Information
Security
Forum

Supply Chain Assurance Framework

The translator for supply chain standards

Adrian Davis

Principal Research Analyst

Information Security Forum

Information Security Forum (ISF)

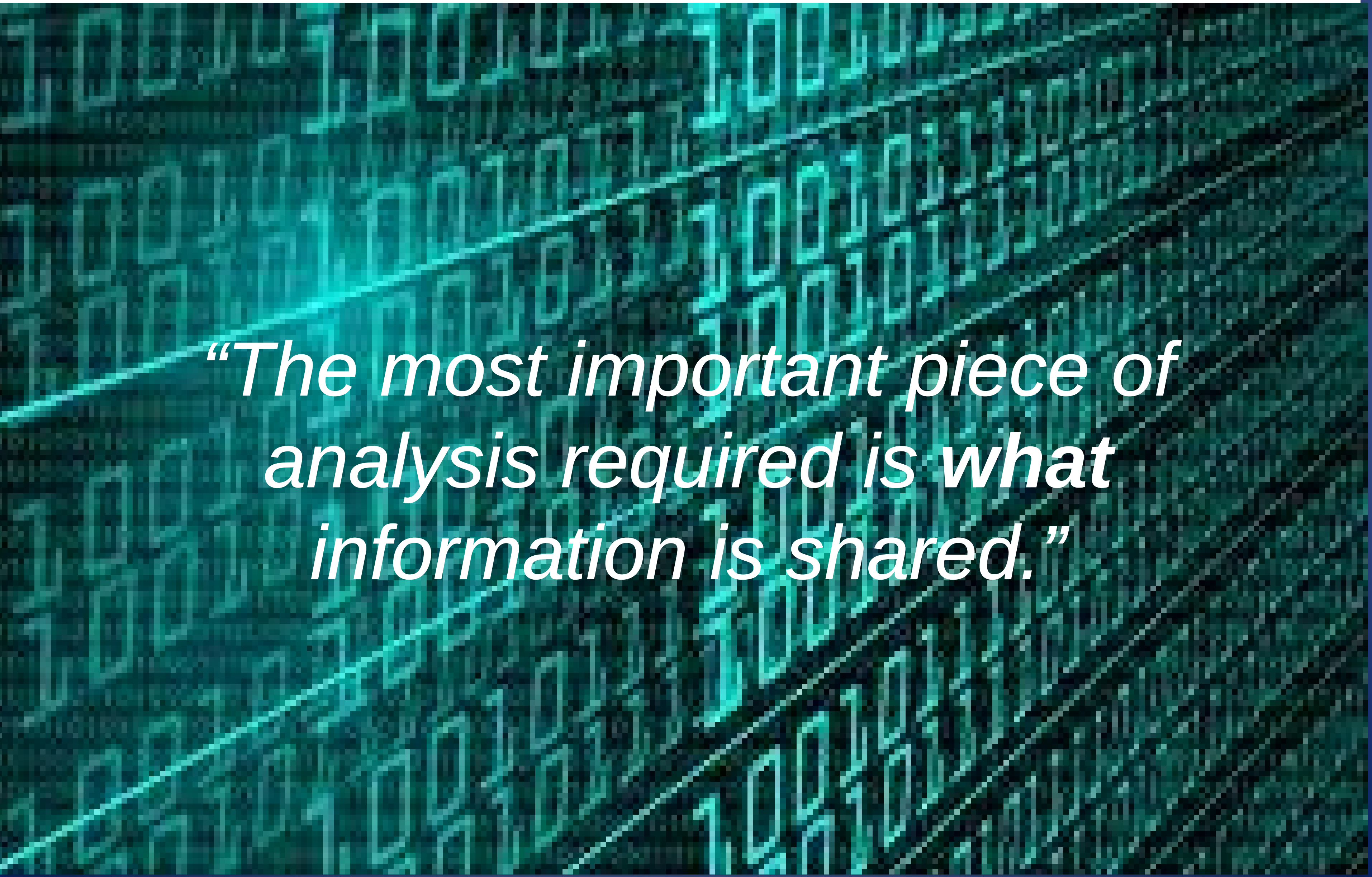
- An international association established in 1989 and now with some 320 leading global organisations, which...
- is wholly independent, driven and owned by its Members
- addresses key issues in information risk management through research and collaboration
- develops practical tools and guidance
- promotes networking within its membership.

