Ensuring Organizational & Enterprise Resiliency with Third Parties

Geno Pandolfi

Tuesday, May 17, 2016
Room 7&8 (1:30-2:15 PM)
Session Review Objectives

- Approaches to Third Party Risk Management
- Core Concepts to Third Party Due Diligence
- Managing Threats and Risks from Third Parties
- Key Practices for Ensuring Third Party Resiliency
- Emerging Regulatory Focus and Direction
Key Learning Points

- Standardizing contract language for recovery and potential third party exit strategies

- Importance of integrating partner resiliency data across the Enterprise

- Understand key critical third party services provided to your organization
Third Party Risk Management (TPRM)
Key Market Drivers

- Increasing reliance upon Third Parties and outsourcing of sensitive functions to Third Parties (Emerging Cloud Service utilization by Organizations)

- Lack of Central control over all Sourcing decisions and understanding of risk exposure from third-party providers

- Incomplete service inventories of third-party sensitive data components

- Lack of alignment to an Organizational TPRM Program Framework

- Enhanced focus on Third Party Security issues and exposures

- Inconsistent Compliance/Risk assessment processes and issue resolution

- Emerging Board Level scrutiny and focus on Third Party Service Provider risks
TPRM Approaches and Core Concepts

Reference Third Party Assessment Questionnaires:

Are these delivering real value to your organization or are they just “Paper-Pushing Exercises”? 
TPRM Program Approaches

High Vendor Volume – Automation Candidates

Risk Based Concepts - Resource Intensive
TPRM Conceptual Framework

Pre-Contract Evaluation
- Identification
- Vendor Due-Diligence
- Source Vendor Information
- Review by Subject Matter Experts*
- Vendor Risk Rating/Evaluation
- Procurement and Contract Structure

On-going Monitoring
- Periodic Vendor Review Program
- Vendor Contracted Data Feedback
- Internal Vendor Performance Rating
- Review by Subject Matter Experts*
- Vendor Risk Rating/Evaluation
- Vendor Analytics/Issues Resolution

* Finance/Credit
  - Security (Info/Physical)
  - Business Continuity
  - Procurement/Legal Area
  - Technology/Operations
  - Risk Management
  - Privacy Control
  - Vendor Management
Standard Assessment Practices

- Third Party In-depth Questionnaires – Rule Driven
- Third Party Annual Reports and Financials
- Standardized Information Gathering Questionnaire (SIG) Initial Assessments IT, Privacy, Security (SIG-Lite)
- Internal Third Party Evaluations and Site Visits
- Third Party External Audit Results (Controls and Processes)
- Standards Certifications (ISO, NIST, NFPA, etc.)
- SOC-2 Reports (Service Controls- Security, Availability, Processing, Confidentiality/Privacy)
- SOC-3 Reports CPA Control Opinions (Controls- Security, Availability, Processing, Confidentiality/Privacy)
- Auditor Centric Reporting
- Cloud Based Subscription Vendor Rating Services

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Доверяй но проверяй!

“Trust But Verify”

President Ronald Regan to Soviet Premier Gorbachev
Washington Intermediate Range Nuclear Forces Treaty
December 8, 1987

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Third Party Contract Due Diligence

“I need two franks, three wieners and one hot dog.”

Licensed from Cartoon Stock-Dave Carpenter
Third Party Contract Considerations

- Ensure utilization of Standard Contract Templates and approved legal contract verbiage
- Determine exception processes for Third-Party paper usage
- Contract structures should include form and content for key contract domains (e.g. Security, Recovery, Operations, etc.)
- Include contract processes for Subject Matter Experts in evaluations of contract variances from templates
- Establish processes and controls for tracking, reporting, and escalation of standard contract and material deviations
Standard Contract Elements

- Services Definitions and specific SLA’s
- Financial Relationship/Feess/Billing
- Rights to Terminate and Exit Requirements*
- Facility and Employee Usage/Constraints
- Rights to audit third provider and sub-contractors*
- Definition of Data Ownership rights, Software licensing, and Equipment utilization
- Confidentiality and Privacy protection of data and delineation of processes due to an unauthorized access*
- Requirements of Third Party to comply with confidentiality, privacy, and appropriate federal and state statues*
- Third Party compliance with company policies and procedures including Third Party program*
- Key contract variance resolution and issue resolution process, with time-frames*
- Applicability of contract provisions to all sub-contractors and suppliers
- Rights of company to receive and review key control reports and various audits (ISS & BCP)*
- Requirements to review business continuity/crisis plans, control, and audits*
- Specific Information Security Controls, Data protection, and required security standards*
- Standard requirements for Data Backup and Data Retention, and Processing Capacities*
- Clear identification of third party reporting and performance review periods*
- Required Insurance Retention Limits and Indemnification requirements
- Penalties for non-compliance with required ISS, Operational, and Continuity requirements
- Liability limits aligned to potential loss by company for contract non-performance
- Right for onsite review service activity and ability to test as needed*
- Itemization of remedies for service and contract non-performance*

*Essential additions
Third Party Contract Participants/Accountability

- **Negotiating Business** – Time to Market and visibility to contract due diligence, responsible for Third Party relationships, performance, risk and compliance.

