Information
Security
Forum

Securing external suppliers and supply chains: the ISF approach

Dr. Adrian Davis, MBCS, CITP, CISMP

Principal Research Analyst

Information Security Forum

Agenda

- Introduction
- The supply chain: business environment
- The supply chain: infosec perspective
- The ISF approach and baseline
- ISF and ISO – collaboration
- Next steps

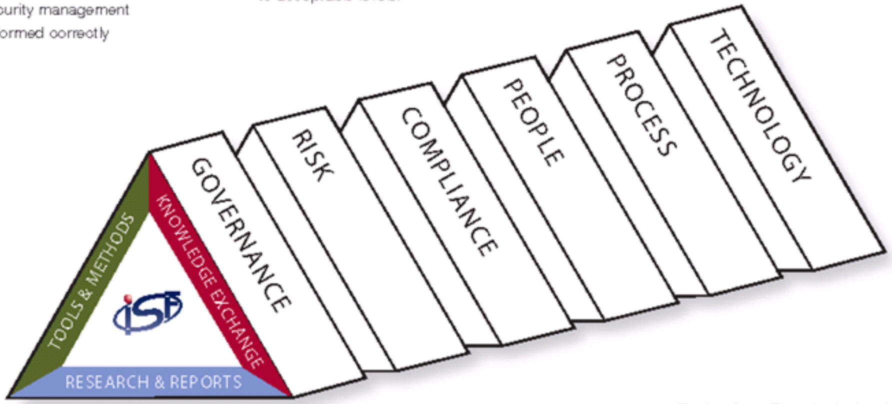
Introduction: Information Security Forum

- A Membership organisation, with 300+ corporate Members spanning the globe and all sectors
- Focus on information security and information risk

Governance The framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently.

Risk The potential business impact and likelihood of particular threats materialising – and the application of control to mitigate risk to acceptable levels.

Compliance The policy, statutory and contractual obligations relevant to information security which must be met to operate in today's business world to avoid civil or criminal penalties and mitigate risk.



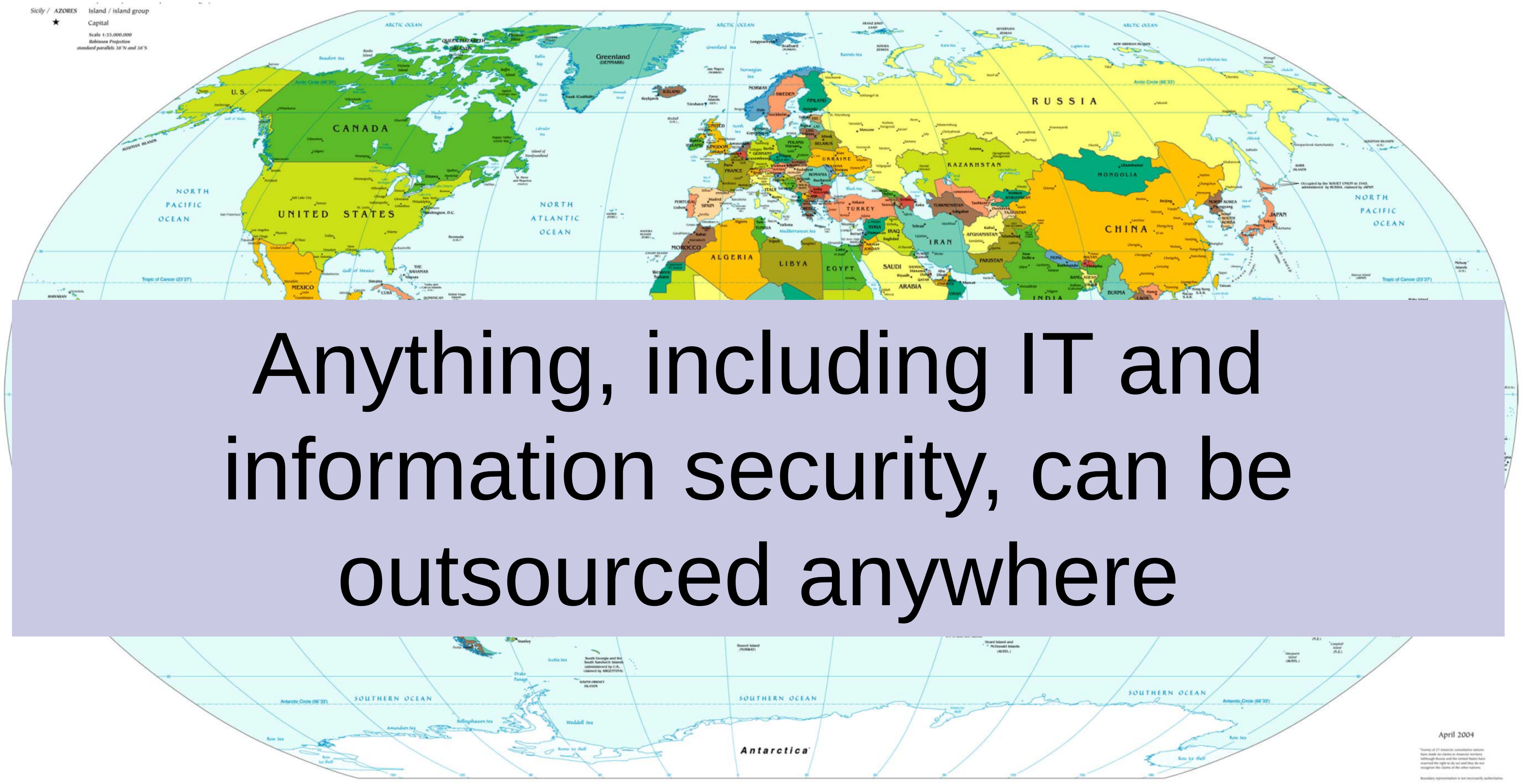
People The executives, staff and third parties with access to information, who need to be aware of their Information Security responsibilities and requirements and whose access to systems and data need to be managed.

