The Hidden Risks:
Managing Risks in Outsourcing Relationships

Brian O'Connor
Chief Security & Privacy Officer
Eastman Kodak Company

Bruce Jones
Global IT Security, Compliance & Risk Manager
Eastman Kodak Company

Session ID: GRC-302

Session Classification: General Interest

RSACONFERENCE2012

Goals

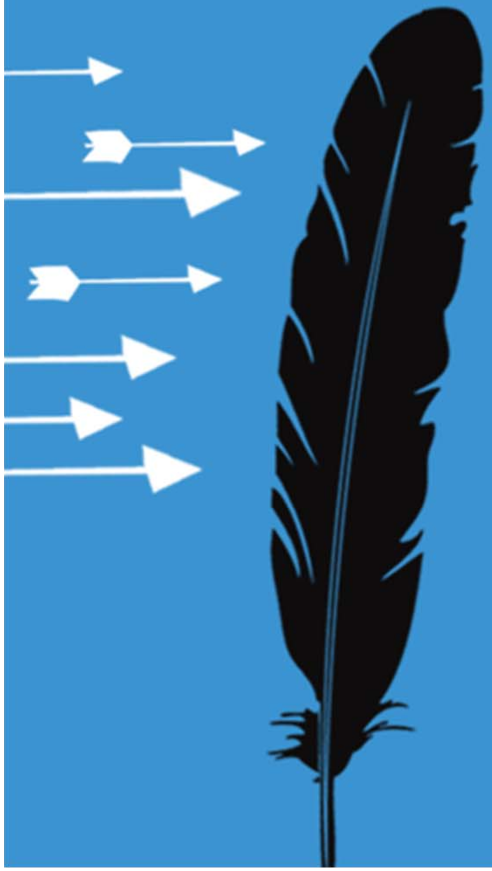
- Provide you with a basic approach to supplier risk management

- Give you tools that you can use to build your own supplier risk management program

  Spreadsheet Tools are available on the RSA Conference Site for you to download.

Key Elements Of Supplier Risk Management

- Policies For High Risk Suppliers
- Risk Assessment Tool
- Supplier Security Self Assessment Tool
- Ongoing Assessments
- External Audits
- Specific Contract Language



Identifying and Assessing Supplier Risk

Challenge: Identifying High Risk Suppliers

- How can I accurately identify all the suppliers that handle my sensitive data and assess the suppliers?

Supplier Risk Management Process

- Engage your Purchasing department.
- Develop clear policies to ensure supplier risk is well managed.

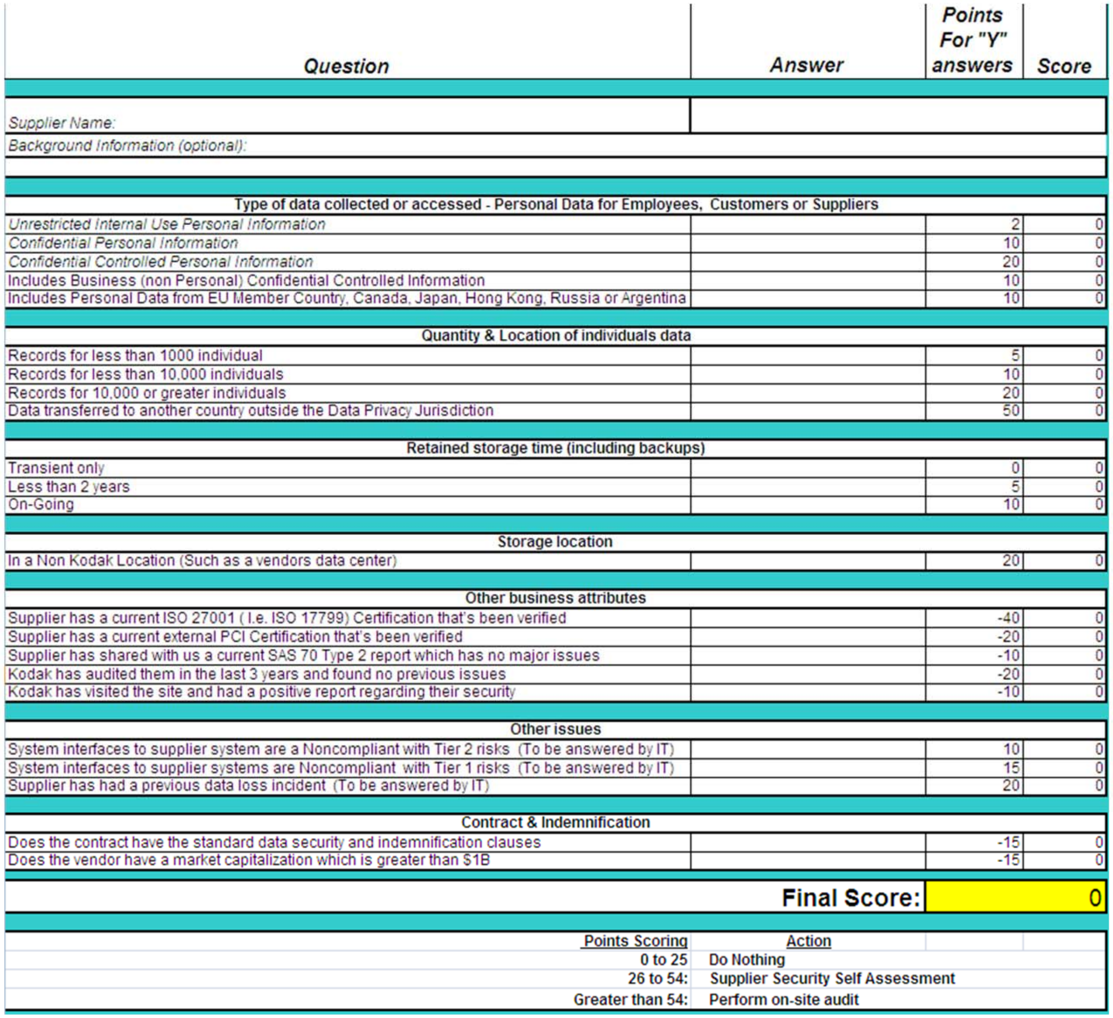
- Create tools to assist with risk assessment.
- Develop standard contract terms that are included as necessary.

