Information
Security
Forum

The Information Security Forum (ISF) and Information security for external suppliers: a common baseline

Gregory Nowak

Principal Research Analyst

What is the ISF?

An international association of some 300 leading global organisations, which…

- **addresses key issues in information risk management through research and collaboration**
- **develops practical tools and guidance**
- **is fully independent, not-for-profit organisation and driven by its Members**
- **promotes networking within its membership**

The leading, global authority on information security and information risk management

ISF Members Public administration and defence

Arbeids- og velferdsetaten
Bergen Kommune (The Municipality of Bergen)
Centrelink
Danish Tax and Customs Administration
Department of Health & National Health Service
Department of Social & Family Affairs
Finnish Communications Regulatory Authority
Finnish Tax Administration
Foreign & Commonwealth Office
GOVCERT.NL
Government of Ontario
Government of South Australia

Infocomm Development Authority of Singapore
Manitoba Provincial Government
Maritime Provinces
National Institute of Standards and Technology
National Patient Safety Agency
National Policing Improvement Agency (NPIA)
Norwegian Tax Administration
Parliamentary Information Communications Technology
RDW
Region Hovedstaden
Revenue Commissioners
South African Revenue Service
The Government of British

Geographical coverage

The ISF currently has Members in…

- Australia
- Belgium
- Canada
- Chile
- Denmark
- Faroe Islands
- Finland
- France
- Germany
- Greece
- India
- Ireland
- Italy
- Latvia
- Luxembourg
- Netherlands
- New Zealand
- Norway
- Saudi Arabia
- Serbia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Arab Emirates
- United Kingdom
- United States of America

Currently 31 ISF Members in the United States

(ISC)^2
AAA Insurance Company
Alcatel-Lucent
Apollo Group
Baxter Healthcare Corporation
Bechtel Corporation
Boeing
Bristol-Myers Squibb
Cargill Incorporated
Citigroup
Fidelity Information Systems
Goldman Sachs & Co
Guardian Life Insurance Company of America
Honeywell International
HP Enterprise Services
ITT Corporation
Kraft Foods
Marsh & McLennan Companies, Inc.
Microsoft Corporation
National Institute of Standards and Technology
Northrop Grumman Corporation
Pemco Corporation
Procter & Gamble Services Company
RSA
State Farm Mutual Automobile Insurance Company
Sungard Data Systems, Inc.
Towers Watson
USAA
Vanguard
Verizon
XL Group plc.

What services does the ISF provide?

ISF Services - an overview

1. ISF Developed Tools and Methodologies

ISF Briefing: DLP tools
Solving the data privacy puzzle
Achieving compliance
Annual Report 2008
Information Security Forum Limited

