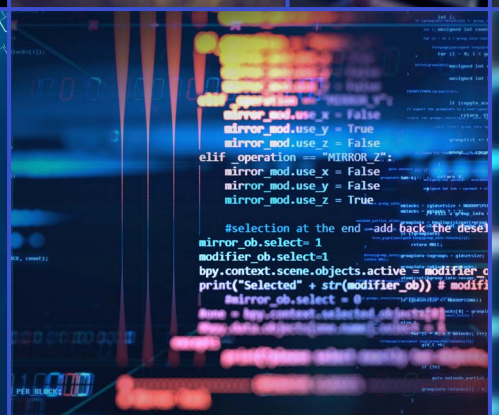


ISF

ANNUAL REPORT 2020



ISF ANNUAL REPORT 2020

April 2021

Published by

Information Security Forum

+44 (0)20 3875 6868

info@securityforum.org

securityforum.org

A series of white geometric lines on a blue background. A horizontal line starts from the left edge, followed by a diagonal line going up and to the right, then a vertical line going down, and finally a diagonal line going down and to the left, creating a stepped effect. Another horizontal line is positioned below the first one, starting from the left edge and ending with a small circle.

CONTENTS

04

Message from
the Chair

06

Our Business
Strategy

08

Securing a Return
on Your Investment

10

2020 in
Numbers

12

Showcasing Major
Products and
Services

15

Solving the New
Cyber Security
Challenges

20

Financial
Report

21

Digital 2020:
The ISF World
Congress

23

Appendix
ISF Elected Advisory Council
and Supervisory Board
Members, 2020

MESSAGE FROM THE CHAIR



Gareth Lindahl-Wise
ISF Chairman

The extraordinary conditions of the last twelve months have left organisations struggling to respond to a unique set of circumstances over which they have little control.

With organisations in every sector grappling with a range of challenges from disruption to a fight for survival, there may never have been a more important time for the ISF to deliver the high quality research, tools and services which will help our Members adapt to the challenges ahead and manage the surrounding risks.

Despite these uncertain times, reflecting on 2020 offers us the chance to share some of the ISF's successes with you. We welcome 45 new organisations who have joined the Membership, and although our growth was affected by the global pandemic, we close the year having delivered a solid financial performance culminating in 433 organisations being Full Members.

We've provided Members with more products over 12 months than we've ever done before. Our research covered a diverse range of

Overall, 21 products were launched with an unprecedented Member feedback rating of 4.9 out of 5.

important topics such as: Legal and Regulatory Implications for Information Security; Deploying Open Source Software; Becoming a Next-Generation CISO; Human-Centred Security; Supply Chain Continuous Assurance and Extinction Level Attacks. During the year we provided the 2020 update to the Standard of Good Practice for Information Security

and the associated additions were translated into the brand new Benchmark, IRAM2 and Aligned Tools Suite, encompassing 14 new and updated ISF Tools.

With major events around the world being cancelled and having reviewed a range of potential options for holding our Chapter meetings, training and workshops, the decision was taken to move to virtual events this year. This decision wasn't taken lightly, but in these exceptional times our primary aim must always be to safeguard our employees' and Members' safety and welfare. To further support Members' implementation efforts, we held 143 digital events over the course of the year.



Digital 2020, our 31st Annual World Congress, saw 3,478 attendees register, over 300% more than we've ever had at Congress before.

Moving our flagship event online has widened our audience to 409 Member organisations from 86 countries compared to 356 from 40 countries in 2019 and we look forward to their continued participation in our future global thought leading initiatives. Feedback from Members has shown how well it was received and how it stood out as a premier digital event of the year.

This 2020 Annual Report showcases some of the ISF's achievements over the last twelve months and provides examples of how organisations are using their ISF Membership to maximise their return on investment. I'd like to take this opportunity to thank you for your ongoing engagement and support.