- **Third-Party** – Negotiates in good faith, executes per contract, shares assessment results, and provides relationship evidence.

- **Procurement and Legal** – Enable the contract process, Identifies contract risks and ensure defensible verbiage and compliance requirements.

- **Risk, Compliance, and Vendor Management** – Maintains overall Vendor Relationship Program Process, Key Policies, Enables review processes, Monitors Risk, Compliance and Reporting, and Third Party Escalations.

- **Subject Matter Experts** – Ensure contract SME template requirements, participates in contract exception process, and conducts relationship domain activity review and due diligence.
Verifiable Resiliency Contract Base

- Business Resumption, Crisis, and Contingency Plans, and Policy warranties by Third Parties, and adherence to specific industry standards, and even notification requirements

- Provisions for ensuring continuation of Services in the event of operational impacts from natural or man-made disasters, international or malicious attacks, system breakdowns and operational issues

- Specifics as to back-up requirements, off-site and data vault storage, and specifications for protecting programs, data, and equipment

- Details regarding Periodic Third Party Plans Maintenance (BCP, DR, and CM plans) and specific as to RTO, RPO, and other SLA’s due to processing delays and/or disasters, and resumption requirements

- Need for periodic or annual review requirements of Third Party BCP, DR, and CM Plans; Internal/External Program audits, and Demonstrated exercise results

- Requirement for alternate work-area recovery, technology, and processing locations, and specific requirements for alternate recovery site specifications

- Periodic ability for site validation visits and the ability to actively participate in multiple scenario exercise concepts (DR to Prod, Prod to DR, CM Communication, Joint-Cyber, etc.)
Info Security Contract Base

- Requirements for the Third Party to maintain a complete set of Information Security policies, standards, and practices

- Adherence to industry and regulatory best practices without limitation, as it relates to (Network Monitoring and Protection, Authentication and Authentication Protection, Intrusion Detection, Data Encryption, Network Structure and Maintenance, Malware Detection, Patching, Security Testing, Countermeasures, Incident Response, and Asset structures)

- Notification by Third Party of specific material changes of Info Security policies, standards or practices, and specific notification time frames

- Ability for periodic review of the Third Party policies, standards, practices and standards adherence, and ability to perform site inspection visits

- Immediate notification requirements of actual or suspected security breaches, and immediate coordination to remedy and investigate all breaches, and notification of performance impacts to the contracting organization

- Right to review all security controls, security testing results, internal/external audits of testing results, and specific program Security program audits, and allowed review time frames
Contract Variances and Exit Concepts

- Establish process to identify, report, and mitigate Material Contract variance from key contract templates

- Assign accountability for contract variance ownership, controls, and review of contract variances

- Ensure cross-domain steering committee review of all material contract variances, and key executive reporting

- Establish realistic exit strategies and internal decision points for managing Third Party Financial failures, consistent SLA failures, and major contract breaches

- Exit strategies need identification of internal processing departmental and systems impacts, internal development and migration plans, and funding requirements

- Identify if alternate third party usage: Time frames and migration processes to alternate third process, and interim work-around processes until full exit strategy implementation,
TPRM Compliance and Risk Management Concepts

Risk: “Someone or something that creates or suggests a hazard”

Compliance “The act or process of doing what you have been asked or ordered to do: the act or process of complying”

