Securing the Supply Chain: Guide to Risk Management

ADRIAN DAVIS

INFORMATION SECURITY FORUM

Session ID: GRC-201B

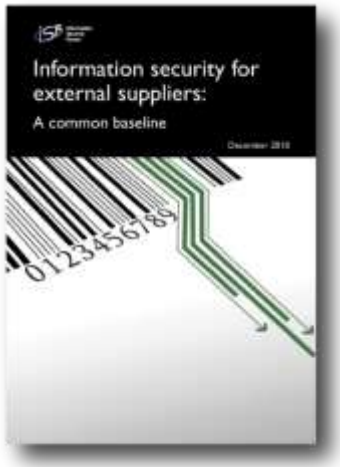
Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

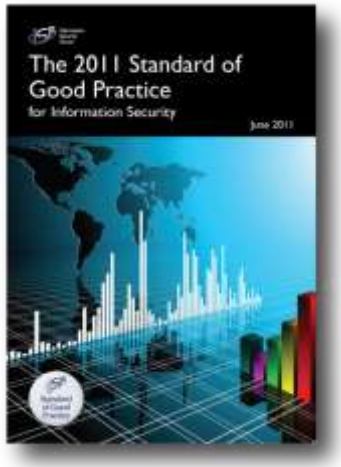
Introduction

Introduction

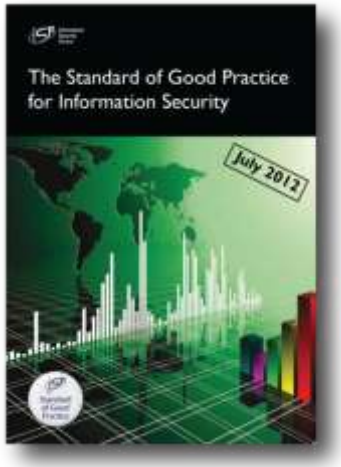
- Presentation based on research across the ISF's 310+ Members
  - Scope: global, covering all sectors
- Builds on our previous work:



Information security for external suppliers: A common baseline (2010)

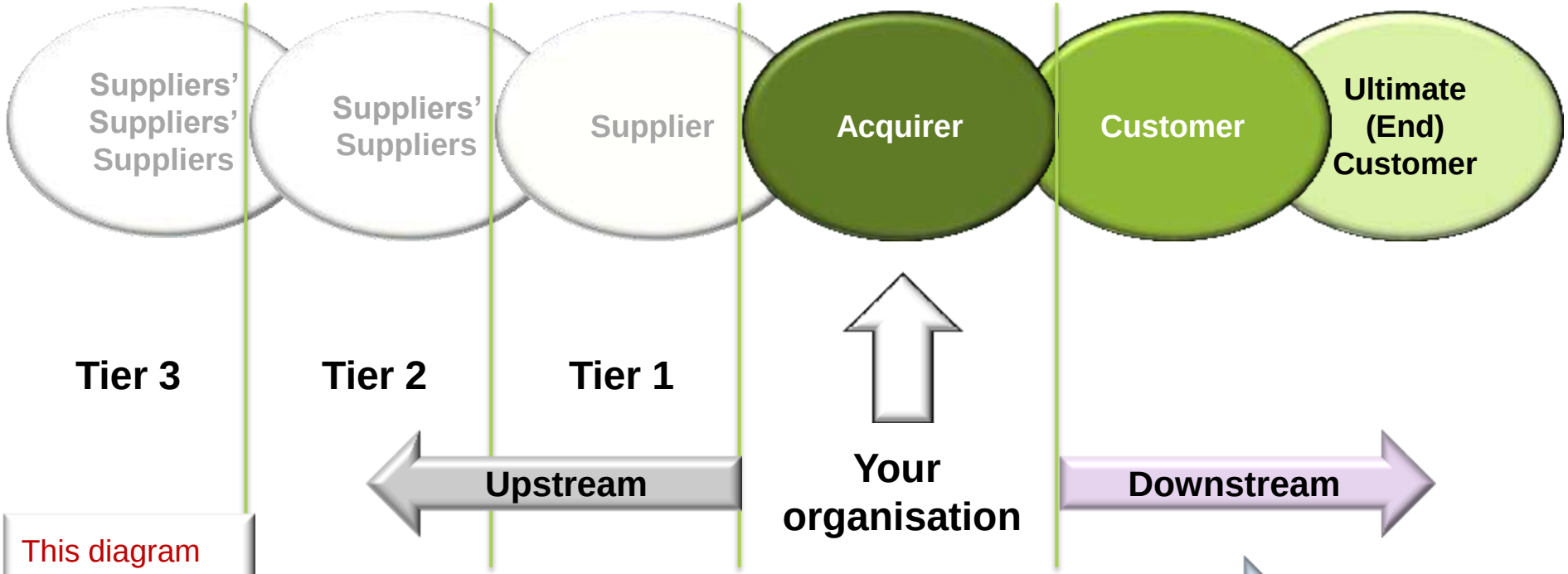


The Standard of Good Practice for Information Security (2011)