Policies

- Mandate These Policies for Suppliers with access to sensitive information:
  - Contract required with standard data privacy clauses.
  - Purchasing must complete the **Risk Assessment Tool.**
  - Supplier must complete a **Supplier Security Self Assessment Questionnaire.**
  - Security Team reviews the assessments along with any supporting material (e.g. SSAE16 reports, copies of policies, etc.) and determines if supplier has “adequate” or better security.

Risk Assessment Tool

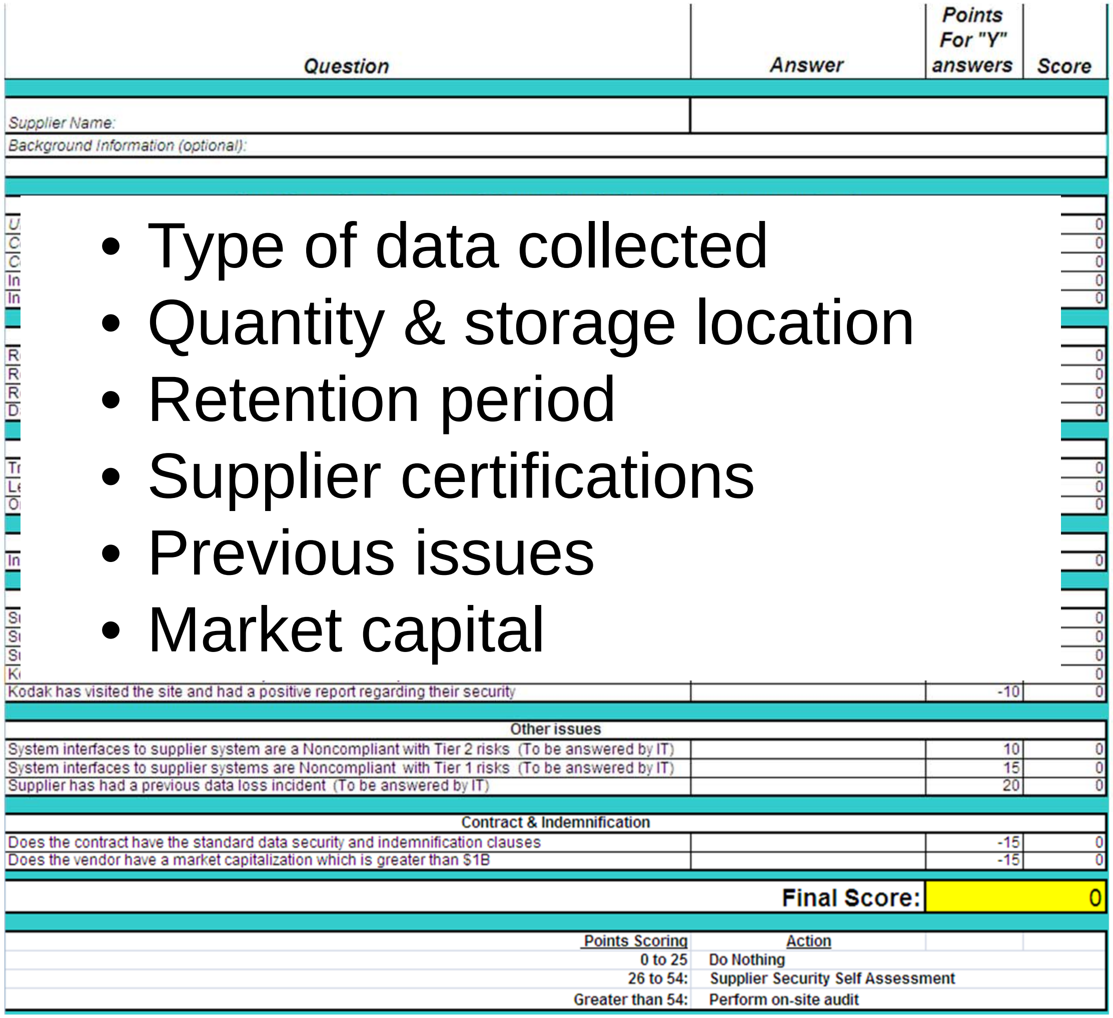
Available on the RSA Conference Website for download