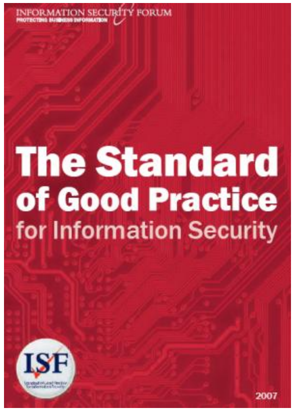
2. ISF Research Programme

3. Knowledge and Information Exchange

ISF 22nd Annual World Congress
17 – 20 September 2011
Berlin, Germany

4. ISF Annual World Congress,
USF Chapter Meetings

The Standard of Good Practice for Information Security



INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

The Standard of Good Practice for Information Security

ISF

2007

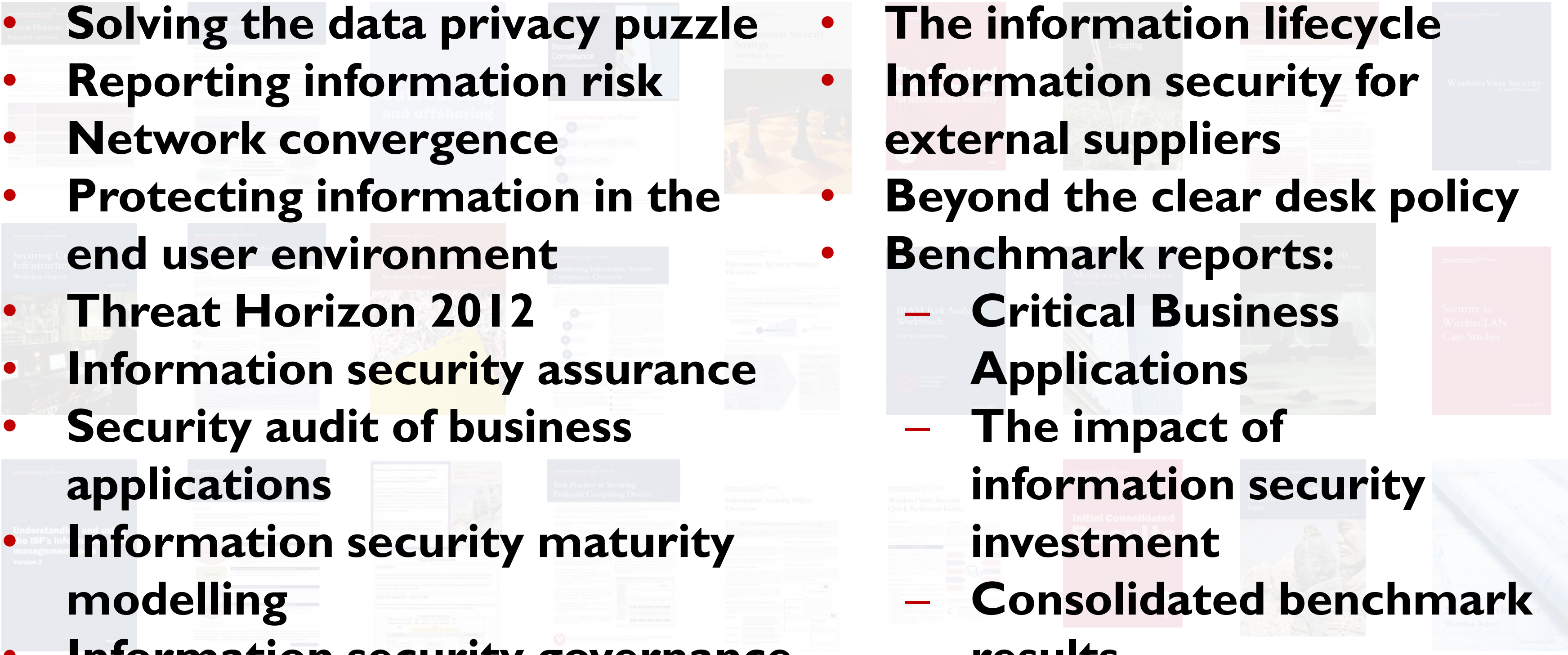
Specialist Tools

The ISF's specialist tools are the result of research projects covering specific challenges in information security.

Tools available include:

- **Continuous Benchmarking Service**
- **Security and Legislation Database**
- **Third party security assessment tool (TPSAT)**
- **Security Function Diagnostic**
- **Return on Security Investment Calculator (ROSI)**
- **Best Practices in Endpoint Security Checklist**
- **Information Risk Analysis Methodology**
- **Risk Analyst Workbench**

Research & reports over the past 12 months



- Solving the data privacy puzzle
- Reporting information risk
- Network convergence
- Protecting information in the end user environment
- Threat Horizon 2012
- Information security assurance
- Security audit of business applications
- Information security maturity modelling
- Information security governance
- Information security principles

- The information lifecycle
- Information security for external suppliers
- Beyond the clear desk policy
- Benchmark reports:
  - Critical Business Applications
  - The impact of information security investment
  - Consolidated benchmark results
  - Cross reference to ISO/IEC 27002, CObIT version 4.1

