

Vendor Management - Privacy and Security Risks

Presented to the New York Metro IIA Chapter

December 11, 2009

*Powerful Insights.
Proven Delivery.™*

protiviti[®]
Risk & Business Consulting.
Internal Audit.

Vendor Risk

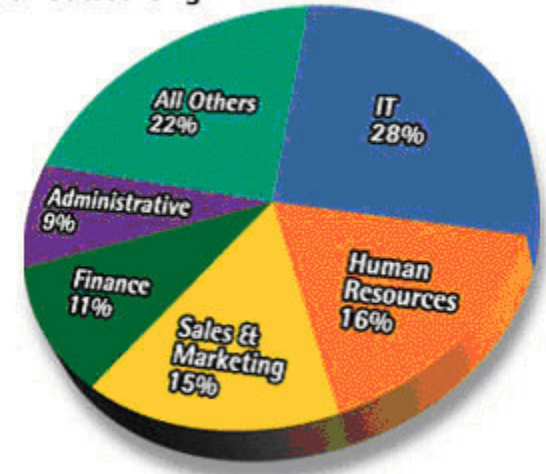
- **ComputerWorld**

- "...At companies with revenues of at least \$5 billion, as many as one quarter of IT jobs will be moved offshore by 2010."

- **Gartner survey:**

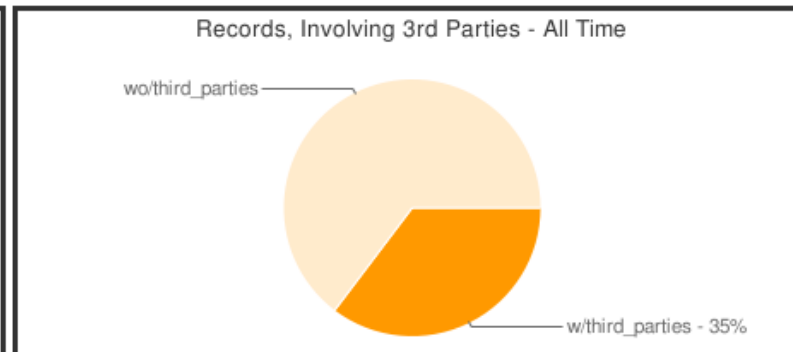
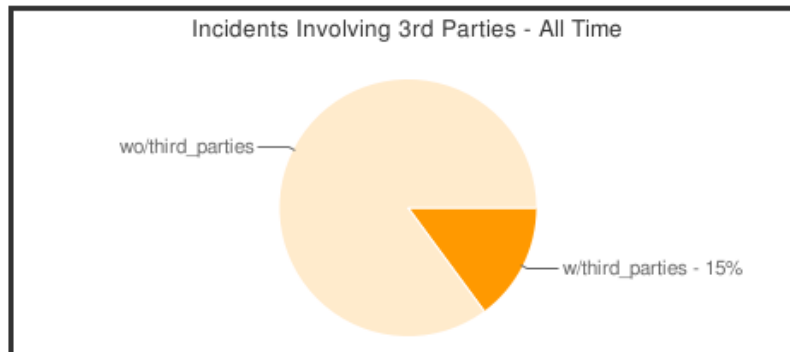
- 60% + spent 3,000 hours, and 20% of spent 10,000 to 30,000 hours a year on vendor risk assessment
 - Vendor risk is frequently an "unbudgeted obligation" that security groups are asked to support

IT Leading As Most Active Area of Outsourcing



THIRD PARTIES AND DATA LOSS

The following graphs highlight a trend that indicates that data loss incidents involving third parties, on average, result in a greater number of records lost than incidents that do not involve third parties. This may be as a result of the type of data handled by third parties, the process of transferring the data between organizations, or other hypothesis, mostly all speculative as little data exists to establish one cause as dominant. The trend is, however, concerning.



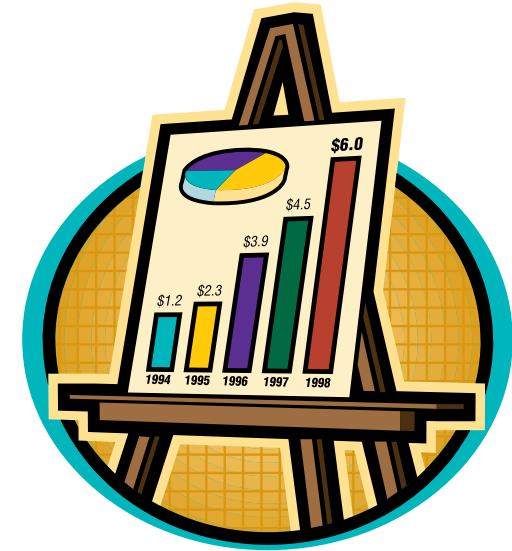
Source:

- ComputerWorld, May 2009
- Gartner Survey Highlights Company Burden of Vetting Third-Party Security Controls, 17 Oct 2008
- http://offshoreitoutsourcing.com/Pages/outsourcing_statistics.asp
- <http://www.privacyrights.org/ar/ChronDataBreaches.htm>



Agenda

- About Protiviti
- Why Vendor Assessments Are Required
- Key Drivers – Regulatory and Risk
- Vendor Review Process
- Vendor Assessment Timeline
- Vendor Assessment Components
- Solution Approach
- Best Practices
- New Trends
- Questions / Next Steps
- Attachments
 - BITS RUP and SIG
 - FRB SR00-4
 - Country Risk
 - Operational Risk
 - Project Risk



Protiviti's Services

Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC, as shown in our offerings below.

