



MANAGING THE REALITY OF IT RISK

New York State Society of
Certified Public Accountants

March 2, 2004



Your Host

Joel Lanz, CPA/CITP, CFE, CISA, CISSP

- Over 23 years of IT risk management experience ranging from one-person “IT shops” to global organizations.
- Principal of a niche technology risk management CPA practice, with prior experience as a Big 5 Business Assurance and Risk Consulting Partner and an Internal Audit Vice President.
- Adjunct Professor at the School of Professional Accountancy, College of Management, C.W. Post Campus of Long Island University – Instruct required graduate course entitled “Advanced Assurance and Computer Auditing.”
- Executive Member – Professional Standards, NYSSCPA Technology Assurance Committee.
- Articles published in The CPA Journal, RMA Journal, Bank Accounting & Finance, Commercial Lending Review, AICPA InfoTech Update, IS Audit & Control Journal, etc.
- Contributed to four books and guides

GO SETTERS!!!!!!!!!!!!!!!!!!!!!!!!!!!!

- MBA
 - Information Systems
- BBA
 - Accounting





Presentation Outline

- Introduction
- Presentation Assumptions
- It's Sorta Like Marriage
- Identifying IT Vendor Risk
- Mitigating the Risk
- References
- Staying In Touch



Presentation Assumptions

- Please ask questions throughout the presentation
- To maximize value to the audience, the following presentation assumptions were made:
 - The decision on whether or not to outsource (especially the whether to outsource to an offshore provider) is beyond the scope of the current presentation.
 - To the extent possible, generally recognized and accepted standards and guidelines are leveraged. This strengthens support for identified IT vendor management recommendations. It also provides better support for those implementing IT vendor management programs in response to heightened regulatory expectations.
- The speaker will be available after the presentation and welcomes any questions on the above or any topics discussed during the presentations



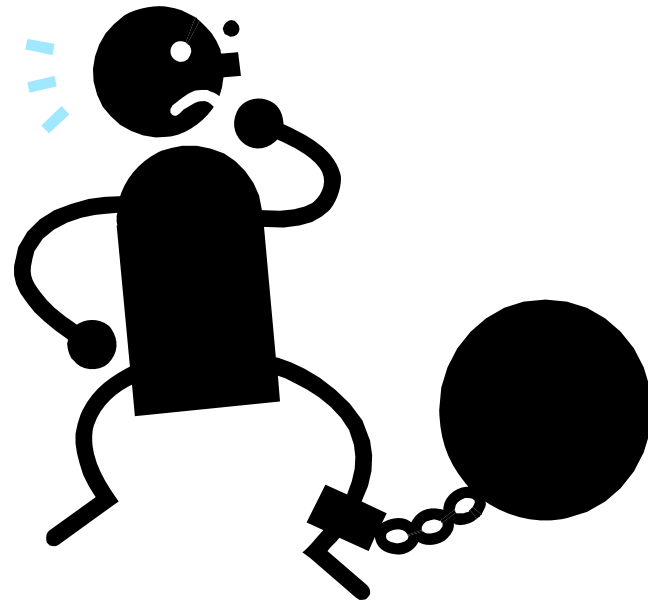
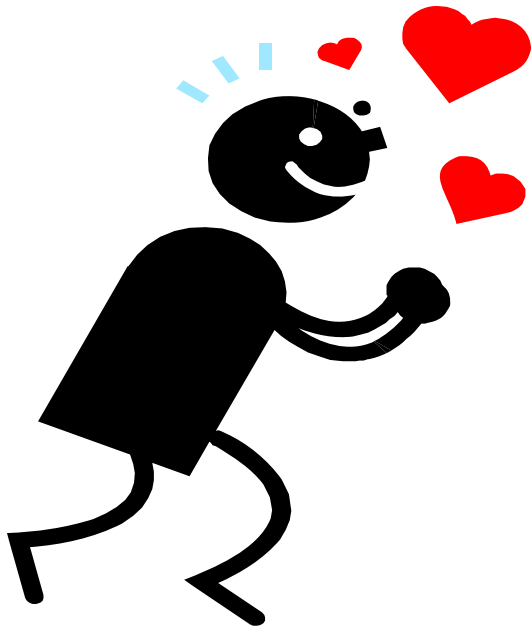
A Friend To Help Me Out

- Vend R. Risk, PhD.
- When you see “The Doc” in the presentation, we will be discussing an extremely critical point – so look out for him.





