SUPPLY CHAIN ASSURANCE FRAMEWORK: THE SUPPLY CHAIN STANDARDS TRANSLATOR

Michael de Crespigny, CEO
Information Security Forum

Security in knowledge

Session ID: GRC-R02B
Session Classification: General Interest

RSA CONFERENCE EUROPE 2013

KEY ISSUE

Our Members tell us there is:

- Confusion and / or frustration amongst acquirers and suppliers
  - Dealing with differing and inconsistent InfoSec requirements
- Inefficiency as a result of suppliers being asked by acquirers to provide assurance against varying standards and / or specifically defined requirements / policies
- Eroded value of suppliers' assurances and / or certification
  - Because acquirers can't compare the suppliers' arrangements with their requirements
- And we've validated this externally

SUPPLY CHAIN ASSURANCE FRAMEWORK

- ISF initiative with industry stakeholders to address these problems
- Develop solution to improve understanding of requirements and acceptability of assurances

Stakeholders involved to:

- Input to and validate design
- Launch and promote to their constituency

Outcomes:

- Improved supply chain risk management
- Reusability of certifications and audit reports (eg SOC2)
- Lower costs

SOME OF THE STAKEHOLDERS INVOLVED IN SCAF

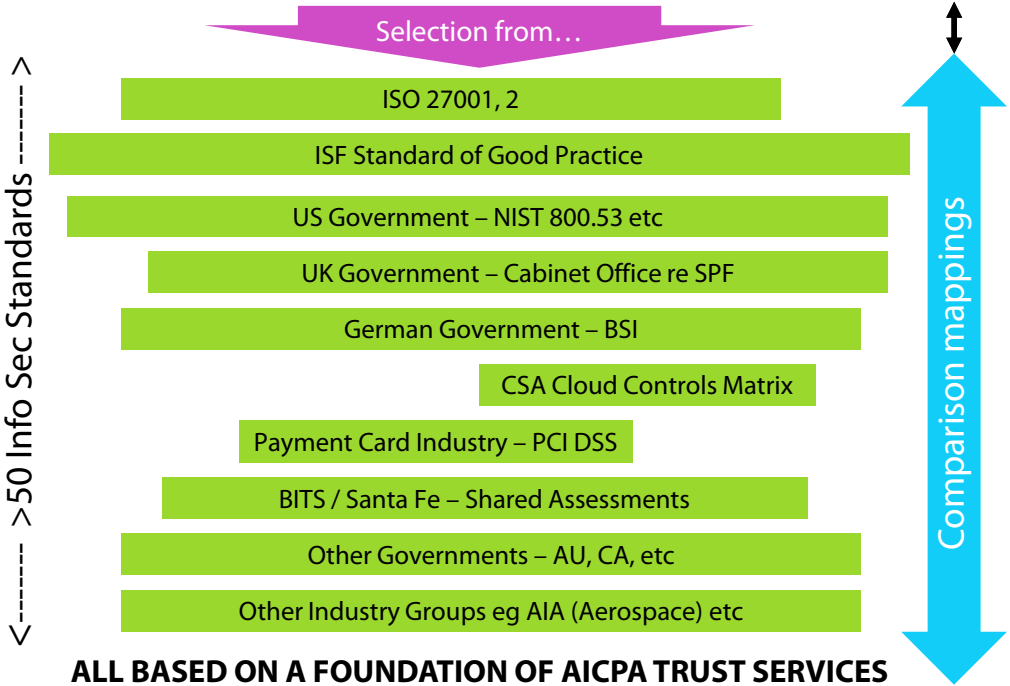
COMPONENTS

Common standards used to identify key information security requirements

WHAT IS CURRENTLY MISSING

Enablers:

- ISO 27036
- People & experience: ISACA, $(ISC)^2$
- AICPA attest standards SSAE16 / ISAE3402 & Trust Services principles
- Recognised maturity model to underpin assurance
- Audit firms
- Procurement professionals
- Contract term templates
- Supply chain / vendor management organisations



