systems deployed in the industrial world – and at an equally runaway pace. Such rapid change is leaving many organisations struggling to secure these systems against cyber-attacks.



This integrated set of deliverables helps ISF Members to:

- define ICS, describing how they work in practice, putting them in context of a wider set of assets relating to ICS environments
- highlight the growing need to protect ICS
- describe how to prepare for an ICS Security Programme; a practical and structured approach for improving information security arrangements in ICS environments
- explain the steps required to implement an ICS Security Programme effectively.

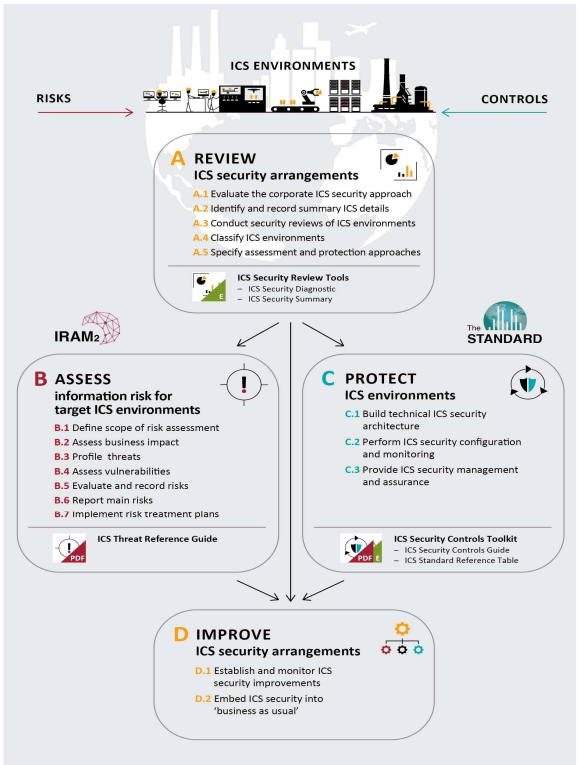
The main ICS security problems are presented under three headings.



The ICS Security programme consists of four main phases, each broken into a series of steps, complemented by useful supporting material, which can be used in many ways – the ICS:

- Threat Reference Guide supports the threat and vulnerability elements of ICS information risk assessments.
- Security Controls Guide and ICS Standard Reference Table help protect ICS environments.
- Security Diagnostic enables effective, consistent security reviews of individual ICS environments.

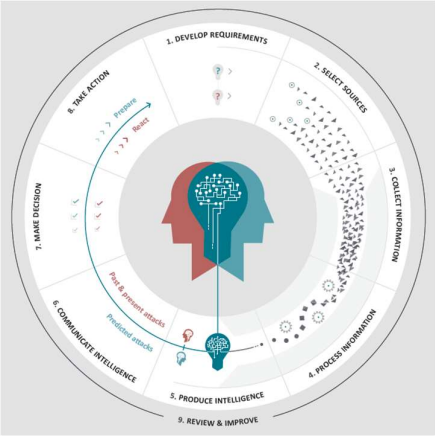
Security Summary Tool compares and contrasts the results of security reviews for a range of ICS environments.



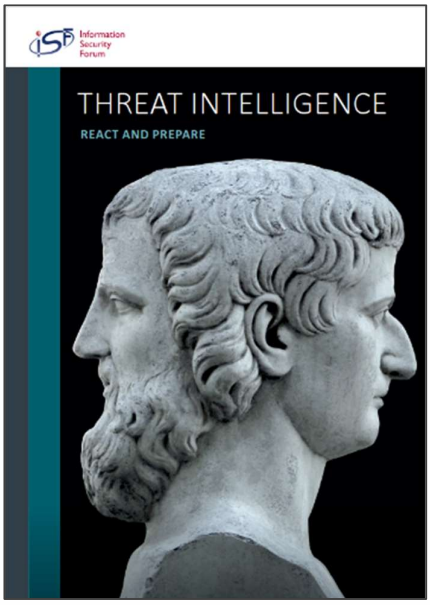
Information Security Forum

Threat Intelligence: React and Prepare

The digital revolution presents opportunities to identify and exploit the rising value of information. But this same value also attracts unwanted attention and the risk from adversaries is increasing in magnitude and complexity. To manage this risk, organisations must build a realistic view of the threats they face – their capabilities, intentions and actions.

