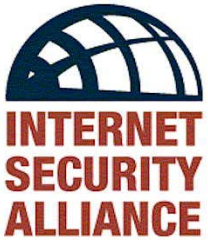


NOVEMBER 2006 VOL. 1 NO. 1

OUTSOURCING RISK MANAGEMENT

ENTERPRISE RISK INTEGRATION PROGRAM: PERSPECTIVE

Carnegie Mellon University
Cylab

AUTHOR

Jody R. Westby

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

Table of Contents

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

ENTERPRISE RISK INTEGRATION PROGRAM: PERSPECTIVE

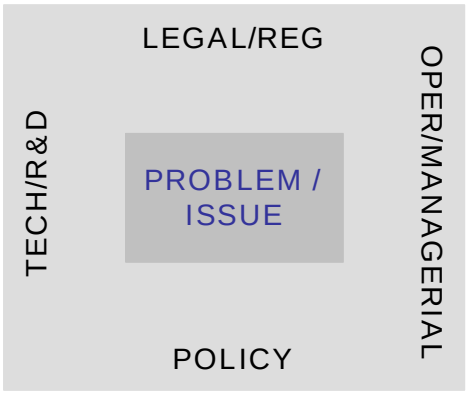
From Jody R. Westby[1]

INTRODUCTION

Technology issues are increasingly impacted by legal/regulatory requirements and operational considerations. Although information technology has historically been unregulated, this period of unfettered innovation is over. An increasingly complex matrix of laws and regulations regarding the use of technology is imposing constraints on operational policies and procedures, system architectures, and research and development (R&D). Today, proper risk management requires an understanding of the interdependencies between the various legal, operational, policy, and technical considerations when approaching business issues.

With this in mind, Carnegie Mellon CyLab, in collaboration with the Internet Security Alliance (ISAlliance), has created an Enterprise Risk Integration Program to examine risk issues from a multidisciplinary perspective. Quarterly Perspectives will be prepared on risk issues identified as important to CyLab members. Each Perspective will focus on one problem/issue area and will address:

- Legal/regulatory obligations
- Technical solutions and R&D information
- Operational and managerial considerations
- Policy considerations



The Perspectives will be distributed to CyLab and ISAlliance corporate members and will be posted in an Enterprise Risk Integration Repository on the members-only section of the CyLab Web site (www.cylab.cmu.edu). It is intended that the Perspectives will be shared with the appropriate people (General Counsel, CIO, CISO/CSO, CTO, CEO & Senior Management) within CyLab and ISAlliance member organizations to help foster a multidisciplinary approach to cyber security, privacy, and risk management issues. A series of CyLab Web seminars will follow each Perspective, with each seminar discussing one dimension of the issue.

This first Perspective focuses on Outsourcing Risk Management. CyLab Web seminars scheduled around the Outsourcing Risk Management Perspective are a five-part series scheduled on:

October 9: Technical Perspective: Software Assurance, Part I
October 16: Technical Perspective, Software Assurance Supply Chain, Part II

[1] Jody R. Westby, Esq. serves as Adjunct Distinguished Fellow for CyLab and is CEO of Global Cyber Risk LLC. She chairs the American Bar Association's Privacy & Computer Crime Committee and is the editor and co-author of four books on privacy, security, cybercrime, and the development of enterprise security programs.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

November 8: Operational/Managerial Perspective, Part III
November 29: Policy Perspective, Part IV
December 6: Legal/Regulatory Perspective, Part V

These programs are archived by program date on the CyLab Web site and can be viewed at any time by personnel from CyLab or ISAlliance member organizations. If there is interest in pursuing one or more aspects of outsourcing risks in greater detail, please notify Jody Westby, jwestby@andrew.cmu.edu. We welcome your input on topics and programs.

Future Enterprise Risk Integration Program topics that have been selected are:

- Security breach notification
- Privacy/security auditing requirements
- Incident handling

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

OUTSOURCING RISK MANAGEMENT

Globalization and competitive pressures are forcing businesses to outsource information technology (IT) services and functions, as well as many other business processing functions that are IT-enabled. Increasingly, this work, known as ITO/BPO (IT Outsourcing/Business Process Outsourcing), is going offshore. Irrespective of whether the vendor is located in the U.S. or in a developing country, the privacy, security, and cybercrime risk considerations – from both the service provider and client perspectives – are similar. There are, however, additional considerations that must be taken into account if the work is being performed offshore. This Perspective will examine the policy, managerial/operational, legal, and technical issues associated with privacy/security risks in the outsourced environment, and it will offer suggestions on how to dovetail these considerations for maximum risk management.

From the policy and managerial/operational perspectives, outsourcing of information technology and business processes requires companies to ensure that their compliance and governance obligations are being met through their service provider's operations. For example, all public companies must consider the integrity of their financial information and compliance with Sarbanes-Oxley (SOX), whether their data is maintained and processed internally or by an external provider. Financial institutions must also take into account regulatory guidance on managing outsourcing risks. From the legal side, there is a myriad of considerations regarding privacy and cybercrime laws, cooperation with law enforcement, search and seizure of electronic evidence, evidentiary and jurisdictional issues, and, of course, the underlying Master Service Agreement (MSA) and Service Level Agreements (SLAs). From the technical perspective, it also depends upon establishing effective controls and metrics and implementing a thorough incident response program. Effective risk management in the outsourced environment also requires knowledge about best practices, standards, and technical solutions and an understanding of the risks associated with software assurance.

