Hot Topics in the Board Room
**Agenda**

- State of the Internal Audit Profession
- Vendor Risk Management
- Privacy & Security
At a glance

- **PwC’s 10th** Annual State of the Internal Audit Profession Study
- Over 1900 respondents, including 1400 CAEs including IA managers, and more than 520 stakeholders (Board and Audit Committee Members, CFOs, CROs, CCOs, etc.)
- Conducted over 125 stakeholder and CAE interviews across North America, Europe, Australia, and Asia to gain further insights
- Interviewed certain key regulators across the globe to understand their expectations of internal audit
- Survey focused on:
  - Understanding what is expected from internal audit for the purpose of identifying potential alignment issues;
  - Understanding stakeholder perceptions related to the value of Internal Audit
  - Understanding internal audit performance related to key attributes
The heart of the matter
Higher performance by design: A blueprint for change

This year’s findings

• Significant differences of opinion exist between stakeholders and CAEs on the nature of what is expected of internal audit, i.e., a misalignment

• On average only 49% of senior management and 64% of board members believe internal audit is performing well at delivering on expectations

• More than half (55%) of senior management do not believe internal audit adds significant value

Leads to the following questions.....

• Is your function aligned to the expectations of its key stakeholders? How do you know what capabilities to develop without clearly knowing what is expected of you?

• Are you aligned with respect to the critical risks?

• Are you expecting enough from your function? Our research shows that when more is expected, internal audit has the opportunity to add more value to the organization

• Higher expectations require increased capabilities and investment

Internal audit must be aligned with the expectations of its stakeholders in order to strategically build the right capabilities and raise its performance and value.
Providing value-added services and proactive strategic advice to the business well beyond the effective and efficient execution of the audit plan

Taking a more proactive role in suggesting meaningful improvements and risk assurance

Bringing analysis and perspective on root causes of issues identified in audit findings to help business units take corrective action

Delivering objective assurance of the effectiveness of an organizations’ internal controls
# Case for change

<table>
<thead>
<tr>
<th>Value</th>
<th>Performance</th>
<th>Critical Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholders have significantly different views of internal audit value</td>
<td>Performance has shown improvement since the prior year but many functions are still challenged</td>
<td>Companies are doing a better job at managing critical risks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Board Member Views</th>
<th>Management Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>79% of board members see significant value, while only 44% of management do</td>
<td>56% of the board ranks IA performance as strong, while 37% of management do</td>
</tr>
<tr>
<td>2014</td>
<td>68% of board members see significant value, while only 45% of management do</td>
<td>64% of the board ranks IA performance as strong, while 49% of management do</td>
</tr>
</tbody>
</table>

* Represents the average of the “performs well” ratings across 18 capabilities vs. 8 capabilities in 2013
The case for change

Engaging and managing a relationship with stakeholders
Leveraging technology effectively in the execution of audit services
Aligning scope and audit plan with stakeholder expectations

CAEs expectation  Senior management expectation  Board members expectation  Performance

Expectation: % who expect this from internal audit; base = total survey responses
Performance: % who believe internal audit performs this well; base = only those respondents that expect internal audit to do this

Stakeholders are not aligned in their expectation of internal audit over key attributes.
The case for change

- Involvement in company initiatives before, during and after deployment
- Identifying thematic issues the organization is facing
- Promoting quality improvement and innovation

Expectation: % who expect this from internal audit; base = total survey responses
Performance: % who believe internal audit performs this well; base = only those respondents that expect internal audit to do this

Stakeholders are not aligned in their expectation of internal audit over key attributes
Expanding the expectation set

Stakeholder perceptions of internal audit departments with Assurance Provider expectations
- Internal Audit adds significant value and performs well: 16%
- Internal Audit adds some value and performs well: 26%
- Internal Audit adds value but performs poorly: 17%
- Internal Audit adds little value or don’t know: 41%

Stakeholders perceptions of internal audit departments with Trusted Advisor expectations
- Internal Audit adds significant value and performs well: 14%
- Internal Audit adds some value and performs well: 17%
- Internal Audit adds value but performs poorly: 56%
- Internal Audit adds little value or don’t know: 13%

Internal audit has the opportunity to drive greater value to the organization by expanding capabilities and skill sets, regardless of expectations/role.
Trusted advisors have higher performance on 8 foundational attributes

Expanded expectations and Alignment of stakeholder expectations creates an opportunity for Internal Audit to raise its performance and provide added value to the organization.