IT'S SORTA LIKE MARRIAGE





The Sarcastic Perspective

- What do IT vendors contribute to the business?
 - Whitepapers on never developed solutions
 - Opportunity for the Legal Department to actually do some work
 - Greater bureaucracy in getting things done
 - Savings on clothes, attaché cases and coffee mug purchases



The Realistic Perspective

- What do IT vendors contribute to the business?
 - Financial flexibility in choosing amongst technology alternatives
 - Ability to focus on the market and core strengths that drive maximum value
 - Avoid the politics of corporate “quality challenges” regarding technical skills and lack of specialized knowledge
 - Products and services needed to implement business strategies

Friend or Foe?

IT Vendors Are A Business Reality

- Are we really strategic partners with mutual long term objectives, or is my company only a cash cow?
- Can an outsider provide the same degree of care and concern as I would exercise?

Bottom Line –

Stop Whining and Start Managing The Relationship



Applying Lessons From Marriage

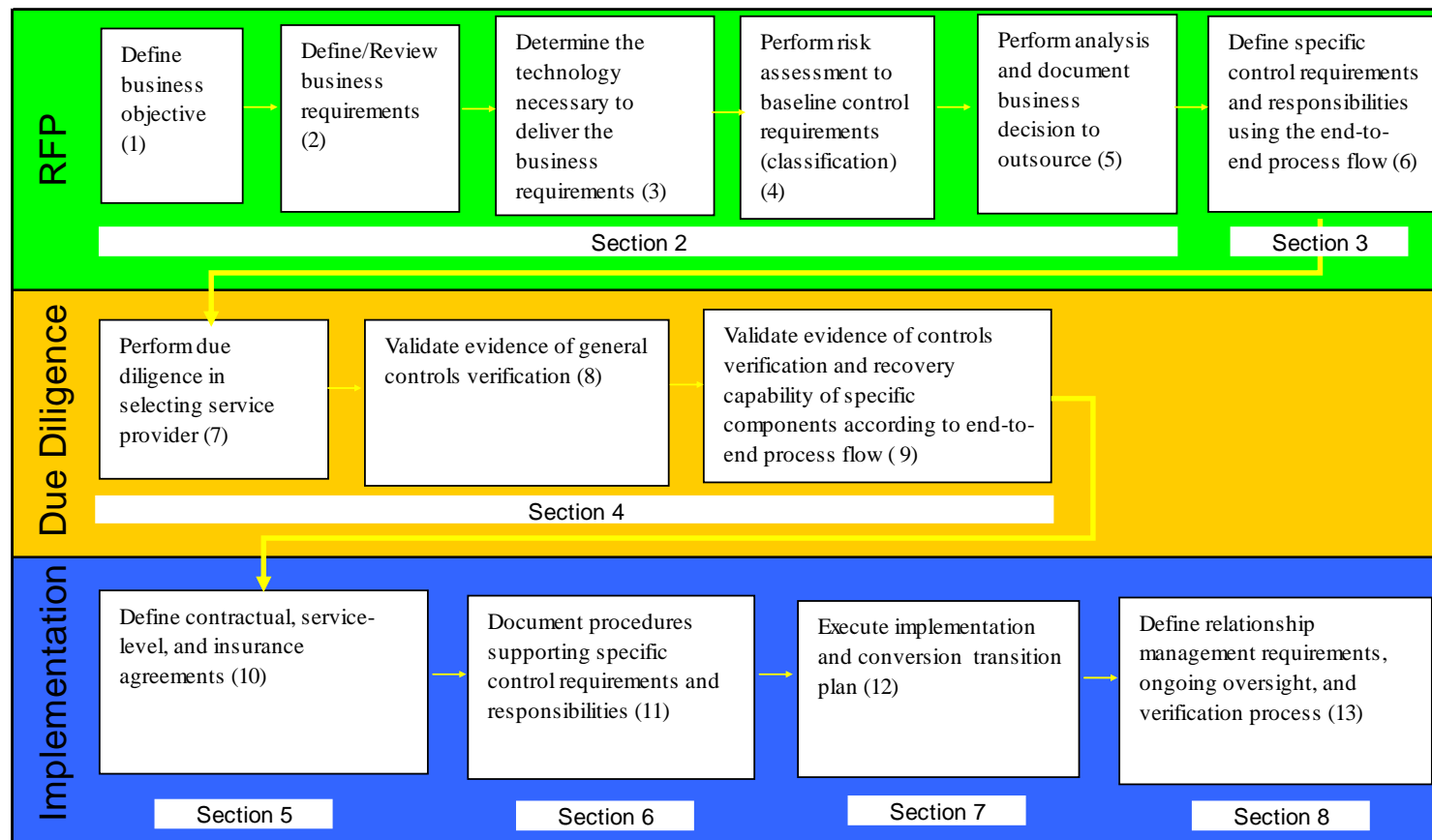
QUOTE ATTRIBUTABLE TO MARRIAGE	HOW IT VENDOR RISK MANAGERS CAN APPLY THE QUOTE
"Can two walk together, except they be agreed?"	Document the understanding and all expectations with the IT Vendor in writing
"in sickness and in health, to love and to cherish, till death do us part"	Beware long term outsourcing agreements. Once signed, it can be very expensive to terminate.
"In an ideal marriage one partner is blind and the other is deaf"	No one is perfect. Seldom is only one party (e.g., the IT vendor) always at fault. Control weaknesses contribute to poor vendor relations.



