VENDOR RISKS

CRITICAL CONSIDERATIONS FOR GRC

Aaron Miller, CISA, CRISC
Information Risk Analyst
Bank of America

PUZZLE

What are the next two numbers in this sequence?

101, 112, 131, 415, 161, 718, ???, ???

TRADITIONAL VENDOR CONSIDERATIONS

- Supply Chain
- Concentration Risk
- Communication / Connectivity
- Effectiveness
- Cost

WHAT'S CHANGED

- Instantaneous Expectations
- Outsourcing / Subcontractors
- Legal / Compliance
- Data and the Cloud
- Cyber

TRADITIONAL METRICS

- RTC
- RPC
- RTO/RPO
- SLA

FFIEC APPENDIX J

- Third Party Risk Management > Technology Service Provider (TSP)
- BC Plans that assess the impact of a disruption to a TSP, including assessments and plans
- Validation through testing with the TSP
- Plans to address cyber events, also with assessments and plans

TSP DUE DILIGENCE

- Understand fourth parties (and potentially their third parties)
- Include data and environmental concerns, especially if data crosses national boundaries
- Understand how the TSP validates and tests with their subcontractors
- Establish a documented methodology for how TSP's are evaluated
- Review the financial viability of TSP's
- Have an exit strategy
- Monitor all TSP's and evaluate on an annual basis

INTEGRATE VENDOR RISK MANAGEMENT (VRM) AND CONTINUITY/GOVERNANCE PROGRAM

- Outsource activity but not responsibility or accountability
- Align risk metrics between VRM, ERM and BCM
- What role does Legal serve?
- Is BCM integrated in the process?
- What role does IT serve?
- Where does the CISO fit into the picture?

VALIDATION AND TESTING CONSIDERATIONS

- Do the TSP's continuity program and metrics meet the requirements of the business?
- Can you validate if TSP fails, or if business fails, or both?
- Both TSP and business should maintain cyber response plans
- Document interdependencies including technological and business

ESTABLISH REQUIREMENTS FOR VALIDATIONS

Applications

- Tier 0: Resilient with near-zero downtime
- Tier 1: up to 4 hours downtime
- Tier 2: Intraday recovery, up to 8 hours
- Tier 3: 48-72 hours downtime

REQUIREMENTS FOR TESTING/EXERCISES

- Tier 0: tested every 6 months
- Tier 1 & 2: tested every 12 months
- Tier 3: tested every 24 months
- Have LOB staff available to validate availability and data integrity
- Internal applications can be challenging due to production requirements
- If applications are hosted, work with vendor to document capabilities. Co-testing is vital.

WHAT IS CO-TESTING

- In exercise, connect your production environment to their DR environment
- Or, connect your DR environment to their production environment
- Not much use/value to connect DR to DR. Likelihood is quite small
- Document processes, timelines and assumptions
- For Tier 0 and Tier 1 applications, insist that vendors run in DR for one full business day
- Affirm that vendors can fail back to production within timelines established and document.

WHO'S INVOLVED

- Vendor representatives
- Vendor managers
- IT/DR staff
- BC staff
- LOB to validate testing

TRACKING AND REPORTING

- Who tracks the cadence of the work for vendors and applications?
- Who establishes/enforces calendar requirements?
- What's the escalation and consequence path for non-compliance?
- Who reports results and to whom?

VENDOR SCORECARDS

- Work with LOB to develop performance metrics for vendor
- Items to consider for inclusion:
  - SLA met/missed
  - Customer service queries answered in timely fashion
  - Uptime and availability of application
  - Changes that would help along with estimated time/cost
  - Overall effectiveness and efficiency of services
  - How often should scorecards be completed (Quarterly, usually)

VENDOR MANAGEMENT

- Is there a database of record?
- How much autonomy / authority do LOB's have to contract "outside the system"?
- Is there analysis of results/spend overall?
- How are RFP's managed, composed, evaluated?
- Are Master Services Agreements and Statements of Work in the database?

PUZZLE

What are the next two numbers in this sequence?

101, 112, 131, 415, 161, 718, ???, ???