MITIGATING RISK THROUGH AN EFFECTIVE VENDOR GOVERNANCE STRATEGY

Session 636

SPEAKERS

Michele Gossmeyer

Director, Information Governance and Compliance

Dentons

Randy Oppenborn

Director, Information Governance

Foley & Lardner LLP

David Forrestall

Managing Partner

SecurIT360

SPEAKER BIOS

- Michele has 20+ years of experience in large global law firms; numerous aspects of legal information technology (information management, security, risk and compliance, communications & customer service and more). Active ILTA volunteer for 10+ years, currently serving on the LegalSEC Steering Committee, Talent Council and Women Who Lead co-chair; previously served as the Board of Directors president & 2008/2009 conference co-chair. Frequent speaker & writer.
- Randy has 25+ years of experience in security, audit, accounting, finance and technology working for large public companies and small private organizations. He is responsible for leading, directing and managing the policies, processes, systems, and team that support Foley's Information Governance program. These include information security and privacy, records and information management, firm-related document holds and mandated destruction, matter mobility, systems assessment, physical security, business continuity and education and awareness.
- David is the founder of SecuIT360, an independent, vendor agnostic, cyber security firm. He has 25+ years of experience in technology and business, the last 12 focused on security and risk management. Over the last 8 years, he has worked with ~150 law firms advising on risk and security programs, including vendor management. The core of the SecurIT360 processes for identifying risks are Security Assessments, including many vendor assessments performed for their clients.

BACKGROUND

TERMINOLOGY

- Vendor Governance – a program and activities that enable organizations to control costs, drive service excellence and mitigate risks to gain increased value from their vendors
- Vendor Management System (VMS) - application that acts as a mechanism for business to manage and procure staffing services as well as outside contract or contingent labor.

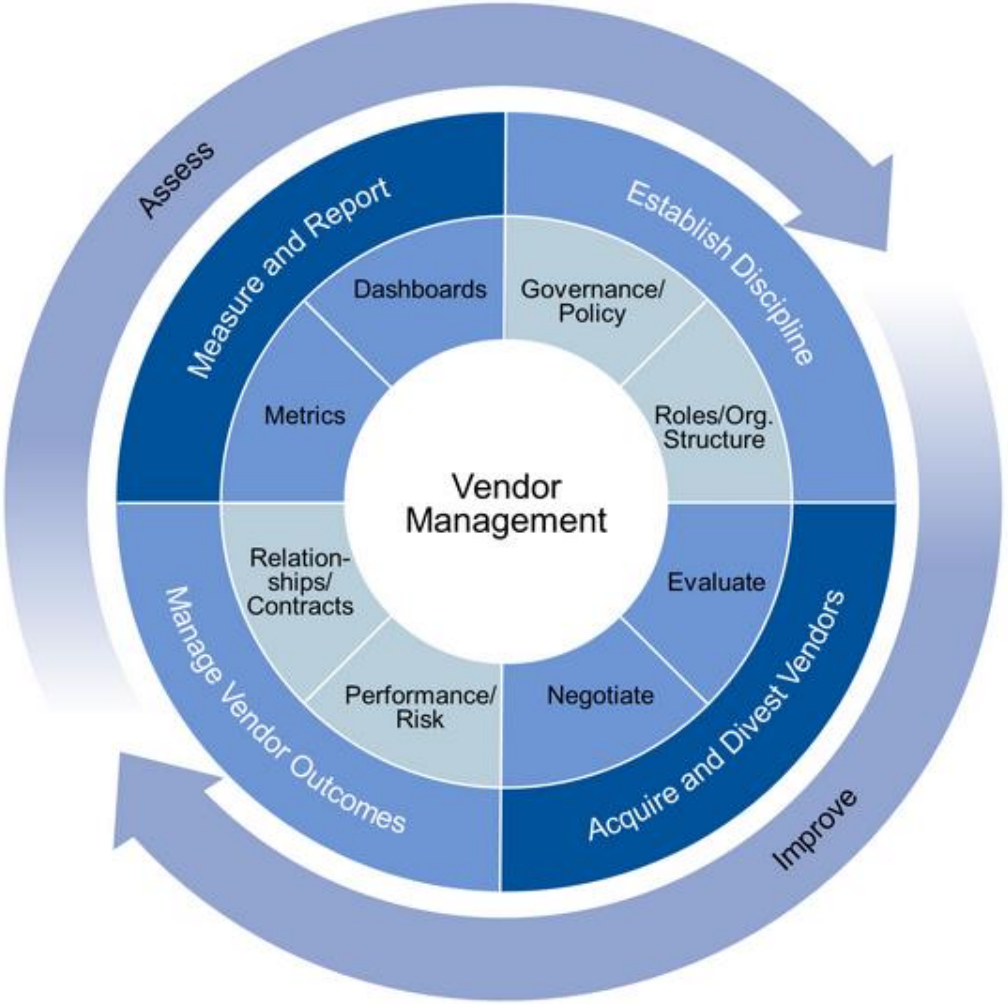
Vendors are Awesome!