Question	Answer	Points For "Y" answers	Score
Supplier Name:			
Background Information (optional):			
Type of data collected or accessed - Personal Data for Employees, Customers or Suppliers			
Unrestricted Internal Use Personal Information		2	0
Confidential Personal Information		10	0
Confidential Controlled Personal Information		20	0
Includes Business (non Personal) Confidential Controlled Information		10	0
Includes Personal Data from EU Member Country, Canada, Japan, Hong Kong, Russia or Argentina		10	0
Quantity & Location of individuals data			
Records for less than 1000 individual		5	0
Records for less than 10,000 individuals		10	0
Records for 10,000 or greater individuals		20	0
Data transferred to another country outside the Data Privacy Jurisdiction		50	0
Retained storage time (including backups)			
Transient only		0	0
Less than 2 years		5	0
On-Going		10	0
Storage location			
In a Non Kodak Location (Such as a vendors data center)		20	0
Other business attributes			
Supplier has a current ISO 27001 (I.e. ISO 17799) Certification that's been verified		-40	0
Supplier has a current external PCI Certification that's been verified		-20	0
Supplier has shared with us a current SAS 70 Type 2 report which has no major issues		-10	0
Kodak has audited them in the last 3 years and found no previous issues		-20	0
Kodak has visited the site and had a positive report regarding their security		-10	0
Other issues			
System interfaces to supplier system are a Noncompliant with Tier 2 risks (To be answered by IT)		10	0
System interfaces to supplier systems are Noncompliant with Tier 1 risks (To be answered by IT)		15	0
Supplier has had a previous data loss incident (To be answered by IT)		20	0
Contract & Indemnification			
Does the contract have the standard data security and indemnification clauses		-15	0
Does the vendor have a market capitalization which is greater than $1B		-15	0
Final Score:		0	

Points Scoring	Action
0 to 25	Do Nothing
26 to 54:	Supplier Security Self Assessment
Greater than 54:	Perform on-site audit

