THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

CSO

Modern Approaches to Vendor Management
&
Managing Risks in Outsourcing Relationships

Bruce Jones
Chief Information Security Officer
Bruce.jones@kodak.com

Kodak



Key Elements Of Supplier Risk Management

- Engage Purchasing, Legal and Management
- Develop clear policies to ensure supplier risk is well managed
- Develop a comprehensive process and tools to identify and manage high risk suppliers
- Develop relationships with external audit firms
- Develop standard contract terms that are included as necessary

Engagement

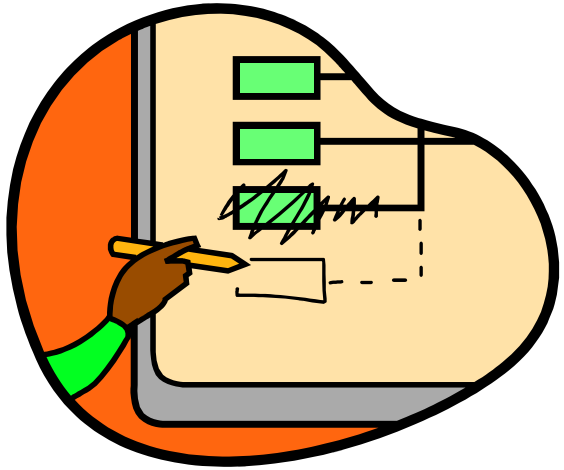
- Management
  - Support and Enforcement of the policy
- Purchasing
  - Assist with identifying key suppliers that may be a risk to the company
  - Gate keepers for the process
  - Interface to suppliers
- Legal
  - Standard contract clauses

Policies

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

Process

- Responsibilities
- Training
- Tools
- RFP/RFQ Expectations
- Risk Acceptance
- Consequences