The 2011 work programme (Q1)

Workshop-based research and development projects:

- Cloud computing – Avoiding the seven deadly sins (**End Jan**)
- Organisational Governance (**End June**)

Research based projects:

- Consumerisation: Securing the next generation of end user environment (**End March**)
- Threat Horizon 2013 (**End Feb**)
- Standard of Good Practice update (**End May**)

Information risk management tools:

- Information Risk Analysis Methodology - Risk Analyst's Workbench v1.0 (**Ongoing**)

Briefing Papers:

- Cyber citizenship (**End March**)

Training workshops:

- Information Risk Analysis Methodology (IRAM)
- Protecting information in the end user environment
- Security audit of business applications

Agenda

- The project
- The need for a standard
- Baseline security controls
- ISF and ISO: way forward
- Wrap-up

Previous ISF work

Major area of interest:

- Managing third party access
- Securing remote access
- Managing information risks from outsourcing
- Information risk management in outsourcing and offshoring
- Information security in third party relationship management

Securing Remote Access by Staff
Briefing Paper
Implementation Guide
Risks and Controls
EUROPEAN SECURITY FORUM
INFORMATION SECURITY FORUM
ISF Digest
Outsourcing and
Management –
Information Security in Third Party Relationship Management
Information risk management in outsourcing and offshoring
January 2006
ISF
Third Party Security Assessment Suite
A
B
C
D

No longer third parties – external suppliers

THIRD PARTIES

- A confusing term
- Difficult to explain
- Has particular legal meanings
- Poorly defined

EXTERNAL SUPPLIERS

- Easier to define
- No legal meaning
- Aligns our terminology with other organisations

‘An organisation that provides goods or services to an acquiring organisation.’

Deliverables

- Executive overview
- ISF report
- Two ISO draft standards
  - Purchasing organisation
  - Third party organisation
- External Supplier baseline maturity assessment tools
- Data analysis pack

Information security for external suppliers: a common baseline

November 2010

External Supplier Baseline Maturity Assessment Tool (BMAT) version 1.0

Information security for suppliers: a common b
Data Analysis Pack

This workbook contains the dataset collected at ISF Member Work Groups on the topic of third party information security management standards.

The workbook presents the analysis of responses. To preserve anonymity, only aggregate data is presented - no Member material is included in this workbook.

If you have any queries, or require assistance in using this workbook, please contact the ISF Research and Services Team on:
+44 (0)207 213 3372 or email isfinfo@securityforum.org.