Percent of respondents indicating internal audit was performing well

- Assurance providers
- Trusted advisors

PwC

April 2014
MM to revise chart to align with 8 attributes

Meredith Martin, 3/28/2014
Developing an aligned set of expectations

- Align and agree on the critical risks the organization faces (fundamental)
- Establish detailed expectations aligned to the eight foundational attributes
- In developing these detailed expectations, consider:
  - Future needs and emerging issues and risks;
  - Regulatory expectations;
  - The first and second lines of defense
- CAE should drive the discussion
- Proactively share your expectations, but do so with open lines of communication across the key stakeholder group

Achieve alignment on the breadth of expectations and critical risks is a significant step towards internal audit improving its relevance and value to the business.
## Internal audit’s communication strategy

<table>
<thead>
<tr>
<th>Activity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific communication with audit committee chair and board on internal audit mandate</td>
<td>77%</td>
</tr>
<tr>
<td>At least an annual discussion with key stakeholders to ensure internal audit’s role is aligned with expectations</td>
<td>73%</td>
</tr>
<tr>
<td>Hold a meeting between internal audit, management and board members to agree on expectations</td>
<td>73%</td>
</tr>
<tr>
<td>Top-down communication with internal audit team members on expectations</td>
<td>71%</td>
</tr>
<tr>
<td>Specific communication with internal audit members on expectations</td>
<td>70%</td>
</tr>
<tr>
<td>Regular survey of stakeholders on internal audit’s performance and adherences to stakeholder expectations</td>
<td>49%</td>
</tr>
<tr>
<td>Hold a meeting with external stakeholders such as regulators and external auditors to discuss expectations</td>
<td>45%</td>
</tr>
<tr>
<td>Post internal audit expectations on company’s internal website</td>
<td>31%</td>
</tr>
</tbody>
</table>

*CAE’s of internal audit functions that are seen as trusted advisors are leveraging the tactics above to communicate across the organization to stay the course of alignment on expectations and delivering value.*
Communicating performance and value

Advanced metrics being used to measure internal audit performance:

- Involvement and value provided in all key initiatives and emerging risk including new systems, acquisitions, dispositions, new products, new regulations, etc.
- Ability of internal audit to provide macro/horizontal views on key issues and areas of critical risk to the organization
- Ability of internal audit to be a “change agent” in the organization, that is, is the overall control environment improving year over year because of internal audit’s influence.
- Annual “voice of the customer survey”
- How well internal audit is able to answer questions from the Board and Management.
- Value of recommendations provided
- Cost savings and revenue enhancement based on internal audit recommendations and findings

Trusted advisors are focused on communicating the value they bring to the organization through the recommendations they provide and their involvement in emerging issues rather than classic value measures such as successful completion of the audit plan.
Taking action

CAE
Lead The Design
Pro-Active Communication

Board Members
Pro-Active Input On The Design
Facilitate alignment when needed
Approve Design

Senior Management
Active Participation in Design
Support The Agreed Upon Design
Opportunity to align on expectations as a first step towards improved performance

- Obtaining training and/or sourcing the right level of talent for audit needs including the use of specialists
- Creating a continual learning and development model to improve IA’s knowledge of business experience & credentials
- Providing their “point of view” on macro risk and control issues that go across the organization

**Expectation:** % who expect this from internal audit; base = total survey responses

**Performance:** % who believe internal audit performs this well; base = only those respondents that expect internal audit to do this

---

PwC

April 2014
Expanding the expectation set

Stakeholder perceptions of internal audit departments with Assurance Provider expectations:
- 16%: Internal Audit adds significant value and performs well
- 26%: Internal Audit adds some value and performs well
- 41%: Internal Audit adds value but performs poorly
- 17%: Internal Audit adds little value or don’t know

Stakeholders perceptions of internal audit departments with Trusted Advisor expectations:
- 14%: Internal Audit adds significant value and performs well
- 17%: Internal Audit adds some value and performs well
- 56%: Internal Audit adds value but performs poorly
- 13%: Internal Audit adds little value or don’t know

Internal audit has the opportunity to drive greater value to the organization by expanding capabilities and skill sets, regardless of expectations/role.
The journey to trusted advisor

Unrealized value

- Trusted advisor
- Insight generator
- Problem Solver
- Problem Solver
- Problem Solver

Align expectations
Build capabilities
Deliver quality
Increase value
BYTES IN THE BOARD
ROOM- INFORMATION
TECHNOLOGY
POP QUIZ

- Which was the biggest (number of records) security breach of 2013?
  - Target
  - Adobe
  - LivingSocial
  - Facebook
POP QUIZ

Which was the costliest (estimated) security breach in recent times?
- Target
- Adobe
- Epsilon
- Sony Playstation
Security breaches can break the bank!
Per the 2014 Cost of Data Breach Study:
- The average cost to a company was $3.5 million in US dollars
- 15 percent more than what it cost last year
- Target’s security breach cost the company $148 million
Attacks on IT infrastructure are no longer isolated occurrences

In the recent Target data breach, reports indicate that hackers found their way into the company through credentials stolen from a contractor that had worked for the retailer

Audit committees should couple risk and IT oversight with financial reporting oversight

Legislators and regulators are increasing pressure on the board to focus on risk oversight aspects of governance
Internal Audit should think about…….