Internal Audit & Financial Controls

Information Technology Effectiveness & Control

Finance & Accounting Excellence

Risk & Compliance

Cost & Working Capital Optimization

Litigation Restructuring & Investigative Services

- **IT Security & Privacy Management**
- **Business Continuity**
- **IT Governance & Risk Management**
- **IT Process Improvement**
- **Application Controls Effectiveness**
- **Enterprise Information Management**

Protiviti's Information Security & Privacy Practice

- Over 250 information security / privacy professionals located around the country;
- Effective, proven methodologies and dedication to training;
- Information Security from a business process perspective:
 - Security Assessments & Reviews
 - Trusted Security Advisors
 - ISO 27001 Assessment & Strategy Development
 - Compliance and Regulatory Solutions & Services
 - PCI Compliance & Remediation Services
 - Incident Response, Forensics and Litigation Support
 - Data Privacy & Work Process Flow Analysis
 - Identity Access Management;
 - Vendor Assessments

Why Vendor Assessments Are Required

- Increased outsourcing and continued cost rationalization
- If something goes wrong it's your company's reputation on the line - Reputation risk cannot be outsourced
- Breach of privacy (GLBA, HIPAA, SB1386, EU plus other US states) – It's still your data
- Loss of service – What is the impact and how long to restore?
- Increase in regulatory requirements – Are service providers, outsourcers and vendors compliant?
- Loss of control - who has access to your data in interconnected networks with many other parties – Who can access your sensitive data?
- Business leaders believe that risk can be outsourced. They need to accept the ramifications of outsourcing and the residual risk.
- Some certifications are available but lack the depth, granularity and reliability: ISO9000, CMMi, EU Privacy, SAS 70 Type 2, etc.

Why is Vendor Assessments Important

- Approximately 229 million customer records have been reported compromised since Jan 2005
 - **Average cost per record: \$198***
 - **Average incident: \$6.3m (approx 26k records)***
- Vendors play an integral role in processing of business operations and customer data
 - **At least 30% of breaches involved 3rd parties***
- Significant financial, reputational and legal consequences are at stake
- Regulators and executive management expect you to understand, manage and reduce risk
- Ignorance is not a valid defense

Source : PGP-Ponemon Institute Cost of a Data Breach Study & ACI

Regulatory Drivers

- GLBA
 - Prevent disclosure of nonpublic personal information
- PCI
 - Prevent disclosure of online credit card and account information
- FTC
 - Breach Disclosure Requirements
- NYSE
 - Rule 340
- FDIC
 - Meet regulatory requirements around core vendors
- State Breach Laws
 - Avoid requirements to disclose data compromised at a vendor
- Business Partners
 - Penalties for non-compliance with contracts and SLAs

Risk Management Drivers

- Information Security Risk Management
 - Manage risk based on data share
 - Ensure minimum standards are met
- Business Continuity – Resiliency at Critical Vendors
 - Ability to meet up time and recovery SLAs
 - Ensure data security during recovery
- Reputation Risk Management
 - Damage to reputation can be a hidden cost of vendor insecurity
- Country Risk
- Operational Risk (includes security and regulatory compliance)
- Project Risks

Vendor Profile - Context

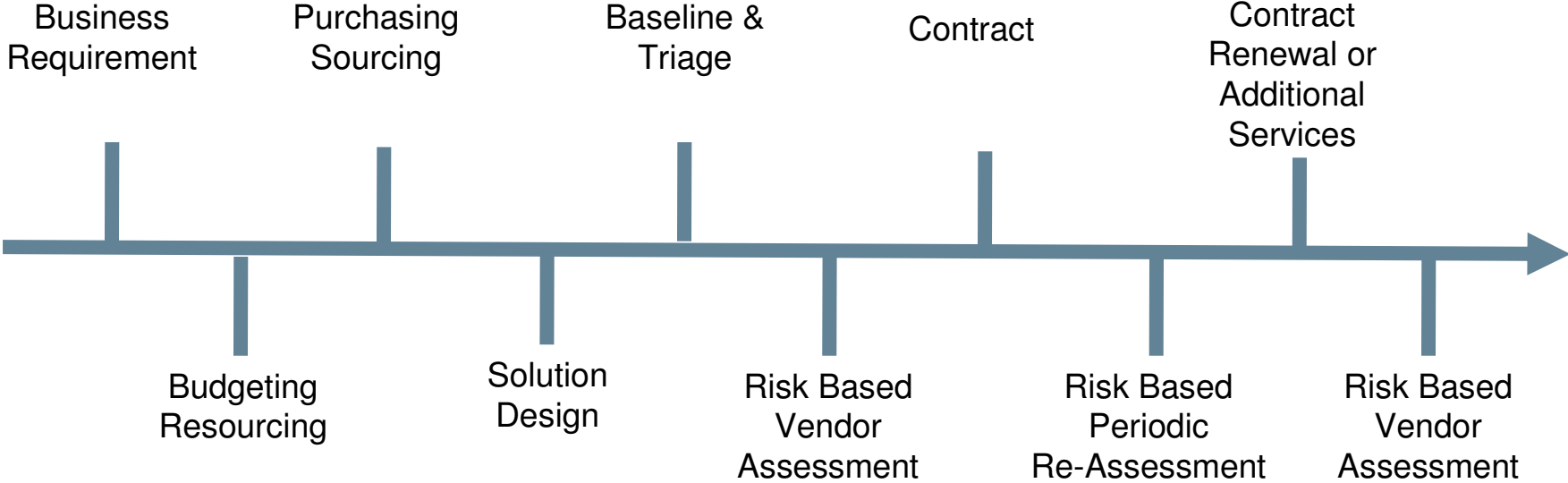
- Business Profile – Who are they?
 - Understand the risk associated with doing business with the vendor
- Relationship Risk – What are they doing?
 - Provide standard measure of value of the business risk
 - What they provide
 - Who they impact
 - How they interact
 - Ease of replacement
 - Information & Data
- Control Assessment – Information Protection?
 - Measure of information and processing protection maturity from a risk and compliance standpoint
 - Self Attest Controls against control standards
 - Validated Controls
- Control Validation – Verification of Controls
 - Due Diligence investigation of a controls in regards to a information protection.
 - Desk, Onsite, or In-depth validation of controls
 - Documentation of Control Evidence
- Monitoring
 - Monitoring of the vendor relationship and how it may affect normal business
 - Changes in the Relationship, Business, Controls and Regulatory Considerations