Process Business processes, applications and data that support the operations and decision making.

Technology The physical and technical infrastructure, including networks and end points, required to support the successful deployment of secure processes.

THE SUPPLY CHAIN: BUSINESS ENVIRONMENT

The world is flat...

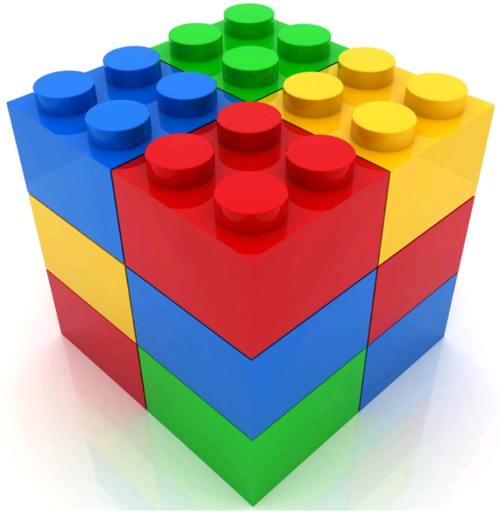


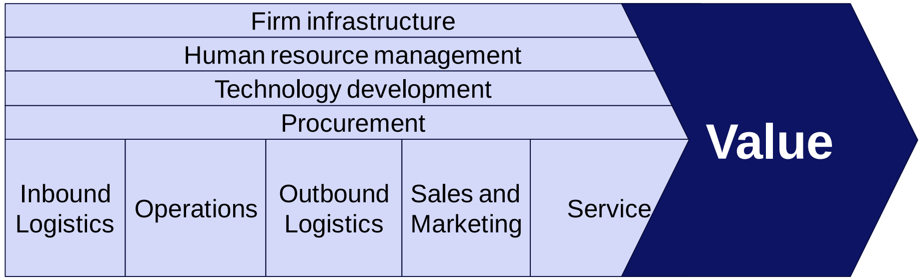
Anything, including IT and information security, can be outsourced anywhere

(With apologies to Thomas Friedman)

From value chain to corporate LEGO®

- Single, vertically integrated organisation
- Did everything and provided everything
- Diverse, management –heavy, operations (cost of coordination)