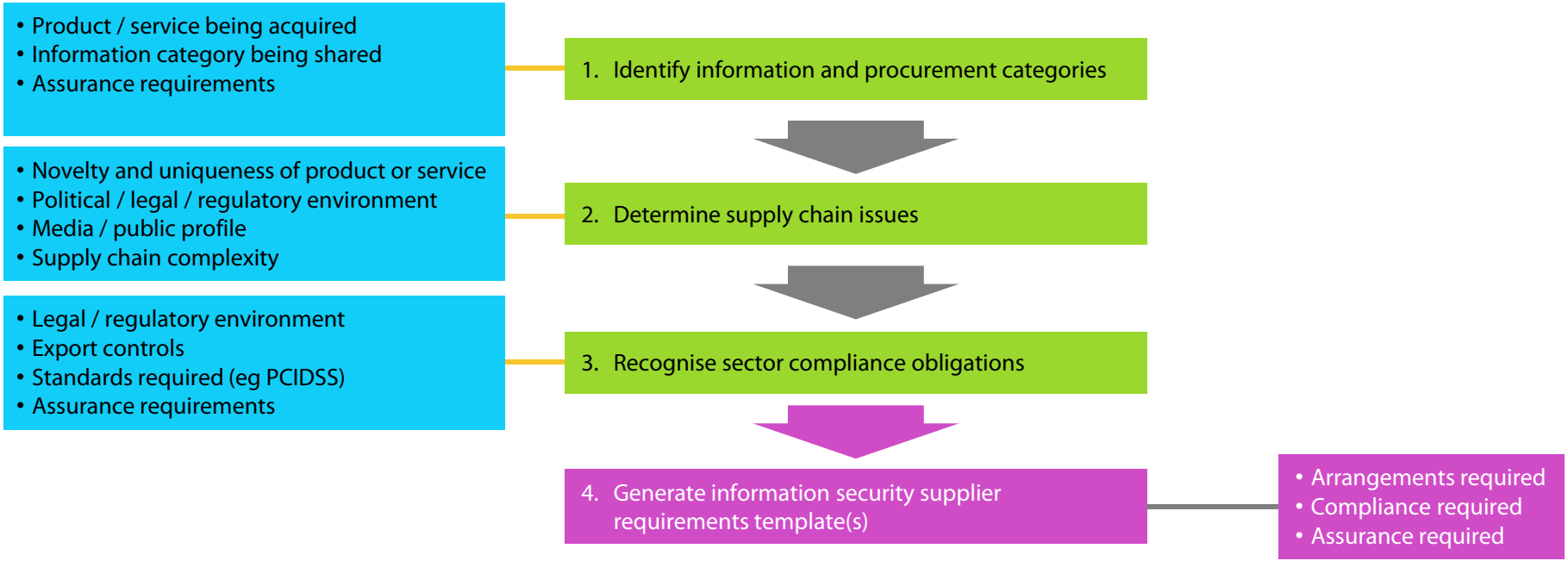
ALL BASED ON A FOUNDATION OF AICPA TRUST SERVICES

Outcomes:

- Effective risk management
- Acquirer requirements defined (risk driven)
- Providers able to translate requirements to own / existing approach – gap identification
- Clear audit / assurance requirements
- Audit reports / SOC2 / Certificates acceptable to multiple acquirers
- Acquirers translate assurances and identify gaps / remedial action
- Process simplified, costs reduced, risks managed

SUPPLIER REQUIREMENTS DEFINITION

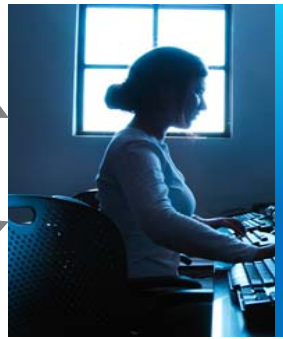
- A framework to define the information security arrangements required of suppliers



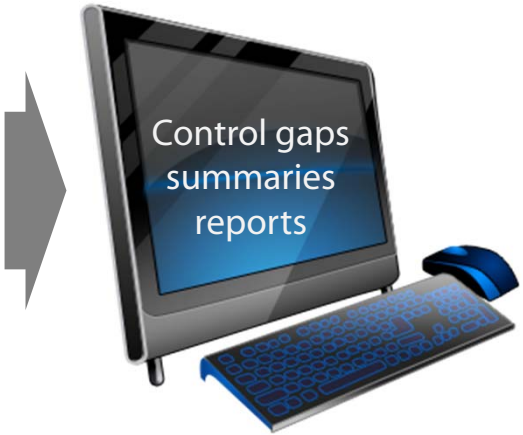
STANDARDS COMPARISON – SAAS

Acquirer Information security supplier requirements

Supplier security in place



Standards comparison tool website



To be used by both suppliers and acquirers

INFORMATION SECURITY STANDARDS COMPARISON

- Used by **suppliers** to compare acquirer information security requirements to their existing information security arrangements.
  - Relevant during the bidding process and when requirements change or assertions are sought
- Used by **acquirers** to compare submissions and identify any requirements not met by suppliers
- Used by information security professionals to compare arrangements and requirements
  - Only they can assess the significance of gaps in the context of information risk

BENEFITS

1. Provides a risk model that can be used by procurement and legal staff for predictable and lower risk transactions
2. Builds information risk and control into procurement
3. Assists acquirers to identify areas of greater risk for more detailed assurance from a supplier
4. Suggests appropriate controls to mitigate common information risks within the supply chain
5. Allows suppliers to identify and cite controls specified in different standards as being equivalent

DELIVERABLES

- Supplier requirements definition
- Standards comparison tool website
- Supporting collateral

Launch & public availability

- **Public domain** – not just for ISF Members
- Free to use to optimise acceptability
- Will have its own LinkedIn group
- Material and links will be downloadable from its own website
- Launch timed around ISO/IEC 27036: **Q1 2014**
- Follow the development on www.securityforum.org

WHAT YOU CAN DO

1. Join our stakeholder group to help refine and test SCAF
   - Contact me: michael@securityforum.org
2. Deploy SCAF in your organisation on launch

Thank you!

Michael de Crespigny
Information Security Forum

michael@securityforum.org

Telephone: +44 20 7212 1796

Mobile: +44 7837 352 661

www.securityforum.org

#RSAC

RSA CONFERENCE EUROPE 2013