IT Security Risk Assessment

What a company should see in its offshore software vendor

By

Kashif Manzoor

Graduate Student, Computer Science

Motivation

- IT is a first class citizen in most of the companies today
- New regulations and legislations require tighter IT security controls.
- Plethora of IT standards create an *IT Standards fish market*
- Standards are too general, overwhelming and costly to implement.

IT Outsourcing

- Declining profits require cost control.
- Outsourcing is a good cost control method.
- Outsourcing has its risks.
- Vendors do not have the same motivation/threat to implement tighter security controls.
- Customers can force the vendor to comply with a standard.

COBIT, ITIL, ISO 17799

- COBIT very thorough – a superset of most of the IT standards (e.g. fully compliant with ISO 17799)
- ITIL more concerned with software development management, competes with ISO 9001:2000 and CMM.
- ISO 17799 (ISO 17799 + ISO 27001(BS 7799)) *relatively* lightweight only concerned with IT security.
- All standards have a financial baggage.
- The context determines which standard to use and how much should it be customized. That is why most of the auditors like protiviti have their own assessment checklist which they improvise from various standards.

Need of the hour

- A lightweight, concise and easy to follow standard.
- More targeted and specific to the given context.
- Minimal Implementation cost.

the context – the solution

- The context:
  - Offshore software development outsourcing.
- The solution:
  - IT security risk assessment of an offshore vendor.

The assessment checklist stats

- 9 sections.
- Each section has 0-3 sub sections.
- 159 security items.
- Items are very specific and concrete.
- Each item can have Yes,No, N/A
- Each yes response is further qualified by *just started*, *partially completed*, *fully implemented*,
- Each item has a severity level
- Risk score is calculated for each of the item.
- Risk abated by the vendor is calculated - the higher the better
- The checklist is implemented as EXCEL sheet with embedded formulae for Risk score calculation.

ORGANIZATION	Response	"Yes" Details	Severity	Risk Score	
SECURITY POLICY	YES. NO. N/A.	Planned / just started. Partially completed. Fully implemented.	High. Medium. Low.	Calculated	Risk Upperlimit
Have the Information Security Policies been issued to all employees, including third party personnel and contractors?	Yes	Planned / just started	Very High	2	4
Have all employees formally acknowledged adherence to the Information Security Policies?	Yes	Partially completed	Very High	1	4
Are employees required to annually re-acknowledge compliance with the Information Security Policies?	Yes	Fully implemented	Very High	0	4
How and when do you perform internal audits to measure compliance with the Information Security Policies?	Yes	Planned / just started	High	1.5	3
How frequently do you perform periodic reviews to update security policies and guidelines for relevancy and emerging topics?	Yes	Partially completed	High	0.75	3
Are controls in place to restrict your ability to transmit customer data to unauthorized personnel outside your company ?	Yes	Fully implemented	High	0	3
Has an organizational policy on copyright compliance been implemented and communicated to all users?	Yes	Planned / just started	Medium	1	2
Do you have a policy that prohibit generic logon account and do you follow the policy?	Yes	Partially completed	Medium	0.5	2
Are all the following subject to data confidentiality agreements? * Permanent employees * Contractors / temporary staff * 3rd Party service providers	Yes	Fully implemented	Medium	0	2
Has your business issued an E-mail Usage Policy ?	Yes	Planned / just started	Low	0.5	1
Do you take action against users who use e-mail in contradiction to the E-mail Usage Policy ?	Yes	Partially completed	Low	0.25	1
Has your business issued an Internet Policy? (e.g. only access the Internet for legitimate work-related purposes, no downloading of games, etc.)	Yes	Fully implemented	Low	0	1
Are all users required to sign an internet usage and responsibility agreement that acknowledges compliance with the stated Internet Policy?	No		Very High	4	4
Are there comprehensive documentation standards for IT development and operational controls?	No		High	3	3
Is there a clear desk policy ?	No		Medium	2	

TotalRisk Score	17.5
Maximum Possible Risk	41
%age risk abated:	0.573171

Be safe

Thank you