Typical Vendor Assessment Process

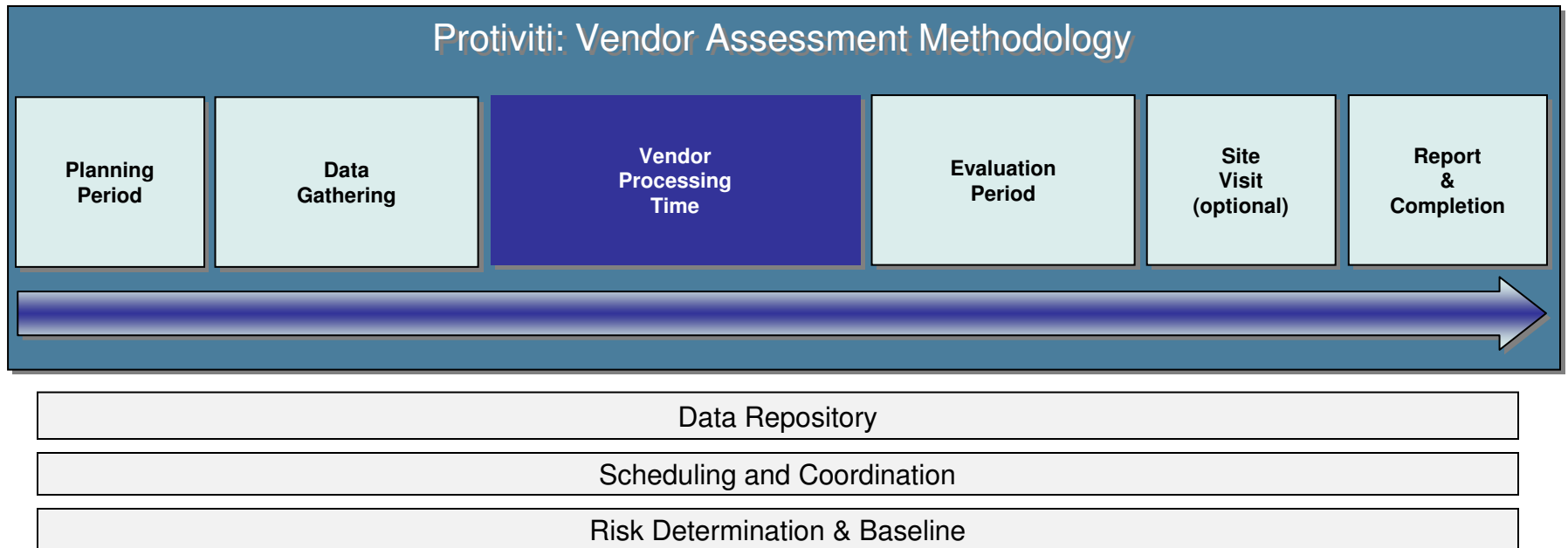
Overview of a typical review process:

- **Risk Ranking**
 - Vendors are ranked according to sensitivity of data (SS#, CC#, name, etc) and volume of data exchanged with vendor
- **Questionnaires**
 - Vendors are sent a questionnaire to complete detailing their security and control environment related to data processed
- **Onsite Assessment**
 - Vendors that are Risk Ranked as highly sensitive receive an onsite audit to confirm and observe the information in the questionnaire
- **Repository**
 - Information retained about each Vendors.
- **Reporting**
 - Develop reports based on finding from the reviews and communicate issues to business owners