Risk Assessment Tool

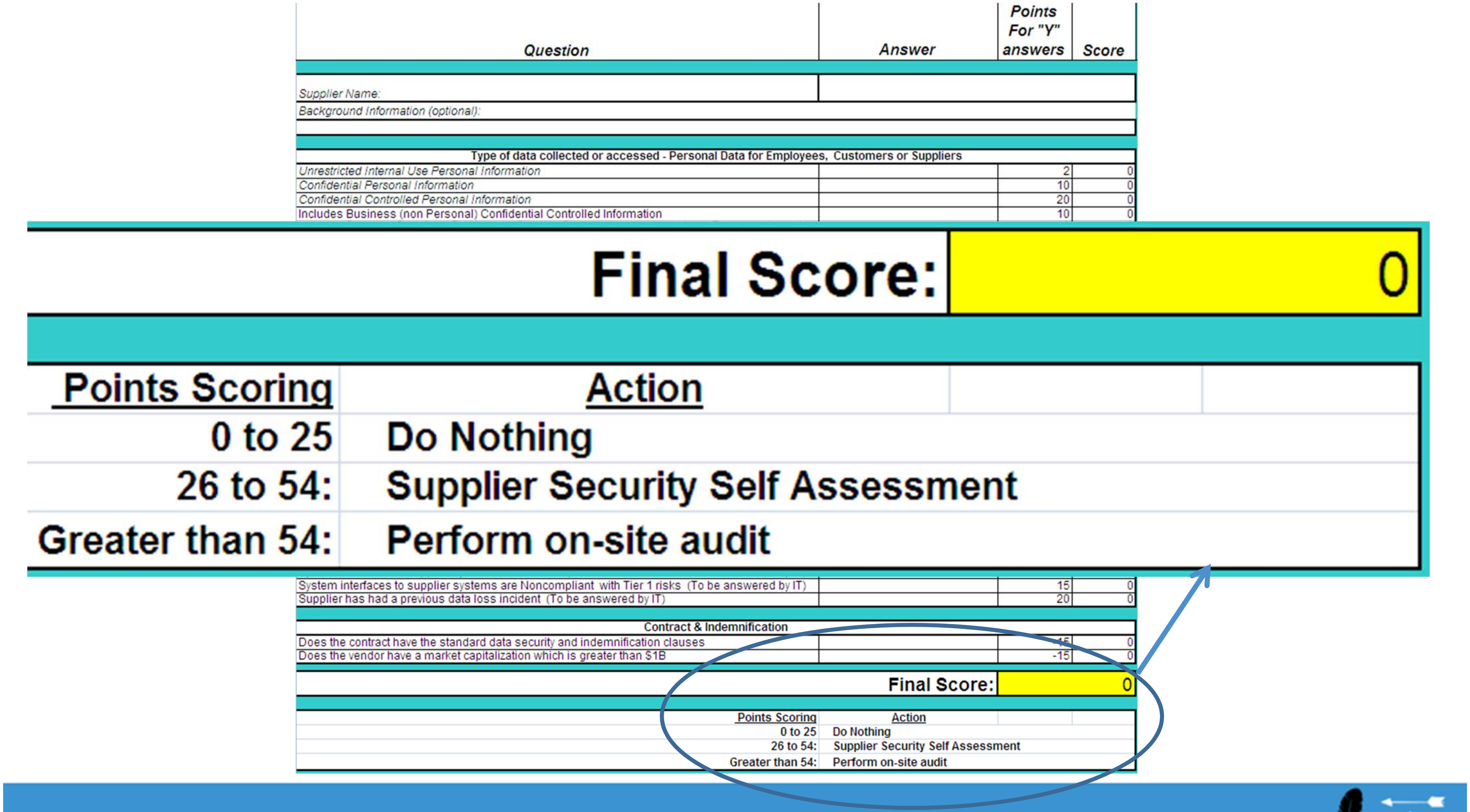


- Type of data collected
- Quantity & storage location
- Retention period
- Supplier certifications
- Previous issues
- Market capital

Question	Answer	Points For "Y" answers	Score
Supplier Name:			
Background Information (optional):			
U			0
C			0
C			0
In			0
In			0
R			0
R			0
R			0
D			0
Tr			0
L			0
O			0
In			0
S			0
S			0
S			0
K			0
Kodak has visited the site and had a positive report regarding their security		-10	0
Other issues			
System interfaces to supplier system are a Noncompliant with Tier 2 risks (To be answered by IT)		10	0
System interfaces to supplier systems are Noncompliant with Tier 1 risks (To be answered by IT)		15	0
Supplier has had a previous data loss incident (To be answered by IT)		20	0
Contract & Indemnification			
Does the contract have the standard data security and indemnification clauses		-15	0
Does the vendor have a market capitalization which is greater than $1B		-15	0
Final Score:		0	

Points Scoring	Action
0 to 25	Do Nothing
26 to 54:	Supplier Security Self Assessment
Greater than 54:	Perform on-site audit

Risk Assessment Tool



Question	Answer	Points For "Y" answers	Score
Supplier Name:			
Background Information (optional):			
Type of data collected or accessed - Personal Data for Employees, Customers or Suppliers			
Unrestricted Internal Use Personal Information		2	0
Confidential Personal Information		10	0
Confidential Controlled Personal Information		20	0
Includes Business (non Personal) Confidential Controlled Information		10	0

Final Score: 0

Points Scoring	Action
0 to 25	Do Nothing
26 to 54:	Supplier Security Self Assessment
Greater than 54:	Perform on-site audit