THE DESIRED DOZEN:

The management of privacy and security risks in the outsourcing environment requires:

1. Understanding how privacy/security risk issues and compliance requirements can be incorporated into master service and service level agreements
2. Knowing what governance structures and policies/procedures need to be in place

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

3. Ensuring trusted and transparent provider-client communications
4. Analyzing cross-border data flows and conducting privacy impact assessments
5. Implementing effective controls and metrics
6. Training service providers on the client's culture, customer expectations, and risk management
7. Transferring operational knowledge from the client to the vendor
8. Enforcing privacy and security policies and procedures through monitoring and testing controls and metrics
9. Establishing effective incident response and crisis communication plans, including disaster recovery and business continuity
10. Integrating effective technical solutions and tools into a system architecture that utilizes best practices and standards
11. Establishing an enterprise security program within the service provider environment that manages client privacy and security risks and upholds compliance requirements
12. Conducting regular reviews and audits.

► THE POLICY PERSPECTIVE

Policy pressures are playing an increasingly important role in managing outsourcing risks. Primarily, these pressures are coming from three sources: (1) government policymakers and legislatures (domestic and foreign), (2) oversight bodies, and (3) public and customer expectations. Increasingly, policy considerations are impacting decisions regarding what functions to outsource, where they should be performed, by whom, under what contractual structure, and with what controls.

SOX requirements and a significant amount of financial regulatory guidance and memoranda on managing outsourcing risks have raised awareness about risks and influenced vendor-client relationships across all industry sectors. The Securities and Exchange Commission's (SEC) Office of the Chief Accountant and Division of Corporate Finance has responded to direct queries regarding third party providers performing activities that affect the initiation, authorization, recording, processing, or reporting of transactions in a company's financial statements, noting that: "In situations where management has outsourced certain functions to third party service provider(s), management maintains a responsibility to assess the controls over the outsourced operations….[and] is still

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

responsible for maintaining and evaluating, as appropriate, controls over the flow of information to and from the service organization."[2]

Pursuant to Section 401(a) of SOX, the SEC issued regulations relating to the disclosure of "all material off-balance sheet transactions, arrangements, obligations (including contingent obligations), and other relationships of the issuer with unconsolidated entities or other persons, that may have a material current or future effect on financial condition, changes in financial condition, results of operations, liquidity, capital expenditures, capital resources, or significant components of revenues or expenses." The regulation defined "off-balance sheet arrangements" to include "retained or contingent interests in assets transferred to an unconsolidated entity" and "material variable interests in unconsolidated entities that conduct certain activities." The SEC adopted a broad view of when disclosures might be material. Some experts have noted that the complexity of certain outsourcing relationships could cause material contingencies that must be disclosed.[3]

"Increasingly, policy considerations are impacting decisions regarding what functions to outsource, where they should be performed, by whom, under what contractual structure, and with what controls."

The greatest body of outsourcing guidance from the policy sphere, however, resides in the financial sector. U.S. financial regulators addressed outsourcing risk management as early as 1999, and have produced a wealth of guidance that serves as valuable resources to other industries and organizations.[4] For example, the Federal Deposit Insurance Corporation's 2004 report, *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks,* has been relied upon by risk managers, auditors, and attorneys across numerous industry sectors as a guide to understanding outsourcing risks.[5] In February of 2005, the Basel Committee on Banking Supervision produced *Outsourcing in Financial Services*, a report that provides high-level principles to guide the management of financial institutions.[6] In addition, the Federal Financial Institutions Examination Council's (FFIEC) IT Examination Handbooks on *Outsourcing*

[2] "Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports: Frequently Asked Questions," Securities & Exchange Commission, Office of the Chief Accountant and Division of Corporate Finance, June 22, 2004, http://www.sec.gov/info/accountants/controlfaq0604.htm.
[3] "Sarbanes Oxley Act of 2002: Disclosure of Material Outsourcing Contract Contingencies," Bierce & Kenerson, P.C., 2003, http://www.outsourcing-law.com/sarbanes_off_balancesheet122_2003.htm.
[4] *See, e.g., Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks*, Appendix D—Outsourcing Related Guidance, Federal Deposit Insurance Corporation, http://www.fdic.gov/regulations/examinations/offshore/appendix_d.html.
[5] *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks,* Federal Deposit Insurance Corporation, June 2004, http://www.fdic.gov/regulations/examinations/offshore/.
[6] *Outsourcing in Financial Services*, The Joint Forum, Basel Committee on Banking Supervision, Bank for International Settlements, Feb. 2005, http://www.bis.org/publ/joint12.pdf.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

Technology Services[7] and *Supervision of Technology Service* Providers[8] have had a significant impact on managing risk in the outsourced environment for many industries.

Industry groups have also had an influence in the policy arena. The Financial Services Roundtable has published some excellent materials for managing outsourcing risks, which have been useful to many companies and referenced by policymakers. Three of the most helpful are:

- *BITS Framework for Managing Technology Risk in IT Service Provider Relationships*[9]
- *BITS Key Considerations for Global Background Screening Practices*[10]
- *Key Contractual Considerations for Developing an Exit Strategy.*[11]

In February 2006, BITS launched a new initiative to develop standardized IT outsource provider risk assessments, dubbed as an "Outsourcing Report Card."[12]