What Drives The “Romance”?

- Senior Manager’s concerns about cost and quality
- Breakdown in IT Performance
- Intense vendor pressures
- Simplified management agenda
- Financial factors
- Corporate culture
- Eliminating an internal irritant
- Other factors
 - Keeping up with the “Joneses”
 - Senior Management Skill Set

BITS IT Service Provider Framework Flow Diagram





Sample BITS Guidance

■ DUE DILIGENCE

- Assess audits, security, and performance
- Determine provider's reliance on third parties
- Determine impact on your current partners
- Determine service availability options
- Assess the recovery plan
- Assess testing of the plan
- Determine market reputation

■ CONTRACTUAL

- Scope of services
- Financial soundness and change in business strategy
- Processing environment
- Confidentiality
- Access administration
- Security
- Controls verification
- Change control
- Records retention
- Business continuity
- Regulatory compliance
- Penalties and exit clause



A Good Contract Is The Foundation to Successfully Managing IT Vendor Risk

- Obtain legal counsel from an attorney familiar with similar transactions
 - Most companies use their general purpose corporate attorneys
 - Consider setting attorney's scope to go beyond simple contract language review
 - Confirm compliance with key industry or regulatory practices – many of which can be identified through basic research on the internet

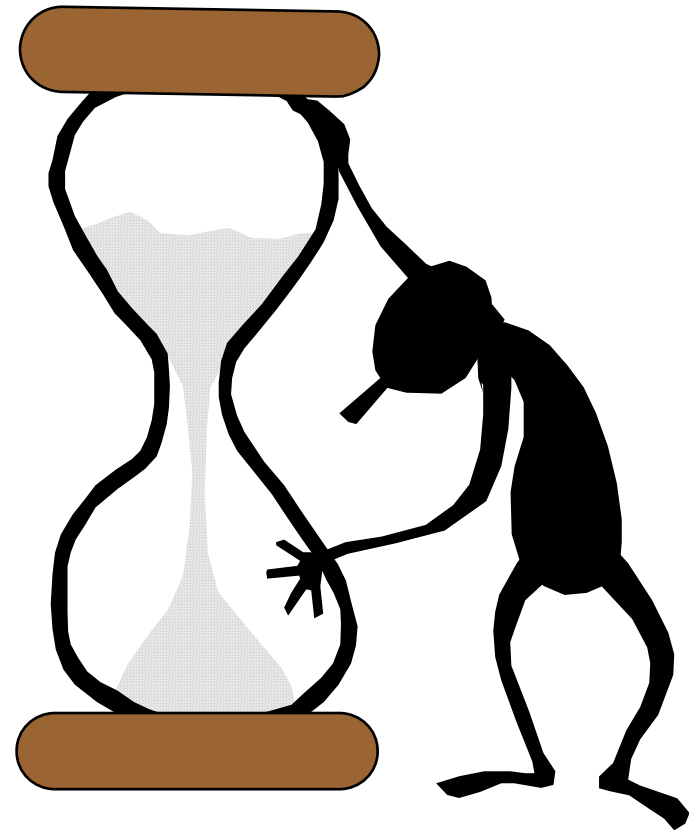


Structuring the Agreement