Vendor Assessment Timeline



Vendor Assessment: Components

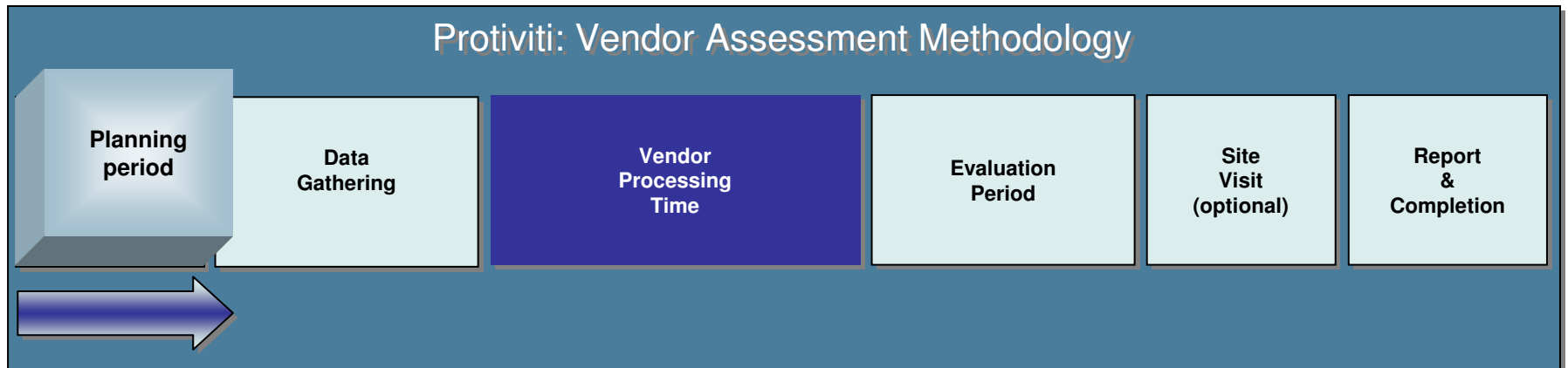


•PWC study findings:

- 25% of respondents perform 3rd party privacy audits
- Only 22% have an inventory of all 3rd parties handling sensitive data
- 43% have established security baselines for partners, customers, and vendors

Source: 2008 Global State of Information Security, PWC

Vendor Assessment: Planning Period



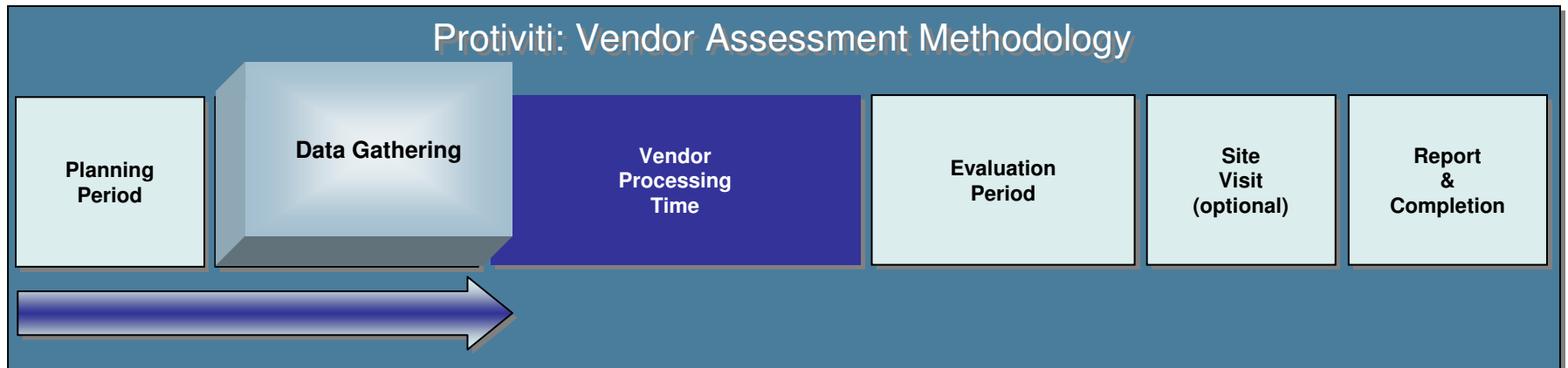
Key Tasks

- Identify appropriate business owners related to the third-party vendor
- Obtain a high level overview of the vendor, service and type of information shared
- Assess risk and priority
- Review agreements or drafts

Key Milestone

- Determination if the service provider requires a review based upon the initial facts

