Outsourcing Tools & Technology Innovation Chapter

Webinar Meeting – April 21, 2010

Webinar Meeting Agenda 4/21/10

(Times Are EDT)

1:00 p.m.	IAOP Update & Tools & Technology Innovation Chapter General Topics
1:10 p.m.	The Use of Tools & Technologies to optimize Risk & Compliance in Outsourcing Contracts/Relationships - Bruce Jones, Global IT Security, Compliance, Data Privacy & Risk Manager for Kodak, Inc.
1:40 p.m.	Q&A and Polling Questions
1:50 p.m.	Future Chapter Meeting Discussion
2:00 p.m.	End of Meeting

Most of the World's Top Organizations are Leveraging IAOP's Programs and Services

100+ Founding & Corporate Members, including:

Abbott Laboratories, Accenture, Aegis, Affiliated Computer Services (ACS), Allstate Insurance, Alsbridge, American Express, Anthem BCBS (Wellpoint), Apple Inc, Applied Materials, Assurant, Atlantic Canada Atlantique, AT&T, Avasant Global Sourcing, Belcan Corporation, Best Buy Company, BeyondCore, Bleum, Blue Cross/Blue Shield of Florida, Blue Shield of California, Booz & Company, Boston University, Business Catalyst International, Cal State Fullerton, Cambridge Assessment, Capgemini, Capital One, Carnegie Mellon University, Cassidy Turley, CB Richard Ellis, Chris Disher & Associates, Cinteger LLC, Computer Associates, Copenhagen Business School, CORFO (Chile), Colliers International, CPA Global, Delve Group, Dextrys, Diebold, Discover Financial, Disney Institute, DNL Global, Duke Energy, Duke University, Enlighta, EquaSiis/EquaTerra, Expense Management Solutions, Express Scripts Inc, Fasken Martineau DuMoulin LLP, Firstsource, Foley & Lardner, GASSCOM/E.Services Africa, General Motors, Genmab, Gorrissen Federspiel, GSOS, Hinduja Global Solutions (HTMT), HCL Technologies, Hexaware Technologies, hiSoft Technology International Limited, Hospira, HOV Services, IDA Singapore, Infosys, Innodata Isogen, Insigma Hengtian Software, Intel, Intetics, ISS A/S, Janeeva, Janus Associates, J & J Consumer Group, John Hancock Financial Services, Kelly OCG (BPO), Kenobi SRL, Kenya ICT, Kirkland & Ellis LLP, Kraft Foods, Liberty Mutual, LifeMasters, Loeb & Loeb , Marsh & McLennan Co, Mayer Brown LLP, Microsoft, Morrison & Foerster LLP, Multimedia Development Corp. (MdeC), NCS, Neusoft Corporation, Nike, Nordea Bank, North Dakota Dept. of Commerce, Océ Business Services, Orange Business Systems, Ortho-McNeil Janssen, PepsiCo, Pfizer Inc, Pratt & Whitney/UTC, Pretium Partners, PricewaterhouseCoopers, Procter & Gamble, Procurisource, Prudential, Qantas Airlines, Quint Wellington Redwood, ResourcePro, Rio Tinto, Roche, RR Donnelley, RTM Consulting LLC, Salmat, SAP AG, Service Corporation Intl, Singtel Optus (Australia), Sitel, SPi Technologies, State Farm Insurance, Sun Microsystems, Symantec, Syracuse University, TEKsystems, TeleTech, Thomson Legal & Regulatory, TransUnion Interactive, Trellis, Univ of Missouri, Univ of Salerno, VanceInfo, Vantage Partners, Vertex Business Services, Verve, Visa, Vodafone, Washington Gas, Whirlpool, Wipro Technologies, WNS Global Services, Xceed, and Yahoo!.

1000+ Professional Members • 100,000+ Affiliate Members

40+ Chapters Around the Globe

www.IAOP.org

IAOP Structure and Programs

- Strategic Advisory Board & Outsourcing Standards Board
- Research, Training, Services, Advocacy & Outreach Committees
- Geographic, Industry, Topical Chapters
- Online Member Directory, IAOPNetwork & Customer-only IAOPNetwork
- The Outsourcing World Summit®
- Regional Summits - part of the Outsourcing World Summit Conference Series
- Topical Forums as part of the Outsourcing Leadership Series
- IAOP Member of the Year Awards
- Outsourcing Hall of Fame Awards
- IAOP Knowledge Center (Firmbuilder.com®)
- Certified Outsourcing Professional® (COP) Program (Attending a chapter meeting earns COP's 1 CEH towards recertification)
- COP Master Class
- The Global Outsourcing 100 ® Program (The Global Outsourcing 100 list and sub lists, World's Best Outsourcing Advisors)
- Outsourcing Professional Code of Ethics