Congress has also kept an eye on outsourcing, especially as public sentiment turns toward job protection at election times. Although most of the demand for restricting work going offshore has died down, security breach notification issues have spurred new policy activities. Most recently, the Government Accountability Office (GAO), at the request of Congress, investigated several aspects of outsourcing and released a report in September 2006 regarding privacy considerations associated with the domestic and offshore outsourcing of personally identifiable information (PII) in Medicare, Medicaid, and TRICARE transactions. The GAO surveyed 378 federal contractors and all state Medicare agencies and found that 90 percent of them engaged in some outsourcing, and 47-39% of them (varies whether Medicare, Medicaid, TRICARE, or state Medicaid) had experienced a privacy breach within the past two years. In addition, the GAO found that security breach notification procedures differed among the entities. The GAO recommended that the Centers for Medicare and Medicaid Services (CMS) require that all contractors handling PII notify CMS of security breaches. CMS and the U.S. Department of Defense (DoD) concurred with the GAO's recommendation. In its comments and evaluation of the report, CMS drew attention to a

---

[7] *Outsourcing Technology Services,* IT Examination Handbook, Federal Financial Institutions Examination Council, June 2004, http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf.

[8] *Supervision of Technology Service Providers,* IT Examination Handbook, Federal Financial Institutions Examination Council, Mar. 2003, http://www.ffiec.gov/ffiecinfobase/booklets/tsp/tech_ser_provider.pdf.

[9] *BITS Framework for Managing Technology Risk for IT Service Provider Relationships,* Financial Services Roundtable, Nov. 2003, http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf#search=%22bits%20framework%20for%20managing%20technology%20risk%22.

[10] *BITS Key Considerations for Global Background Screening Practices,* Financial Services Roundtable, June 2005, http://www.bitsinfo.org/downloads/Publications%20Page/bitsbcheck.pdf#search=%22BITS%20key%20considerations%20for%20global%20background%22.

[11] *BITS Key Contractual Considerations for Developing an Exit Strategy,* Financial Services Roundtable, May 2005, http://www.bitsinfo.org/downloads/Publications%20Page/bitsbcheck.pdf#search=%22BITS%20key%20considerations%20for%20global%20background%22.

[12] *See* "Risk Management: BITS Offers Outsourcing Report Card," *Bank Technology News,* Feb. 2006, http://www.banktechnews.com/article.html?id=20060201S19QWD9H.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

June 9, 2006 memorandum requiring security breach notification and stated that it is developing specific instructions for responding to such notifications. CMS also said it was adding provisions to its vendor contracts that would require written approval from CMS before any work involving PII could be performed offshore.[13] These decisions will impact numerous private sector contractors.

GAO and Congressional Research Service reports can also be useful tools in predicting legislative trends or action. The GAO, for example, noted in a 2005 report that "Concerns that offshoring could pose added risks to the privacy of personal information have led to a variety of proposals to enhance protections." Such proposals included requiring companies to keep work involving sensitive personal information in the U.S.; notification and consent requirements from U.S. residents before information can be sent abroad; and providing rights of action against foreign outsource contractors.[14]

"The GAO, for example, noted in a 2005 report that 'Concerns that offshoring could pose added risks to the privacy of personal information' have led to a variety of proposals to enhance protections."

Foreign policymakers also influence risk management of outsourced work. India's Prime Minister Singh, for example, has urged his government to enact a data protection law to improve privacy protections in India and to curb overly broad police powers in investigating cybercrimes, in order to enhance India's reputation as a responsible location for outsourced functions. At the other end of the policy spectrum, recent actions by Chinese policymakers in censoring and monitoring Internet communications have increased concerns among U.S. businesses about the confidentiality of outsourced work and business communications and the protection of intellectual property in China.

Lastly, public or customer expectations can have as much or more impact on the management of risks in outsourced operations as legislative, regulatory, or policy initiatives, and they should not be omitted from risk analysis of outsourced operations. Public expectations are driven, in part, by culture and thus can vary from location to location. U.S. citizens, for example, are especially concerned about what personal information the government has access to. EU citizens, however, are more concerned about what PII the private sector has about them – and what the people who have such PII will do with it. Regardless of what the law requires (or does not require), expectations of privacy regarding certain types of information, of notification in the event of a security

[13] *Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE,* U.S. Government Accountability Office, GAO-06-676, Sept. 2006, http://www.gao.gov/new.items/d06676.pdf#search=%22gao%20outsourcing%22.
[14] *Offshoring of Services,* U.S. Government Accountability Office, GAO-06-5, Nov. 2005, http://www.gao.gov/new.items/d065.pdf.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

breach, or of how risks are managed in the outsourced environment, cannot be ignored, lest market share, stock price, and reputation be placed at risk.

► THE MANAGERIAL & OPERATIONAL PERSPECTIVE

Management has the responsibility to ensure that reasonably foreseeable internal and external risks associated with outsourcing are identified and managed. It is imperative that management understand the full scope of the risks associated with outsourced work, ensure they are aligned with corporate risk strategy, establish adequate governance structures, and conduct annual reviews and audits.

All too often, however, risk assessments are conducted without all the critical inputs to the process, thereby ignoring important factors. Risk assessments must include:

- Compliance requirements
- The identification of critical digital assets and processes
- Technical considerations
- Risk management plans and input from previous reviews and audits.

Thorough risk assessments help management determine which risks it will accept, which ones it will reject, and which ones it will manage and mitigate through insurance, controls, governance checkpoints, and operational requirements (such as employee background checks, facility security, system availability, and business continuity requirements). They serve a particularly important role in managing privacy and security risks.
In the outsourced environment, companies do not have direct control over their outsourced business operations and so must pass risk determinations on to the service provider in the form of contractual obligations in the MSA and SLAs.