Vendor Assessment: Data Gathering



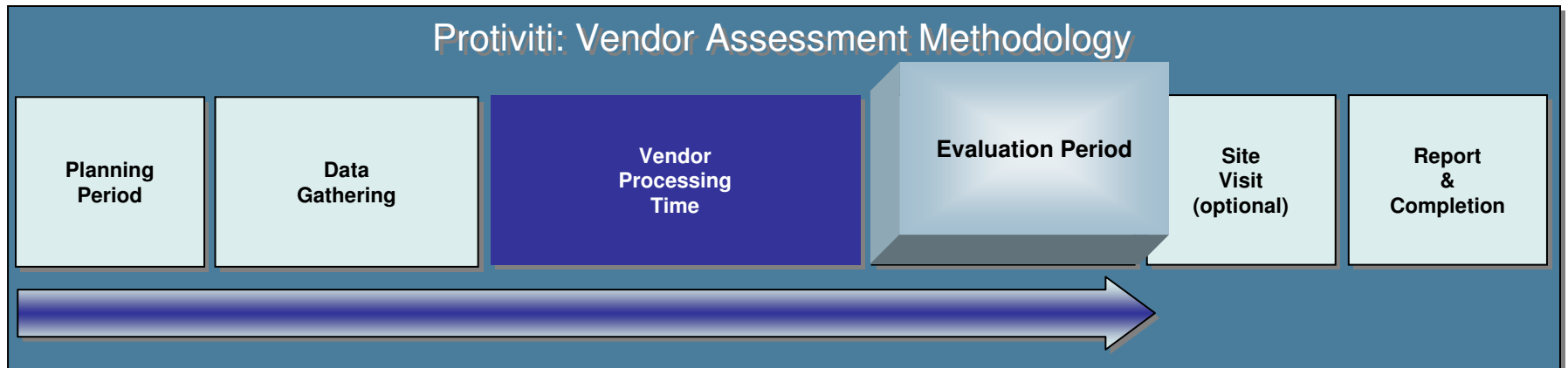
Key Tasks

- Obtain a full record layout of information shared with the vendor from the business owner
- Send the Security Questionnaire for completion and support completion
- Obtain any third party audit reports (SAS 70 Type II, PCI, Pen Test, etc...)

Key Milestone

- Receive all related and requested documentation

Vendor Assessment: Evaluation Period



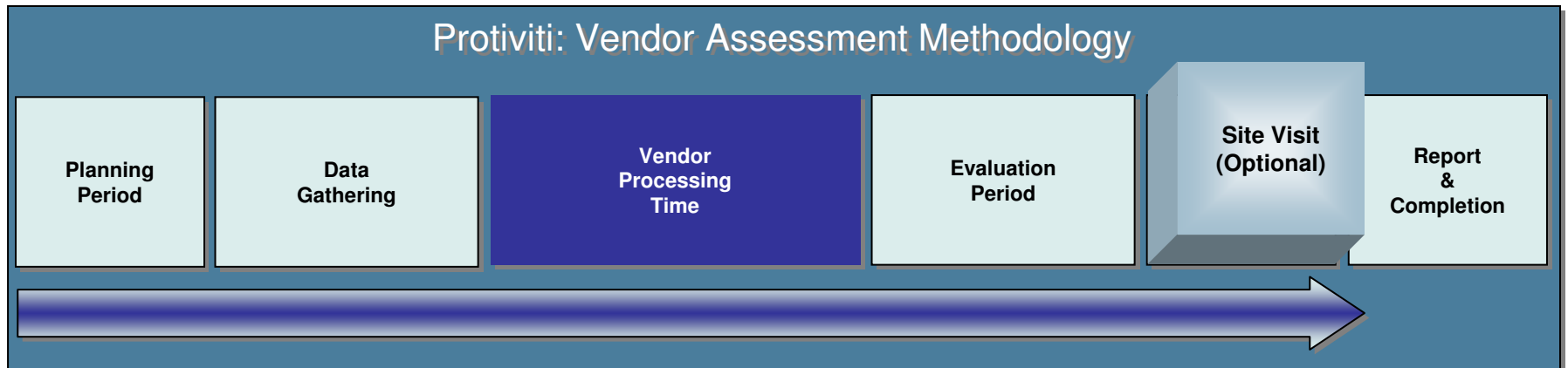
Key Tasks

- Review gathered documents
- Determine all locations that process, store, transmit sensitive data

Key Milestone

- Schedule travel to vendor site and complete logistics

Vendor Assessment: Site Visit



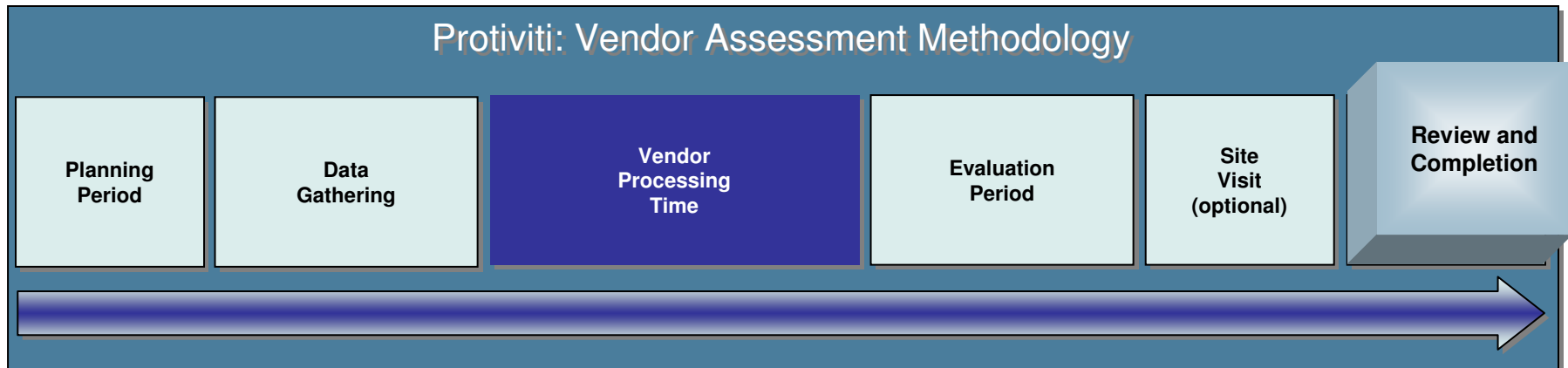
Key Tasks

- Travel to vendor locations
- Meet with vendor management to verify the answers provided on the Security Questionnaire
- Review the physical security of the facility being visited
- Review service recovery capabilities