- Contract Flexibility
- Standards, Control and Regulatory Compliance
- Areas Outsourced/Purchased
- Financial Considerations
- Cost Savings (if premise for the transaction)
- Supplier Stability and Quality
- Management Fit
- Conversion Management

Case Study - Background

- Client is a \$7 billion regional bank that outsources core processing
- Contracts have been reviewed and approved by internal and external counsel.
- Quality of service is perceived as poor by the bank. Outsourcer very focused on managing costs.
- My engagement scope is an “internal controls review” to review the relationship with the outsourcer and to determine the “right things are happening.”
- This case study limited to procedures over contract review





Case Study – Relevant Procedures and Obstacles

■ Procedures

- Obtain and review all relevant contracts with the vendor
- Assess procedures used by the bank to monitor compliance with contract terms - including charges
- Determine that regulatory recommendations for outsourcing contracts included in this particular contract

■ Obstacles

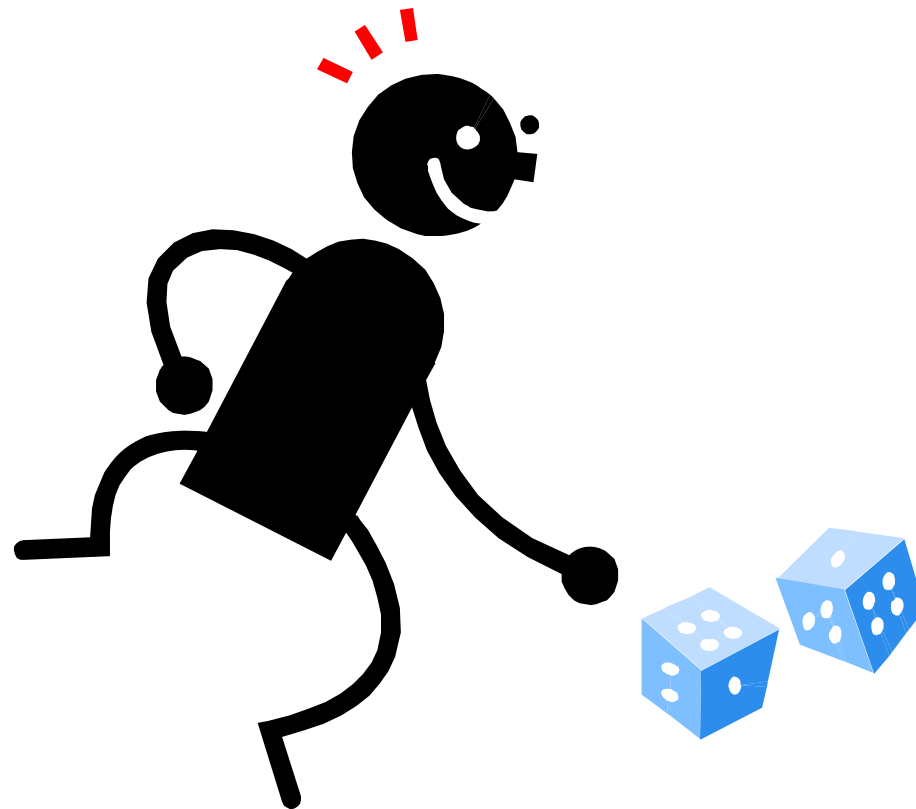
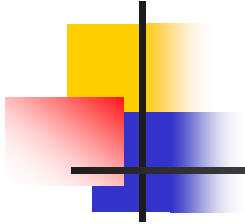
- CFO (who was responsible for contract negotiation, thought it a waste of time).
- No accountable executive or function assigned to manage the contract.
- Each business unit forced to fend for itself in dealing with the vendor.
- Management has minimal skills in technology matters and considers the vendor a “strategic partner.”