- Target – 110M
- Verizon – 6M
- US Office of Personnel Management – 22M
- Home Depot – 56M
- Personal Experience

Why Vendor Governance or Management

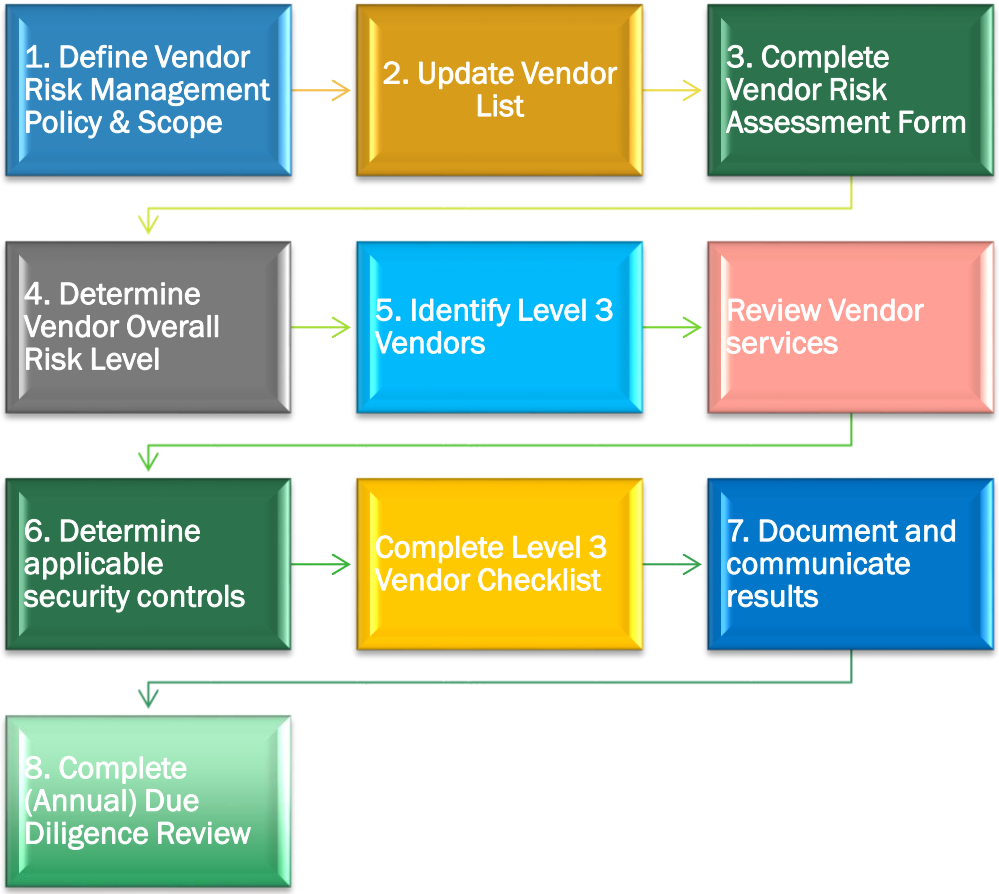
- We all use vendors
- Vendors have access to our resources
- Vendors are humans
- Which ones cause us more risk
- Which ones need to be compliant
- Cyber Insurance & Client Requirements

VENDOR MANAGEMENT PROGRAM



Key Components of VMS?