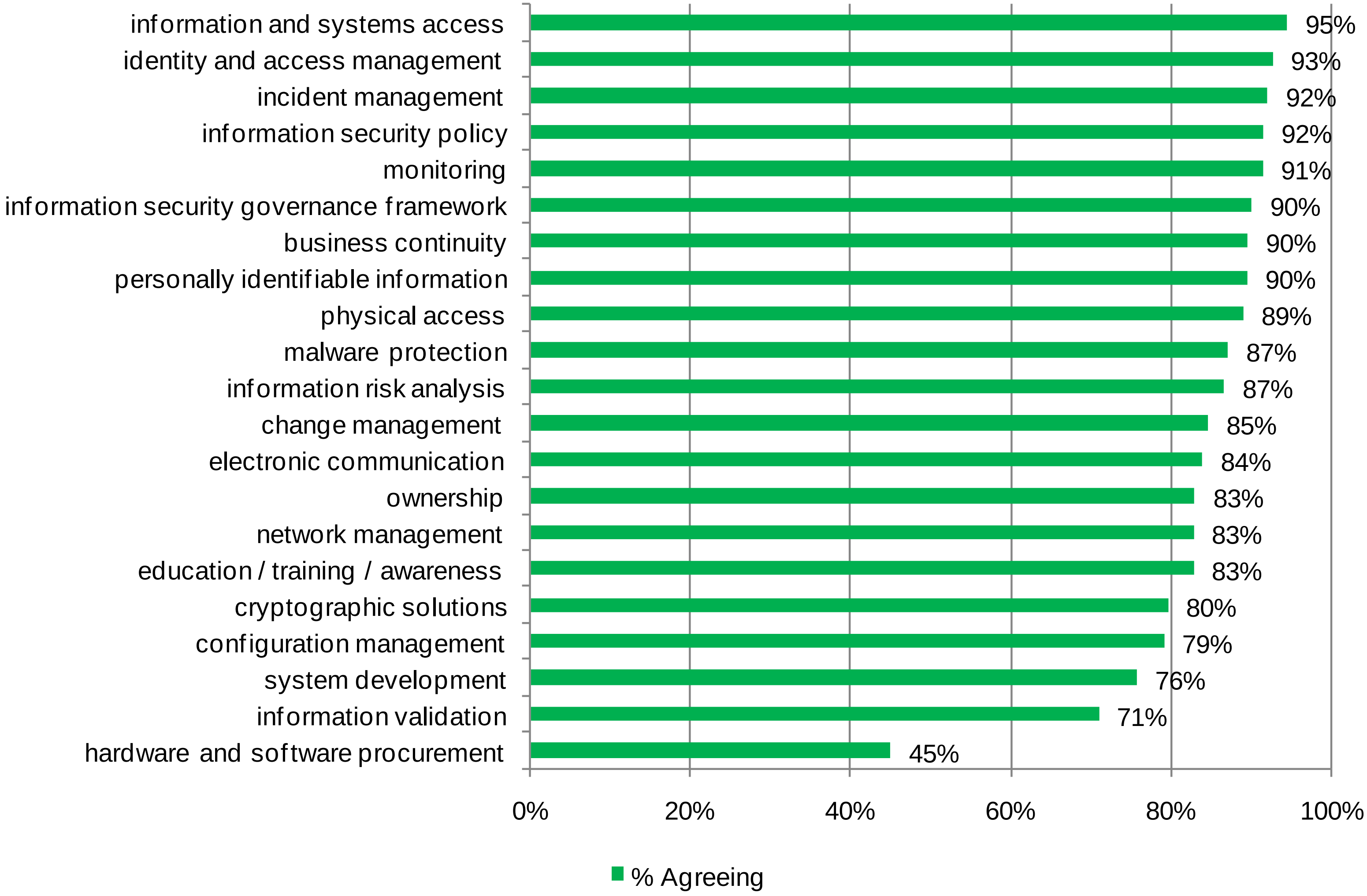
The need for a standard…

- There are many out there:
  - Outsourcing standards (IAOP OSP v8.0, Healthcheck)
  - Security Standards (SOGP, ISO 2700X series, BITS SIG)
  - IT Standards (COBIT, ITIL, ISO 20000)
  - Other standards (ISO 28000, ISO 25999 / ISO 27031)
  - Auditing standards (SAS 70, ISAE 3402)

- Many of these standards:
  - Address different topics at different levels of detail
  - Are written independently of others
  - Offer differing certification or accreditation procedures
- Some standards:
  - Offer lists of controls – others provide no controls
  - Controls may not be mandatory

BASELINE SECURITY CONTROLS

High-level control areas



Information security baseline arrangements

- Based on ISF Standard of Good Practice
- Based on the 21 Guidelines for Information Security
  - Aligned with the Benchmark
- Eleven specific controls highlighted
  - Identified by Members

Mandatory ***for all external suppliers***

Domains

1. Governance, Risk and Compliance
2. System management
3. Access management
4. System monitoring and response
5. Network connectivity
6. Electronic communication
7. Business control
8. Development