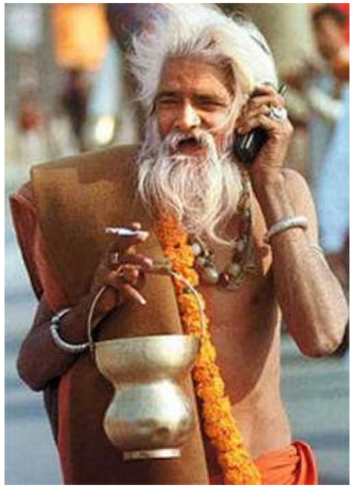


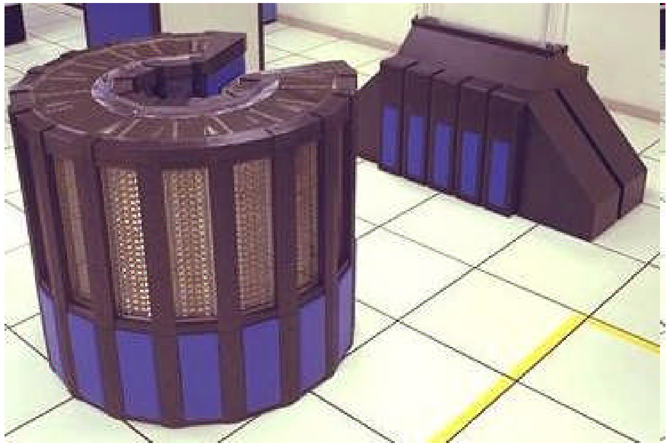


- Outsourcing means that organisations can assemble, break apart and reassemble themselves using different components
- Focus on core competences
- The supply chain can also be similarly reconfigured

From mainframe to commodity

- Services accessed across a network by a user at a 'dumb' terminal
- Multiple applications
- Multiple users
- Charged on a per-use basis





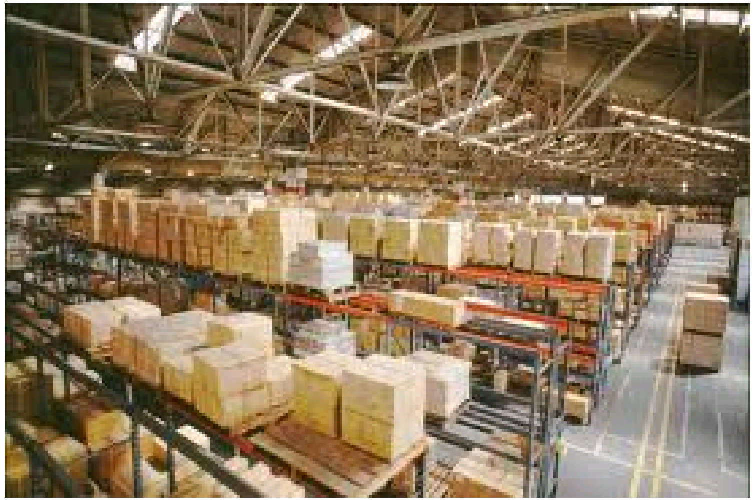
- Relentless technological innovation
- The rise of the 'app'
- Availability, affordability, connectivity, interactivity...

From data centre to cloudification...

- Specialised, highly specified, purpose built facilities
- Often owned by the organisation or provided as part of an outsourcing deal
- Fairly easy to audit and monitor

- Black box – the service is bought 'as is'
- Opportunity to specify is lower
- Your suppliers may be using the cloud
- Audit and monitoring may be very different

From in stock to just in time



- Wasting asset – stock takes up space, time and cash
- Opportunity for shrinkage and obsolescence
- Information is concentrated in warehouses

- Logistics is king
- Minimal storage overhead
- Reduced shrinkage and obsolescence
- Information has to be freely shared across supply chain

THE SUPPLY CHAIN: INFOSEC PERSPECTIVE

The scale of the challenge

Members organisations typically work in **>50** jurisdictions

83% outsource functions such as IT, HR or payroll

55% outsource business processes

A typical Member organisation has over **2030** external supplier relationships

Key findings from ISF studies

25% highly or very highly satisfied with the level of controls in non-critical external suppliers

52% are highly or very highly exposed to external supplier risks

70% do not have a complete inventory of external suppliers

27% highly or very highly satisfied with the level of controls in critical external suppliers

72% highly concerned about external supplier security arrangements

37% outsource information security, wholly or partially

... And we can’t specify a standard of protection...