Pretend for a moment that you are the CEO, general counsel, or CSO of a publicly traded company that has (1) has outsourced its employee benefits processing to an offshore provider, or (2) outsourced the software development of a component of a secret design initiative to a provider located in the U.S., or (3) outsourced systems administration and help desk functions to an offshore provider.

The realities of privacy/security breaches in any of these situations are harsh:

- Your company's data is in the hands of a company you do not control; the service provider's CEO, General Counsel, or CSO will get the call about a breach before you do.
- You have little or no ability to control either service provider personnel, or how monitoring and enforcement of privacy/security policies and procedures are conducted.
- The service provider may not inform you if a breach occurs, or may inform you much later.
- The service provider might lack an adequate incident response plan – or have a plan but not follow it.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

- The provider may not capture adequate log data or preserve evidence.
- The service provider may make statements to the press, law enforcement, government officials, or employees that could harm your brand, impact your stock price, reduce your market share, or arouse regulatory or Congressional scrutiny.
- The offshore service provider may have a contractual obligation to protect data, but no statutory obligation or cybercrime law, thereby hindering law enforcement assistance or prosecution.
- The service provider may have other clients whose data or operations attract hackers and economic espionage, thereby jeopardizing your data.
- The service provider may get legal requests for your data or law enforcement may seize servers containing your data when investigating a matter involving another client of the provider.

Effective governance strategies create a balanced risk/reward environment between the client and service provider that encourages communication versus concealment of problems or issues. Much of the focus on outsourcing occurs in the front-end stages when companies are grappling with what to outsource, to whom, and where. There is often a lack of consideration regarding the governance structure, controls, metrics, measurement, and communication that are so important *after* the deal is done.

Computer Sciences Corporation (CSC), one of the world's leading outsourcing providers, admits that: "Over 50 percent of the [outsourcing] deals fail and around 75 percent fail to deliver the value expected by both parties. Well over half need to be renegotiated in the first 18 months due to 'material divergence between supplier and customer.'"[15] Something is obviously wrong. In part, it is the failure of the client to consider outsourcing from a lifecycle perspective, addressing legal and operational ramifications ahead of time, and developing a strategy with senior management that balances risk and reward and minimizes legal fallout. CSC confirms this view by acknowledging that:

> Traditional outsourcing arrangements do not cope well with radical change. They are transactional in nature and assume that much of what may happen in the next five to 10 years can be envisaged and captured in contract. They focus on legal remedies against nonperformance and attainable penalties rather than on the behaviors that each party will exhibit when faced with opportunity, threat, or regulatory requirement.
>
> No surprise then that in the "failed arrangements" . . . suppliers are almost always discharging their contractual obligations in full. The real issue is that those contracts

[15] David Thomas and Simon Knowles, "Shaping Deals That Last: The Principles of Dynamic Outsourcing," Oct. 2005, http://www.csc.com/cscworld/102005/fa/fa003b.shtml.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

> no longer reflected clients' needs and actually discouraged suppliers from meeting clients' real, rather than contractual, needs.[1]

On the client side, effective governance of outsourcing requires a different skill set than that needed when performing the activities internally. Companies cannot simply retain a few people to govern from their side and send the rest of the affected workforce over to the service provider. Outsourcing risk management requires clear communication channels between client and vendor, effective controls and metrics, useful knowledge transfer (two ways), and a balancing of risk and reward that encourages the vendor to disclose and resolve problems. Establishing a transparent, trusted relationship with the service provider is a critical step toward managing privacy and security risks.

Management also has the responsibility to ensure that the service provider has the requisite skills and capabilities to perform the outsourced tasks. Certifications are the preferred method of measuring capability. Carnegie Mellon's Software Engineering Institute (SEI) applied Total Quality Management (TQM) concepts to software development and created the Capability Maturity Model (CMM) for Software, with a certification program designed to certify an organization's capabilities in this area.[16] The CMM Software certificate quickly became a seal of approval for outsource service providers. Today, India has more CMM Level 5 certified organizations than the U.S., and these certifications have helped India become the trusted, global leader in outsourcing.

Effective governance strategies create a balanced risk/reward environment … and encourage communication versus concealment of problems or issues.

The success of the CMM model led to the development of the Software Acquisition CMM,[17] People CMM,[18] and CMM Integration (CMMI).[19] Drawing from the success of the CMM model, Carnegie Mellon's IT Services Qualification Center (ITsqc) was established to help address the needs of IT-enabled service providers and their clients and provide certification to client and service provider organizations. ITsqc developed the eSourcing Capability Model (eSCM) for Service Providers (eSCM-SP) and the eSourcing Capability Model for Clients (eSCM-CL) to help clients and service providers improve sourcing relationships and governance. The eSCM-CL addresses a full range of issues across the outsourcing life cycle. It enables client organizations to

[16] "Capability Model for Software (CMM-SW), http://www.sei.cmu.edu/cmm/.
[17] "Software Acquisition Capability Maturity Model (SA-CMM)," http://www.sei.cmu.edu/arm/SA-CMM.html.
[18] "People Capability Maturity Model (P-CMM) Version 2," http://www.sei.cmu.edu/cmm-p/.
[19] "CMMI," http://www.sei.cmu.edu/cmmi/.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

appraise the client-service provider relationship and better manage the outsourcing strategy and risks and establish effective governance. The eSCM-SP and its methodologies help determine service provider capability levels.[20]

It is also important that management and operational personnel consider areas where cultural differences may impact performance, such as in customer-facing activities. Successful outsourcing requires that a significant amount of knowledge be transferred between the client and vendor. Clients must train the vendor and its workers regarding their operational policies, organizational culture, and privacy and security requirements. In addition, it is important to transfer operational knowledge from the client to the vendor to ensure a smooth transition of the operations or function.

