

# Vendor Management

in a continuous compliance environment



## The Garland Group

- IT Audit / Security Testing
- Continuous Compliance
- Collaboration Consulting

riskkey.com

The screenshot shows the RiskKey website homepage. At the top, there is a navigation menu with links for HOME, PRODUCTS, OUR COMPANY, SERVICES, PARTNERS, and BANKTASTIC BLOG. The main content area features a large orange banner with the RiskKey logo and the text 'Risk Management Software' and 'FREE 30 day trial'. Below the banner, there is a 'Project Overview' section with three cards showing '11 Incomplete', '27 Incomplete', and '7 Incomplete' items. The text below the banner reads 'Compliance Made Simple.' and describes RiskKey as a web-based application for compliance. A sidebar on the right lists 'Existing RiskKey Users' with a 'Login' button and 'RiskKey Screencasts' including 'Assessing Risk', 'Managing Objectives', 'Messaging', 'RiskKey Overview', and 'RiskKey Data Sheet'.

# Why Vendor Management?

- Understand Risk
- Handle Breaches
- Negotiation/Price Breaks
- Big Brother Says So!



# Best Strategy is the Compliant One

- Policy
- Due Diligence
- Contract
- Risk Assessment
- Ongoing Monitoring



# Policy

- KISS, just do what the policy says!
- Due Diligence Requirements
- Risk Assessment Definitions
- Ongoing Monitoring Requirements
- Crisis Management/ Incident Response Plan



# Due Diligence

- Don't tell current vendor about upcoming conversions....ssshhhh!
- Selection team with power users - 3 to 12 people
- Narrow down to 3 to 5 candidates with a Request for Proposal
- Demo in the same time frame based on what YOU want to see
- Select vendor based on Function, Integration, Scale, Training, Price

# Contract



- NEGOTIATE Everything
- Terms/Conditions/Pricing/Auto-Renew
- GLBA - Privacy
- Just ask a lawyer.....

# Risk Assessing Vendors

- Base risk assessment from policy definitions
- Access to customer information or institution secrets
- Ease of conversion
- Financial condition
- Security controls

RiskKey

# Ongoing Monitoring

- Use the Risk Assessment!!!!
- Review High Risk Vendor more diligently
- Financial Reviews
- Controls Reviews, NOT JUST SAS 70's
- Billing



# Make it work!

- Do what your POLICY says
- Thorough DUE DILIGENCE saves you in the long run
- Negotiate everything in the CONTRACT
- RISK ASSESS all vendors, based off importance to your operation
- Monitor vendors CONTINUOUSLY based off the risk assessment

# Thanks.

Email: [heath@thegarlandgroup.net](mailto:heath@thegarlandgroup.net)

Web: [thegarlandgroup.net](http://thegarlandgroup.net)