- Management knowledge and tracking of who is logging on to the network and from where
- Monitoring and tracking of information leaving the organization
- Staying apprised of IT security risks and threats and developing timely responses
- Developing a response plan for when an intrusion or other negative event occurs
Social Media and Regulation FD

- Regulation FD, adopted by the SEC in 2000, prohibits “selective disclosure”

- Disclosure of material information by an authorized person through a social media post may not be considered “reasonably designed to provide broad non-exclusionary distribution of information to the public”.

- In December 2012, the SEC issued a notice to Netflix because of a personal Facebook post written by Netflix CEO Reed Hastings
Here’s how ‘IT’ is monitored

- The audit committee should review company policies and internal controls related to social media usage.
- The company should have a clear compliance policy that specifically addresses the use and misuse of social media.
- Efforts should be made to monitor the comments made on social media outlets in which company spokespersons participate.
Privacy and Security
Breaches are frequent and large

- **47,000+** reported security incidents

- **700m+** records lost last year

- **44m+** compromised data records

- Organizations reporting losses of **$10M** or greater increasing **75%** from 2011. *2014 PwC Global State of Information Security*

- Average cost of data breach is approximately **$5.4m**

- Average cost per record: **$188**
  *Source: Ponemon Institute’s “2013 Annual Study: U.S. Cost of a Data Breach”*
# Significant Data Breaches

<table>
<thead>
<tr>
<th>Company</th>
<th>Breach Stats</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>110 million records</td>
<td>A data breach over a three week period capturing credit and debit card records. Encrypted PIN information also stolen. Other Customer Information may also have been stolen.</td>
</tr>
<tr>
<td>Schnuck Markets</td>
<td>2.4 million records</td>
<td>In October, Schnucks agreed to a proposed class-action settlement stemming from the breach of its computer systems.</td>
</tr>
<tr>
<td>CorporateCar Online.com</td>
<td>850,000 records</td>
<td>Hackers stole and stored information online related to customers who used limousine and other ground transportation for this St Louis based limo software provider. The online information included plain text archives of credit card numbers, expiration dates, names, and addresses. Many of the customers were wealthy and used credit cards that would be attractive to identity thieves. Some of the big names on the list include Tom Hanks, Sen. Tom Daschle, and Donald Trump.</td>
</tr>
</tbody>
</table>
| Adobe                        | 38 million customer accounts  
3 million credit card accounts | Originally just thought to be a compromise of 3 million PII records, the loss of a vast trove of login credentials was subsequently, and, more also its source code for various applications                                           |
| LivingSocial                 | 50 million accounts   | Computer systems were hacked, resulting in “unauthorized access.” The company updated its password encryption method after the breach. Names, email addresses, dates of birth, and salted passwords were stolen. |
| Advocate Medical Group       | 4 million patient records stolen | The theft of four computers from offices owned by this medical company exposed more than 4 million patient records. One of the largest losses of unsecured health information since notification to the Department of Health and Human Services became mandatory in 2009. |
The actors and the information they target

**Adversary**
- Nation State
- Hacktivists
- Organized Crime
- Insiders

**What’s most at risk?**
- Industrial Control Systems (SCADA)
- Emerging technologies
- Payment card and related information / financial markets
- Advanced materials and manufacturing techniques
- Military technologies
- R&D and / or product design data
- Healthcare, pharmaceuticals, and related technologies
- Business deals information
- Health records and other personal data
- Information and communication technology and data


*Adversary motives and tactics* evolve as business strategies change and business activities are executed; ‘crown jewels’ must be identified and their protection prioritized, monitored and adjusted accordingly.
Has your organization kept pace?

Questions to consider when evaluating your ability to respond to the new challenges.

Identify, prioritize, and protect the assets most essential to the business

- Have you identified your most critical assets and know where they are stored and transmitted?
- How do you evaluate their value and impact to the business if compromised?
- Do you prioritize the protection of your crown jewels differently than other information assets?

Understand the threats to your industry and your business

- Who are your adversaries and what are their motivations?
- What information are they targeting and what tactics are they using?
- How are you anticipating and adapting your strategy and controls?

Evaluate and improve effectiveness of existing processes and technologies

- Have you patched and upgraded your core platforms and technology?
- How are you securing new technology adoption and managing vulnerability with your legacy technology?
- Have you evolved your security architecture and associated processes?

Enhance situational awareness to detect and respond to security events

- How are you gaining visibility into internal and external security events and activities?
- Are you applying correlation and analytics to identify patterns or exceptions?
- How do you timely and efficiently determine when to take action?

Develop a cross-functional incident response plan for effective crisis management

- Have your business leaders undertaken cyberattack scenario planning?
- Do you have a defined cross functional structure, process and capability to respond?
- Are you enhancing and aligning your plan to ongoing business changes?