The cost and time demands required for such training are significant and can be the factor that eats away at the expected savings from the outsourced function. Moreover, this training has to be repeated for new employees and to accommodate changes in operational policies or procedures. For large projects or lengthy contracts, it is often repeated simply to ensure workers maintain an awareness of their client's needs. E-learning provides an excellent solution that ensures a consistent approach, and it can be delivered across oceans and time zones by the personnel most qualified to impart the required knowledge or train the workforce.

Customer-facing call center workers, for example, must understand their client's customer expectations, the culture of the client organization, and the performance that is expected of them. Some vendors in developing countries have embarked on call center activities, only to discover that their local workforce did not possess the skills necessary to answer incoming calls from the U.S. or Europe and conduct customer-facing communications. They did not understand what data comprised PII and why there were compliance concerns regarding how information is gathered and handled. Crash training courses conducted by frantic vendors are costly, largely ineffective, and erode the service provider-client relationship, while damaging the client's relationship with its customers and perhaps even tarnishing its brand, impacting market share, -- or worse – resulting in headlines regarding a privacy breach. This situation serves as an excellent example of why clear communication channels and mechanisms to detect and resolve problems at an early stage is central to successful sourcing.

Application development and maintenance (ADM) is another area where knowledge transfer is essential. Many U.S. companies are outsourcing their ADM work to India, China, the Philippines, and Eastern European locations. The software developers in these countries, while qualified, need to understand the business operations in which the software will be deployed and the operational considerations that will impact its deployment. They also need to learn what security measures apply to the system design and code and understand the processes for testing and transitioning the software into the production environment. BPO functions, such as fund management, legal

[20] "The IT Services Qualification Center," http://itsqc.cs.cmu.edu/.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

research, human resource activities, and medical transcription, require particularized training to ensure the successful transfer of the function from client to vendor without privacy and security problems.

A sound management plan for outsourcing will analyze all of these factors, set levels of risk, determine capabilities required, establish policies, and ensure the service provider implements the requisite privacy and security program.

► THE LEGAL & REGULATORY PERSPECTIVE

Although an IT or business process function can be outsourced, compliance requirements cannot. The global legal framework is far from static. Varying privacy, security, and cybercrime laws around the globe present a fractured international legal framework that compounds compliance issues in the outsourced environment. Cross-border data flows and differences between the U.S. and European Union (EU) in privacy protections present corporations with complex compliance and enforcement issues. The U.S. has one of the most complex privacy legal frameworks. It favors protections to specific types of data, often within industry sectors, such as medical or financial; has no centralized body charged with enforcement of U.S. privacy protections; and has a patchwork of state privacy laws. The EU, on the other hand, relies upon its omnibus Data Protection Directive ("EU Directive") to protect data that is considered personally identifiable information.

"It is important to remember the rule … the protections follow the data irrespective of how many borders it crosses. "

The EU seized the global stage on privacy protection with its adoption of the Data Protection Directive in 1995, and it has been the controlling force in privacy ever since. With a centralized regulatory body, the Article 29 Working Party, the EU demands that PII data sent beyond the borders of the EU be afforded "adequate protections" equivalent to those of the EU Directive. It is important to remember the rule, "Once EU data, always EU data;" the protections follow the data irrespective of how many borders it crosses.

The U.S. and EU were at loggerheads for years over the "adequacy" requirement of the Directive until the EU finally agreed that U.S. corporations that voluntarily joined the Safe Harbor Program would be deemed to provide "adequate" protection to PII (Safe Harbor is administered through the U.S. Department of Commerce and enforced by the Federal Trade Commission (FTC).[21] Companies that sign up for Safe Harbor must acknowledge their compliance with the seven basic principles of the EU Directive (notice, choice, onward transfers, access, security, data integrity, and enforcement) through their privacy policy. In addition, companies must self-certify annually that they are in compliance with the Directive's principles. All is not well, however, with the Safe Harbor program. A

[21] "Safe Harbor," U.S. Department of Commerce, http://www.export.gov/safeHarbor/index.html.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

2004 report to the Article 29 Working Party was critical of the implementation of the Safe Harbor program and its enforcement by the FTC.[22] Nevertheless, because the EU lacks enforcement authority over the Safe Harbor program, U.S. companies that at least make a good faith effort to comply with the principles of the program are not likely to encounter direct interference from the EU.

The cross-border data flow issue can become quite complex in outsourcing relationships. Basically, EU data may be sent out of the EU to another country if at least one of the following requirements is satisfied:

- It is going to another country deemed to have "adequate" protections by the EU;
- It is going to an organization in the U.S. which is a member of the Safe Harbor program;
- The sending party has the clear and informed consent of the person whose data is being transmitted;
- The sender and receiver have entered into a contract with standard contractual clauses approved by the EU; or
- The companies sending and receiving data are part of a multinational group with approved binding corporate rules.

Binding corporate rules (BCR) require an extraordinary amount of bureaucratic back-and-forth to get approval from each EU country involved. Although the EU is exploring a one-stop-shop approach for BCR, it has yet to be implemented. Therefore, contractual model clauses are used by many businesses in managing cross-border data flows. The Internet Security Alliance developed *Contracting for Information Security in Commercial Transactions: An Introductory Guide*[23] to help guide large and small businesses in using contractual model clauses to protect information and meet compliance requirements.

"…none of the top three outsourcing jurisdictions – India, China, and the Philippines – has a privacy law."