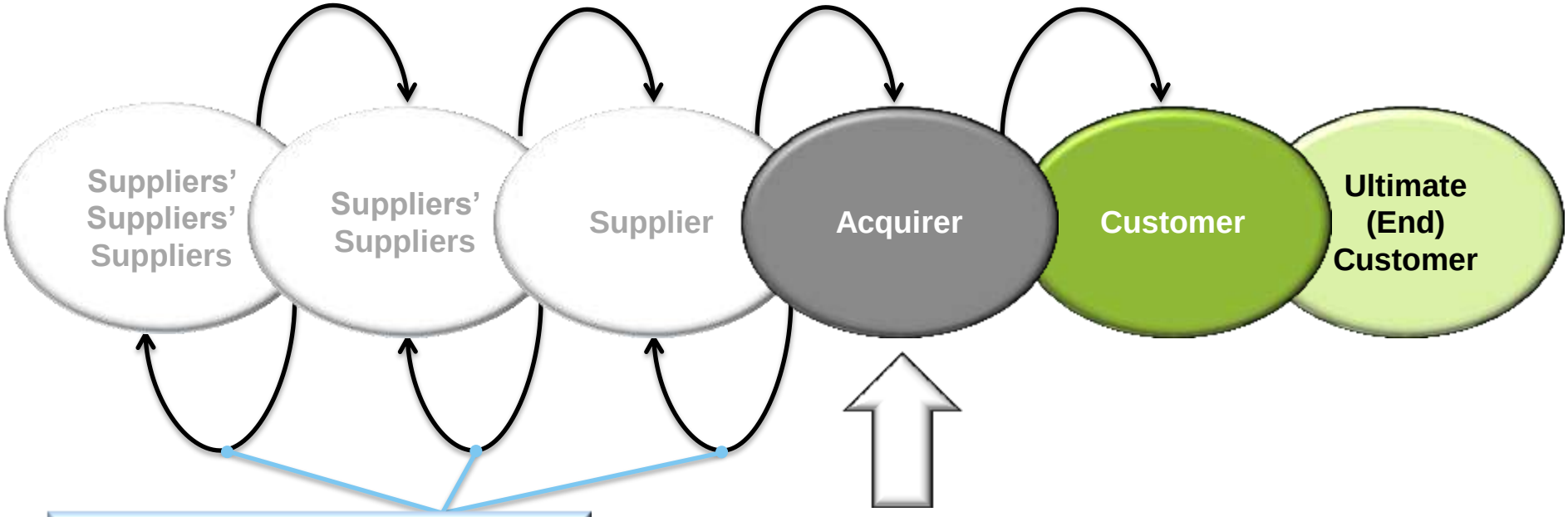
The Standard of Good Practice for Information Security (2012)

A typical supply chain



This diagram has been adopted by ISO for the upcoming ISO/IEC 27036 standards

Supply chain: the information risk view



Shared information:

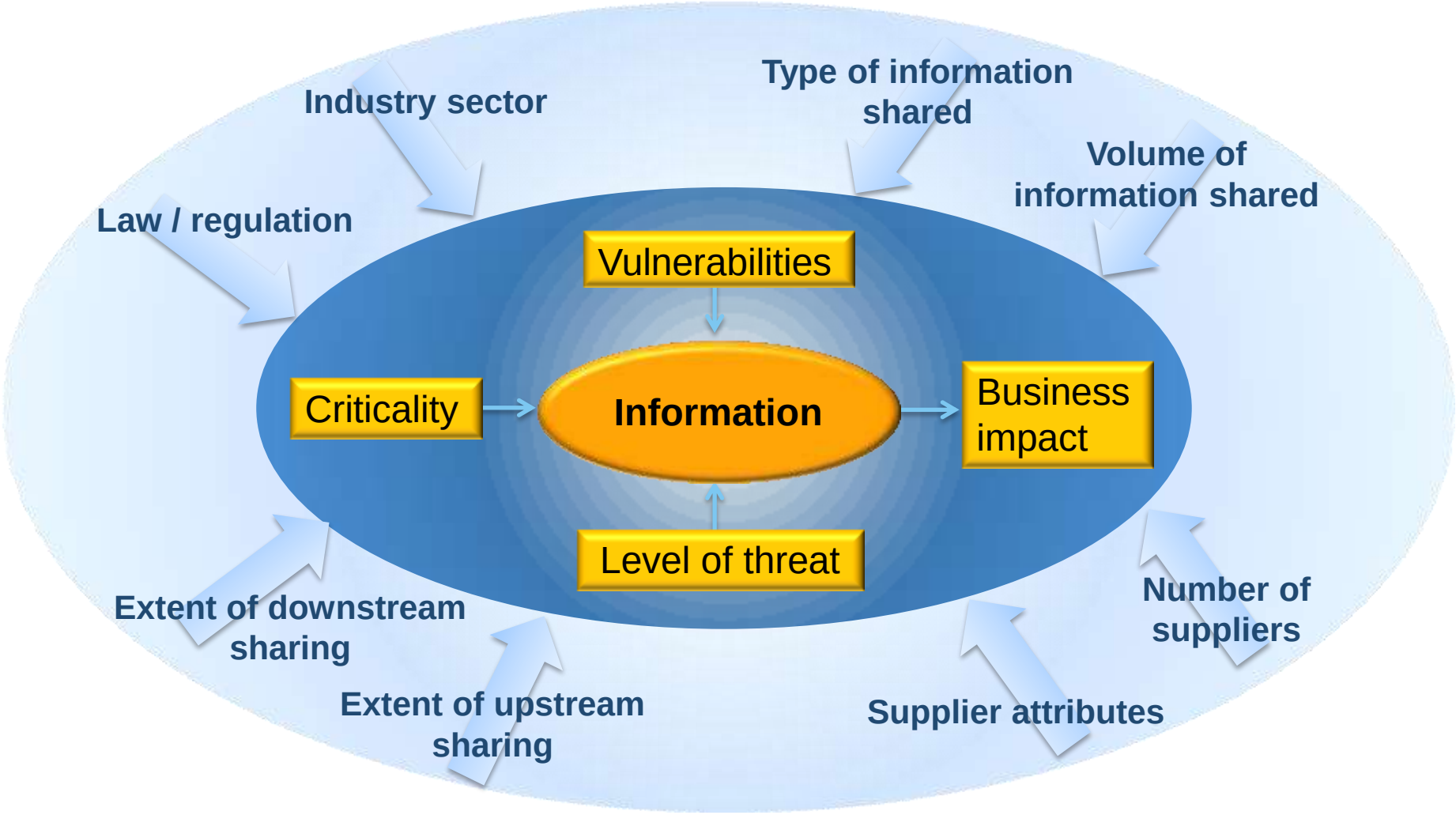
- Personally identifiable
- Intellectual property
- Commercial
- Logistical
- Management
- Legal, regulatory and privileged