Other IAOP Upcoming Dates of Interest

- **COP Master Class**

  May 3-5, 2010 – Cal State University, Fullerton, California

  COP Governance Workshop

  May 6, 2010 – Cal State University, Fullerton, California

- **2011 Outsourcing World Summit – Call for Papers**

  Look for more information end of May – beginning of June

- **2011 Outsourcing World Summit**

  February 21-23, 2011 – Indian Wells, California

New Member Services from IAOP

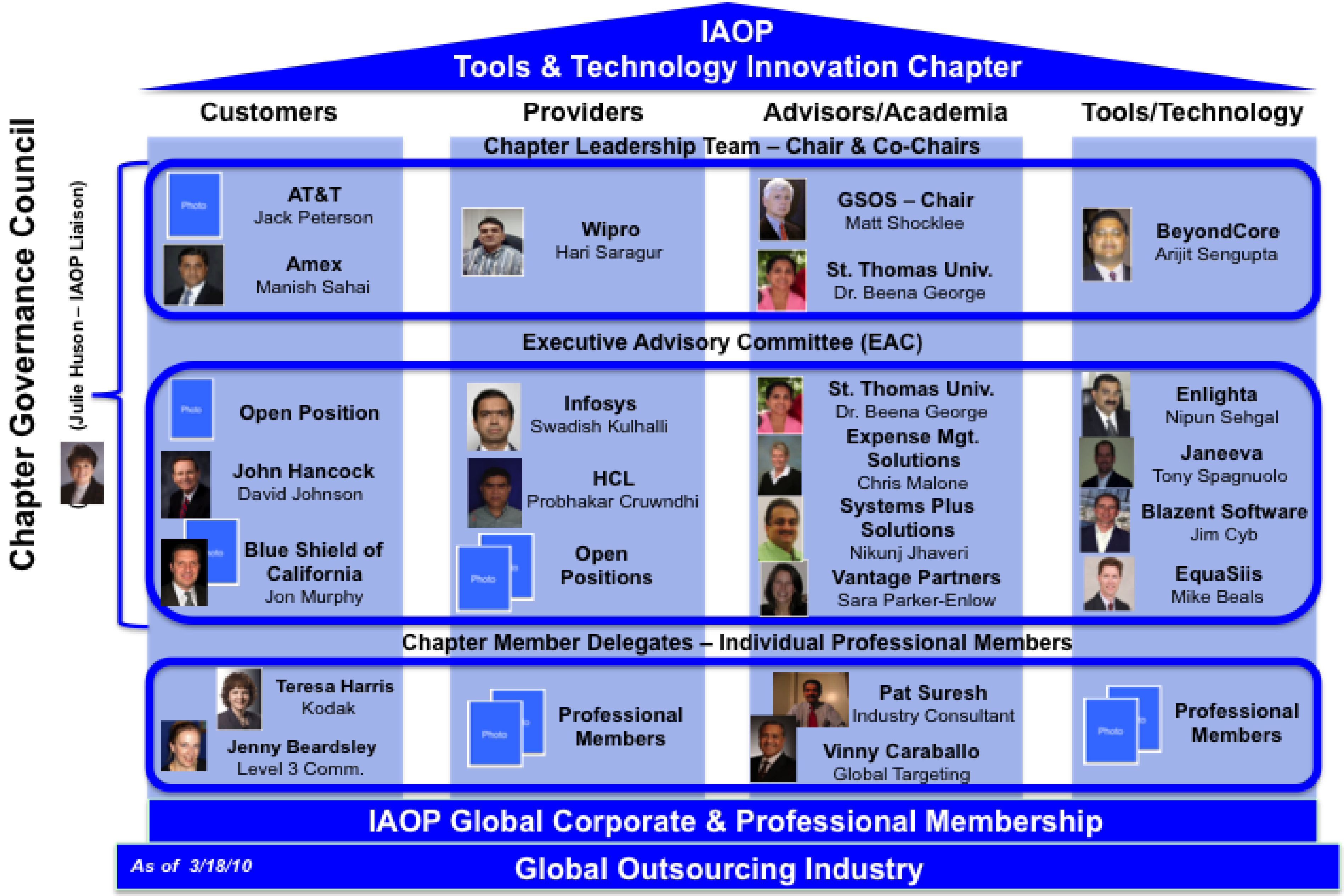
At IAOP, we are always looking for programs & services that will add value to your membership and we have three new offerings for you!