Coverage by domain

Domain	Baseline information security arrangement
Governance, Risk and Compliance	Information security framework
	Information security policy
	Awareness / education
	Information risk management
	Accountability / ownership
System management	Robust resilient design
	Purchase of hardware and software
	Configuration and security settings
	Input / process / output validation
	Physical protection
Access management	Identity and access management
	Access control
Security monitoring and response	Continuous monitoring of systems and networks
	Change management
	Malware protection
	Incident management
Electronic communications	Protection of electronic communications
	Use of cryptographic solutions
Business control	Business continuity
	External supplier management
System development	System Development Life Cycle methodology

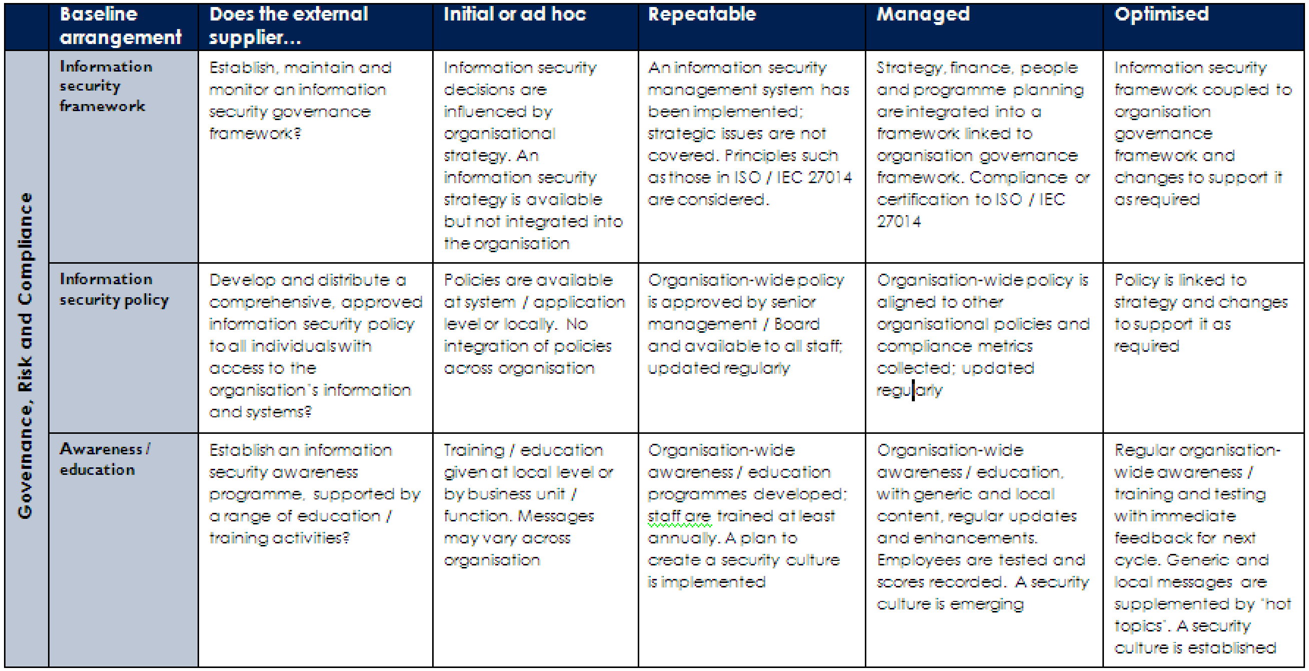
Coverage by domain

Domain	Baseline information security arrangement
Governance, Risk and Compliance	*Identification and protection of information that is commercial, sensitive, regulated or personal in nature*
System management	*Separation of primary functions*
	Separation of client databases / data sets
	Control of portable storage devices
Access management	*Privileged user management*
	Segregation of duties
Security monitoring and response	*Patch management*
	e-discovery, e-forensic audit and trail of evidence creation
Network Connections	*Network security*
	Control of network access / connectivity
Business control	*Security audit and review*