I will take the opportunity to thank the ISF team and my colleagues on the Advisory Council and Supervisory Board. The ISF team itself faced many of the challenges that we have faced in our own companies and personal lives, yet continued to deliver, improve on and expand the range of deliverables to the Membership. This is a testament to the individuals and to the leaders at all levels in the organisation. The Advisory Council and Supervisory Board continued to uphold their responsibilities on behalf of the Membership in contributing to and guiding the work the ISF has done – again, at a time of great strain in our 'day jobs'. To you all, I say a heartfelt 'Thank you'.

We are now looking forward to a new, and hopefully better year. We have an exciting line up of research reports on Threat Horizon 2023; Virtualisation; Cyber Insurance and a new Quantitative Information Risk Analysis Methodology are all set for release in the coming months.

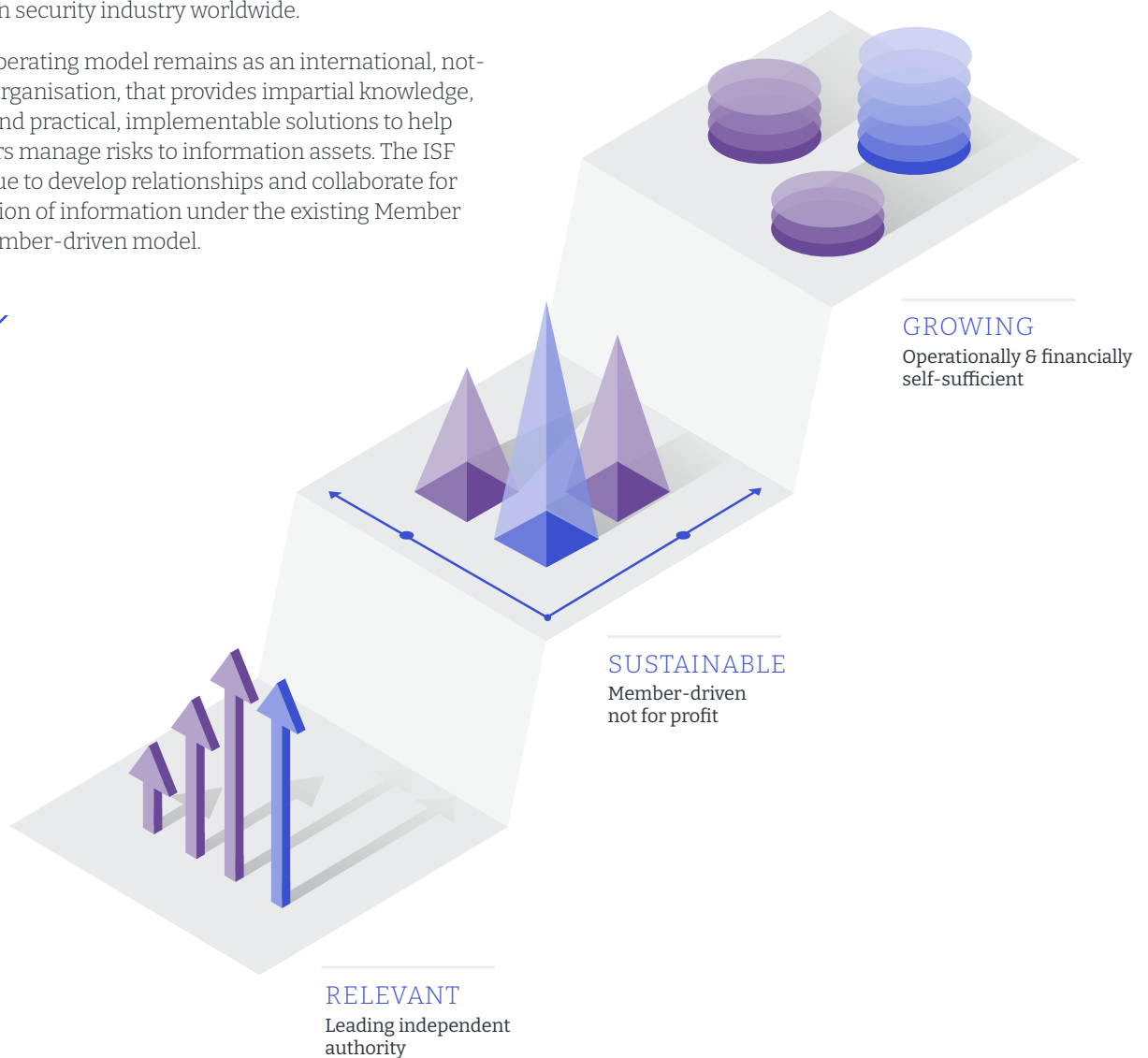
I do hope you will continue to take full advantage of everything the ISF offers you and your organisation over the course of 2021.