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

Today’s biggest information security challenges

- External threats, criminals, activists
- Visibility and influencing senior executives and the Board
- Keeping pace with business strategy and managing risk
- Mobility – people, devices, information
- Secure Cloud computing
- Protecting information in your Supply Chain

THE INFORMATION SECURITY PERSPECTIVE



*“The most important piece of analysis required is **what** information is shared.”*

1. Lack of awareness of the sensitive information being shared in contracts

- Organisations may not understand how information is shared and the information and assets suppliers can access
- Information to be shared may be agreed in the contract
- But products and services change and so does the shared information
- Typically little visibility of the information shared upstream (ie Tier 2 and beyond)

Information typically shared in the Supply Chain

- Personally identifiable information
- Intellectual property
- Commercial information
- Logistical information
- Management information
- Legal, regulatory and privileged information

All valuable, sensitive or regulated

If not protected by your Suppliers your organisation is exposed to loss and consequential sanctions

You can’t outsource the risk

"Our procurement function doesn't handle anything less than £5 million.."

2. Too many contracts to assess individually

- ISF Members have thousands of Tier 1 (direct) suppliers
  - Highest number: ~120,000
- Deliver everything from towels to Big Data capability
- Typically, the focus is on contract size

- Contracts are a poor measure –
  - What about corporate credit cards?
  - Business unit or regional procurement?

*“Beyond your direct suppliers,
you face a black hole…”*

3. Lack of visibility and controls as information is shared in the supply chain

http://www.flickr.com/photos/amerigo/526435438/

Today’s biggest information security challenges

- Ex
- Vi
- Ke
- M
- Se
- Protecting information in your Supply Chain

With enough funds and capable resources, all can be managed –

Except the last!

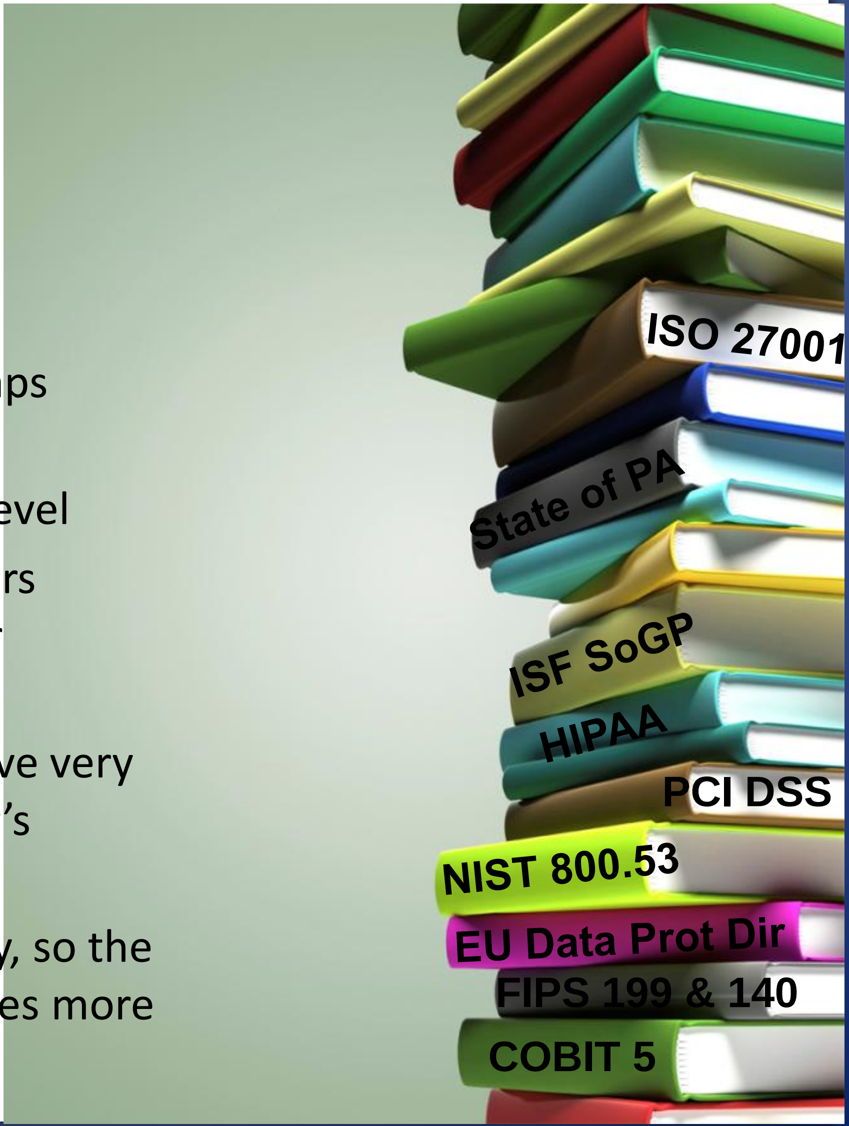
Barriers to protecting information in the Supply Chain can’t be resolved by any organisation in isolation – we have an “industry” issue

THE INDUSTRY PERSPECTIVE

THE “industry” issue ...