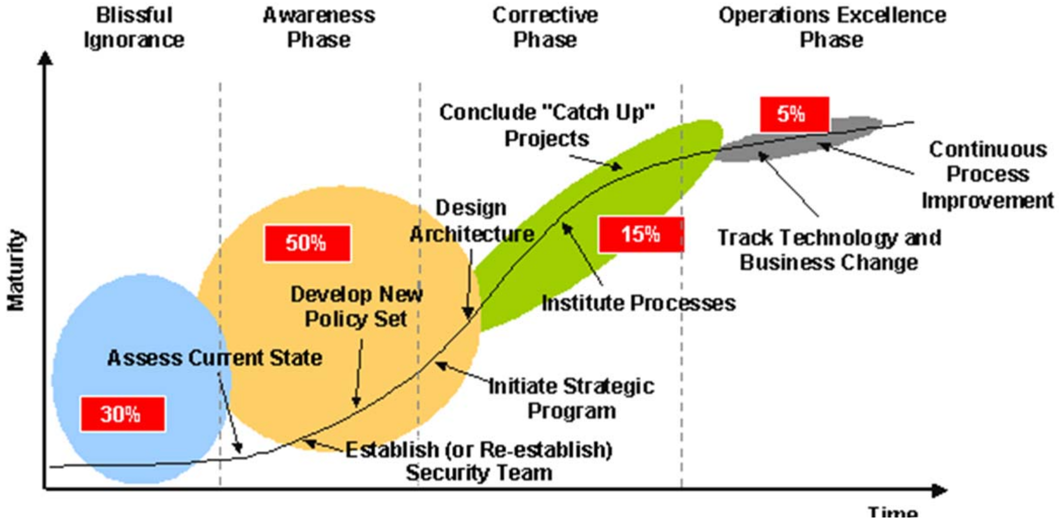
Question	Answer	Points For "Y" answers	Score
System interfaces to supplier systems are Noncompliant with Tier 1 risks (To be answered by IT)		15	0
Supplier has had a previous data loss incident (To be answered by IT)		20	0
Contract & Indemnification			
Does the contract have the standard data security and indemnification clauses		-15	0
Does the vendor have a market capitalization which is greater than $1B		-15	0
		Final Score:	0

Points Scoring	Action
0 to 25	Do Nothing
26 to 54:	Supplier Security Self Assessment
Greater than 54:	Perform on-site audit

Security Self Assessment Questionnaire

- 139 Questions across 36 Major categories

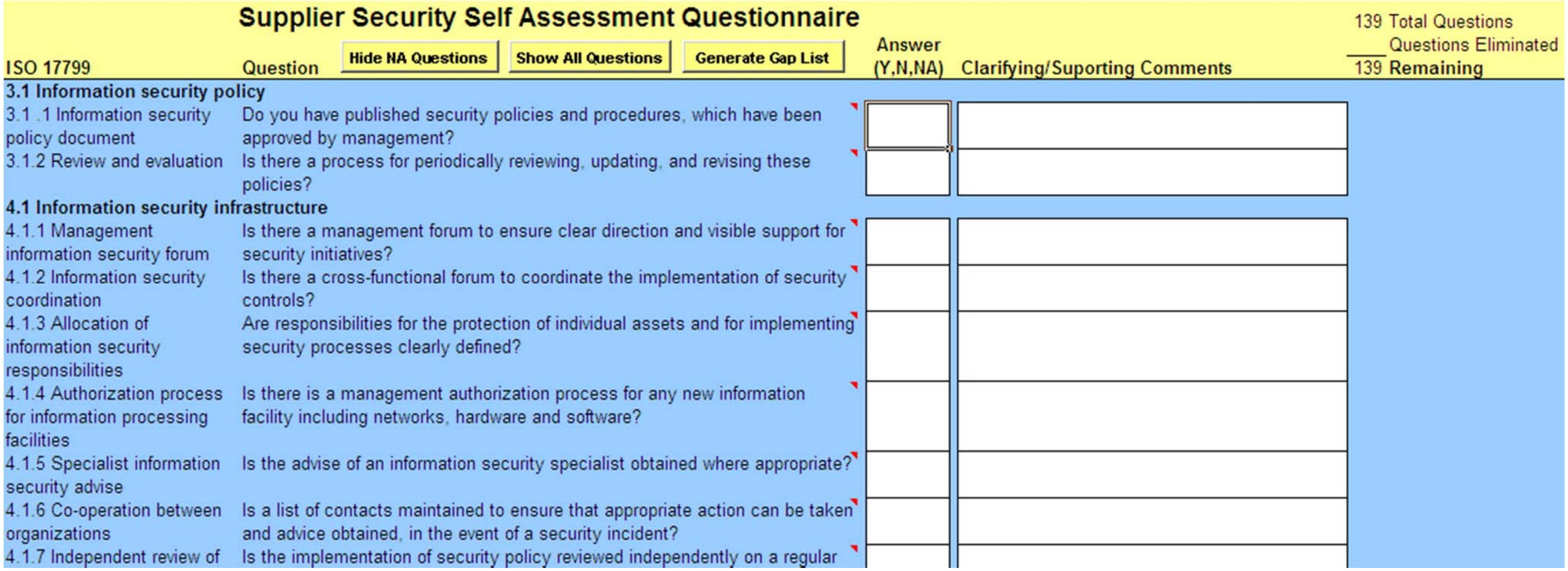
- Indicator of maturity of the supplier security