Your organisation

90% of suppliers are upstream of tier 1

Building in information risk

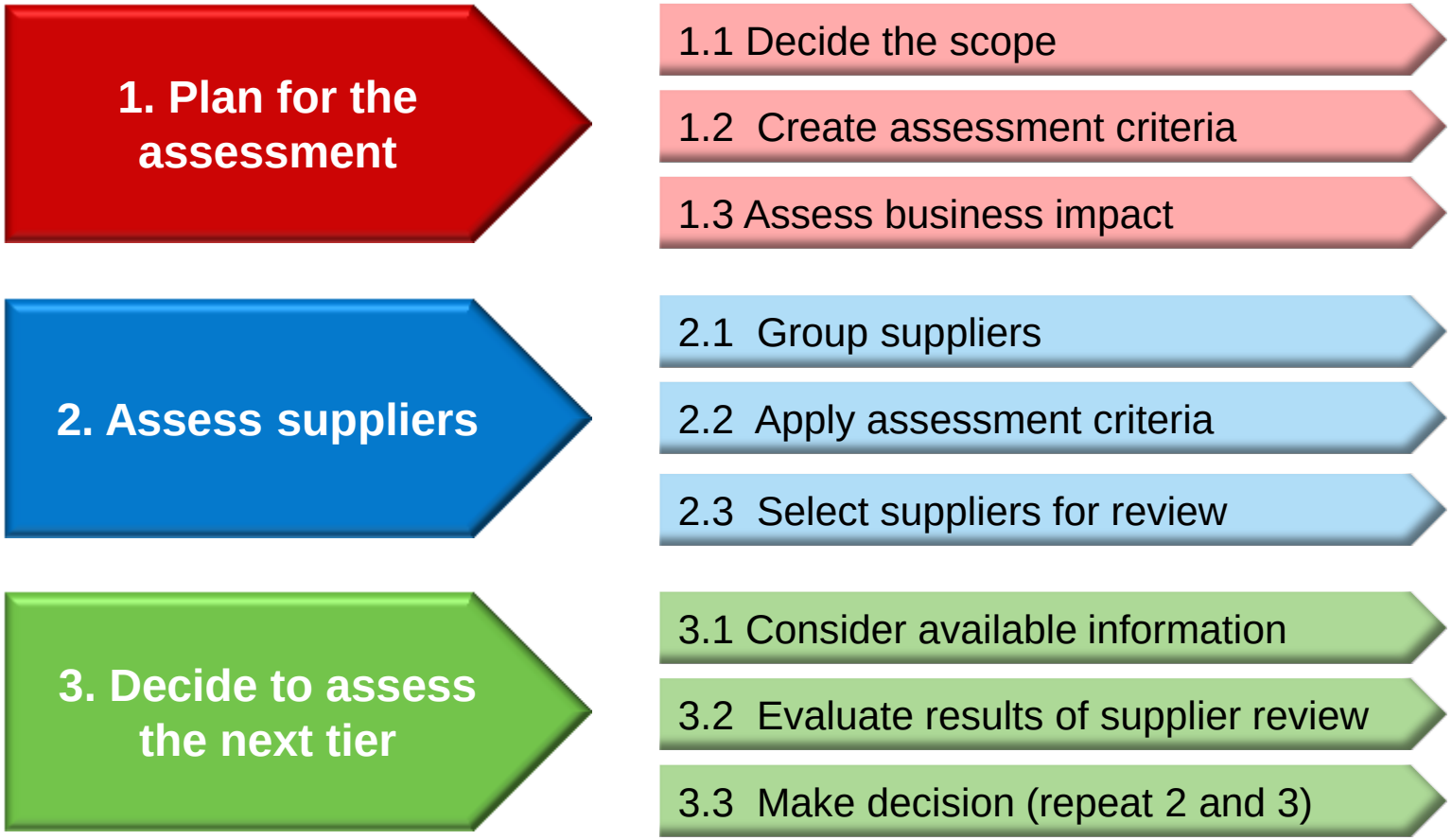
Supply chain information risk components



Information risks by sector

Risks	Impacts	Solution
Finance		
• CIA • Fines • **Franchise risks** • Regulatory risks	Vary depending on issue and data. We look at type, volume, frequency, whether it gets moved.	Use these criteria to produce a risk level which spans from 'very high' to 'very low'. This determines how quickly we will go on site after agreeing the contract with a supplier.
Insurance		
• Fines • Suppliers financial ratings • Integrity of data • **Loss of data**	Reputational damage is the biggest impact. If we lose our data we won't be seen as the best in the industry!	• Identify data types and use a matrix tool to get a weighting • Business units analyse the impact of loss of data and produce a score for it • Assess suppliers against 3 threats, one being loss of data
Production		
• Integrity • Security • **Regulatory requirements (across borders and industries)**	Impacts vary widely, we try to focus on enterprise impacts i.e. Regulatory (PCI, privacy...) E.g. With food traceability if you couldn't comply, the worst case scenario is losing your business.	Standards vary from industry to industry and country to country. To help, we rely on localised business resources to give more clarity on standards and how to map them. A tool to map all regulations we need to comply with to our internal framework and other global standards would be useful.
Logistics		
• **Customer information leakage**	• Brand reputation • Fines from data protection commissioner • Loss of customers	Only collect and use the minimal amount of customer information that is required for processing bookings.

SCIRAM – Supply Chain Information Risk and Assurance Methodology



Next steps

ISF Supply Chain Assurance Framework

- Defines fundamental controls
  - Based on ISF ***Standard of Good Practice 2012*** and
  - Encompasses regulatory compliance requirements
- Allows comparison of suppliers against a known baseline
- Consistent approach, driven by risk
- Offers a single approach to assurance
- Provides common language for acquirers and suppliers
  - Aimed at the business, not just information security

What you can do

- Follow the information
- Identify suppliers
- Assess the risk they present
- Based on risk:
  - Select controls at the supplier
  - Decide whether to review upstream suppliers

Thank you

adrian.davis@securityforum.org
http://uk.linkedin.com/in/adriandaviscitp