OUR BUSINESS STRATEGY

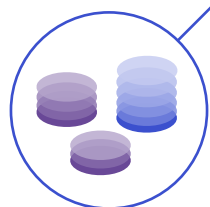
The ISF aspires to be a leading, independent authority on information security and risk management.

Our strategy will position the ISF for sustainable long-term growth with agility and flexibility, building on a period of sustained investment for our Members and staff, allowing the ISF to continue to be seen as a thought leader in the information security industry worldwide.

The ISF's operating model remains as an international, not-for-profit organisation, that provides impartial knowledge, guidance and practical, implementable solutions to help its Members manage risks to information assets. The ISF will continue to develop relationships and collaborate for the protection of information under the existing Member owned, Member-driven model.



Successful execution of the strategy will enhance the overall value proposition for Members by means of:



RELEVANCE

Security and risk functions are going through significant change. This requires the information security professional to work with not just information security functions, but also those responsible for Audit, Legal, IT, Risk and Compliance, Corporate Governance and Policy. The ISF must reflect this change and serve both seasoned professionals and newcomers from the CxO, CISO, CSO to the security practitioner. Individual Member organisation relevance will be enhanced further via a tailored relationship management model with the Member's cyber programme at the core of this activity.



SUSTAINABILITY

The ISF is an international Member-owned, Market-led and not-for-profit organisation. Providing impartial knowledge, guidance and practical, implementable solutions via a collaborative and leading infrastructure that supports both Members and ISF employees, will allow the ISF to continue to attract and retain both Members and key individuals. Our people are at the heart of the ISF strategy and by developing capabilities, skills and empowering them to give their best we will create greater engagement throughout the company and a reputation for valuing and respecting our workforce. This will enhance Member value and ensure that ISF employees are regarded as being at the forefront of the information security and risk management industries.



GROWTH

The ISF serves both Member organisations and the broader information security community. Working with organisations from the F2000 to mid-size, from government to academia, worldwide, the ISF delivers valuable, independent and actionable insight resulting in a growing Membership and sought-after perspective and services from Members and non-Members alike.

Please see 2020 in Numbers on pages 10–11 for a depiction of how we're progressing our strategy.

SECURING A RETURN ON YOUR INVESTMENT

The ISF provides a unique, professional network of over 18,000 information security professionals.

Time being in short supply, our trusted forums, both online and face-to-face, enable confidential interaction based around your topics of interest – as well as focus on local and industry issues – to ultimately identify sustainable best practices that can be implemented with confidence throughout your organisation.



Leverage the network

Participate by sharing your knowledge and experiences with others and gain an inside perspective on how fellow Members are solving business problems and mitigating information risk. Expand your personal contact base to call upon peer support when you most need it and be recognised by your peers as an expert in your field.



Ensure we build products that matter

Contribute to product design and development by suggesting and shaping topics you'd like the ISF to research. Use our social media business platform or attend workshops to enrich our thinking while ensuring our products are practical, relevant and beneficial to you. Influence the outcomes to be sure they meet the challenges you're facing today.



Consult topic experts

Engage with an ISF analyst. Use the ISF's social media business platform to pose questions or gain advice and product support to supplement your implementation efforts. Invite your colleagues from audit, risk, legal, compliance or any other relevant function to join these communities and accelerate the realisations of benefits by gaining business-wide alignment with your initiatives and goals.