VENDOR MANAGEMENT PROCESS (FOLEY)



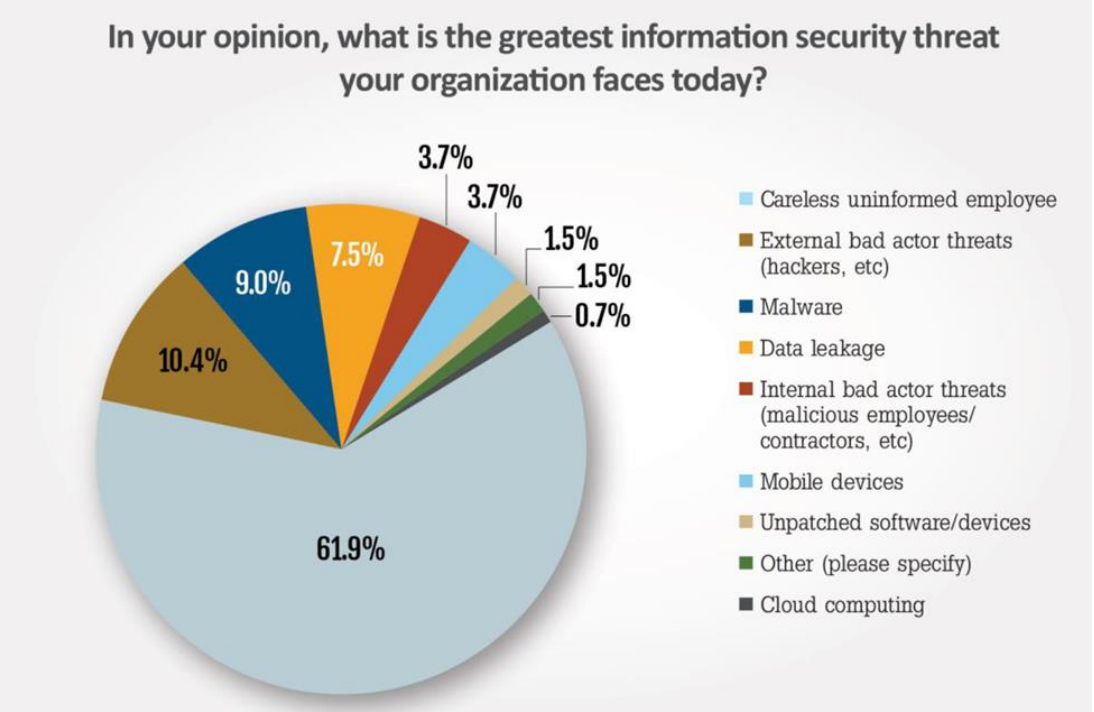
Standards

- Shared Assessments
- ISO 27000
- NIST
- FFIEC