Key Milestone

- Completion of site visit to all in-scope locations

Vendor Assessment: Review and Completion Phase

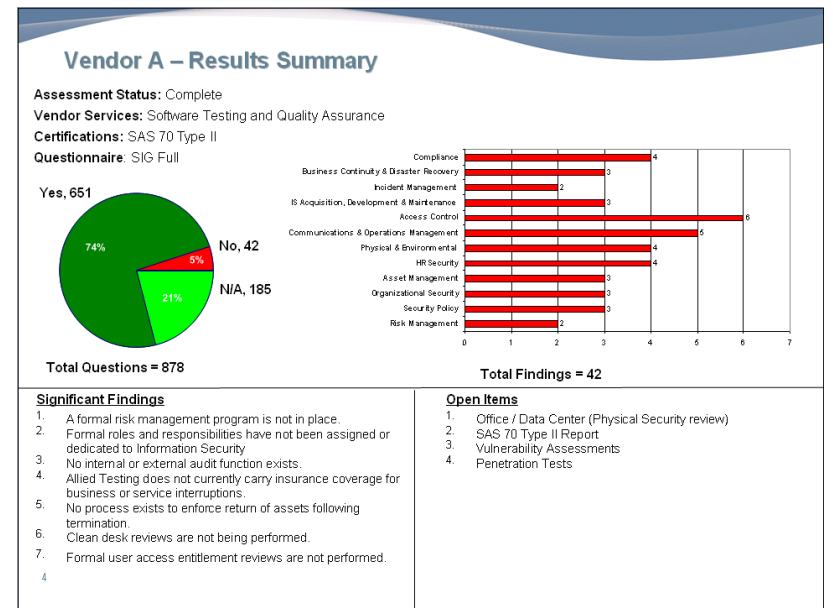


Key Tasks

- Close out any relevant follow-up from the site visit
- Create review report outlining any issues

Key Milestone

- Communicate results to the business sponsor / partner
- Agreement upon any remediation items and develop a remediation action plan



Solution Approach

- Success Factors:
 - Assessments Commensurate with Risk:
 - Sensitivity of data (Full SSN or last four?)
 - Volume of data (1,000 records, or all of your records?)
 - Public Relations Exposure (VIPs and sensitive client's data?)
 - Regulatory Impact (Is compliance audited regularly?)
 - Ensure minimum standards are met
 - Ensures spend on Vendor Due Diligence is justified by the benefits
 - A standard, repeatable approach
 - Tie assessment to policy/framework and meet audit requirements
 - Assess risk as a function of vulnerability severity and potential loss
 - Include an exceptions process

Solution Approach (Con't)

- Functional Approach:
 - Develop an assessment from existing policies or procedures (or new procedures)
 - Linking with the RFP and SDLC processes enables smooth integration
 - Granular approach via on-site review or questionnaire
 - Address special cases: PCI compliant vendors, SAS-70, ISO 27001 specialty services
 - Track findings assessed to ensure consistent assessment of risk
 - A database or risk management tool can significantly magnify the results of efforts
 - Standardized finding language can shorten reporting cycle as many findings will be repeated from vendor to vendor
 - Continuing assessment of risk as remediation plans from vendors arrive
 - Enables continuous management of risk
 - Accurately represents risk to decision makers
 - Reassessment on a periodic basis depending on the severity of risk
 - Document in policy to ensure continued compliance
 - Link to a risk reporting, review and acceptance process
 - Or use as a driver to establish one

Best Practices

- Baseline Due Diligence and Follow-Up Work on Risk and Business Impact
 - High, Medium and Low
- Less reliance on SAS 70 for compliance
- Privacy and security intertwined
- Vendor Management Strategy (Integration => Due Diligence => Assess => Decide => Periodic Review)
- Integrate Process due to Risk convergence - *KEY*
 - Purchasing
 - Legal
 - Compliance
 - Security
 - Audit
 - Physical Security
 - Business

More Best Practices

- Strong logistics and program management capability
- Define risk in your environment in a reusable and shareable format
- Make requestor pay for assessment – play hardball, especially for onsite assessments
- Complete and accurate inventory of your vendor landscape
- Comprehensive and repeatable approach to assessing vendor security
 - Common response
 - Reusable questionnaires
 - Reuse (if possible) existing reports (e.g. SAS 70, PCI)
- Ability to analyze and report on the state of vendor risk to enterprise constituents, vendors and executive management
- Ability to track and report improvement and/or degradation of the state of vendor security over time
- Integrate Process with other assessment processes – KEY be part of "go or no-go" decision
 - Purchasing
 - Legal
 - Compliance
 - Security



New Trends

- ISO 27001 certification
- SAS70
- Response pooling
- FISAP (Financial Institution Shared Assessments Program), it was an initiative started in 2006 by BITS
- Bits UAP
- Internal Controls Required to Support Outsourcing
 - Code review
 - Secure Data Transmission
 - Logging & Monitoring
 - Privileged User Review
 - Employee Background Checks
 - User-Id Validation

Management Considerations



- Know Regulations
- Due Diligence
- Monitor
- Implement an integrated process.
- Recognize that the company maintains continued ownership of the data.
- Prohibit any subcontracting without the company's written consent.
- Prohibit the collection of personal data directly from the company's customers.
- Ensure all workers sign confidentiality agreements that prohibit release of the material.
- Implement internal and external security safeguards that are to be appropriately updated.
- Provide prompt notice of any privacy or security breach or loss of personal data.