ISF



Enhance your skills

Improve your knowledge and understanding of topical and complex information security issues and how to set about resolving them by attending ISF events to share practices with fellow Members and learn more about how the ISF can help you manage information risk.



Get tailored insight and on-site advice

Commission an ISF analyst or topic expert for a tailored service. The ISF offers virtual and on-site services to supplement the implementation of our products. These services can be designed around your needs and delivered working alongside your teams to help advance your aims.



Send your global teams to local Chapter Meetings

Enhance the global network and capacity of your team to deal with security challenges by attending ISF Chapter meetings. The ISF encourages Members to attend Chapter meetings wherever they're based, irrespective of affiliation, to help build these valuable networks and identify new business opportunities.

2020 IN NUMBERS

MEMBERSHIP

45  New Members

433  Full Members

STRATEGY

Strategy to guide activities and investments until

2023



RELEVANCY



482 Media placements



31,772

LinkedIn Group
members/followers



2,951

Twitter followers



18,040

Podcast listens

PRODUCTS & SERVICES

3,478

Congress registrations
Our biggest ever audience



4.4/5



Overall rating

51

Digital Chapter Events
and Workshops



4.2/5



Average rating

92

Launch & Training
Webinars held



1,622

Webinar attendees

7

Research Reports launched



4.9/5



Average product rating

14

New and updated Tools



17,995

ISF LIVE

Registered users



32%

increase from 2019

SHOWCASING MAJOR PRODUCTS AND SERVICES

2020 was a great year for the delivery of new products and more workshops.

The ISF worked in close collaboration with Members, industry experts, academics and expert practitioners to deliver more highly rated products and services over the course of the calendar year.



Click for more
information



Click to access product
(for ISF Members only)



Threat Horizon 2022: Digital and physical worlds collide

The 2022 edition of the ISF's annual publication forecasts the most likely information security-related threats organisations will be facing in the immediate future, encapsulated by the following themes:

- Invasive technology disrupts the everyday
- Neglected infrastructure cripples operations
- A crisis of trust undermines digital business.

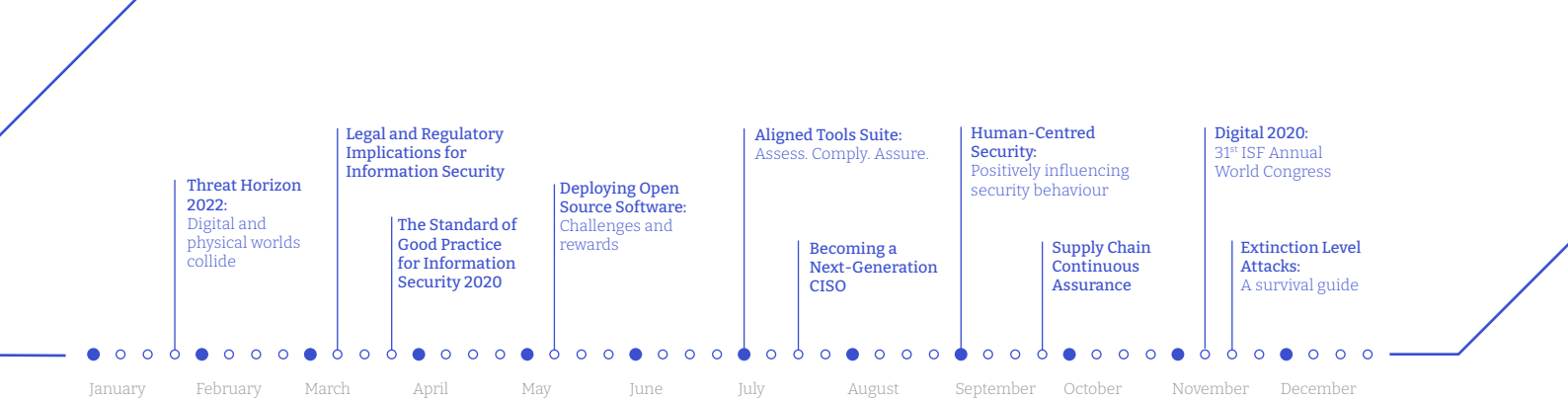


Legal and Regulatory Implications for Information Security

This interactive report provides comprehensive analysis of legal and regulatory obligations for information security by:

- detailing over 400 legislations applicable to 93% of ISF Members
- highlighting legal issues related to emerging technologies and trends
- outlining key elements of European Union laws.