- COBIT
- ITIL

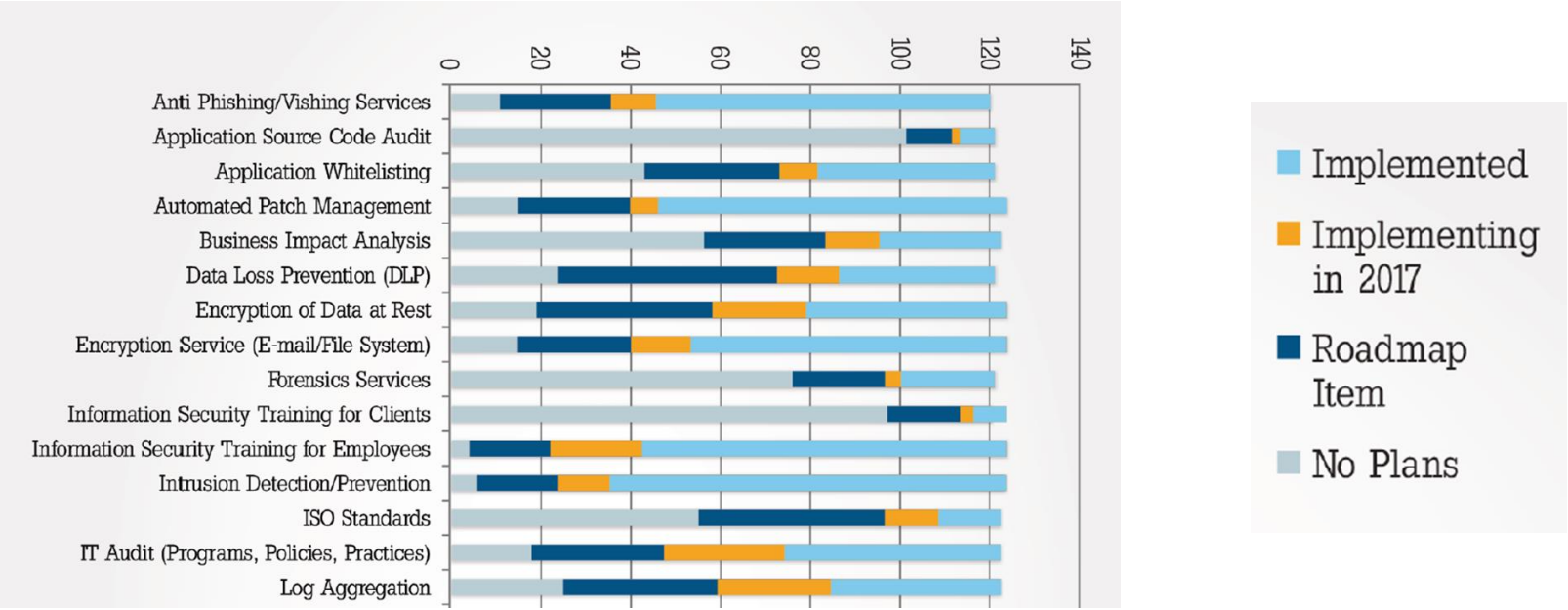
CURRENT STATUS

LEGALSEC SURVEY

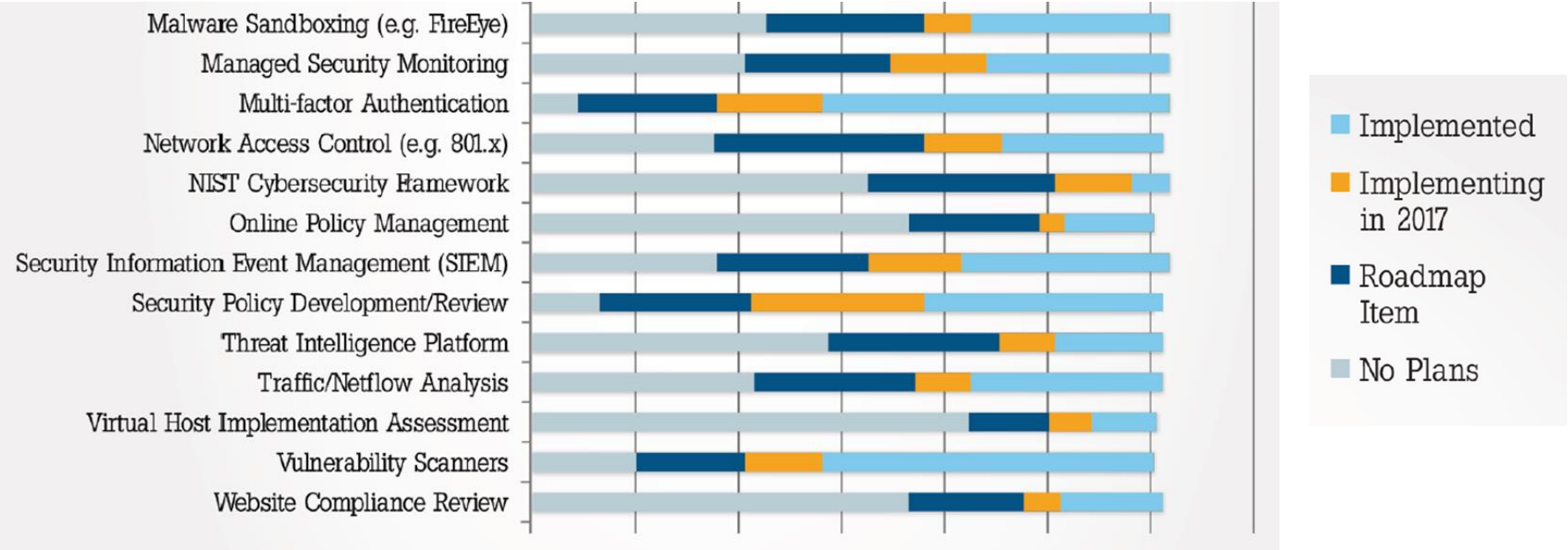
VENDORS?