Establish values and behaviors to create and promote security effectiveness

- How is leadership engaged and committed to addressing cyber risks facing the business?
- What sustained activities are in place to improve awareness and sensitivity to cyber risks?
- How have your business practices evolved to address the threats to your business?
Data Privacy & Information Security Risks

- Compliance with government or industry regulations/ enforcements (HIPAA, PCI, GLBA, COPPA, FTC Act)
- Compliance with self-regulatory frameworks (i.e., U.S.-EU Safe Harbor, TRUSTe, DMA OBA Principles)
- Negative impact to the brand
- Loss of employee, customer, & investor confidence
- Companies face several financial risks associated with a breach:
  - Federal/state regulatory fines
  - Stock price decline
  - Remediation efforts
- Companies are experiencing increasing lawsuits from:
  - Employees
  - Customers
  - Investors
- Enforcement actions from federal and state agencies
- Regulatory inquiries may require long-term third party remediation in order to verify regulatory compliance
# Risks generally not perceived as well managed

## Risks seen as increasing the most in the last year
- Economic uncertainty
- Regulations and government
- IT security/cyber security
- Data privacy
- Government spending and taxation
- Competition
- Commercial market shifts
- Financial markets
- Large Programs (such as ERP)
- Talent and labor

## Risks seen as the most well managed last year
- Talent & Labor
- Competition
- Reputation/brand
- Financial markets
- Fraud and ethics
- Government spending and taxation
- Mergers, acquisitions and JVs
- Regulations and government policies
- IT / Cyber Security
- Economic uncertainty

85% believe security threats are increasing, yet only 12% think their organization manages risks extremely well.

Source: PwC’s 2013 State of the Internal Audit Profession Study
Organizations with high-performing internal audit functions manage risk better than others
Having a Program In Place to Protect Data

A comprehensive program is needed to address the myriad of compliance requirements, and to protect consumer information and sensitive company information.
Data protection and privacy is a relatively new consideration within the Risk Management disciplines. As a result, the manner with which organizations address this risk could differ widely. Some of the typical stakeholders associated with data protection and privacy concerns are listed below:

<table>
<thead>
<tr>
<th>Process Area</th>
<th>Concern (examples)</th>
</tr>
</thead>
</table>
| Legal              | • FTC complaints  
                     • Records Management                                                             |
| Marketing          | • eCommerce initiatives  
                     • CRM  
                     • Social media campaigns                                                        |
| Information Security| • Audit findings  
                        • PCI readiness  
                        • Data breaches  
                        • Network vulnerabilities                                                      |
| Internal Audit     | • Board or Audit Committee requests  
                        • Increasing the enterprise risk scope                                           |
| Compliance         | • HIPAA (healthcare), GLBA (financial)  
                        • Regulatory examination                                                          |
| Privacy Office     | • Governance structure  
                        • Operating privacy, how to “live” by the privacy policy                        |
Ongoing auditing or monitoring of a company’s data protection and privacy program is essential. Example of areas that auditing and monitoring activities should focus on include:

• Data protection and privacy program gap assessment
• Evaluation of, or assistance with, the company’s periodic data protection and privacy risk assessment process
• Compliance with established data protection and privacy policies and procedures
• Data protection and privacy training and awareness programs
• Data protection and privacy related remediation
• Third party/vendor data protection and privacy practices
Considerations for Your Organization

Understanding threats
• Has your data been exposed – and would you know if it were?
• Do you know what breach indicators you should be monitoring?

Building protections
• Has the company established formal governance and controls to protect the sensitive data?
• Are the controls and safeguards periodically tested?
• Have the controls and safeguards been updated to respond to changing business models?

Responding to incidents
• Are you prepared to respond to legal actions?
• If a Regulator were to inquire or investigate the company, would the company be prepared to respond?
• Has the company established formal plans to respond to incidents when they occur?
Considerations for Your Organization

Understanding Company Governance & Awareness

- What are the company’s compliance requirements?
- What is the culture of the company and what is the philosophy regarding information security and privacy?
- Who leads the efforts for information security (e.g., Steering Committee)?
- How does the company ensure alignment between the management and staff?
- What is the company trying to achieve with their information security/privacy program?

Understanding sensitive data

- What sensitive data do you have that needs to be protected?
- Has the company classified and inventoried that data?
- Who has access to sensitive data – internally and externally?
- Who is responsible for protecting your sensitive data?
- Who is responsible for the oversight of vendors that may hold sensitive data?
Coordinated lines of defense

1st
Line of defense: Management
Functional and line management are responsible for operationalizing risk management and internal controls

2nd
Line of defense: Risk Mgmt & Compliance
Risk management and compliance functions are responsible for establishing and monitoring effective risk management policies & standards

3rd
Line of defense: Internal Audit
Internal audit is responsible for providing objective assurance and advice on governance, risk, and compliance to the board and executive management
**The role of internal audit**

Internal Audit can play a role in the ongoing independent monitoring of a company’s data protection and privacy program.