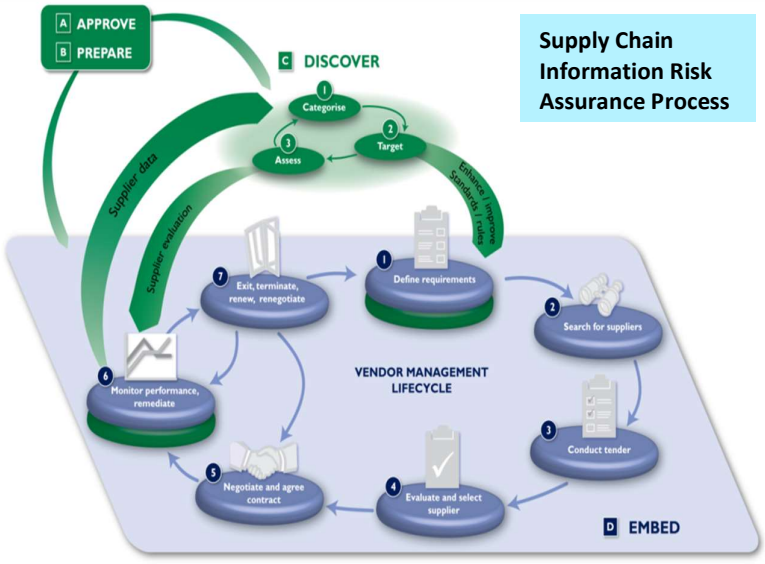


The *ISF Approach for Managing a Threat Intelligence Capability* equips organisations to build and manage a capability that delivers tangible value. It explains three key concepts of effective threat intelligence and how they can be achieved using the intelligence cycle. Requirements-driven and skilfully produced through analysis, threat intelligence harnesses the expertise and experience of others to provide insight into past, present and predicted attacks against an organisation. This insight informs security decision making, enabling organisations to act.

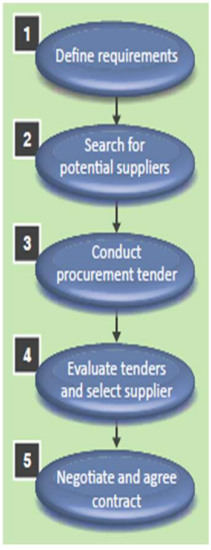


Managing Information Risk in the Supply Chain

ISF Membership includes access to tools which assist you in identifying where information risk exposure exists in your current supply chain (and in third party relationships more generally); and in implementing robust mechanisms for ensuring that third party risk is managed well via your processes going forward. These approaches are depicted below. Detailed guidance is available here: https://www.isflive.org/community/risk/supply-chain



Supply Chain Information Risk Assurance Process



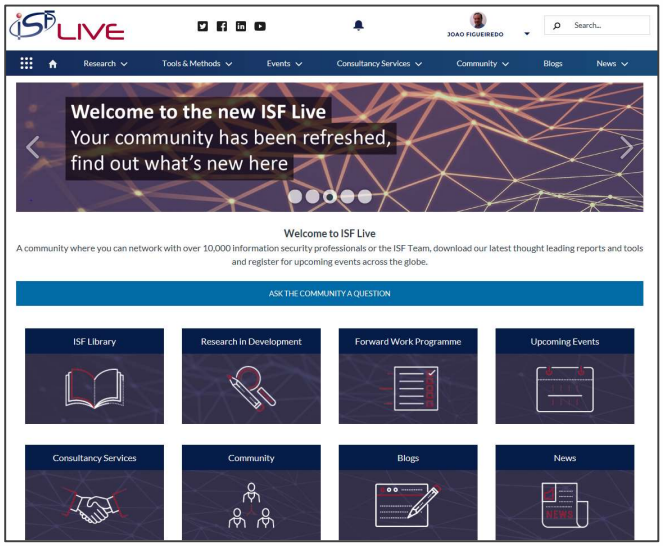
Supply Chain Assurance Framework

2. Research and reports

The ISF undertakes an extensive annual work programme of research. Each research project:

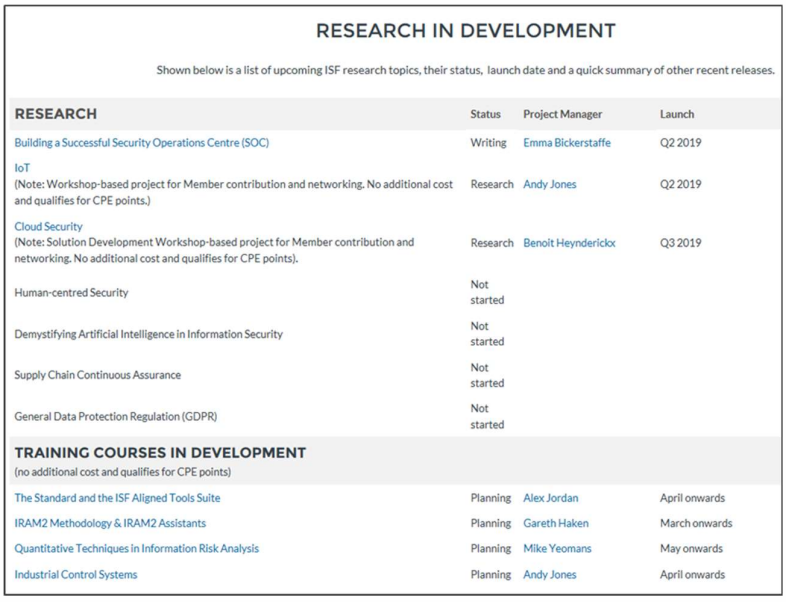
- results in high quality, easy-to-use reports and tools:
  - briefing papers for top management
  - practical implementation guides and methodologies
- provides insights from fellow Member organisations
- is based on the business needs of Members
- represents best practice across the membership.

An overview of the ISF's current work portfolio can be found on ISF Live by selecting 'Research in Development' from the Research dropdown menu, as shown below. From the portfolio, you can navigate to more information and Member collaboration associated with each project.



1. Select 'Research in Development' from the research Menu

2. Click on the project name to access the relevant group in ISF Live

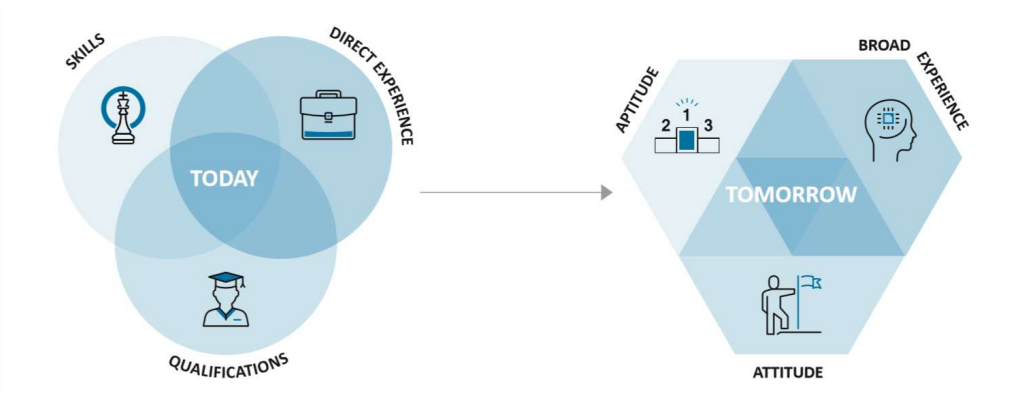


RESEARCH IN DEVELOPMENT

Shown below is a list of upcoming ISF research topics, their status, launch date and a quick summary of other recent releases.

RESEARCH	Status	Project Manager	Launch
Building a Successful Security Operations Centre (SOC)	Writing	Emma Bickerstaffe	Q2 2019
IoT (Note: Workshop-based project for Member contribution and networking. No additional cost and qualifies for CPE points.)	Research	Andy Jones	Q2 2019
Cloud Security (Note: Solution Development Workshop-based project for Member contribution and networking. No additional cost and qualifies for CPE points).	Research	Benoit Heynderickx	Q3 2019
Human-centred Security	Not started		
Demystifying Artificial Intelligence in Information Security	Not started		
Supply Chain Continuous Assurance	Not started		
General Data Protection Regulation (GDPR)	Not started		
TRAINING COURSES IN DEVELOPMENT (no additional cost and qualifies for CPE points)			
The Standard and the ISF Aligned Tools Suite	Planning	Alex Jordan	April onwards
IRAM2 Methodology & IRAM2 Assistants	Planning	Gareth Haken	March onwards
Quantitative Techniques in Information Risk Analysis	Planning	Mike Yeomans	May onwards
Industrial Control Systems	Planning	Andy Jones	April onwards