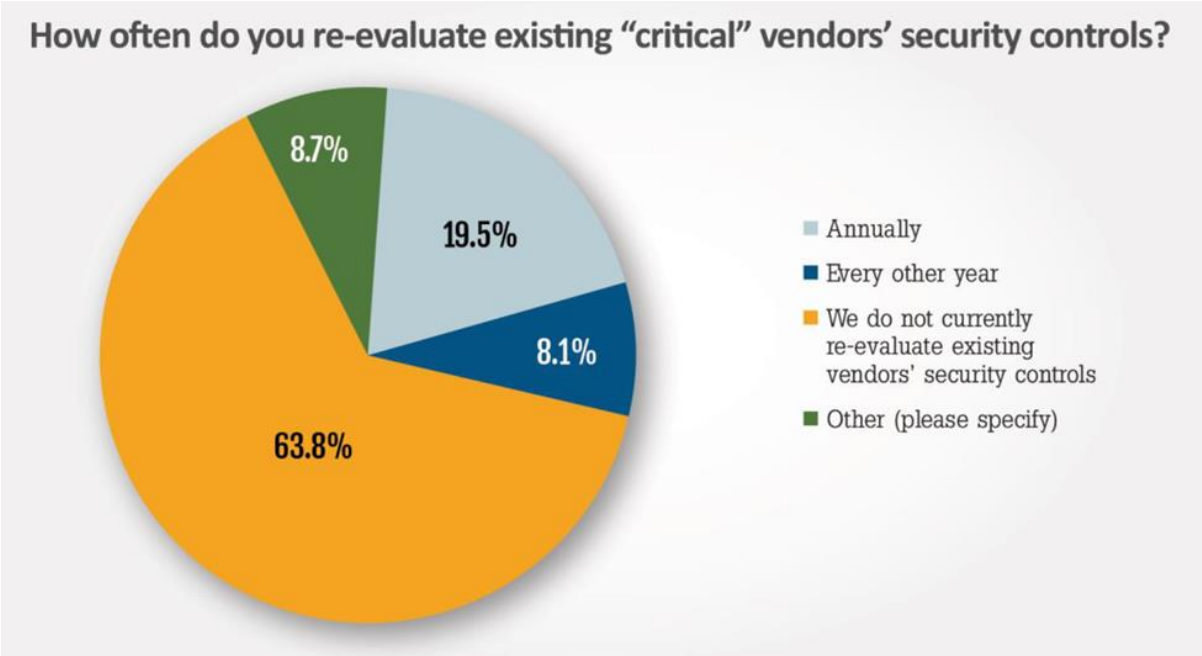
LEGAL PRIORITIES (1)



LEGAL PRIORITIES (2)