And there’s a maturity model…

The baseline arrangements are described against five categories

- Non-existent
- Initial or ad-hoc
- Repeatable
- Managed
- Optimised

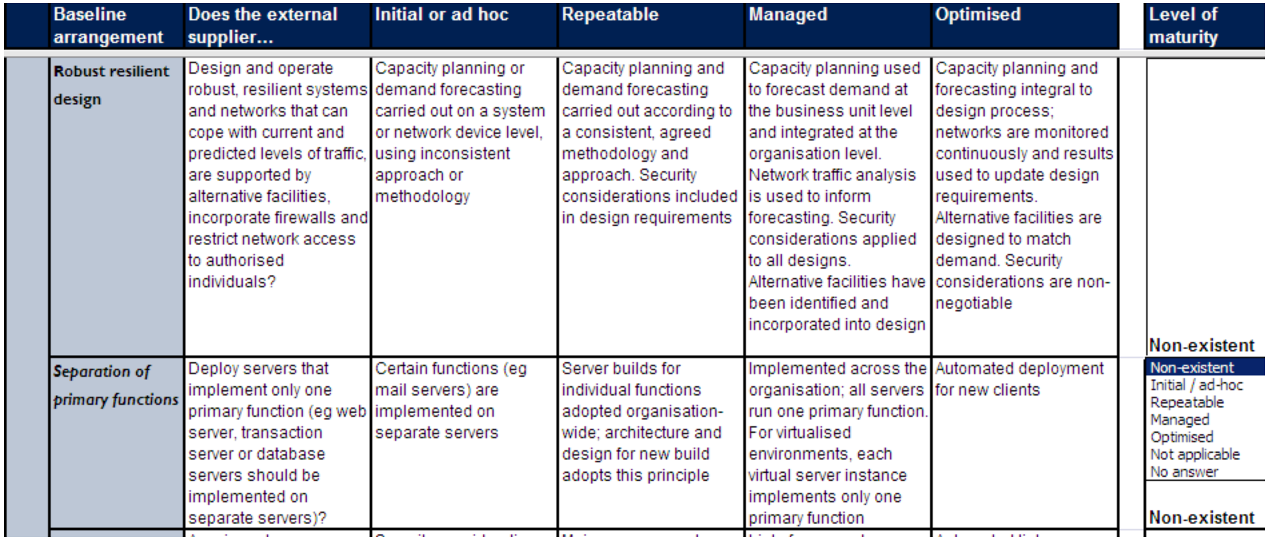


	Baseline arrangement	Does the external supplier…	Initial or ad hoc	Repeatable	Managed	Optimised
Governance, Risk and Compliance	Information security framework	Establish, maintain and monitor an information security governance framework?	Information security decisions are influenced by organisational strategy. An information security strategy is available but not integrated into the organisation	An information security management system has been implemented; strategic issues are not covered. Principles such as those in ISO / IEC 27014 are considered.	Strategy, finance, people and programme planning are integrated into a framework linked to organisation governance framework. Compliance or certification to ISO / IEC 27014	Information security framework coupled to organisation governance framework and changes to support it as required
	Information security policy	Develop and distribute a comprehensive, approved information security policy to all individuals with access to the organisation`s information and systems?	Policies are available at system / application level or locally. No integration of policies across organisation	Organisation-wide policy is approved by senior management / Board and available to all staff; updated regularly	Organisation-wide policy is aligned to other organisational policies and compliance metrics collected; updated regularly	Policy is linked to strategy and changes to support it as required
	Awareness / education	Establish an information security awareness programme, supported by a range of education / training activities?	Training / education given at local level or by business unit / function. Messages may vary across organisation	Organisation-wide awareness / education programmes developed; staff are trained at least annually. A plan to create a security culture is implemented	Organisation-wide awareness / education, with generic and local content, regular updates and enhancements. Employees are tested and scores recorded. A security culture is emerging	Regular organisation-wide awareness / training and testing with immediate feedback for next cycle. Generic and local messages are supplemented by ‘hot topics’. A security culture is established