Building Tomorrow's Security Workforce - Briefing Paper



To build tomorrow's workforce and rectify the shortage, organisations should realign their focus to candidates with aptitude, attitude and broad experience:

– **Aptitude**: a natural ability to do something (e.g. numerical reasoning, verbal reasoning and situational strengths)
– **Attitude**: a 'settled' way of thinking or feeling about something to show an individual's disposition
– **Experience**: the knowledge or skill acquired by a period of practical experience of something, especially (but not limited to) that gained in a particular profession.

Delivering an Effective Cyber Security Exercise

The ISF Approach is supported by the:

- *Cyber Security Exercise Planner*
- *Cyber Attack Scenario Builder*

PHASE A: PREPARE
- Select target of exercise
- Assess constraints
- Design cyber attack scenario
- Choose type of exercise
- Make logistical arrangements
- Define success criteria
- Build playbook

PHASE B: RUN
- Brief participants
- Start exercise
- Facilitate exercise
- End exercise
- Gather immediate feedback

PHASE C: FOLLOW-UP
- Conduct cyber security exercise review
- Create action plans
- Present to stakeholders
- Implement action plans

Recent research reports include:

- Building a Successful SOC: detect earlier, respond faster – Report
- Establishing a business-focused security assurance programme – Report
- Threat Horizon 2021: The digital illusion shatters
- Blockchain and Security: Safety in numbers - Briefing Paper
- Building Tomorrow's Security Workforce - Briefing Paper
- Delivering an Effective Cyber Security Exercise
- Emerging Quantitative Techniques in Information Risk Assessment – Executive Summary and Report
- Data Leakage Prevention – Briefing Paper
- The ISF 2018 aligned tools suite:
    - Supplier Security Evaluation(SSE) Summary Tool
    - Supply Chain Assurance (SCA)
    - Security Healthcheck V7 Summary tool
    - IRAM2: Vulnerability Assessment Assistant
- Benchmark Update 2018 fully aligned with SoGP 2018
- Securing Mobile Apps: Embracing Mobile, Balancing Control - Briefing Paper
- The Standard of Good Practice for Information Security 2018
- Threat Horizon 2020
- Industrial Control Systems: Securing the systems that control physical environments
- Embedding Security into Agile Development: Ten principles for rapid improvement
- Preparing for the GDPR: Digest and Implementation Guide
- Threat Intelligence: React and Prepare
- Securing Collaboration Platforms – Briefing Paper
- Aligning Information Risk Management with Operational Risk Management
- Protecting the Crown Jewels
- Security Architecture - Application Security Framework
- Engaged Reporting: Fact and Fortitude

3. Knowledge Exchange

Effective knowledge exchange lies at the heart of the ISF's collaborative approach. This is achieved through a combination of online and physical events. These are outlined below.

Chapter meetings

The ISF operates a number of Chapters and regional networks around the globe. Regular Chapter meetings provide a great opportunity to:

- network with other local ISF Members; learn how other Members use ISF deliverables to deliver value
- hear from authoritative external speakers on current topics in information security and risk management
- stay up to date on recent and forthcoming ISF initiatives.

In addition, Chapters often run supplementary events, such as implementation workshops focused on how to extract maximum value from recent ISF deliverables. There is no limit on the number of people globally that can participate in Chapter activities. Please consider becoming an active member of your own Chapter. Click on the links below to find out more about activities in your region.

ISF Chapters:

 Australasia	https://www.isflive.org/groups/australasia
 Canada	https://www.isflive.org/groups/canada
 Denmark	https://www.isflive.org/groups/denmark
 Finland	https://www.isflive.org/groups/finland
 Francophone	https://www.isflive.org/groups/francophone
 Grey (Germany, Austria, Switzerland)	https://www.isflive.org/groups/grey-group-germany-switzerland
 India	https://www.isflive.org/groups/india
 Ireland	https://www.isflive.org/groups/republic-of-ireland-regional-network
 Middle East	https://www.isflive.org/groups/middle-east
 Norway	https://www.isflive.org/groups/norway
 Orange (Benelux)	https://www.isflive.org/groups/orange-benelux
 Singapore	https://www.isflive.org/groups/singapore-regional-network
 South Africa	https://www.isflive.org/groups/south-africa
 Sweden	https://www.isflive.org/groups/sweden
 United Kingdom	https://www.isflive.org/groups/united-kingdom
 United States	https://www.isflive.org/groups/united-states