- Keep the board abreast of emerging security and privacy risks
- Embed yourself in key activities that roll out new business processes, products or information systems (i.e., privacy by design)
- Communicate with the board and executive management
- Privacy/Security program gap assessment
- Network Vulnerability scanning and Attack & Penetration testing
- Evaluation of, or assistance with, the company’s periodic privacy/security risk assessment process
- Audits of established privacy/security policies and procedures and/or controls
- Audits of privacy/security training and awareness programs
- Audits of third party/vendor data protection and privacy practices
## Questions you should be asking

### Enhancing security strategy and capability

1. Is our cybersecurity program aligned with our business strategy?
2. Do we have the capabilities to identify and advise on strategic threats and adversaries targeting us?
3. Can we explain our cybersecurity strategy to our stakeholders? Our investors? Our regulators? Our ecosystem partners?

### Understanding and adapting to changes in the security risk environment

1. Do we know what information is most valuable to the business?
2. Do we know what our adversaries are after / what would they target?
3. Do we have an insider threat program? Is it inter-departmental?
4. Are we actively involved in relevant public-private partnerships?

### Advance their security posture through a shared vision and culture

1. How was our last security crisis identified; in-house or government identified?
2. Who leads our incident and crisis management program? Is our program cross functional / inter-departmental?
3. How often are we briefed on our cyber initiatives? Do we understand the cyber risks associated with certain business decisions and related activities?
What is important to regulators

- Accountability and program ownership
- Considerations of data protection, privacy and security throughout the organization and its processes
- Training and awareness programs
- Risk assessment processes
- Policies/procedures
- Data protection controls
- Monitoring technologies and capabilities
- Focus is on transparency in notice to consumers
  - Do the systems and controls process data as described by your privacy notice?
  - Do consumers have choice, and do they consent?
Vendor Risk Management
Globalization continues to grow and business partnerships are increasingly being leveraged as strategic enablers.

According to PwC’s 14th Annual Global CEO Survey:

- Companies are reshaping strategies and operating models—focusing on innovation, collaboration, and talent—to find new sources of revenue growth and competitive advantage
- Partnership will be key
  - 40% of CEOs expect the majority of innovations over the next three years to be co-developed with partners
  - 50% said their companies will enter into a strategic alliance or JV in the coming year
- Roughly a third of CEOs indicated their companies plan to complete a cross-border merger or acquisition, or outsource a business process or function in the next year

As organizational models shift and risk profiles evolve, executives and Boards seek greater transparency and increased assurance that the company’s most significant risks are appropriately mitigated
Vendor risk management (VRM) is focused on understanding and managing risks associated with vendors and other third parties with which the company does business and/or shares data.
Of the numerous risks to consider for a VRM program, the chart below outlines the majority of risks that are generally covered when assessing and managing the risks provided by vendors to your organization.

**VRM - Risk spectrum**

- **Exit Strategy**: The risk that the organization will have an inability to service its clients based on the termination or exit from a third-party relationship.
- **Regulatory**: The risk of an organization being out of compliance due to a third-party's failure to comply with laws/regulations.
- **Information Security and Privacy**: The risk of unauthorized loss of data or that an organization's data security has been breached at your third-party.
- **Reputational**: The risk and impact to the organization's reputation based on services provided by your third-party.
- **Service Delivery**: The risk that a third-party fails to meet your needs based on the delivery of their products/services.
- **Financial**: The risk of financial loss to the organization due to the third-party being unable to operate due to financial instability.
- **Business Continuity and Resiliency**: The risk of third-party inability of the organization to serve its clients.
- **Global Geographic Location**: The political, geographic, regulatory, legal, and economic risks of outsourcing to a country or region.
- **Reputational**: The risk and impact to the organization's reputation based on services provided by your third-party.

**Vendor risk spectrum**
# VRM - Program maturity

A standardized maturity framework helps organizations benchmark their program against peers and optimize their program to the level of maturity desired.

<table>
<thead>
<tr>
<th>Program Level</th>
<th>Process &amp; Procedures</th>
</tr>
</thead>
</table>
| **Level 5** Optimized | - Measure effects of process improvements against quantitative objectives  
- Define policies for integration with enterprise risk and vendor functions |
| **Level 4** Managed and Measurable | - Review security language in contracts periodically  
- Enforce corrective action for non-compliance with contract security requirements  
- Detect potential issues to enable preventative actions |
| **Level 3** Defined Process | - Define quantitative objectives for program and processes  
- Establish and execute communication strategy |
| **Level 2** Repeatable but Intuitive | - Monitor changes to security language in contracts at contract signing  
- Monitor and track compliance to contract security requirements  
- Define key risk indicators (KRIs) for all program risk assessment activities |
| **Level 1** Initial/Ad Hoc | - Update policies and procedures to meet organizational standards  
- Define exceptions policy tailored to organizational guidelines  
- Define responsibility for managing vendor risk relationship  
- Define process for vendor evaluation and selection activities  
- Update security risk assessments materials to map to organizational standards  
- Develop reporting to monitor and track vendor risk across program activities |
| **Level 0** Non-existent | - Define program scope and update strategy  
- Standardize policies and procedures  
- Standardize program roles and responsibilities  
- Develop security language templates for contracts  
- Update risk assessment processes to incorporate vendor security risk activities external to the program at a high-level  
- Develop basic reporting to capture process volume and activity status |
| | - Expand definition of policies and procedures to cover additional security risk activities and contract signoff  
- Define initial measurement criteria for assessment and program activities  
- Begin standardization of security language in contracts  
- Expand security risk assessment process scope to include ad hoc assessments  
- Define initial integration points with other vendor and risk functions to acquire data  
- Define initial processes to perform basic vendor security risk evaluation |
VRM - Quality review and oversight process