The Standard of Good Practice for Information Security 2020 (SOGP 2020)

During these unprecedented times, the SOGP 2020 provides timely guidance on ensuring a secure business operating environment across all aspects of cyber resilience, information security and risk management. This latest edition of the SOGP includes enhanced coverage of the following hot topics: 'Security Workforce', 'Core Cloud Security Controls', 'Security Operation Centres', 'Mobile Application Management' and 'Asset Registers'.



Deploying Open Source Software: Challenges and rewards

This briefing paper explores what OSS is and debunks some of the myths linked to its use, exposing the true reality of the benefits that OSS can bring. The paper describes the measures that should be implemented to reap the rewards of effectively managing OSS.



Becoming a Next-Generation CISO

Building on interviews with CISOs, and extensive survey results, the ISF's research into the changing role of the CISO has revealed six core characteristics that next-generation leaders exhibit. This report describes the forces at play that have prompted the emergence of the next-generation CISO, and explains the novel characteristics and capabilities that this demanding role will require now and in the future.





Supply Chain Continuous Assurance

Monitoring supplier security

This report provides guidance to organisations aiming to continuously monitor the security of their suppliers by:

- outlining the need to manage information risk throughout the duration of a supplier relationship
- examining a range of tools and techniques that can be used to monitor supplier security
- exploring methods to continuously report on supplier security.



Human-Centred Security:

Positively influencing security behaviour

Building on the findings from the ISF's first paper in the human-centred security research series, the second instalment leverages existing psychological theory to positively change and sustain security behaviour. This paper outlines the key aspects of a successful human-centred security programme to help Members reduce the risks posed by poor security behaviour.



Extinction Level Attacks:

A survival guide

It is no longer possible to overlook the reality of encountering an extreme, high-impact cyber attack. The ISF's report explains the tasks organisations need to undertake to survive such an attack:

- Prepare – tasks to complete before an attack, to ensure that the organisation is better prepared to respond to the attack when it happens.
- Respond – tasks to execute during an attack, in order to lessen its impact and to speed the recovery.
- Resume – tasks that are instrumental in returning to a stable and secure organisational state as quickly as possible.



SOLVING THE NEW CYBER SECURITY CHALLENGES

with the ISF Aligned Tools Suite 2020

The 2020 pandemic has brought an inevitable economic downturn and organisations are now faced with budget restrictions and the need to do more for less. Like many other digital industries, cybercrime has flourished in the economic downturn. As organisations seek to broaden their digital footprints, their attack surfaces also increase, providing a variety of opportunities for malicious actors.