Solution Development Workshops

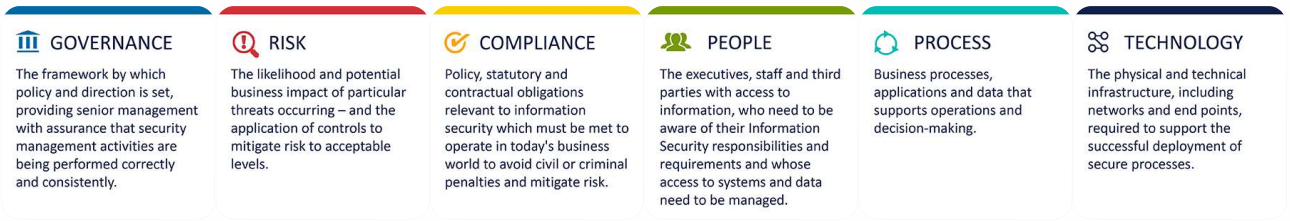
From time to time the ISF will invite Members to attend Solution Development Workshops (SDW) focused on a particular topic. The aim of these workshops is to help shape the ISF's research, both in terms of understanding Member challenges and the solutions that are most likely to make a real difference in overcoming those challenges. Information about SDWs is available on the ISF Live site.

ISF Live

ISF Live is the ISF's secure Member website, accessible here: https://www.isflive.org. The site provides a number of benefits, enabling you to:

- access the ISF's full library of research
- download the ISF's tools
- find out about current ISF projects
- keep up-to-date about ISF activities in your region
- register to attend Chapter meetings, Solution Development Workshops, and webcasts
- collaborate with other Members on specific topics, for example to share challenges and solutions.

To assist in navigation, ISF Live presents content in six core communities:



Annual World Congress

ISF Membership includes two fully-funded places at the ISF Annual World Congress, which will take place between 26th – 29th of October 2019 in Dublin. Benefits of the Congress include:

DUBLIN 2019
ISF 30th ANNUAL WORLD CONGRESS

- 1000+ participants
- 3 core days – Sunday to Tuesday
- 6 Plenary sessions with global leaders
- 7 topic streams with ~40 breakout sessions delivered mainly by Members on solutions to problems
- chapter gatherings
- optional ISF research and tools sessions on Saturday, Sunday and Monday afternoons
- access to experts at the ISF exhibition stand
- comprehensive sponsor programme
- full social programme – meals & 3 nights' accommodation included
- only travel and Saturday evening meal incurred by participants.

4. Helping you derive maximum value from your Membership

ISF Account Management

Every ISF Member is assigned an Account Manager. The Account Manager's role is to assist your organisation in gaining maximum value possible from the Membership. If you are unsure as to who the Account Manager is for your organisation is, please get in touch with the ISF Primary Contact for your organisation or contact us at info@securityforum.org.

ISF Consultancy

The ISF's Consultancy programme offers Member organisations an opportunity to purchase short-term, customized support to supplement the implementation of ISF deliverables. These services are provided by qualified ISF Consultants with significant implementation experience. Examples of services available include undertaking information security assessments using the ISF's Benchmark / Security Healthcheck tools; implementation of the ISF's Standard of Good Practice; conducting information risk assessments using the ISF's IRAM2 Information Risk Analysis methodology; and delivery of training to equip the Member to implement ISF tools / methodologies consistently over time. For more information contact your Account Manager or steve.durbin@securityforum.org

Member Referrals Reward Programme

Members that introduce a new Member to the ISF are eligible to receive a reward of the Member's choice. Choices include 2 additional months of Membership, a contribution of £2000 towards travel to the Annual World Congress and 2 additional places at Congress. To refer a new Member, please contact steve.durbin@securityforum.org

Where can I find out more?

To find out more, visit https://www.isflive.org to register for a user account.

Alternatively, contact the ISF's Global Account Manager at: ivo.goncalves@securityforum.org