The Asia Pacific Economic Cooperation forum (APEC) recently adopted a Privacy Framework which is designed to accommodate cross-border data flows. Based on a self-regulatory model that incorporates some aspects of the EU Directive while embracing the unrestricted flow of data that is the hallmark of the U.S. model, the APEC Privacy Framework offers a hybrid approach that may well guide a number of developing countries as they seek to enact data protection laws which are consistent with the global legal framework.[24]

---

[22] "Safe Harbour Decision Implementation Study," Apr. 19, 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf.
[23] *Contracting for Information Security in Commercial Transactions: An Introductory Guide,* Internet Security Alliance, 2005, http://www.isalliance.org/.
[24] "APEC Ministers Endorse the APEC Privacy Framework, 2004/AMM/014rev1, Nov. 17-18, 2004, http://www.apecsec.org.sg/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

The most troublesome outsourcing legal/regulatory issues arise, however, in the context of a breach of privacy or security. In these instances, jurisdictional issues immediately become complex and can control the outcome of a matter. Many of the jurisdictional issues are driven by the fact that numerous developing countries engaged in outsourced operations do not have a data protection law or adequate cybercrime laws. For example, none of the three top outsourcing jurisdictions – India, China, and the Philippines – has a privacy law. India has been working on one for several years, but has been vacillating between the EU and US legal models. The APEC framework may give them a way to try to appease both the US and EU governments, except they cannot expect the APEC model to result in an "adequacy" decision from the EU Article 29 Working Party.

"The student, however, was beyond prosecution because, at that time, the Philippines did not have a cybercrime law that made such acts illegal."

Cybercrime investigations of privacy and security breaches are complicated by offshore outsourcing. Although cyberspace has no borders, law enforcement, diplomats, and prosecutors do; their authority stops at their national borders, and they must request assistance and cooperation from other countries. If the country where the outsourced work is performed does not have a Multilateral Assistance Treaty (MLAT) with the client's country, the U.S., for example, the government of the vendor's country may require the U.S. to use the cumbersome Letters Rogatory process to obtain international cooperation from law enforcement. In addition, many developing countries do not have law enforcement trained in handling cyber investigations and the search and seizure of electronic evidence. This, in turn, creates numerous investigatory and evidentiary issues.

Additional complications may arise if the country has dual criminality restrictions (the offense must be a criminal act in the country where it was committed as well as in the U.S.) or extradition restrictions. The most famous example of this was put forth in 2000 when the Love Bug virus damaged public and private sector computer systems around the world. The FBI tracked the attacks back to a student in the Philippines. The student, however, was beyond prosecution because, at that time, the Philippines did not have a cybercrime law that made such acts illegal. In developing governance plans and vendor policies and procedures, companies should plan ahead and work through international cooperation issues to the maximum extent possible.[25]

In addition, companies that outsource activities involving sensitive information or data, such as ADM, must ensure their service provider's operations meet the legal thresholds of economic espionage laws. The U.S. Economic Espionage Act of 1996 (EEA) requires proof beyond a reasonable doubt that:

[25] Jody R. Westby, ed., *International Guide to Combating Cybercrime, 2003,* http://www.abanet.org/abapubs/books/5450030l/.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

1. The person stole, obtained, destroyed, or conveyed the information without authorization of the owner;
2. The person knew or believed the information was a trade secret (broadly defined to cover confidential and proprietary information);
3. The information was, in fact, a trade secret within the definition of the EEA;
4. The person intended to convert the trade secret to the benefit of someone other than the owner;
5. The person intended that the owner of the trade secret would be injured; and
6. The trade secret was related to or included in a product produced or placed in interstate commerce.

If the government can establish that the person acted with the intent to benefit a foreign government, foreign instrumentality, or foreign agent, elements 4-6 are not required. [26]

In response to rampant identity theft and a well-known reluctance by companies to acknowledge security breaches, over thirty states in the U.S. have enacted some form of security breach notification law, requiring companies to inform people if their PII has been breached. The form and requirements for such notification varies and requires close coordination with outsourcing vendors and a coordinated communications plan.[27]

"Over thirty states in the U.S. have enacted some form of security breach notification law…the form and requirements for such notification varies…"

In addition, business continuity and disaster recovery considerations raise significant legal liability issues. Companies whose operations are dependent upon offshore vendors must ensure that the vendor's business continuity and disaster recovery plans are in line with their own risk management policies, that they mitigate any damages, and contain controls to ensure that the client remains in control of its operations and potential liabilities.

An analysis of cross-border data flows, privacy impact assessments (PIAs), and privacy audits are useful exercises that help guard against privacy and security breaches and ensure that controls, policies/procedures, training, and enforcement programs are effective. Privacy audits are also useful in identifying legal liabilities or conflicts associated with cross-border data flows. The U.S. Department of Homeland Security has released guidelines for development of PIAs, that provide valuable guidance to private sector entities as well.[28]

---

[26] "VIII. Theft of Commercial Trade Secrets," U.S. Department of Justice, Computer Crime and Intellectual Property Section, Apr. 23, 2001, http://www.cybercrime.gov/ipmanual/08ipma.htm.
[27] "2006 Breach of Information Legislation," National Conference of State Legislatures, Sept. 14, 2006, http://www.ncsl.org/programs/lis/cip/priv/breach06.htm.
[28] "Privacy Office – Privacy Impact Assessments," U.S. Department of Homeland Security, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

► THE TECHNICAL PERSPECTIVE

Outsourcing risk management can be assisted and facilitated by technical solutions, but the complexity of the issues and problems puts it beyond a "silver bullet." In the outsourced environment, the miles and oceans between client and service provider make technical solutions all the more attractive. They cannot, however, be deployed in isolation; they require policies and procedures and integration throughout the outsourcing lifecycle.