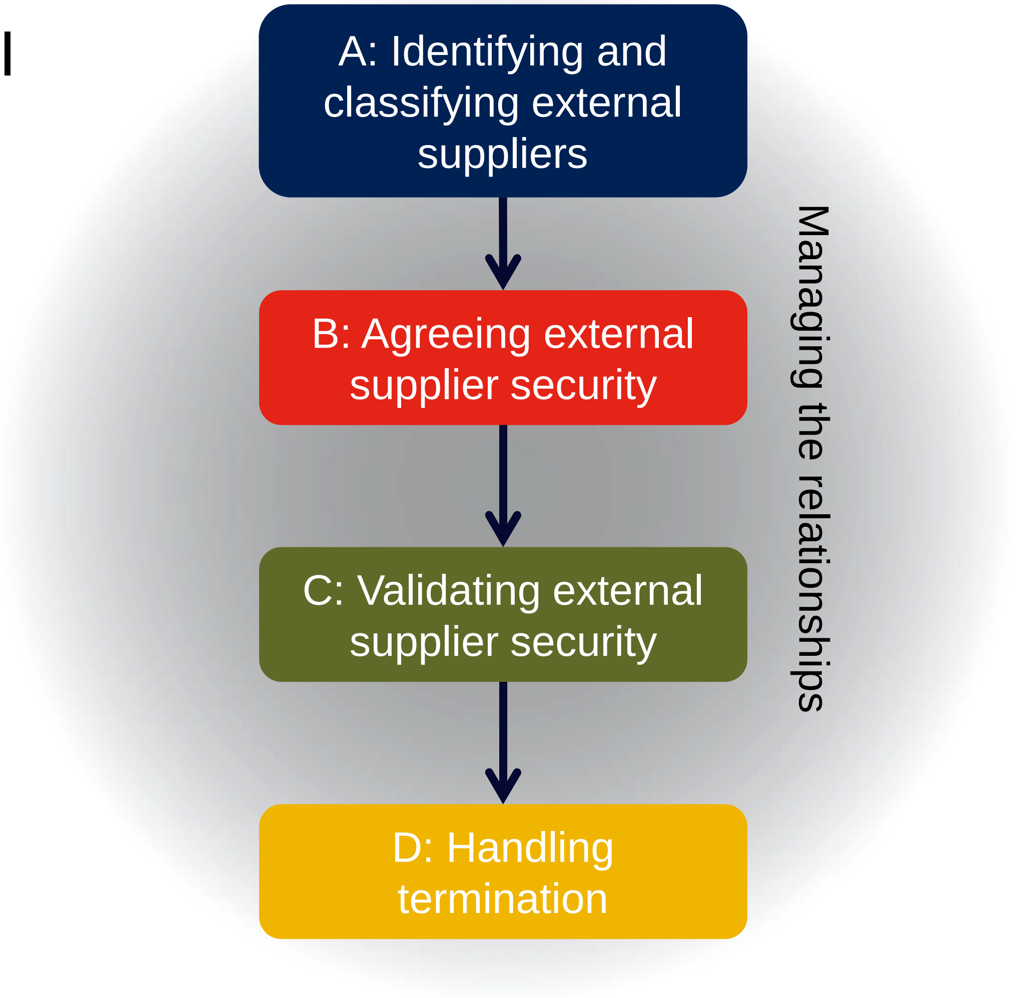
- There are many out there:
  - Outsourcing standards (IAOP OSP v8.0, Healthcheck)
  - Security Standards (SOGP, ISO 2700X series, BITS SIG)
  - IT Standards (COBIT, ITIL, ISO 20000)
  - Other standards (ISO 28000, ISO 25999 / ISO 27031)
  - Auditing standards (SAS 70, ISAE 3402)

- 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

THE ISF APPROACH AND BASELINE

Developing an organisational response

1. Identify and classify external suppliers (BIA/risk-driven)
2. Define a baseline of information security and privacy arrangements
3. Validate external supplier information security and privacy arrangements regularly
4. Plan for the end


A: Identifying and classifying external suppliers
B: Agreeing external supplier security
C: Validating external supplier security
D: Handling termination
Managing the relationships

Information security baseline arrangements

Based on:

- Input from over 300 organisations
- ISF 21 Guidelines for Information Security
    - Aligned with the Standard of Good Practice and Benchmark

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

ISF Standard of Good Practice: External Suppliers

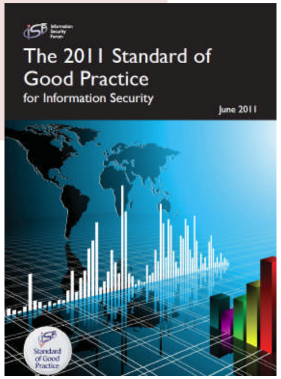
CONTROL FRAMEWORK

FUNDAMENTAL

AREA CF16 – External Supplier Management

List of Topics

CF16.1 External Supplier Management Process
CF16.2 Hardware / Software Acquisition
CF16.3 Outsourcing
CF16.4 Cloud Computing Policy
CF16.5 Cloud Service Contracts


The 2011 Standard of Good Practice for Information Security
June 2011
Standard of Good Practice

Measuring external supplier security: ISF Tools

Baseline Maturity Assessment Tool (BMAT)