Case Study - Findings

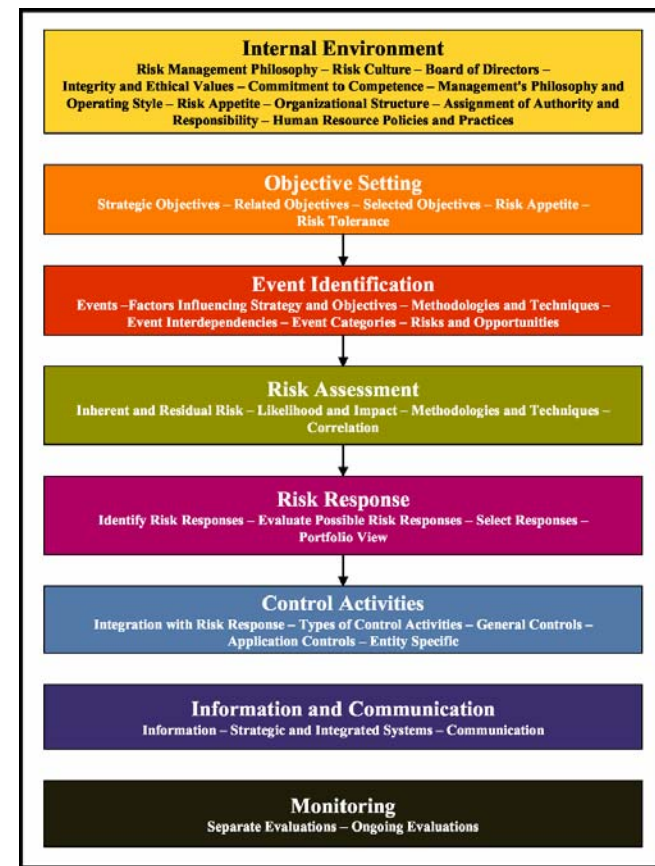
- Existing contract, although reviewed by legal counsel, did not include key contract provisions required by the bank's regulators.
- Many of these omitted provisions are "best practices" that should be included because they make business sense – not just because of the regulatory expectation.
 - Service levels and performance expectations not specified
 - Audit clause provisions not included
 - No provision for coordinating continuity plans
 - Security responsibilities over "networks" not specified
 - Insurance coverage to protect the bank not mentioned
 - Confidentiality of information and ownership of data not specified
 - Required supporting details (and documentation standards) for variable expense charges billed to client not mentioned.
- Subsequent review by legal determines that although over 75% of variable expenses charged by the IT vendor could not be substantiated, based on existing contract provisions, the bank was responsible for payment.