- **Value Health Check Survey** – An exciting new diagnostic tool that will enhance the value of your outsourcing contracts & relationships! Each IAOP Corporate Member receives two complimentary survey's as part of their annual corporate membership – Call us today to learn more!
- **BestOutsourcingJobs.com** – Companies seeking the best talent for outsourcing jobs, as well as professional looking for employment opportunities, can benefit from our new online portal for outsourcing jobs!
- **OperatorEvaluator** – An exciting new solution available as part of our suite of outsourcing skills and professional development offerings. Call us today to find out more about this dynamic service!

Contact Michael Forbes at mike.forbes@iaop.org for more detailed information on any of these service offerings!

www.IAOP.org

Tools & Technology Innovation Chapter – Governance Model



IAOP

Tools & Technology Innovation Chapter

Customers

Providers

Advisors/Academia

Tools/Technology

Chapter Governance Council

(Julie Huson – IAOP Liaison)

Chapter Leadership Team – Chair & Co-Chairs

AT&T
Jack Peterson

Amex
Manish Sahai

Wipro
Hari Saragur

GSOS – Chair
Matt Shocklee

St. Thomas Univ.
Dr. Beena George

BeyondCore
Arijit Sengupta

Executive Advisory Committee (EAC)

Open Position

John Hancock
David Johnson

Blue Shield of California
Jon Murphy

Infosys
Swadish Kulhalli

HCL
Probhakar Cruwndhi

Open Positions

St. Thomas Univ.
Dr. Beena George

Expense Mgt. Solutions
Chris Malone

Systems Plus Solutions
Nikunj Jhaveri

Vantage Partners
Sara Parker-Enlow

Enlighta
Nipun Sehgal

Janeeva
Tony Spagnuolo

Blazent Software
Jim Cyb

EquaSiis
Mike Beals

Chapter Member Delegates – Individual Professional Members

Teresa Harris
Kodak

Jenny Beardsley
Level 3 Comm.

Professional Members

Pat Suresh
Industry Consultant

Vinny Caraballo
Global Targeting

Professional Members

IAOP Global Corporate & Professional Membership

As of 3/18/10

Global Outsourcing Industry

Webinar Meeting Agenda 4/21/10

(Times Are EDT)

1:00 p.m.	IAOP Update & Tools & Technology Innovation Chapter General Topics
1:10 p.m.	The Use of Tools & Technologies to optimize Risk & Compliance in Outsourcing Contracts/Relationships - Bruce Jones, Global IT Security, Compliance, Data Privacy & Risk Manager for Kodak, Inc.
1:40 p.m.	Q&A and Polling Questions
1:50 p.m.	Future Chapter Meeting Discussion
2:00 p.m.	End of Meeting

Kodak
it's time to smile

Data Protection
Supplier Risk Management

IAOP – Outsourcing Tools & Technology Chapter

Approach

- Kodak has a multilevel, tiered approach to Supplier Risk Management

- Key Elements Include
  - High-Level Risk Assessment Tool
  - Security Self-Assessment Tool
  - Ongoing Assessments
    - External Audits
    - Security Self Assessment
  - Specific Contract Language

High-Level Risk Assessment Tool

- This tool is designed to help determine the level of risk to Kodak if there was a data breach
- This tool looks at the following data elements to calculate the risk score
  - 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):			
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
CCD Personal Information		20	0
Includes Business (non Personal) CCD 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 X individuals		5	0
Records for less than 10X individuals		10	0
Records for 10X 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		-40	0
Supplier has a current external PCI Certification		-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			
Kodak interfaces to supplier system have a DORA for Tier 2 risks (To be answered by WWIS)		10	0
Kodak interfaces to supplier systems have a DORA for Tier 1 risks (To be answered by WWIS)		15	0
Supplier has had a previous data loss incident (To be answered by WWIS)		20	0
Contract & Indemnification			
Does the contract have an appropriate indemnification clause		-15	0
Does the vendor have a market capitalization which is greater than $X		-15	0
	Final Score:	0	
Points Scoring			
0 to 25		**Do Nothing**	
26 to 60:		**ISPQ (Self Assessment)**	
Greater than 60:		**External Audit Required**	