Acquirers can specify external supplier maturity against this model

Non-existent *not shown – it’s blank!*

Baseline maturity assessment tool



Baseline arrangement	Does the external supplier…	Initial or ad hoc	Repeatable	Managed	Optimised	Level of maturity
Robust resilient design	Design and operate robust, resilient systems and networks that can cope with current and predicted levels of traffic, are supported by alternative facilities, incorporate firewalls and restrict network access to authorised individuals?	Capacity planning or demand forecasting carried out on a system or network device level, using inconsistent approach or methodology	Capacity planning and demand forecasting carried out according to a consistent, agreed methodology and approach. Security considerations included in design requirements	Capacity planning used to forecast demand at the business unit level and integrated at the organisation level. Network traffic analysis is used to inform forecasting. Security considerations applied to all designs. Alternative facilities have been identified and incorporated into design	Capacity planning and forecasting integral to design process; networks are monitored continuously and results used to update design requirements. Alternative facilities are designed to match demand. Security considerations are non-negotiable	Non-existent
Separation of primary functions	Deploy servers that implement only one primary function (eg web server, transaction server or database servers should be implemented on separate servers)?	Certain functions (eg mail servers) are implemented on separate servers	Server builds for individual functions adopted organisation-wide; architecture and design for new build adopts this principle	Implemented across the organisation; all servers run one primary function. For virtualised environments, each virtual server instance implements only one primary function	Automated deployment for new clients	Non-existent Initial / ad-hoc Repeatable Managed Optimised Not applicable No answer Non-existent

- Provides an easy to use tool
- Lists the baseline information security arrangements and provides descriptions of the maturity levels
- Acquirers and external suppliers can measure maturity

External suppliers and the baseline arrangements

- Designed to be adopted in full by external supplier organisations
- Demonstrates commitment to information security
- Reduces the overall complexity of information security
- Allows the focused deployment of resources.

- Benefits:
  - Reduce negotiation required to set information security
  - focus on meeting the acquiring organisation's additional requirements
  - demonstrate their maturity to acquiring organisations
  - offer different levels of information security, based on the maturity required by the acquiring organisation.

ISF AND ISO: THE WAY FORWARD

ISO SC 27: Berlin October 2010

- Body charged with creating and maintaining ISO 270XX series
- ISF has liaison status with WG1 so can:
  - Comment on drafts
  - Submit changes, new ideas
  - Work with national bodies

ISF proposed that the results of this should become an ISO standard

- Very high interest
- Other projects in progress – eg Outsourcing and supply chain, ISO 28000…

Outcomes from Berlin (1)

- Great support for the ISF proposal for a standard on third party relationships
- For legal reasons the term third party has been changed to external suppliers
- A new multi-part standard will be introduced, called 'Information security for supplier relationships'
- Common elements based on the ISF proposal
  - distinctly separate parts for ICT supply chain and outsourcing.