Planned and systematic activities that ensure that the VRM program is designed and operating as per the organizational requirements. Typically, this is achieved by performing both Quality Assurance (QA) and Quality Control (QC) processes.

Quality Assurance (QA)
Planned and systematic activities performed throughout the VRM lifecycle, that help ensure that quality of the functional requirements are achieved

- Example - Review of due diligence assessments prior to their finalization

Quality Control (QC)
Testing and validation to discover errors or non-compliance with initial scope or objectives.

- Example - Review of a sample of due diligence assessments on a quarterly basis

QA & QC Considerations

<table>
<thead>
<tr>
<th>Scope</th>
<th>Sample / Review</th>
<th>Report / Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program areas, regulations and requirements</td>
<td>Overall risk level</td>
<td>Report findings</td>
</tr>
<tr>
<td>Inherent risk assessments</td>
<td>Prior findings</td>
<td>Review and identify operational areas for improvement</td>
</tr>
<tr>
<td>On-going due diligence assessments</td>
<td>Passive review</td>
<td>Execute improvement plans</td>
</tr>
<tr>
<td>Emerging regulations</td>
<td>Detailed review</td>
<td>Improvement compliance</td>
</tr>
<tr>
<td>Inventory vs. GL</td>
<td>Extensive review</td>
<td>Risk management practices</td>
</tr>
<tr>
<td>AP spend</td>
<td>Nature of relationship</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Process quality trends</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outsourcing</td>
<td></td>
</tr>
</tbody>
</table>

For adequate oversight on VRM processes, an organization should design and implement a quality review and oversight process which includes elements from both QA and QC. The process should be designed based on the needs of the organization as well as degree of centralization of the VRM function.
Inventory, Risk Stratification & Risk Assessment Execution

The PwC Vendor Risk Management Program Framework

- Inventory
- Risk Stratification Framework
- Risk Assessment Methodology

- Technology
- Due Diligence
- Contract Negotiation
- Planning
- Policy & Procedures
- Governance & Organization
- Operating Mgmt
- Program Mgmt
- Reporting, Metrics & Scorecards
- Change Mgmt
- Issues Mgmt
- Complaints Mgmt
- Training
- Ongoing Monitoring

Design Build Operate

Pre-contract
Post-contract
Establishing vendor inventory

This framework will assist the Vendor Assurance Due Diligence program in honing in on the inventory list by analyzing multiple sources in a rapid manner and identifying the vendors that need to be included as part of the program, and segmented by risk.

Total Vendor Inventory from multiple data sources

- Begin with A/P Spend file and remove categories that don't pose risk
- Identify unique vendors and validate services against existing invoices/data sources. Remove categories that don't pose risk
- Perform cleansing and enhancement of vendor data

In-scope vendor inventory for risk segmentation

- Inherent risk assessment
- Risk segmentation structure

Starting with commodity categories, we use a process to focus on those products/services that do and do not pose inherent risk and thus to be included as part of the program.

We then clean and enhance the existing vendor data to be put into the inventory repository.

Common Vendor Inventory Data Attributes

- Vendor Name
- Vendor Parent Name / Associated Vendors
- Product / Service
- Vendor Type (Business Process Outsourcing, Partnership, Technology etc.)
- Spend
- Business Lines / Processes supported by the Vendor
- Country / Region where Vendor is based
- Contract Date (Engagement Date)
- Results of Vendor Risk Classification
- Results of Vendor Risk Assessments (e.g., Vendor Information Security Assessments)
Due diligence and contract clauses

In addition to generating a risk rating/segment based on the inherent risk of the relationship to your organization, the results of your pre-contract due diligence should drive contractual protections.

Example Due Diligence Assessments
1. Country Risk
2. Financial
3. Reputational
4. Legal & Compliance (e.g., Reg Chng, Anti-Corruption, Watch List)
5. Information Security
6. Business Continuity
7. Disaster Recovery
8. Physical Security
9. Privacy
10. 4th Parties
11. Technology
12. Operational Competency
13. Insurance
14. Contracts

Example Contract Clauses
1. Nature and scope of service
2. Performance standards
3. Subcontracting & 4th Parties
4. Diversity
5. Indemnification
6. Default and termination
7. Confidentiality & Security
8. Regulatory requirements
9. Ownership, license and access
10. Business continuity and contingency planning
11. Controls verification
12. Notification & escalation procedures
13. Limits in Liability
14. Insurance
15. Right to Audit
16. Records management
17. Pricing
18. Cost and compensation
19. Payment terms
20. Dispute Resolution
21. Management Information Systems reporting responsibilities
22. Customer complaint handling
23. Amendments
**Residual risk maturity framework – Risk rankings**

The residual risk maturity framework enables the program to rank and refresh the residual risk of a vendor’s control maturity to further drive on-going due-diligence testing efforts to the vendor base.