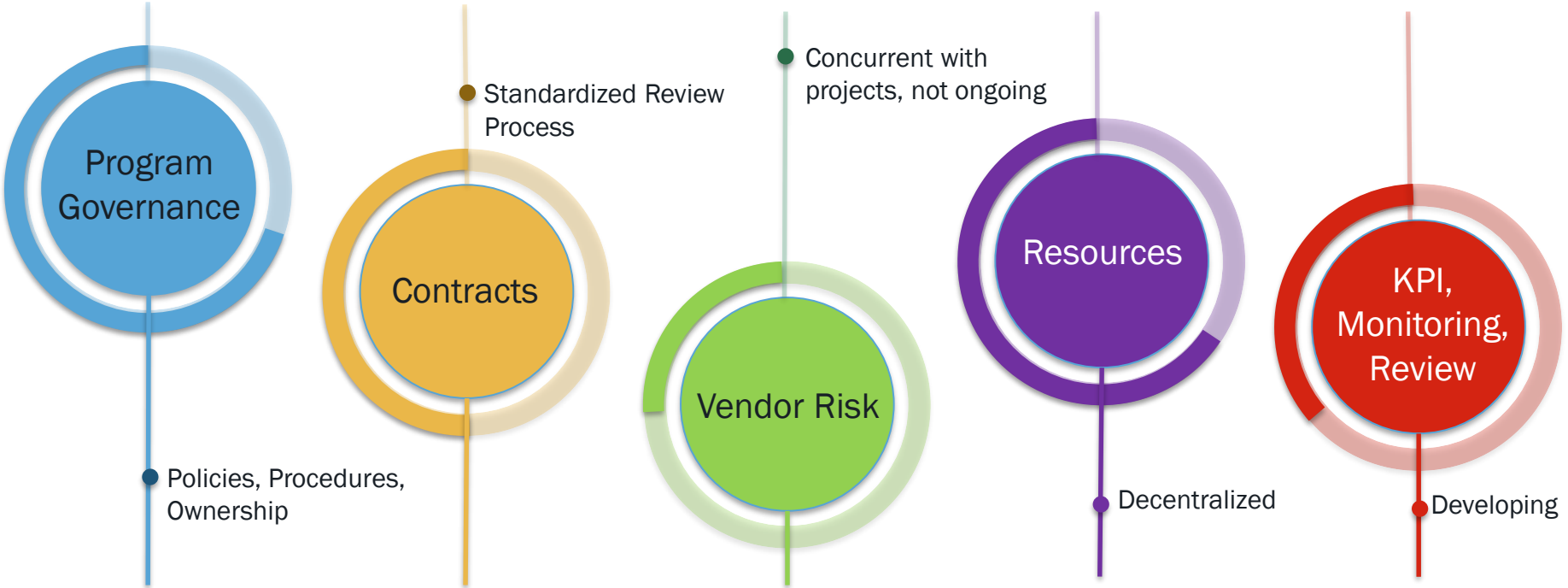
WE HAVE CRITICAL VENDORS? (NO STAFF...)



Vendor Risk Management at Dentons

- Maturing
  - Ad hoc > formalized manual questionnaire > Prevalent
    - Mix of manual & Prevalent based on:
      - Likely adoption
      - Global scope
      - Level of client / sensitive data

VENDOR GOVERNANCE MATURITY AT FOLEY



Roles and Responsibilities

- Set Enterprise Expectations
- Integrate multiple vendors
- Evaluate and Select
- Negotiate Contracts
- Drive more value
- Manage Relationships
- Monitor Risk
- Measure Performance
- Change Contracts
- Resolve issues
- Interface with multiple areas of the Firm

Where to get help

- Many valuable sources
  - Security consultants
  - Clients (assessments)
  - Colleagues (ILTA, LS-ISAO, Infraguard)
  - Shared Assessments
  - PM/Analysts, etc.

Impact of Client Questionnaires

- Input into Technology Risk Management process
- Best practice key > client requirements help drive support/adoption/funding
- Discussions in one area feed into others (e.g. asset mgmt trigger thoughts on asset vendor mgmt)

TAKEAWAYS

Getting Started

- Identify Key Vendors
- Rank Vendors
- Socialize with key departments (IT, Procurement, Acct, OGC)
- Identify key resource(s) to manage
- Send out Questionnaires
- Document
- Refine Program

Taking VM to the next level

- Pick a framework
- Write Policy
- Use External Resources
- Expand outside of IT
- Integrate with ERM

How Vendor Management Fails

- Lack of management support
- Improper resources
- Inability to track / follow up
- Lack of Internal staffing and Responsibility

REFERENCES

- Gartner - http://gartnerinfo.com/futureofit2011/MEX38L_D3%20mex38l_d3.pdf
- Prevalent - https://www.prevalent.net/resources-page/
- NIST
- ISACA
- ISO 27000