For example, numerous technical solutions exist to address issues such as personal identity verification (PIV), authorization controls, anomaly detection, and data integrity. The National Institute of Standards and Technology (NIST) has developed Federal Information Processing Standard (FIPS) for PIV, FIPS 201.1, and certain products have undergone a certification process to certify that they meet this standard. Utilization of these products and this standard at least affords outsourcing service providers and clients a technical solution that is tested and in compliance with U.S. Government requirements.

"It is imperative that the vendor technical team work shoulder-to-shoulder with client's outsourcing team of legal, management, operational, and security personnel."

Other solutions that are valuable in the outsourcing environment include private sector steganography detection software that can help prevent the loss of confidential and proprietary data, and live investigatory and forensic tools which help organizations adopt a proactive posture against security breaches. Anomaly detection software also helps detect unauthorized access to data, networks, and applications and can serve as an early warning system by flagging unusual communication paths. Encryption, monitoring software, and management dashboard tools are also valuable in the outsourced environment and can reduce legal and operational risks and improve client-vendor trust and facilitate the resolution of issues. It is imperative that the vendor technical team work shoulder-to-shoulder with client's outsourcing team of legal, management, operational, and security personnel in determining what technologies to use, the policies and procedures required, and controls and reporting needed.

Technical considerations in ADM are some of the most vexing, and, to date, many of them do not have developed solutions. Software assurance and malicious code detection are among the most difficult issues facing companies that are outsourcing ADM functions. It is important that client companies know if the software that is developed on their behalf contains malicious code or is vulnerable to attacks. Approaches in general use include systems-level penetration testing, code inspection, process oversight, and various kinds of certification such as ISO 15408 Common Criteria. As software becomes more complex and interconnected, system-level black-box testing becomes relatively less effective, because it cannot provide accurate assessment on internal phenomena such as fault tolerance policies, audit and logging, intermittent errors, and deliberate combination vulnerabilities. In the past five

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

years, tools and techniques have started to emerge that focus more closely on direct white-box and gray-box evaluation of code. These tools focus on particular categories, or *attributes*, of flaws and vulnerabilities. These attribute-specific, product-focused tools enable the direct analysis of code for a particular attribute, such as buffer overflows or synchronization errors.

The CyLab Software Assurance Interest Group (CSAIG), co-chaired by Professor William Scherlis, Director of CMU's Institute for Software Research, and Larry Maccherone, CyLab Manager of Software Assurance Initiatives, is focusing on:

- Understanding current best practice, including market drivers, metrics, and representative case histories.
- Assessing new opportunities and emerging technology, including core ideas, promising lab concepts, and expectations of benefits, costs and risks. This includes tools and techniques for direct code evaluation, as well as practices that can apply at higher levels of architecture and frameworks.
- Developing an understanding of how to plan, including means to make assessments and integrate new techniques into practice without disruption and with acceptable risk.
- Identifying common issues relating to software assurance, including evaluation of technologies and techniques, tool roles in practice, and the market significance of software assurance.

Some of the specific ideas being explored include:

- Attribute-specific product-focused tools
- Technical infrastructure
- Explicitly managed design intent
- Emerging ROI case
- Market drivers
- Certification challenges.

The CSAIG is identifying a framework for understanding the range of possible points of intervention within software "supply chains" and across the software development lifecycle.

The challenge is what steps can be taken beyond the baseline best practices for software security evaluation, such as:

- Federal Information Security Management Act & NIST guidance/standards
  - Evaluate system controls
  - Evaluate management practice
  - Evaluate operational practice

- CMM/CMMI
  - Evaluate the team
  - Evaluate the process

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

- National Infrastructure Assurance Partnership (ISO 15408) Common Criteria
  - Evaluate the process
  - Evaluate the design
  - Sample the product.

These three techniques are all limited because they focus on observables that are only indirectly connected with the actual software that will execute in critical systems. (Prof. Scherlis notes that Common Criteria is generally viewed as effective for specific narrow functionalities, but less so for larger general-purpose components such as operating systems databases and application servers.) This motivates the focus of CSAIG on more direct means for software assurance.

It is the need to directly assess the software itself that is driving the broad range of work underway in the community related to direct software analysis. Microsoft is a leader in this area, particularly with respect to its own internal software development. Direct assurance tools are needed that can assure attribute-specific, objective analysis of the quality, dependability, and security of the software itself. In addition to the usual measures for technical and security-focused acceptance evaluation, Professor Scherlis offers the following examples of critical technical elements for evaluating outsourcing software components and subsystems:

- What are the software interfaces that mediate between the outsourced code and the enterprise operating environment? Are these interfaces well defined in the sense that verification can be done of compliance for both clients and service providers?
- Are auditing and logging mechanisms in place to monitor behavior within components and across components (as a way to facilitate both real-time detect and forensic analysis)?
- Is the architecture designed to be robust, in the sense of containing or mitigating failures within components, including outsourced components? Is logging in place to support forensic analysis of internal failures?
- Is the architecture designed to centralize or delegate security-critical functions to appropriate central components (e.g., maintain tight controls over regions of code that must handle the most critical security-related information -- the "trusted code base")?