<table>
<thead>
<tr>
<th>Residual risk maturity ranking</th>
<th>Standard risk definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Controls do not exist/are not in place</td>
</tr>
<tr>
<td>2</td>
<td>Controls are in place but are not documented appropriately or currently are not reviewed/ tested; controls are not consistently followed</td>
</tr>
<tr>
<td>3</td>
<td>Controls are in place and are documented and reviewed; manual or partial automation</td>
</tr>
<tr>
<td>4</td>
<td>Controls are in place, are documented appropriately, are reviewed on a periodic basis, have continuous control monitoring and fully automated if available</td>
</tr>
</tbody>
</table>

These maturity ratings would then be utilized to determine the nature, timing and extent of successive testing on an ongoing basis. After each successive due diligence test is completed the vendor ranking should be refreshed and re-ranked (if applicable).
## Risk assessment control categories

We see a wide-range of different control categories that are covered as part of a vendor due diligence assessment framework.

### Technology/Security

- Security policies
- Change controls
- Electronic mail and Instant Messaging
- Encryption
- Data integrity
- Logical access Control
- Monitoring, communication and connectivity
- Website management
- Incident response
- Disaster Recovery and Business Continuity
- Backup and offsite storage
- Media and vital records
- Vendor Relationship management
- Sub-Service Vendor Relationships
- Regulatory requirements
- Organization background
- Standard builds
- Operations
- Asset management
- Desktop
- Application management
- System development
- Customer contact

### Geographic Location

- Political
- Geographic
- Regulatory
- Legal
- Economic

### Reputational/Integrity

- Litigation or ethical flags
- Media coverage
- OFAC or other factors
- Red flag criminal or civil complaints

### Financial

- Liquidity
- Leverage
- Profitability
- Transaction Processing

### Capability

- Demonstrated capability
- Competitor comparison
- Size of vendor vs. size of service
- Organization

### Compliance

- HIPAA
- CFPB
- SOX
- GLBA
- PCI

### Performance

- Contract compliance
- SLA compliance
- Customer complaints handling
The PwC Vendor Risk Management Program Framework

- Design
- Build
- Operate

- Pre-contract
- Post-contract

- Reporting, metrics & scorecards

- Technology

- Policy & Procedures
- Governance & Organization
- Operating Model
- Program Mgmt
- Change Mgmt
- Risk Stratification Framework
- Risk Assessment Methodology
- Training
- Complaints Mgmt
- Issues Mgmt
- Inventory
- Due Diligence
- Contract Negotiation

- Reporting, Metrics & Scorecards

PwC
Metrics, reporting & scorecards

We believe in a top down approach to the development to a metrics and reporting function.

**Approach**

Start by determining key risks for the VRM program. These risks will be supported by risk metrics that are linked to thresholds, weighted and tuned to become Key Performance Indicators and Key Risk Indicators and will help establish risk reporting views.

1. **Identify risks for the VRM program**
   - Vendor access to sensitive data or support of critical processes may have reputational, financial or regulatory impact

2. **Identify sources of data**
   - Vendor Risk Profiling Data
   - Issue and Corrective Action Plan System

3. **Identify key risk indicators**
   - Total number of vendor relations with access to sensitive information (by risk tier)
   - Total number of vendor relations supporting critical processes (by risk tier)
   - Count of total number of identified issues by vendor, reported over time

**Sample Dashboards and Reports**

![Sample Dashboards and Reports](image)
# Key Performance and Risk Indicators (KPIs and KRIs)

There are numerous indicators from a performance and risk perspective to take into account as part of your VRM program. Some examples are noted below:

<table>
<thead>
<tr>
<th>#</th>
<th>KPI/KRI Description</th>
<th>KPI dimensions</th>
</tr>
</thead>
</table>
| 1  | # of issues by Vendor | • By Supplier  
  • By Statement of Work  
  • By issue severity rating (R1 - R5)  
  • By Line of Business |
| 2  | # of Vendors in the VRM program | • # by Line of Business  
  • # Inherent Risk Scores/rating  
  • # by Product/Service |
| 3  | % of employees whose performance metrics and rewards reflect risk management objectives | • By Lines of Business Relationship Owner  
  • By Line of Business Sponsor  
  • By Inherent Risk Score or Rating  
  • By Supplier  
  • By Global Supplier Relationship Manager  
  • By Third Party Management Office Liaison |
| 4  | % of risk issues with tracking of expected reduction in frequency and magnitude | • By Business Facts Questionnaire or Statement of Work  
  • By Line of Business  
  • By Third Party Risk Manager  
  • By Assessment type  
  • By Inherent Risk Score or Rating  
  • By Supplier |
| 5  | % of staff trained in active risk management | • # of Third Party Risk Manager in population  
  • # of completed training  
  • Average Time Between Supplier Meetings  
  • # of Supplier Meetings per Year  
  • # of Scorecards Completed Per Year By Supplier |
| 6  | Action Plan tracking to closure | • By Line of Business  
  • By Third Party Risk Manager  
  • By Vendor  
  • by past-due 30 days, 60 days, and 90 days |
# Intermediary Oversight Model Considerations