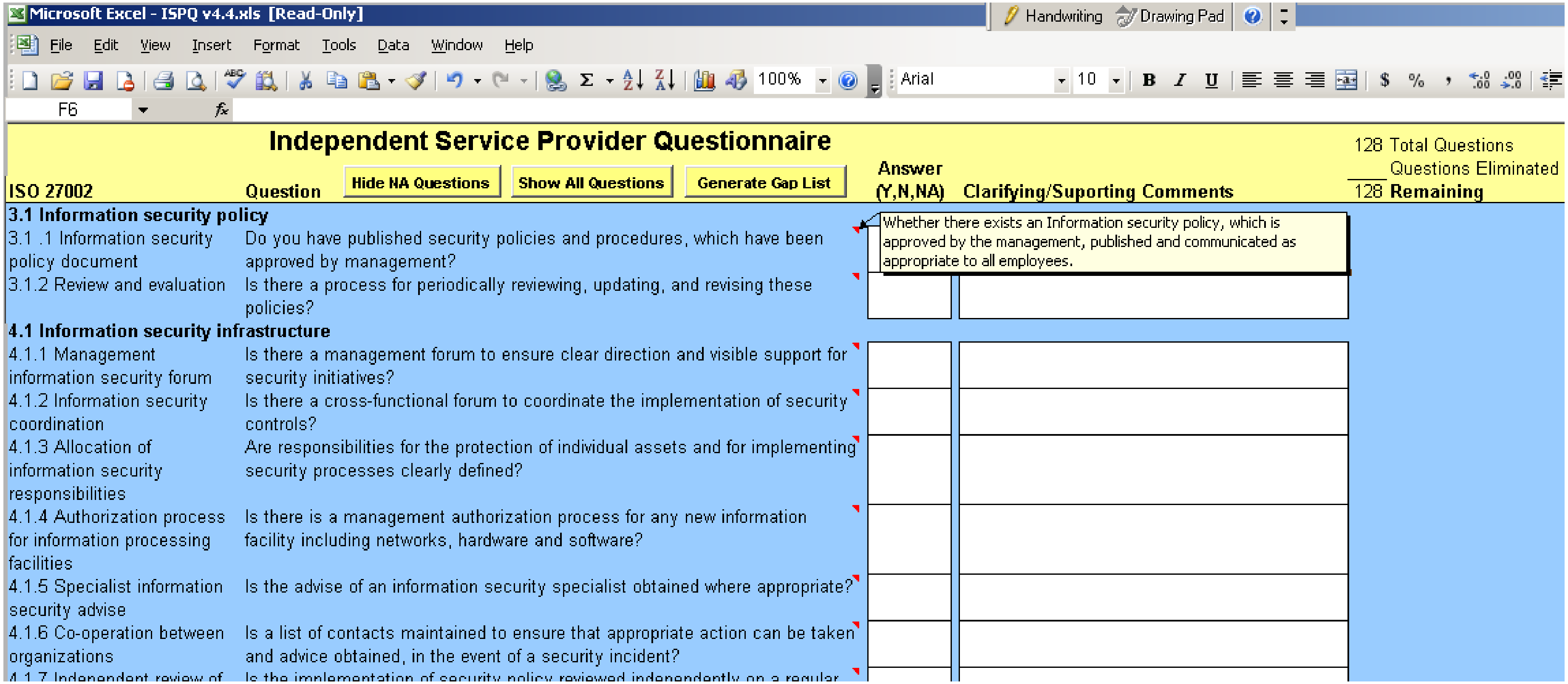
Security Self-Assessment Tool

- Excel based self-assessment tool
- 36 Major categories and 128 Questions based on ISO 27002
- Used to gauge the maturity of the supplier security program
- Required for all contracts where supplier will have access to personally identifiable information or highly confidential business data

Security Self-Assessment Major Categories

Information security policy	Exchange of Information and software
Information security infrastructure	Business Requirements for Access Control
Security of third party access	User Access Management
Outsourcing	User Responsibilities
Accountability of assets	Network Access Control
Information classification	Operating system access control
Security in job definition and Resourcing	Application Access Control
User training	Monitoring system access and use
Responding to security incidents and malfunctions	Mobile computing and telecommuting
Secure Area	Security requirements of systems
Equipment Security	Security in application systems
General Controls	Cryptographic controls
Operational Procedure and responsibilities	Security of system files
System planning and acceptance	Security in development and support process
Protection against malicious software	Aspects of Business Continuity Management
Housekeeping	Compliance with legal requirements
Network Management	Reviews of Security Policy and technical compliance
Media handling and Security	System audit considerations
Information security policy	Exchange of Information and software

