1 = very basic customer information, such as name and contact information.
2 = isolated information about particular transactions
3 = information about type of account, as well as identification details
4 = transaction history, high balance, low balance, credit limits, or account number
5 = full account/loan information.

Risk Assessment Matrix			
	Service Provider is not bound by a code of conduct or the infosec guidelines.	Service provider is bound by a code of conduct relating to privacy/confidentiality .	Service provider is directly bound by the infosec guidelines.
Sensitivity Level = 1			*Zone of **least** danger. Because of low data sensitivity and direct application of the infosec guidelines, service providers who fall within this category should not require your monitoring.*
Sensitivity Level = 2			
Sensitivity Level = 3			
Sensitivity Level = 4			
Sensitivity Level = 5	*Zone of **greatest** danger – you should plan to monitor any service provider who fits here on the matrix.*		

Background and Instructions

The level of scrutiny and monitoring you must give to the privacy/information security practices of a service provider will depend upon two factors: whether the service provider is directly subject to the information security guidelines or a code of conduct that mandates confidentiality and the sensitivity of the information to which the service provider has access.

To use this tool, write the service provider's name in the appropriate box. There will be some boxes that will have multiple names.

I suggest you color code the boxes and decide, as a matter of internal policy, what your level of monitoring will be. Maybe you could adopt a variation on the alert levels of the Office of Homeland Security. A service provider with access to customer data with a sensitivity level of 5 who is not bound by a code of conduct and not directly subject to the information security guidelines would be red; a service provider who accesses customer information with a sensitivity level of 1 and who is directly bound by the information security guidelines would be green.

Once you decide which colors will go where, you need to decide what action, if any, you need to take for service providers who fall within each color zone. Do you need to conduct your own security reviews or tests? Will they have audit results and test results that you can review? What frequency of monitoring is appropriate?

Then, create a legend to go with your matrix. The legend should explain what the color codes mean and the action you intend to take on service providers within each color region.

Each time you add a new service provider, remember to add them to the matrix.