New ISO / IEC standard for information security in supplier relationships

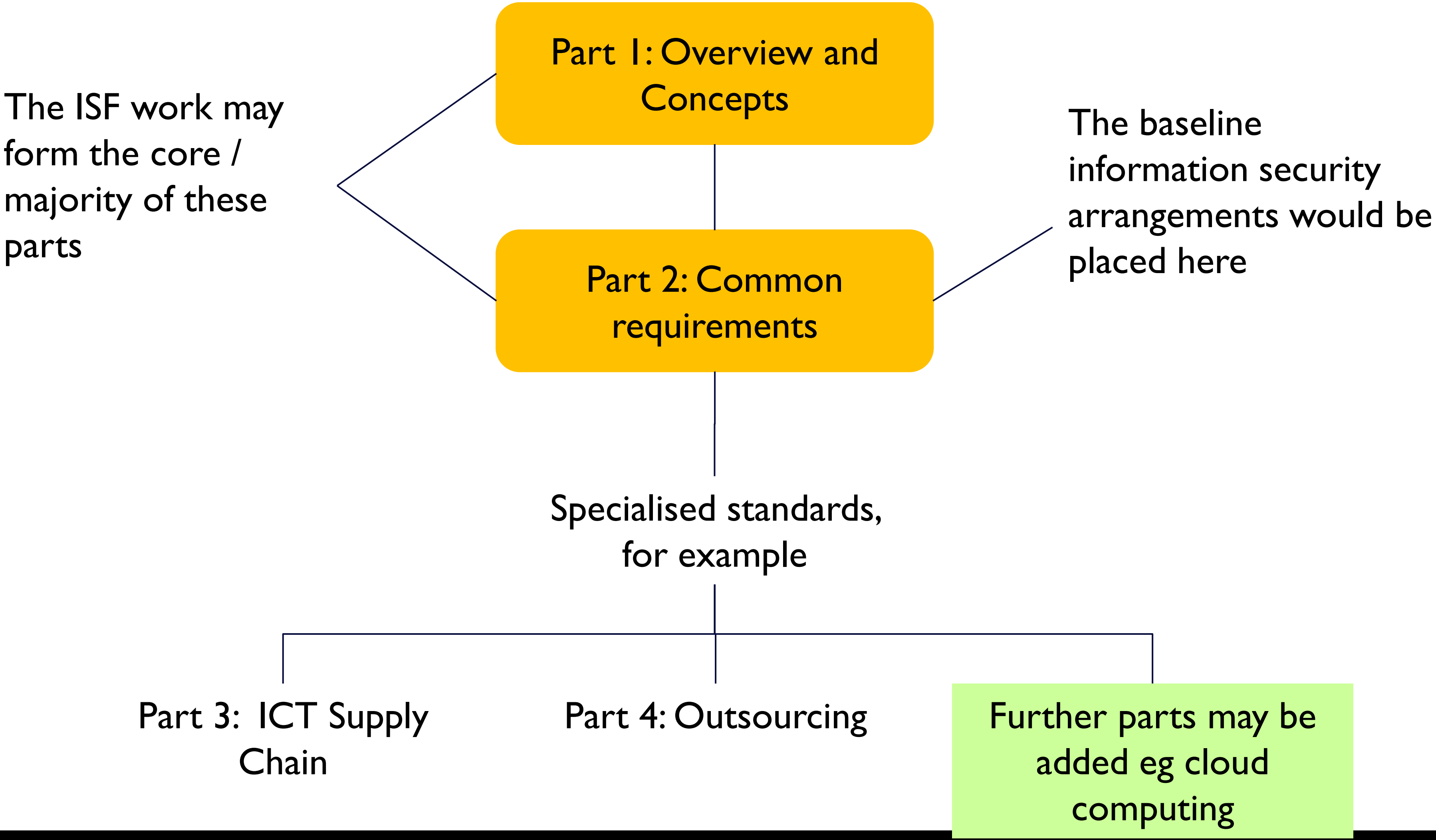
Outcomes from Berlin (2)

- The existing working draft standard on outsourcing (ISO / IEC 27036) will be absorbed by this new standard, but number retained
  - Allows progress to be made more quickly

- ISO keen to have ISF on-board (allowing for their internal rules), which is very encouraging
- Will require on-going ISF resources, and ISF to gain liaison status category C for SC27 WG4, as well as WG1 (already formally applied)

New ISO / IEC standard for information security in supplier relationships:
ISF will have opportunity to shape

Potential form and content of the new standard



The ISF work may form the core / majority of these parts

Part 1: Overview and Concepts

Part 2: Common requirements

The baseline information security arrangements would be placed here

Specialised standards, for example

Part 3: ICT Supply Chain

Part 4: Outsourcing

Further parts may be added eg cloud computing

Thanks!

Information Security Forum

gregory.nowak@securityforum.org

www.securityforum.org

http://uk.linkedin.com/in/adriandaviscitp/