Key Contacts



Rocco Grillo, CISSP

Managing Director - IT Security and Privacy Management

212.603.8381

Rocco.Grillo@protiviti.com



*Powerful Insights.
Proven Delivery.™*



Attachments

1. **BITS RUP and SIG**
2. **FRB SR00-4**
3. **Country Risk**
4. **Operational Risk**
5. **Project Risk**

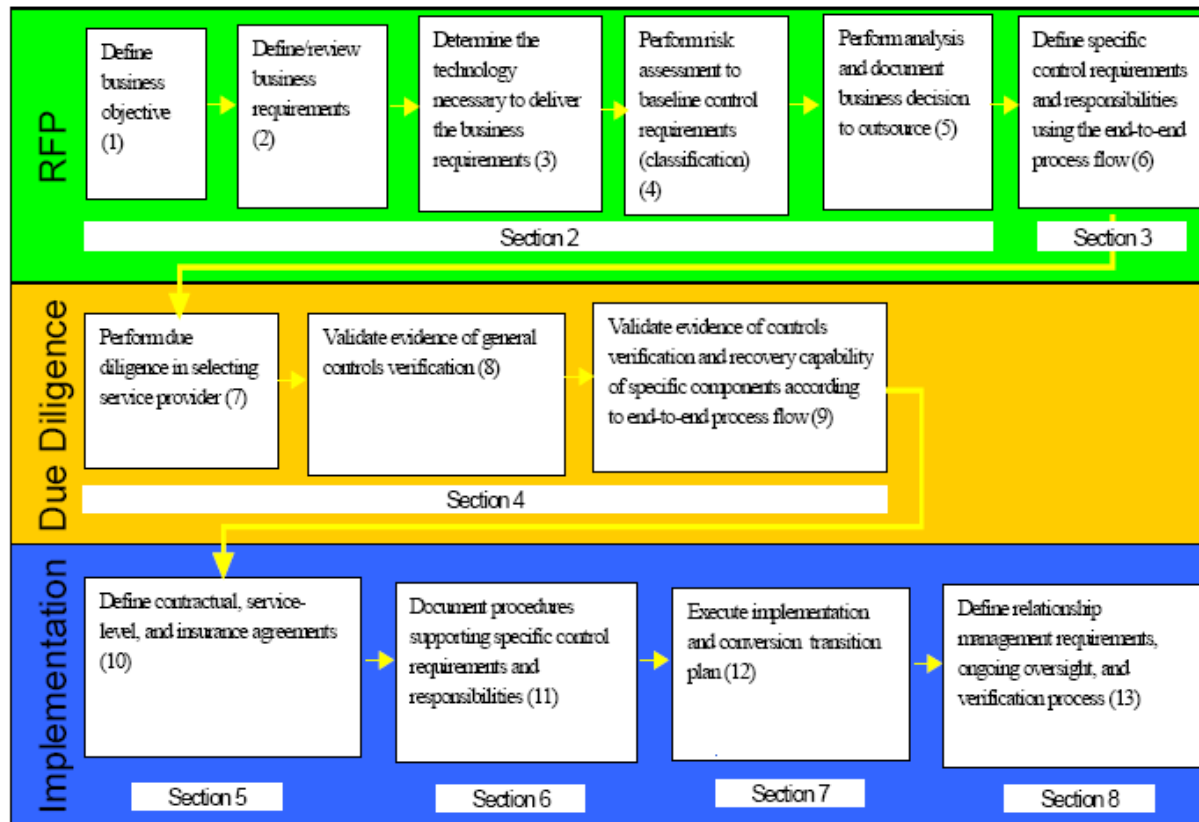
BITS Agreed Upon Procedures (AUP)

Agreed Upon Procedures (AUP): Developed by BITS members with the Big 4 accounting firms acting as Technical Advisers. The AUPs provide objective and consistent procedures to be performed under each control area during an onsite assessment. Procedures address control objectives in:

- risk management
 - information security policy
 - organization of information security
 - asset management
 - human resources security
 - physical and environmental security
 - communications and operations management
- access control
 - information systems acquisition
 - development and maintenance
 - information security incident management
 - business continuity management
 - compliance

BITS Agreed Upon Procedures (AUP) Process Flow

BITS Framework Flow Diagram



Objectives:

- Objectively test a control and report results
- Test and validate service provider information security controls
- Institutions view results in the context of their risk management requirements

BITS SIG/SIG Lite

- 1. Standardized Information Gathering Questionnaire (SIG):** The SIG was developed by BITS members to address the control areas covered in ISO 27002:2005. The questionnaire can be used to obtain required documentation, establish a profile for each control area, and obtain verifiable information for each. As a standalone document, the SIG is used by financial institutions and service providers to assist in evaluating information security controls.
- 2. Standardized Information Gathering Questionnaire Lite (SIG Lite):** Is a 54 question tool that can be used when a complete SIG questionnaire is not required. The SIG Lite was developed in response to member requests for a tool to qualify prospective vendors for further due diligence and evaluate low-risk vendors' security profiles.