Source: Merriam-Webster's Learner's Dictionary
## Risk Management Factors

<table>
<thead>
<tr>
<th>Category</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic</strong></td>
<td>Reliance upon Third Parties to provide Mission Critical processing, technology, process outsource, systems, and recovery services. Potential for significant impacts to corporate strategic objectives, direction, and response.</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Failure of Third Parties to meet their contracted Service Level Agreements, Product’s or Service Delivery to customers that impacts corporate revenue and profits. Potential for significant litigation and exit expenses.</td>
</tr>
<tr>
<td><strong>Reputational</strong></td>
<td>Resulting from major internal issues exposed to general public including failed system delivery, major outages, data breaches, and customer service issues. Customer confidence and trust may take years to regenerate and require significant unplanned investment to reclaim the Brand.</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td>Impacts to delivery of service for transaction activity, service operations, information security, denials of services and data breaches, continuity of services and/or systems availability.</td>
</tr>
<tr>
<td><strong>Geopolitical</strong></td>
<td>Third party operations conducted in other countries where political, cultural, or financial structures may impact or prevent service delivery or the ability to conduct business. Potential data or information exposure from retention off-shore of key customer sensitive information outside of US jurisdiction.</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Third Party violation of regulations, laws, industry requirement (PCI, etc.), and internal policies. Potential for contracting business to be exposed to government oversight, increased regulatory scrutiny, and/or fines.</td>
</tr>
</tbody>
</table>
Third Party Compliance Stratification

Define Third Party Compliance Scope
- Initial Inventory and Third Party Categorizations
- Preliminary Assessments and Evaluations
- Rules based Decisions

Secondary Compliance Filtering:
- Key Exposures
  - Financial
  - Reputational
  - Security
  - Business Continuity
  - Technology
  - Geopolitical
  - Strategic

Due Diligence Third Party Review and Monitoring Requirements
- Ranking based upon Risk Sensitivity
- Risk based Levels of Due Diligence
- Periodic review and monitoring
- Ongoing Performance Analytics

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Key Compliance Control Requirements

- Third-Party Contractual Status, Content, Exception Tracking and Mitigation
- SME Review Tracking, Assessment, and Issue Resolution Management
- Service and Contract Performance Levels and Assessments (Score Cards-Include Service Complaints and Resolution)
- Third Party Secondary and Tertiary Supplier Performance Measurements
- Appropriate Significant Change Control and Activity Tracking
- Third Party Compliance Evidence Levels - Quality Control and Assurance
- Key Performance Indicators for Operational and Executive Analytics
Managing Third Party Risks

- Determine Third Party Relationship Risks – Inherent Risk Definition
  (Level of Monetary Contract Value; Reputational Risk from Risk Data Breach, Threats from Security Violation, Potential Operational Disruptions, Level of Regulator or Contractual Exposure, Geopolitical Concentration Risk, etc.)

- Complete Assessment of Third Party Controls and Mitigation Solutions

- Assess Third Party Operating Profile Risk – Define Third Party Risk Levels and Residual Third Party Risks

- Complete Periodic Control Validation and Evidence Review dependent upon Compliance and Risk Tier Assessment

- Provide Key Risk Indicators, Risk Control Metrics, and Executive Reporting and Analytics
Third Party Resiliency Practices

Celebrating a decade of guiding security professionals.
Third Party Resiliency Data Concepts

- Utilize integrated data points with federated and aligned technologies

- Align Third Party Program work-flow and SLA’s with the integrated technologies, aggregate data from Trusted Sources

- Automate standard key Program Performance, Compliance and Risk Indicators and Analytics/Trend Analysis

- Provide Internal Stakeholders and Third Parties real-time access to Trusted information/metrics (External and Internal with Data Segmentation)
Trusted Data Sources

- Third Party Centralized Inventory and Services
- Procurement Contracts and Contract Material Issues
- Third Party Performance Tracking and Monitoring
- Third Party Recovery, Info Security, and Operational Data Components
- Compliance and Risk Aggregation Report Elements
Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Third Party Recovery - Resiliency Plan Linkage

- Business Impact/Process Assessments
- Process Recovery Strategies
- Business Continuity Plans
- Application/Technology Assessments
- Technology Recovery Strategies
- Service Continuity Plans
- Crisis Response/Communication Plans

Operational Continuity Systems

- Internal Recovery Plans Linkage to Third Party Services and Components

Continuity Repository

Federate Third Party Inventory and Key Data

Third Party Inventory/Content

- Inventory Stratifications
- Service/Technology Definitions
- Risk Sensitivity Ratings
- External Evidence

Internal Third Party Recovery Plans

Organizational Response to Third Party Events:
- Security
- Availability
- Operational

Third Party Resiliency Components:
- Internal Recovery Plans and Strategies
- Recovery Plan Activity/Exercise Results
- BCP Process Linked Activity/Exercise Results
- SCP Process Linked Activity/Exercise Results
- Multi-Scenario Exercise Results
- Exercise Issues and Mitigations

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Third Party Exercise Concepts