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish Working Group &amp; Oversight Committee</td>
</tr>
<tr>
<td></td>
<td>- Identify working group members involved with intermediary oversight and governance</td>
</tr>
<tr>
<td></td>
<td>- Establish oversight committee with senior executives and working group members</td>
</tr>
<tr>
<td></td>
<td>- Establish Committee charter and mission</td>
</tr>
<tr>
<td></td>
<td>- Consider potential emerging risks, priorities and contingency plans</td>
</tr>
<tr>
<td></td>
<td>- Consider those involved in omnibus conversions</td>
</tr>
</tbody>
</table>

| 2    | Develop Oversight Model & Strategy |
|      | - Identification/scope of intermediary relationships and related oversight responsibilities |
|      | - Perform top down risk review with clear and explicit linkage to priorities |
|      | - Develop framework and key areas for oversight |
|      | - Prioritize risks and develop metrics |
|      | - Develop risk matrix and scorecard |
|      | - Determine data collection models |
|      | - Developing periodic monitoring of models |
|      | - Review contract requirements including FICCA |

| 3    | Perform Oversight/ Monitoring |
|      | - Determine monitoring approach/tools to use |
|      | - US vs. Non-US program |
|      | - New intermediaries vs. existing relationships |
|      | - Consider sub-service providers (e.g., sub-accounting agents) |
|      | - Establish FICCA review program. Consider report types (e.g., SSAE 16), scope, level of coverage, and cited issues. |
|      | - Consider integration of other staff (e.g., relationship managers) |

| 4    | Reporting & Communication |
|      | - Define frequency of communication |
|      | - Determine reporting capabilities and process |
|      | - Provide clear and concise communication to those charged with governance: transfer agents, legal/compliance, fund boards and committees |
**Oversight Tools**

- On-site visits/reviews
- Certifications
- Questionnaires
- Data analysis/recalculations
- Monitor for negative news
- Use of FICCA and other 3rd party reports
Some quick fixes to take back control……

- Consolidate remote access tools
- Eliminate all redundant remote access
- Multi-factor authentication
- Employ granular permissions
- Secure audit trails
## Insights and lessons learned

Through our extensive experience in the development and execution of VRM programs, we can bring a high level of wisdom to any type of VRM engagement.

<table>
<thead>
<tr>
<th>Strong sponsorship and leadership</th>
<th>Successful vendor risk organizations are consistently underpinned by visible executive sponsorship and strong leadership at a functional and program level.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Start Smart”</td>
<td>By focusing on the target operating model when designing a vendor risk management program, significant cost saving and minimal operational impact to business operations may be achievable. Areas that help include vendor stratification, leveraging of existing risk processes and governance structures, focus on products/services, leverage three-lines-of-defense model, etc.</td>
</tr>
<tr>
<td>“Work Smarter NOT Harder”</td>
<td>When designing a vendor risk management program, focus on having the third parties do as much of the “heavy lifting” as possible, to recue the operational burden of program to the enterprise. This can be accomplished through the use of automated workflow and leveraging third party accessible tactical and strategic technology solutions.</td>
</tr>
<tr>
<td>Clear business engagement</td>
<td>Working in a transparent and integrated fashion with all functional and operating group stakeholders is required to develop a solution that delivers against the needs of the organization. Many companies have a designated liaison in the business to build relationships, increase awareness and harmonize business needs with vendor risk capabilities.</td>
</tr>
<tr>
<td>Aligning to a common risk language and process</td>
<td>Agreeing upon a common set of terms and definitions is necessary to create a consistent process for defining, managing and measuring vendor risks. Once done, it is easier to develop new processes to address changes to regulatory and business requirements.</td>
</tr>
<tr>
<td>Leveraging effective processes and technologies</td>
<td>Leading tools and technology drive groups to use common risk management processes, which enhances the effectiveness and efficiency of the VRM program. This will allow management to have a better view of metrics and enables them to make better decisions around governance, risk and compliance management and corresponding communications.</td>
</tr>
<tr>
<td>Disciplined information flow</td>
<td>Communication to stakeholders, employees and business partners is critical throughout the entire vendor risk management program process. Managing these communications throughout the development of the program is critical for success.</td>
</tr>
</tbody>
</table>
Questions