IDENTIFYING IT VENDOR RISK



Brainstorm the Impact of IT Vendors on Enterprise Risk

- Leverage COSO's "Enterprise Risk Management Framework (Draft)" to identify potential areas that rely on IT Vendors and therefore generate risk





Typical IT Vendor Risks

- Common integrity, value and risk appetites
- Alignment of strategic goals and business objectives
- Appropriate and well-thought out methodologies to deliver solutions
- Existence of risk management program to mitigate vendor service delivery risk
- Adequate insurance coverage
- Appropriate security and application controls
- Reporting on service levels
- Reviewing independent third-party reports (e.g., SAS 70, Trust Services)



Atypical IT Vendor Risks

- Organizational structures that facilitate cooperation and partnerships
- Allocation of IT Vendor resources to your account
- Overall coordination plan for handling “incidents” especially when insurance and the media are involved
- Consideration of unique client risks such as regulatory or industry (e.g., Privacy)
- Mismatched attitudes or appetites relating to internal control
- Adequacy of IT vendor billing and service quality controls
- Defining and managing the “right” service levels
- Quality of “right-to-audit” clauses and ability to actually conduct an audit



MITIGATING THE RISK



Prioritizing Vendor Activities by Risk

<i>Perceived Risk</i>	<i>Percentage of Vendors</i>	<i>Percentage of Effort</i>	<i>Applicable References</i>
HIGH	5-10%	80%	Software Engineering Institute BITS
MEDIUM	10-20%	15%	CoBIT DoD Contractor Fraud Handbook
LOW	10-90%	5%	Relevant articles and generic workprograms (e.g., contract compliance and payables)



“Good” Practices

- Be careful “whom you marry” (due diligence)
- Document ALL expectations – including getting a “pre-nup” agreement
- Assign accountable executive – both for service delivery and cost of service
- Develop contract extracts (in english) so that “the team” knows the rules
- Measure and monitor what’s important
- Trust but verify (use the audit clauses)
- Implement “fraud prevention” program (to catch honest mistakes)
- Exercise prudent business judgement



REFERENCES

- "The Pros and Cons of IT Outsourcing," Antonucci, Lordi and Tucker, Journal of Accountancy, June 1998.
- "BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships – Version II," November 2003
- "Guide to Information Technology Security Services: Recommendations of the National Institute of Standards and Technology," Special Publication 800-35, October 2003.
- "Outsourced Managed Security Services," Carnegie Mellon Software Engineering Institute, January 2003.
- "CoBIT," IT Governance Institute, 2000.
- "AICPA Audit Guide – Service Organizations: Applying SAS No. 70, As Amended," April 15, 2002.
- "Suitable Trust Services Criteria and Illustrations," AICPA/CICA, 2003.
- "Worst Information Technology Practices in Small to Mid-Size Organizations," Lanz, The CPA Journal, April 2002.
- "Handbook on Fraud Indicators for Contract Auditors," Inspector General Department of Defense, March 1993
- "Fraud Examiners Manual," Association of Certified Fraud Examiners, 2003



Staying In Touch with Joel

- Contact Joel directly at:
Joel Lanz
Joel Lanz, CPA, P.C.
P.O. Box 597
Jericho, NY 11753-0597
(516) 933-3662
jlanz@infotechcpa.com
- Visit www.infotechcpa.com for upcoming vendor management related articles:
- "Managing IT Outsourcing Risks" (Influential Accounting Journal – June 2004 Tentative Date).
- "Incorporating SAS No. 70 and Other Reports into a Vendor Management Program" (The RMA Journal – April 2004).
- "Unmasking IT Fraud: Practical Applications of SAS-99" (Bank Accounting & Finance – April 2004)
- "Five Must Ask Outsourcing Due Diligence Questions" (Western Banker – January 2004)