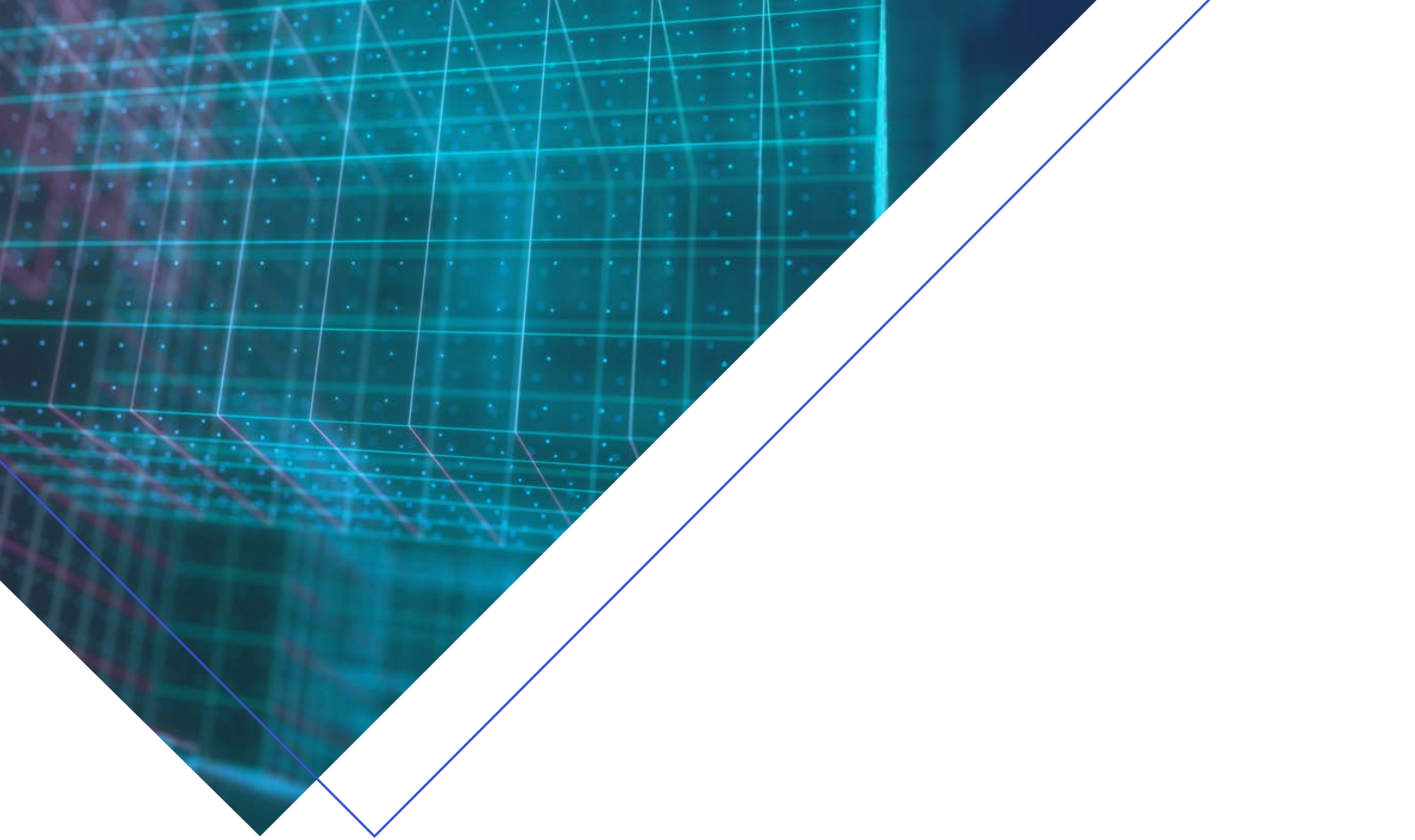
The need to protect data and critical assets has never been more important and the ISF Aligned Tools Suite 2020 has been designed to help Members act in an agile and confident manner, helping guide them towards making the right cybersecurity decisions and investments.

The ISF Aligned Tools Suite 2020 brings together 14 ISF tools and cross reference aids, including a modernised Benchmark platform and the new IRAM2 WebApp. Aligned to the latest version of the Standard of Good Practice for Information Security 2020 (SOGP 2020), the suite – which also includes Security Healthcheck, Supply Chain accelerator tools and SOGP 2020 cross-references – helps Members to demonstrate compliance with international standards and assure security across their external suppliers.

Building on over 30 years of information security expertise, the ISF Aligned Tools Suite helps organisations understand the key issues facing the security of their information, including:

- How to prioritise cyber security investments when resources are tight
- How to determine a manageable level of information risk
- How to assure supply chains
- How to manage compliance across multiple standards

Available exclusively to ISF Members, the ISF Aligned Tools Suite 2020 helps organisations save time, prioritise investment and make smarter decisions.



How to prioritise cyber security investments in an economic downturn?