Background

- Over 50 information security standards and over 550 laws and regulations
- All different but with substantial overlaps ... but no easy way to grasp the overlaps & gaps
- No ISO standard for Supply Chain InfoSec yet ... but ISO 27036 (due Q3 2013) is very high level
- Organisations define requirements of suppliers ... but probably won’t be understood by their Suppliers
- Some Industry & regulatory requirements have very high penalties for non-compliance – Acquirer’s exposure!
- As organisations manage risk better internally, so the Supplier information risk “black hole” becomes more apparent



The Industry issue ...

Leads to:

- Acquirers defining unique requirements for Suppliers
  ... but Suppliers finding little commonality across their clients
- Suppliers facing an array of requirements from their clients (see E&Y report for NASCOM / DSCI India)
- Cost and inefficiencies imposed on Suppliers
- Auditors can’t agree scope to report to Acquirers
- Assurances sought by Acquirers either not provided
  ... or expressed in language / standards not understood
  ... so they can’t relate to their own requirements

- That is why it is so difficult to agree requirements in contracts

A NEW INITIATIVE: SUPPLY CHAIN ASSURANCE FRAMEWORK

ISF, IAOP and others collaborating on ....

... a solution:

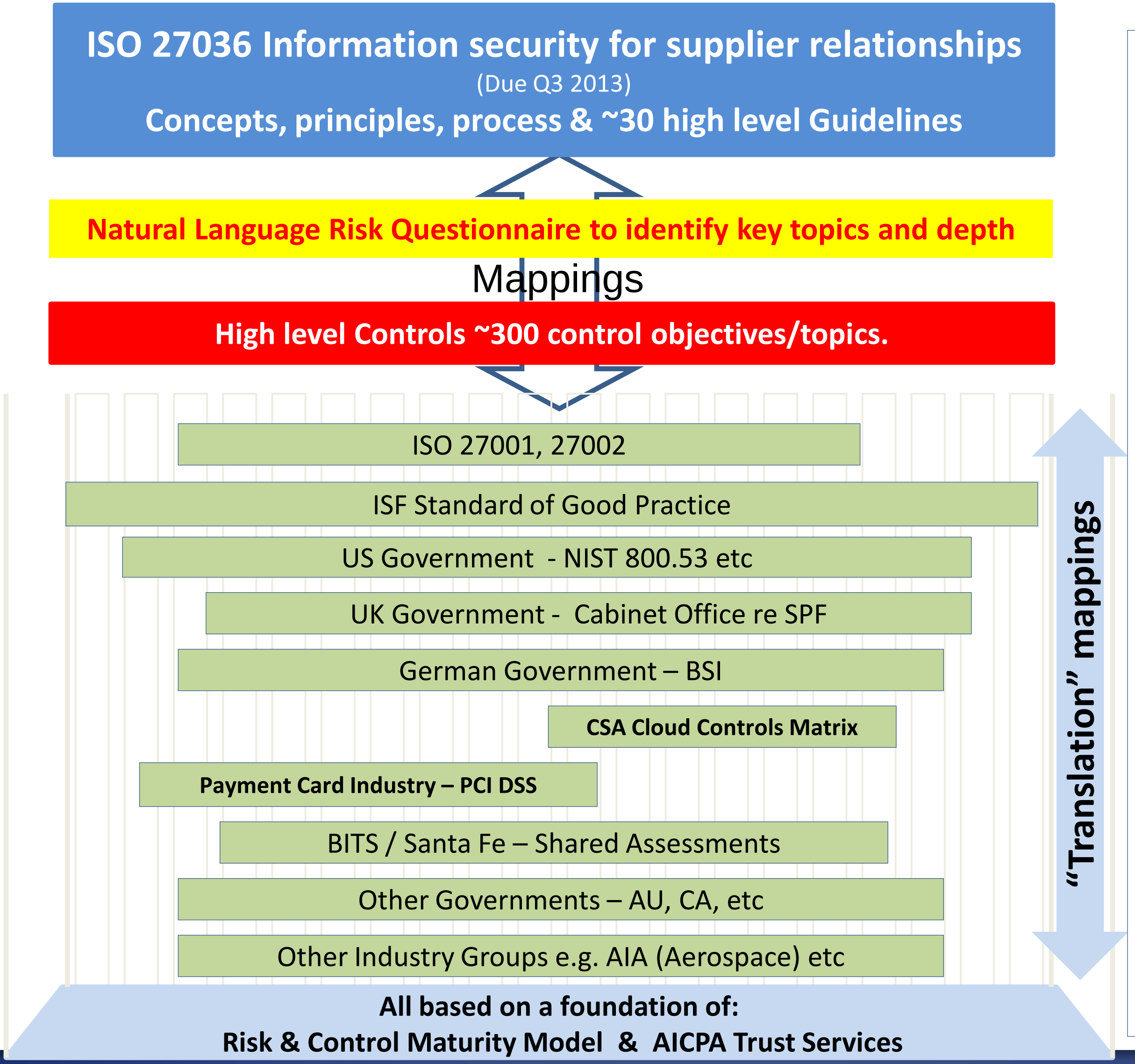
1. Not another security standard!
2. An open framework to enable organisations to “translate” and compare requirements of one standard or law relative to another
3. A risk and maturity model to identify suitable requirements and reporting frequencies
4. Enabling Acquirers to define requirements using their own standard and regulations