He does note, however, that trust relationships and effective engagement processes for producers and consumers remain the most critical element of outsourcing relationships. It is important to consider:

- What representations and warrants are offered by the outsourcing provided regarding support for acceptance evaluation of provided products?
- What collaborative process is defined to assure mutual satisfaction on the scope of requirements, even in situations where requirements are rapidly evolving?

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

- Does the outsource provider have sufficient staff to co-locate with the client to ensure requirements gathering and validation will be successful?

For code-level software assurance, new technologies are emerging that can support direct evaluation for particular attributes related to quality and security. Software assurance is a concern both at the system level (with concerns ranging from intermittent overall failures to SQL injections and buffer overflows on the "attack surface") and also at the code component level (with a much broader range of concerns appropriate to internal software interfaces, ranging from null references to race conditions and framework compliance). There are many new technologies that are emerging that can provide useful capabilities to support direct evaluation for a broadening range of critical attributes. We see that these are already showing value in many production situations and they will be continuing to mature and expand in scope over the next few years. There are a number of commercial and research tool offerings. Preliminary results suggest that multiple tools perform better than any one of them.

"Software assurance is a concern both at the system level…and also at the code component level..."

One example is the Carnegie Mellon Fluid project, led by Professor Scherlis, which is focused on creating practicable tools for programmers to assure and evolve production software systems. The drivers of the Fluid project are considerations of software scale, composability (to link results separately obtained for components of a system), adoptability (particularly by developers and immediate managers), and measurement of value. The project's focus is on the program properties that bear primarily on code safety, vulnerabilities and security, Application Programmer Interface (API) compliance, and dependability. The project is focusing on those critical program properties that tend to defy traditional testing and inspection regimes because, for example, they may involve non-determinism or they are non-local in character, in that there may be no single place in the code where they are manifest.

The Fluid team has explored properties including race conditions and locking policies, threading policy, unique references, and other programmer- significant properties such as aliasing, effects, real-time threading policies, and single-threading policies. A key feature is the use of composable analyses to assure consistency of code and programmer expressed models of code-related design intent. Thus, a failure to achieve assurance can indicate an error in the model, an error in the code, or occasionally an insufficiently powerful analysis. A principal result is that design intent is highly valued by developers, and that it can drastically reduce false positives, and that it can enable the tool, for many critical properties, to offer positive assurance—that is, an absence of false negatives (i.e., for a particular critical attribute no defects found means no defects exist). The team has validated many of the key concepts relating to the project's goals through an aggressive program of field trials with multiple CyLab member companies, with the result that the tool is undergoing commercialization and is in increasing demand for production software development and evaluation.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

Other materials developed by technical auditing experts provide valuable guidance on software security assurance and useful management compliance checklists.[29]

► CONSIDERATIONS AT-A-GLANCE

Policy	Oper/Managerial	Legal	Technical
Balance competitiveness v risk	Identify critical assets & processes	Identify compliance requirements, contractual obligations, jurisdictional issues, liability issues	Consider existing system architecture, interconnection points, existing policies/procedures
Consider legislation • Privacy & Security • Offshore restrictions • Cross-Border data flow restrictions	Consider compliance requirements & contractual obligations	Analyze cross-border data flows	Privacy & security technical tools needed: viruses, worms, malicious code detection
Consider regulatory guidance and memoranda • SOX (integrity, reporting material transactions) • Financial guidance & memoranda	Consider technical considerations, restraints	Check privacy, security, and cybercrime laws in outsourcing jurisdictions (including economic espionage)	Determine authentication/authorization access controls (personal identity verification), encryption technologies needed
Review GAO & Congressional Research Svc reports	Review previous reviews/audits, risk plan	Identify IP considerations, protections needed	Determine monitoring, anomaly detection technologies needed
Review industry best practices	Analyze governance structure needed, communication channels (including crisis communications)	Review MSA/SLAs re provider moving work to new location (in and out of country); Determine restrictions needed	Determine incident and investigation tools needed (steganography detection, live investigatory and forensic tools, logging tools, etc.)
Consider foreign policy initiatives	Define operational criteria, business continuity, disaster recovery criteria	Identify legal requirements & risks re security breach notification	Consider R&D underway
Consider foreign trade restrictions	Consider client and vendor cultural issues	Identify business continuity/disaster recovery legal issues	Determine if export control issues

[29] *See, e.g.,* Charles H. LeGrand, *Software Security Assurance: A Framework for Software Vulnerability Management and Audit,* 2005, http://www.ouncelabs.com/audit/.

© Carnegie Mellon University and Jody R. Westby. All rights reserved.

Policy	Oper/Managerial	Legal	Technical
Consider customer & public expectations	Define vendor privacy/security requirements, push down of policies Define vendor qualification level, personnel background check requirements Identify best practices to use Identify knowledge transfer issues & training needs Define controls needed Evaluate ROI	Identify legal issues associated with cybercrime & investigations, map intl cooperation plan Prepare privacy impact assessments on PII Review vendor audits Conduct privacy audits Review MSA/SLAs	Determine management reporting and vendor dashboard technologies needed Determine adequacy of physical facilities' security systems Review best practices & standards Define technical policies & procedures
Web Seminar Pgm – OCT 9	**Web Seminar Pgm – OCT 16**	**Web Seminar Pgm- Nov 8**	**Web Seminar Pgm – Nov 29**
Software Assurance, Part I	Software Assurance, Part II	Managerial/Oper Considerations, Part III	Policy Considerations, Part IV
Web Seminar Pgm – Dec 6			
Legal Considerations, Part V			

© Carnegie Mellon University and Jody R. Westby. All rights reserved.