- provides **a governance level** summary of the maturity of an external supplier's baseline information security arrangements
- BMAT tells you **how good** the external supplier is

Third Party Security Assessment Tool (TPSAT)

- provides a **detailed assessment** of an external supplier's baseline information security arrangements
- TPSAT tells you if a **control is present** in the external supplier

Both tools cover the four-step ISF organisational response

What’s in it for me? – the ISF approach

Acquirer / Buyer

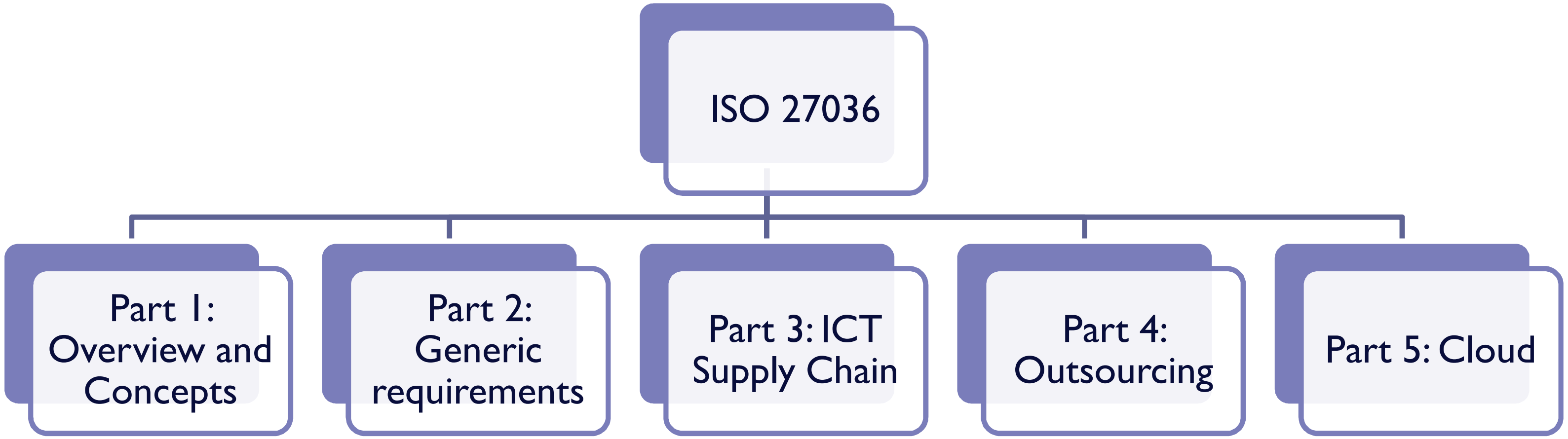
- Understand your capability
- Define what I want in my contract
- Measure and hold suppliers to account (audit!)
- Discuss improvements
- Provide assurance to my bosses and regulators…

Supplier

- Set our baseline
- Report against that baseline
- Demonstrate how good we are
- Provide extra services based on a strong foundation
- Manage multiple responses and audits

ISO AND ISF – COLLABORATION

A global response: ISO / IEC 27036



A new multi-part standard, called: ‘Information security for supplier relationships’

- ISF heavily involved in its development and in producing content
  - ISF joined SC27 Working group in October 2010
  - ISF also helping JNSA with the Part 5: Cloud
- Working to harmonise ISF and the ISO efforts for maximum benefit

Development of ISO 27036

ISF Information security baseline arrangements adopted in Part 2

Most ISF recommendations accepted:

- Shaping Part 1 Concepts, and Part 2 Generic Requirements – both of which are normative requirement documents, meaning they are mandatory and can be used for certification purposes (like ISO 27001)

ISF continue to provide ISO (working group only) excerpts from ISF documents as input only

- For example, ISF Cloud, BMAT and TPSAT

New MX area to be launched end 2011 to capture Member comments on future drafts electronically

NEXT STEPS

Future work

External suppliers

- Continued liaison with and input into ISO/IEC 27036
- ISF External Supplier SIG
  - Next teleconference in December
  - Members will have the opportunity to comment on ISO/IEC 27036
- Further refinements to ISF tools

Supply Chain Paper

- New initiative
- Examines how ISF can support Members secure their supply chain
- Several options proposed, including:
  - ISF Supply chain toolkit
  - Alliances with other organisations (not just ISO)
- Decision in Q1 2012

Information Security Forum

adrian.davis@securityforum.org

www.securityforum.org

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