ISF, IAOP and others collaborating on ....

... a solution:

5. Enabling Suppliers to translate / compare Acquirer requirements against their own standard & approach and identify gaps
6. Enabling Suppliers to confidently appoint auditors to independently attest (SSAE16/AS3402) against their own standard and approach
7. Enabling Suppliers to provide assurance expressed in their own standards and approach knowing if they meet Acquirer requirements
8. Acquirers being able to translate assurances received from Suppliers to their own to assess if their requirements are met

The model



ISO 27036 Information security for supplier relationships

(Due Q3 2013)

Concepts, principles, process & ~30 high level Guidelines

Natural Language Risk Questionnaire to identify key topics and depth

Mappings

High level Controls ~300 control objectives/topics.

ISO 27001, 27002

ISF Standard of Good Practice

US Government - NIST 800.53 etc

UK Government - Cabinet Office re SPF

German Government – BSI

CSA Cloud Controls Matrix

Payment Card Industry – PCI DSS

BITS / Santa Fe – Shared Assessments

Other Governments – AU, CA, etc

Other Industry Groups e.g. AIA (Aerospace) etc

"Translation" mappings

All based on a foundation of:
Risk & Control Maturity Model & AICPA Trust Services

Outcomes:

1. Risk management
2. Acquirer requirements risk driven - "menu" controls selection
3. Suppliers to translate requirements & compare to own / existing approach – identify gaps
4. Clear Audit / Assurance requirements
5. Audit reports useful for multiple Acquirers
6. Acquirers translate assurances and identify any gaps

Process simplified,
Costs reduced,
Risks managed

How SCAF can help an Acquirer

- Provides a risk model that can be used by procurement and legal staff for predictable and lower risk transactions
  - Defines information security requirements without reference to Information Security experts
- Assists Acquirers to identify areas of greater risk for more detailed assurances from Suppliers
- Provides an assessment of residual information security risk against information types

How SCAF can help a supplier

- Allows a Supplier to identify and cite controls specified in different standards as being equivalent to those demanded by the Acquirer
- Enables an “audit once reuse many times” approach to assuring Acquirers on security requirements

Framework Implementation

- Release planned for Q2 2013
- Will help you define standards and regulation appropriate to new or renewed outsourcing or procurement contracts
- Work with your Information Security team:
  - to adapt the risk model and select controls appropriate to your organisations' risks
  - to define frequency of reporting for given risk types and levels
  - to decide if an independent audit or inspections are required
  - to build requirements into your contract templates
- Promote the framework to your counterparties as a means for them to understand your requirements in their "language"
- IAOP input through Pat Fisher, who chairs the IAOP Data Security chapter

Information Security Forum
adrian.davis@securityforum.org
www.securityforum.org
http://uk.linkedin.com/in/adriandaviscitp