Blissful Ignorance
Awareness Phase
Corrective Phase
Operations Excellence Phase
Maturity
Time
Conclude "Catch Up" Projects
5%
Continuous Process Improvement
Design Architecture
15%
50%
Track Technology and Business Change
Develop New Policy Set
Institute Processes
Assess Current State
30%
Initiate Strategic Program
Establish (or Re-establish) Security Team

Source: Gartner , The Evolving Role of the Chief Information Security Officer, 23 January 2006 , www.gartner.com

Security Self Assessment Questionnaire

Available on the RSA Conference Website for download

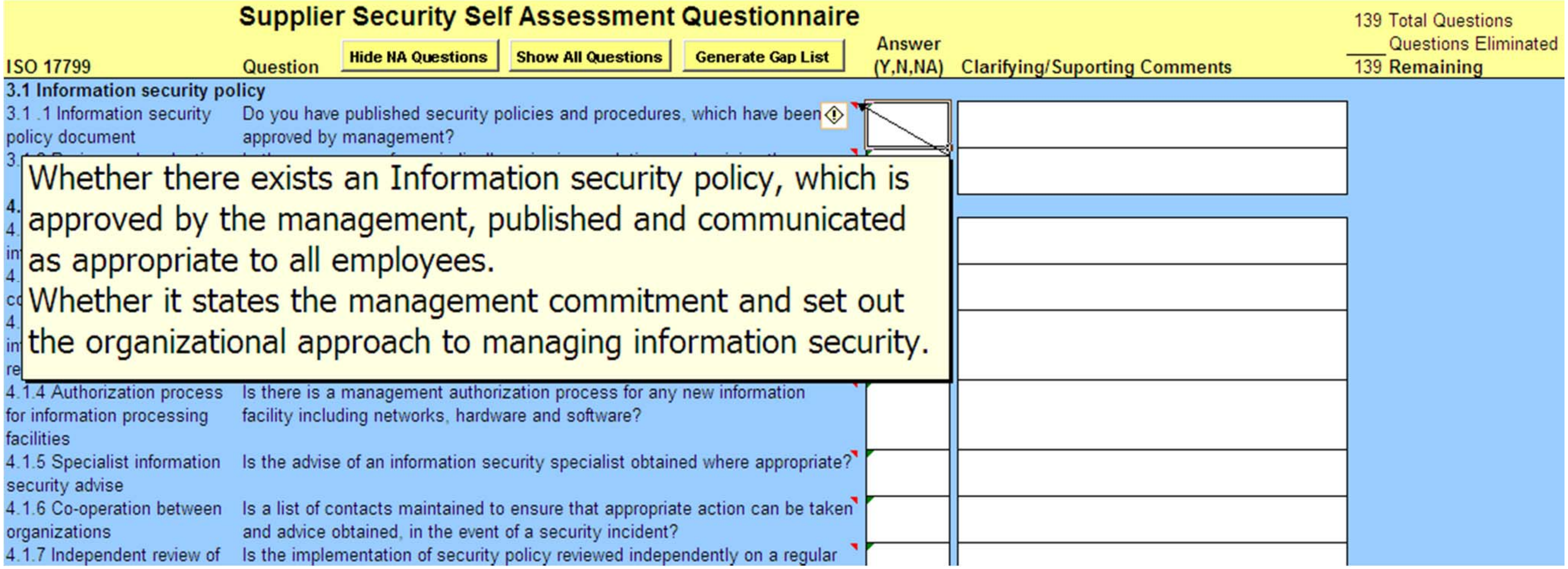


Supplier Security Self Assessment Questionnaire

139 Total Questions
____ Questions Eliminated
139 Remaining

ISO 17799	Question	Answer (Y,N,NA)	Clarifying/Suporting Comments
3.1 Information security policy			
3.1 .1 Information security policy document	Do you have published security policies and procedures, which have been approved by management?		
3.1.2 Review and evaluation	Is there a process for periodically reviewing, updating, and revising these policies?		
4.1 Information security infrastructure			
4.1.1 Management information security forum	Is there a management forum to ensure clear direction and visible support for security initiatives?		
4.1.2 Information security coordination	Is there a cross-functional forum to coordinate the implementation of security controls?		
4.1.3 Allocation of information security responsibilities	Are responsibilities for the protection of individual assets and for implementing security processes clearly defined?		
4.1.4 Authorization process for information processing facilities	Is there is a management authorization process for any new information facility including networks, hardware and software?		
4.1.5 Specialist information security advise	Is the advise of an information security specialist obtained where appropriate?		
4.1.6 Co-operation between organizations	Is a list of contacts maintained to ensure that appropriate action can be taken and advice obtained, in the event of a security incident?		
4.1.7 Independent review of	Is the implementation of security policy reviewed independently on a regular		