Challenge

As the coronavirus pandemic comes to an end, so too will the expansive economic support funded by governments across the world. Businesses who have furloughed staff, held off on investments, or even hibernated entire functions, will all have to take tough decisions as to how to spend what little money they have in reserves. Within cyber security, budgets will be cut as businesses invest money elsewhere to drive revenue back to pre-pandemic levels. With a reduced budget, security leaders will have to make tough choices on how and when to prioritise the funds available to them.



Opportunity

Managing cyber security budgets has often been a challenge for security professionals, who are used to dealing with limited budgets and demands to demonstrate return on investment. At the forefront of these tools is the ISF Benchmark, a controls assessment platform designed to highlight an organisation's strengths and weaknesses across a variety of cyber security domains. These strengths and weaknesses can be used to demonstrate areas for targeted investment, as well as the impact of this investment on an organisation's cyber security posture. Newly upgraded in 2020, with results shown across six industry-leading standards and frameworks, and the option to compare data against industry peers, it has never been easier to target effective security spend.

How to determine a manageable level of information risk?



Challenge

As businesses continue to react to the global landscape in light of the pandemic, many organisations are shifting working practices to more flexible models, including greater reliance on remote working technologies. As both organisations and individuals adapt to a new way of working, cybercriminals and other malicious actors are exploiting weaknesses in hastily adopted products and preying on individuals' insecure actions in order to gain the upper hand.



Opportunity

One of the first steps in securing these new environments should be a full information risk assessment to identify any gaps in existing arrangements. IRAM2 offers a simple, practical, yet rigorous approach to identifying and assessing risks in a target environment. It is fully supported by the IRAM2 WebApp which enables organisation's systems to be identified in terms of their criticality to the business, and then protected in line with that criticality. With a focus on the business perspective, any available resources can be maximised in order to bring overall risks down to an acceptable level.

How to manage compliance across multiple standards?



Challenge

Fuelled by new technologies and opportunities, the scale and complexity of cyber attacks will continue to grow and have wide-ranging impacts on organisations. The commodification of cyber attacks, where even low-level attackers can pay for time limited access to powerful techniques, and the advent of AI, will present new challenges to organisations looking to protect the Confidentiality, Integrity and Availability of their data.



Opportunity

The response to sophisticated cyber attacks must be holistic and focus on a wide range of measures. The SOGP provides extensive coverage of information security topics including those associated with security strategy, threat intelligence, incident management, business continuity, cyber resilience and crisis management. These topics present practical advice that enables an organisation to improve resilience against a broad range of threats including sophisticated cyber attacks and low-probability, high-impact events that can threaten the success and sometimes even the survival of an organisation.



How to assure supply chains?



Challenge

Budgets are strained as the economic downturn starts to bite. This extends to procurement, and businesses are under pressure to seek services from suppliers who can offer 'more for less.' In response, even well-established suppliers will trim out as much cost (and potentially information security) as possible in order to protect margins. Heightened information risk exposure is an inevitable consequence.



Opportunity

The ISF Supply Chain Security suite of resources provides everything needed to manage supplier risk in a way that leverages resources as efficiently as possible. The Supply Chain accelerator tools support procurement teams by offering a framework for managing supplier risk (SCA), whilst also enabling specific suppliers to be assessed and managed in line with their level of criticality to the business (SSE).

FINANCIAL REPORT

The ISF enhanced its financial position, closing 2020 with strengthened reserves. 45 new Members were acquired over the period, closing the year with 433 Full Members.

The below table provides an extract from the 2020 audited financial statements.

	2020 (£000's)	2019 (£000's)
Revenue/Income	10,711	11,806
Surplus/(defecit)	1,349	825
Fixed assets	103	128
Other debtors	1,002	957
Trade debtors	2,160	3,038
Cash at bank	11,749	10,078
TOTAL ASSETS	14,911	14,073
Creditors: amounts due within one year	(7,637)	(8,128)
Net Current Assets	7,274	5,945
Total assets less current liabilities	7,377	6,073
Net Assets	7,132	5,783
Capital & reserves Profit & Loss for the year	1,349	825
Members' Reserve Funds	7,132	5,783

Note from Nexia Smith & Williamson the ISF's independent statutory auditors:

The financial information presented on this page is an accurate reflection of the 2020 statutory financial statements for Information Security Forum Limited, produced in accordance with the Companies Act 2006.