- Periodically Exercise Internal Third Party Recovery Plans with Bi-directional Notification with Third Parties
- Conduct Applications and System Technology testing with Third Party Technology Systems in DR Exercises
- BCP Processes execute Recovery and Utilization of Third Party Technology and Process Environments during BC Plan exercises
- Actively participate and jointly test with Third Parties during their DR/BCP exercises
- Perform enhanced testing with Risk Sensitivity Third Parties
- Engage and Test with Third Parties during Industry-wide Table-Top and Active Sector Exercises
Third Party Resiliency Exercises

- Conduct Active Scenario Exercises with Third Parties including:
  - End-to-End Process Testing (Organizational and Third Party)
  - Connectivity Testing Organizational DR to Third Party System Environments
  - Execute Organizational Production to Third Party BCP/DR Testing
  - Multi-System Integration Testing with Third Parties
  - Performing Major Operational Disruption Simulations
- Develop active Cyber Exercise Plans and execute Joint Incident Management Exercises inclusive of:
  - DDoS
  - Data Breach
  - Data Corruption
  - Data Ransom
  - Operational Continuity
“... it is no surprise that the OCC deems operational risk to be high and increasing. Indeed, it is currently at the top of the list of safety and soundness issues for the institutions we supervise.”

“... Due diligence in identifying, measuring, and monitoring the risk from third-party relationships, and establishing mechanisms for controlling and continuously monitoring those risks, is thus an essential part of managing operational risk”...

“... Third-party relationships warrant close attention, because poor performance on the part of service providers has the Potential to do enormous damage to the banks that employ them”...

“Thomas Curry-Controller of the Currency”
Excerpts 2012 & 2014 Speeches
Focused Regulatory Directions

- OCC 2015-44 Revised IT Handbook (IT Risk Management; Cyber Security)
- OCC 2015-31 Cyber Assessment Tool (Self-Assessing Bank Cyber Security-Inherent Risk Profile)
- OCC 2015-09 Strengthening Resilience of Outsourced (Technology Services (New Appendix J BCP IT Handbook))
- OCC Supervisor Tips Bulletin 12/2014 (Cyber Threats & Operational Resiliency)
- OCC 2013-29 Risk Guidance (Third Party Relationships)
- OCC 2012-34 Supervisor Guidelines (Technology Service Providers)
- OCC2002-16 Third Party Service Providers (Bank Usage of Foreign Service Providers)
- OCC2001-35 Guidance Procedures IV (Safeguarding Customer Information)
- OCC2001-47 Third Party Management (Risk Management)

- SR 00-4 (SUP) Division Supervision (Outsourcing of Information and Transactions Processing)

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
Key Regulatory Drivers

- Increasing level of Outsourcing by Financial Institutions to Third Party Suppliers

- Emerging Nature of Third Party Relationships Products and Services offered to Financial Institutions

- Increased concentration risk exposure to FI’s due to Industry Consolidations

- Increase Media Focus and Volume of Third Party Data Breaches

- Increasing Compliance Scrutiny from Dodd-Frank Regulations including Third Party servicing of FI Customers
New FFIEC Appendix J Direction

Ensure appropriate practices are embedded in banking institutions BC Programs to comply with the Appendix J Regulation

• The recently added Appendix J (of the FFIEC examination procedures) requires financial institutions to address management’s responsibility to control the business continuity risks associated with utilizing Outsourced Technology Services for critical business functions.

• Primary objectives of Appendix J impactful to Corporations are to:
  - Ensure Third-party management addresses a financial institutions (FI) risk management of Third Parties and their sub-contractors
  - Demonstrate ability to keep critical processes functioning during a third party or corporate service disruption
  - Develop recovery validation procedures for the disruption when the service becomes available
  - Validate the third party service continuity capability and capacity through a robust testing program, including Cyber Risk testing
  - Continuous monitoring and reporting of Performance and Key Risk along with gaps and risk mitigation of Third Parties
FFIEC Regulatory Exercise Guidance

- Threat based scenario testing should include incident response plan, crisis management, security breaches, and communication processes with TSP

- Demonstrated FI Outage Disruption Testing with Third Parties (FI DR to Third Party Prod)

- Financial Institution (FI) Testing should demonstrate both ability to fall-over to secondary site but also test for continuous operations in DR to Prod Scenarios

- Table-Top or Simulation scenario exercises of a major regional Outage (FI DR to Third Party DR) - Impacts to both production environments

- FI and Third Party ability to respond to attacks such as DDoS or Data Corruption events - Consider Simultaneous Attack exercise simulation exercises

- Include exercises that Third Party, Subcontractors, and other service providers including end to end testing

- Participation of FI and Third Party in joint Industry centric Testing simulations

Celebrating a decade of guiding security professionals.
QUESTIONS
THANK YOU,

Geno Pandolfi
genopand@yahoo.com