Security Self Assessment Questionnaire



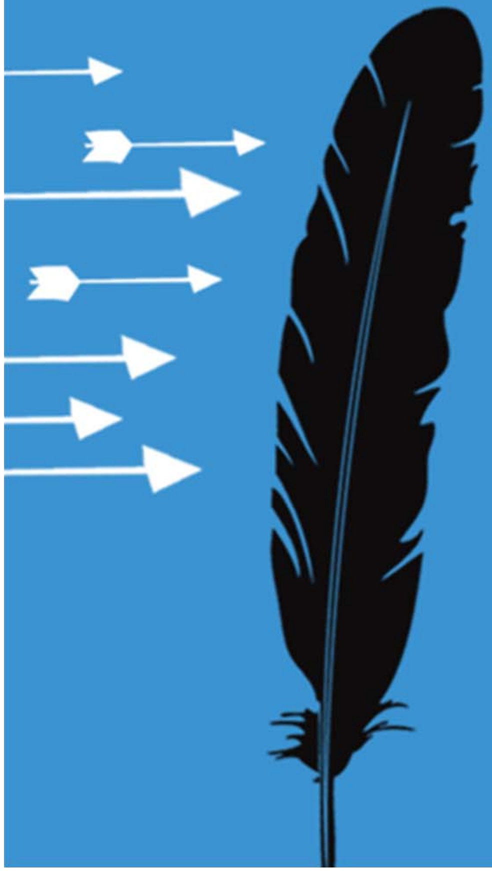
Supplier Security Self Assessment Questionnaire

139 Total Questions
____ Questions Eliminated
139 Remaining

ISO 17799	Question	Answer (Y,N,NA)	Clarifying/Suporting Comments
3.1 Information security policy			
3.1 .1 Information security policy document	Do you have published security policies and procedures, which have been approved by management?		
4.1.4 Authorization process for information processing facilities	Is there is a management authorization process for any new information facility including networks, hardware and software?		
4.1.5 Specialist information security advise	Is the advise of an information security specialist obtained where appropriate?		
4.1.6 Co-operation between organizations	Is a list of contacts maintained to ensure that appropriate action can be taken and advice obtained, in the event of a security incident?		
4.1.7 Independent review of	Is the implementation of security policy reviewed independently on a regular		

Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.
Whether it states the management commitment and set out the organizational approach to managing information security.

- Each question has additional help text.



Key Contract Clauses To Help Manage Supplier Risk

Four Main Contract Issues

Security

Four Main Contract Issues

Security

Subcontractors

Four Main Contract Issues

Security

Subcontractors

Liability

Four Main Contract Issues

Security

Subcontractors

Liability

Audits

Security Provisions

- Supplier will comply with all applicable laws on data privacy and data security
- Medical data?
  - may need HIPAA “Business Associate Agreement”
- Payment card data?
  - Must comply with PCI-Data Security Standard
- Massachusetts resident data?
  - Must comply with Mass. Law 201 CMR 17.00
- EU resident data?
  - need to attach “model contract” provisions or Safe Harbor requirements

Security Provisions

- Require compliance with ISO 27002 et seq. (or other standard)?
- Prohibit data storage outside server?
- Encryption requirements for storage and transfer?
- Prohibit transfer of data to any third party other than subcontractor
- Require return or destruction of data at contract termination?

Subcontractor Provisions

- Subcontractors must agree to same provisions
- Require training for subcontractors who access data?

Liability Provisions

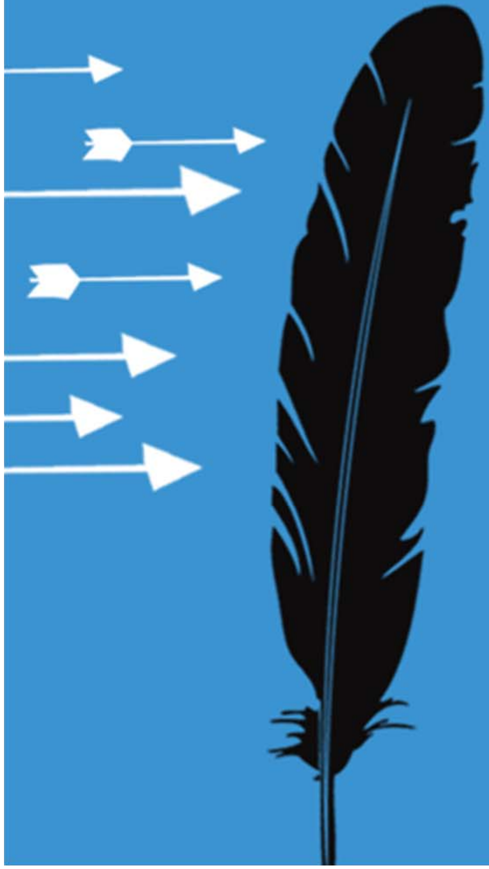
- Notify us of any security breach
- Cover costs of breach notice under relevant laws, credit monitoring, etc.
- Must indemnify for third party claims arising from breach