Example



Independent Service Provider Questionnaire

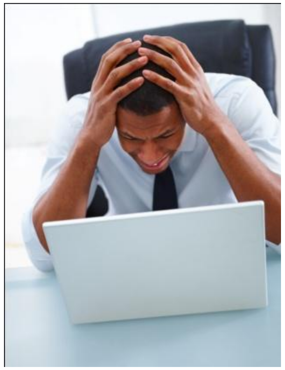
128 Total Questions
___ Questions Eliminated
128 Remaining

ISO 27002	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		

Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.

Problems Encountered

- Security Self Assessment filled out with only Y or N answers and no detail
- Suppliers not willing to fill out the Security Self Assessment
- Not a test of the effectiveness of their controls
- Some only want to provide a SAS 70 Report
- BITS Shared Assessment as an alternative
  - http://sharedassessments.org/



Ongoing Assessment

Kodak
it's time to smile

- When contracts are renewed, the Security Assessment must be updated
- If supplier falls into High-Risk category we require an annual independent external security audit
- If supplier is ISO 27001 Certified we will accept their certificate in lieu of the Security Self Assessment and audits

Problems

- Manual process
- Requires Purchasing Agents to remember to
  - Request an updated Security Assessment
  - Request proof of external audit
- Language barriers

Specific Contract Language

- Use of Data
- Protection of data
  - Meet or exceed ISO 27002
  - Encryption if stored on Laptop or removable media
  - Limit access
- Destruction of Data
- Subcontracting Requirements
- Notification of losses & breaches of data
- Liability & Indemnification
- Audit Requirement
- EU Safe Harbor
- HIPAA
- PCI

Potential Improvement Opportunities

- Web-enabled system where suppliers can enter their assessments, audit results and updates
- Automated work flow-enabled solution
- Tool that supports multiple languages
- Automated compliance metrics
  - Who has completed their assessment
  - Who has posted their audit results
  - Suppliers past due
  - Other risk metrics (Market Capital, audit issues, etc.)
- Include annual assessment of compliance with Foreign Corrupt Practices Act

Questions

Kodak

it's time to smile

Webinar Meeting Agenda 4/21/10

(Times Are EDT)

1:00 p.m.	IAOP Update & Tools & Technology Innovation Chapter General Topics
1:10 p.m.	The Use of Tools & Technologies to optimize Risk & Compliance in Outsourcing Contracts/Relationships - Bruce Jones, Global IT Security, Compliance, Data Privacy & Risk Manager for Kodak, Inc.
1:40 p.m.	Q&A and Polling Questions
1:50 p.m.	Future Chapter Meeting Discussion
2:00 p.m.	End of Meeting

Tools & Technology Innovation Chapter Schedule

As of 4-20-10

Month 2010	Tools Chapter Webinar or Events (Webinars are 1:00-2:00 pm EST)	Chapter Webinar Topic & Presenter(s)
January	None	
February	Tuesday – 2nd	Outsourcing Value Framework & Health Check Survey Update/Shocklee, ToolsMAP Update/George
February	Monday - 15th at World Summit	All Tools Chapter Members join us at the Tools & Technology Chapter Table during the Showcase
March	Thursday – 18th	Use of Tools to Optimize Financial Performance of Outsourcing Contracts/Relationships
April	Wednesday – 21st	Use of Tools to Optimize Risk/Compliance in Outsourcing Contracts/Relationships
May	Thursday – 20th	Use of Tools to Optimize the Contracting Process Partnering with Contract Process Chapter - Mayer Brown, LLC & Contract Process Chapter
June	Tuesday – 8th 3:30 – 7:00 p.m. Offices of Morrison & Foerster in Downtown, NYC	Use of Tools & Technologies to Optimize Overall Governance of Outsourcing Contracts/Relationships - Joint Meeting with NYC Chapter & Governance Chapter
July/August	No Meetings/Vacation	
Fall 2010 (Sept-Oct)	Date TBD Location: San Francisco Area Joint Chapter Meeting with San Francisco Chapter & Technology Industry Chapter Mega-Chapter Meeting on	Outsourcing Tools and Technology Symposium: - Full day of speakers, demonstrations and hands-on workshops - Location to be determined in SF Bay Area - Sponsorship opportunities - Must confirm within the next 30-45 days if to be held