DIGITAL 2020: THE ISF WORLD CONGRESS



Our flagship global event offers attendees an opportunity to find solutions to current security challenges and gain practical advice from some of the world's foremost authorities in the industry whilst the Member speaker programme delivers valuable content that in many cases would not be shared in any other environment.

Digital 2020, was well received by ISF Members and sponsors alike, attracting an overall feedback rating of 4.5 out of 5 and featuring presentations from the ISF, Keynotes and Members.



SPONSORS

Digital 2020 was generously supported by the following companies who enabled us to deliver a unique digital event of the quality and comprehensiveness that you've come to expect.



PLATINUM SPONSORS



GOLD SPONSORS



ENHANCED SILVER SPONSORS



SILVER SPONSORS



EXHIBIT & MEDIA SPONSORS

For more information on sponsoring the 32nd ISF World Congress, visit securityforum.org

DIGITAL 2020 ISF WORLD CONGRESS

ATTENDANCE

89%

Attendance from the Membership

409

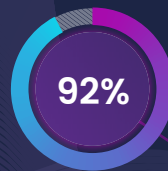
Member organisations

86

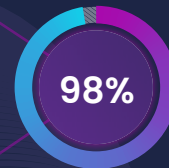
Countries

% of Members rated 4 or 5/5:

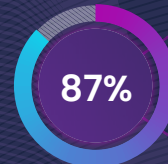
EXPERIENCE



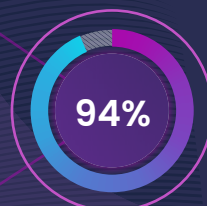
Relevance



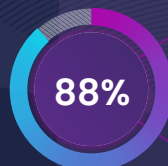
Support



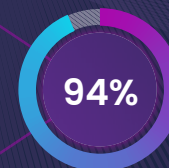
Benefit



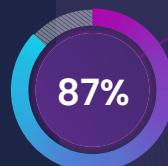
Overall Experience



Keynote Sessions



ISF Sessions



Breakout Sessions



ISF ELECTED ADVISORY COUNCIL AND SUPERVISORY BOARD MEMBERS, 2020

	CHAPTER	ORGANISATION
Brian Abdoll	South Africa	Sanlam
Rory Alsop*	UK	HSBC Bank Plc
Anna-Stina Berg	Sweden	Svenska Handelsbanken
Mathieu Cousin	Francophone	AXA
Morten Dalsgaard Andreasen	Denmark	Nordea Bank
Thorsten Delbrouck – Deputy-Chair*	Grey	Giesecke & Devrient GmbH
Werner Gutau*	Grey	Infineon Technologies AG
Vivek Khindria	Canada	Loblaw Companies Limited
Kimberly Lemmens	Orange	ABN-AMRO Bank
Gareth Lindahl-Wise – Chair*	UK	Klint Risk Consulting
Johnny Mathisen	Norway	Telenor ASA
Kevin McQuade	US	Enterprise Holdings, Inc
Jari Pirhonen*	Finland	TietoEVERY
Anne Reinsnes	Norway	Norges Bank
Vishal Salvi	India	Infosys
Mark Slatter	UK	Bank of America
Bryson Tan	Canada	Ernst & Young
Johan van Beek	Orange	Achmea
Josef Van Wyk*	US	Graham Holdings
Torben Voight Olsen	Denmark	H. Lundbeck A/S
Koos Wolters	Orange	KPMG
Claire Vishik	US	Intel Corporation
Torben Voight Olsen	Denmark	H. Lundbeck A/S
Koos Wolters	Orange	KPMG
Resigning Advisory Council Members during 2020:		
Thomas Hemker	Grey	Symantec

*ISF Supervisory Board Member.

ABOUT 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.

ISF

For further information contact:

Information Security Forum
+44 (0)20 3875 6868
info@securityforum.org
securityforum.org