Audit Provisions

- Periodic IT Security Audits required for “high risk” suppliers

- Audit by third party or by your auditors?

Sample Contract Clauses available on the RSA Conference Website for download.



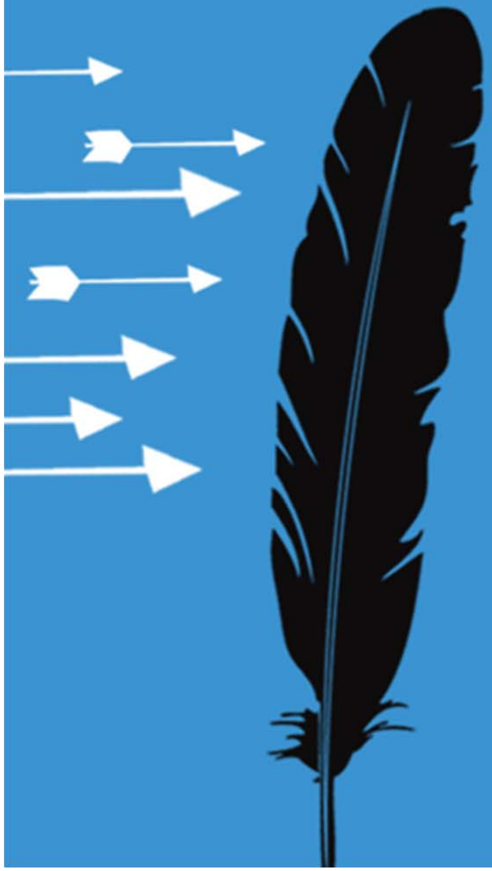
Problems & Improvement Opportunities

Problems Encountered

- Supplier provides little or no detail
- Supplier not willing to complete Security Self Assessment
- Supplier requires a nondisclosure agreement
- No test of the effectiveness of their controls
- Language barriers
- Not willing to agree to our standard contract language

Potential Improvement Opportunities

- Web-enabled system with built-in work flow
- Expand to include the annual assessment of compliance with Foreign Corrupt Practices Act
- Engage suppliers early in the process

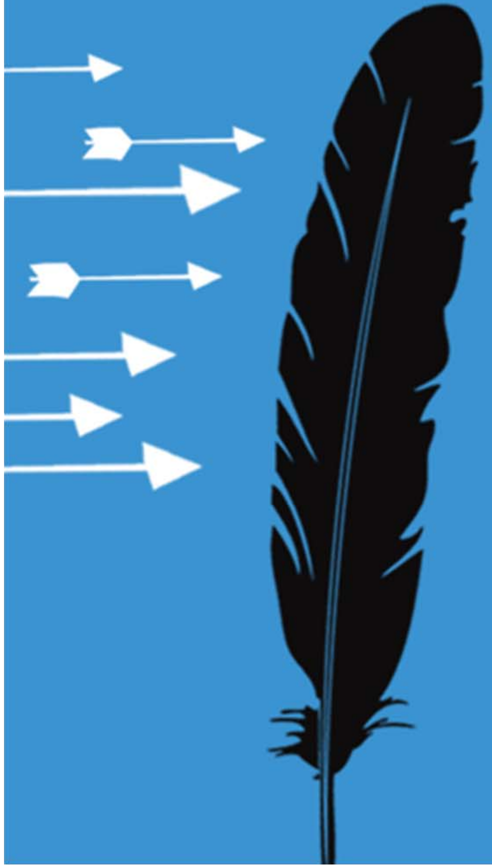


Conclusions

Supplier Risk Management

- Engage both Legal and Purchasing in the development of your program
- Ensure you get top management support for the policies
- Look at commercial solutions if you have the budget
- Start now using the tools we have provided

Questions



Reference Material

Reference Websites

- BITS Shared Assessment as an alternative
  - http://sharedassessments.org/

- SANS – A Security Guide For Acquiring Outsourced Service
  - http://www.sans.org/reading_room/whitepapers/services/security-guide-acquiring-outsourced-service_1241