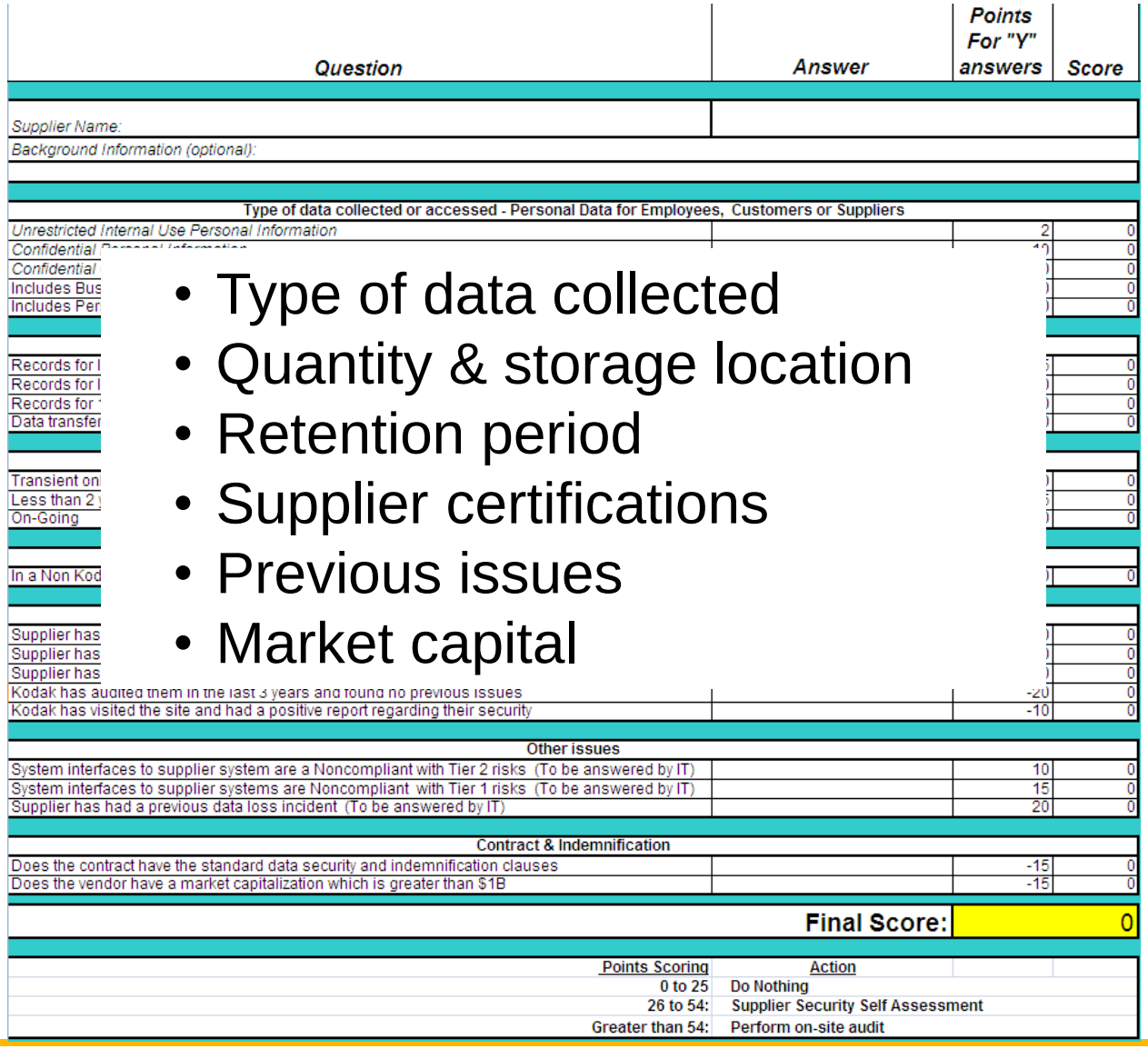
Tools - Kodak Risk Assessment Tool

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
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

Kodak

Tools - Kodak 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			0
Includes Bus			0
Includes Per			0
Records for I			0
Records for I			0
Records for			0
Data transfer			0
Transient on			0
Less than 2			0
On-Going			0
In a Non Kod			0
Supplier has			0
Supplier has			0
Supplier has			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

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

Kodak

Tools - Kodak 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
Includes Personal Data from EU Member Country, Canada, Japan, Hong Kong, Russia or Argentina		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

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

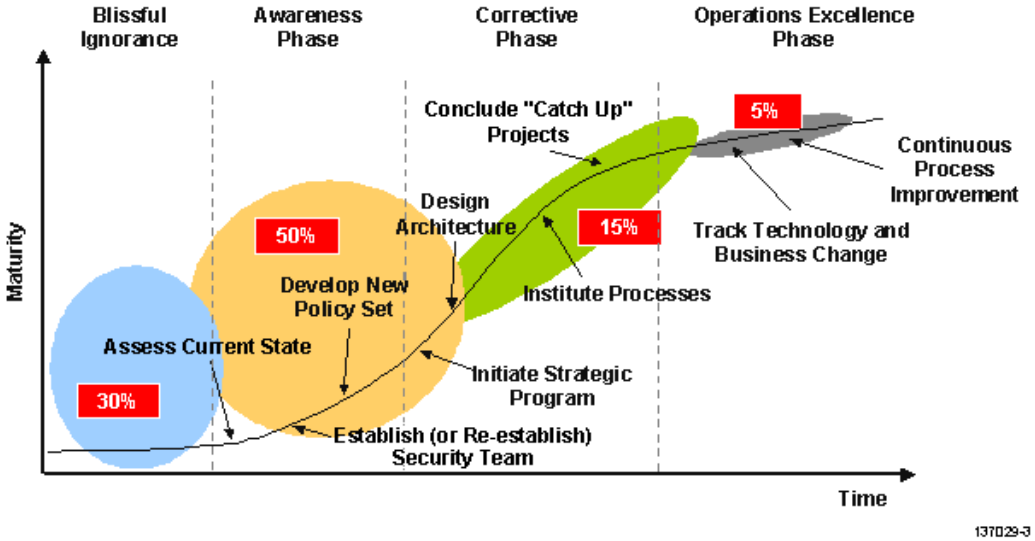
Kodak

Tools - Kodak Security Self Assessment Questionnaire

- 139 Questions across 36 Major categories

ISO 27002

- Indicator of maturity of the supplier security



Kodak

Tools - Kodak Security Self Assessment Questionnaire

Supplier Security Self Assessment Questionnaire

Hide NA Questions | Show All Questions | Generate Gap List

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		

Kodak

External Audit Firms

- Develop a relationship up front with a couple audit firms
- Define the scope of audit that would be required
- Get an estimate of the cost of an audit
- Get agreement to share cost estimate with your suppliers

Five Main Contract Clauses

Security

Subcontractors

SLA

Liability

Audits

Kodak

Security Provisions

- Supplier will comply with all applicable laws (e.g. data privacy, data security, FCPA, etc.)
- Require compliance with ISO 27002 et seq. (or other standard)
- Encryption requirements for storage and data transfer
- 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, credit monitoring, Call Center, etc.)
- Must indemnify for third party claims arising from breach
- Optional – Require Data Breach Insurance

Audit Provisions

- Periodic IT Security Audits required for “high risk” suppliers
- Audit by third party or by your auditors
- Cost of audit is suppliers responsibility

SLA Provisions

- Service levels identified with clear measurable goals
- Timely Service level reporting requirements
- Penalties for failure to meet service level

Conclusions

- 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

Kodak

Bruce Jones
Chief Information Security Officer
Bruce.jones@kodak.com









THE SECURITY STANDARD

Adapting Enterprise Security to New Realities, Threats and Endpoints

September 10-11, 2012 | New York Marriott at the Brooklyn Bridge | New York City

Produced by

CSO