Example Requirements (FRB-SR00-4)

Risk assessment: Before entering into an outsourcing arrangement, the institution should assess the key risks that may arise and options for controlling these risks. Factors influencing the risk assessment could include, for example,

- the criticality of the function to the institution
- the nature of activities to be performed by the service provider
- the availability of alternative service providers for the particular function
- insurance coverage available for particular risks
- cost and time required to switch service providers should problems arise.

Selection of service provider: sufficient due diligence to satisfy itself of the service provider's competence and stability, both financially and operationally, to provide the expected services and meet any related commitments.

Contracts: The written contract between the institution and the service provider should clearly specify, at a level of detail commensurate with the scope and risks of the outsourced activity, all relevant terms, conditions, responsibilities, and liabilities of both parties. Included:

- Required service levels, performance standards, and penalties.
- Internal controls, insurance, disaster recovery capabilities, and other risk management measures maintained by the service provider.
- Data and system ownership and access.
- Liability for delayed or erroneous transactions and other potential risks.
- Provisions for and access by the institution to internal or external audits or other reviews of the service provider's operations and financial condition.
- Compliance with any applicable regulatory requirements and access to information and operations by the institution's supervisory authorities.
- Provisions for handling disputes, contract changes, and contract termination.
- Terms and conditions should be assessed by the institution to ensure that they are appropriate for the particular service being provided and result in an acceptable level of risk to the institution.⁴ Contracts for outsourcing of critical functions should be reviewed by the institution's legal counsel.

Policies, procedures, and controls: The service provider should implement internal control policies and procedures, data security and contingency capabilities, and other operational controls analogous to those that the institution would utilize if the activity were performed internally.

Ongoing monitoring: Review the operational performance of critical service providers on an ongoing basis to ensure that the service provider is meeting the terms of the arrangement. Staff should have sufficient training and expertise to review the performance and risk controls.

Information access: The institution must ensure that it has complete and immediate access to information critical to its operations that is maintained or processed by a service provider. Records maintained at the institution must be adequate to enable examiners to review its operations fully and effectively even if a function is outsourced.

Audit: The institution's audit function should review the oversight of critical service providers.

Contingency plans: The serviced institution should ensure adequate business resumption planning and testing by the service provider.

Country Risk Considerations

Offshore outsourcing can lead to many problems that are associated with the geographical location of the offshore destination. Some of these problems can be language problems, accent problems, political instability, change in laws and regulations, labor laws, cultural issues etc.

- How stable is the country politically?
- Is there civil strife in the area of operations?
- How easy is it to travel, obtain visas?
- Are there any political “strains” that could undermine the Program between the two countries?
- What is the legal framework that supports the activity?
- How well are Intellectual Property rights enforced?
- What are tax implications for the country?
- Will the country permit a 100% owned subsidiary?
- How easy is it to setup an operation?
- What are the labor laws?
- How easy is it to exit?
- What are the customs and duties and other licensing requirements? What overheads are needed to manage these?
- Are we allowed to export the technology we have in mind for operations in that country?
- Ease and speed of getting domestic import licenses?
- What is the quality of the education system?
- What is the capacity generation capability of the country?

Operational Risk Considerations

- Does the Company have a Disaster Recovery plan?
- What is the Disaster recovery plan?
- Can it sustain a development operation?
- What about power?
- How efficient is the Voice and Data communications to the country?
- Is high bandwidth available?
- How easy is it to establish voice and data communications?
- Is the environment secluded?
- Are the facilities shared with other companies? In that event how are the networks and people physically isolated?
- How is access limited or controlled?
- What kinds of physical security exist to prevent movement digital resources?
- What are the network security policies?
- What are the password policies?
- What SCM expertise is in use?
- What is the personnel management process? How are the people hired, trained, rewarded?
- What is the attrition management process?
- What is the chain of command and control?
- What could be cultural issues?
- Are we internally prepared for outsourcing?
- Are systems in place to support outsourcing?
- Are people in the Company enlisted to support the Outsourcing process?
- Have we defined all the processes needed to make the engagement successful?
- Is there internal buy-in?
- Do we have corporate sponsorship?
- Have we defined the standards to be used for outsourcing?
- Have we defined success criteria?
- How will we measure Quality?
- How will we measure service levels?
- How will we maintain visibility into the development?
- How will we manage change of personnel within our Company who are part of the outsourcing process?
- Are the facilities insured? Fireproof?
- Does the Company understand compliance risk including the impact of failing to meet the terms of the serviced institution's regulatory compliance obligations.

Project Risk

- Are requirements clear?
- Is there a well-defined performance and acceptance plan?
- Do we have a Project and outsourcing management process in place?
- Is there a Software development lifecycle methodology?
- Has this been certified?
- Have the processes been defined and if so has the capability been assessed?
- Is data collected to measure performance? What data is collected and at what stages? Is causal analysis performed?
- What is the hiring, training, rewarding and staffing process?
- What is the attrition in the last three years?
- What is the experience of people who leave?
- What is the average experience of a team?
- What is the attrition management process?
- How are activities base lined? What activities are base lined?
- Is there a Project management process?
- Is there a separate QA team that looks at QA processes?
- Is there a QC process and what is the process? When is QA/QC planned?
- How will we validate deliverables?
- How will we approve intermediate deliverables?
- How will we manage technology risks?
- How will we measure service levels?
- How will we assess Quality?
- How effective is the handover process? Are the interfaces well defined



Confidentiality and Disclosures

"This presentation contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly owned subsidiary of Robert Half International Inc. ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public."