rma
THE RISK MANAGEMENT ASSOCIATION

SARS-COV-2

RECOMMENDATIONS FOR THIRD PARTIES WORKING FROM HOME & RETURNING TO FACILITIES

DECEMBER 2020

Every firm in every sector operates within a complex extended enterprise, with extensive reliance on third- party relationships. COVID-19 is a sharp reminder of the importance of proactive third-party risk management, which is necessary for risk treatment, risk insight, and risk governance.

In this document, senior level third-party risk management practitioners and subject matter experts, members of RMA's Third-Party Risk Management Round Table, will share "lessons learned" (so far) during COVID-19. The level of detail makes this an ideal tool for third-party and operational risk management professionals, and business owners in the 1st Line of Defense.

Many thanks to:

- **Jim Berghs**, SVP, Third-Party Risk Management, US Bank
- **Bob Koszkalda**, Director, Third-Party Risk Management, Key Bank NA
- **Daniel Schiemel**, Operational Risk - Third-Party Risk Management, Guardian Life Insurance Company
- **Christe Smith**, Director of Third Party Risk, Bank OZK
- **Linda Tuck Chapman**, CEO, Third-Party Risk Institute Ltd.

In this document, we present many high impact "Problem Statements" and how the pandemic has highlighted risks and highlighted deficiencies in current practices and controls. Leveraging their expertise and experience, the working group makes specific, actionable recommendations to mitigate or treat the risks.

The paper is arranged into the following sections:

- COVID-19's impact on Third-Party Risk Management Practices
- COVID-19's Impact on Business Resilience Strategies
- Harmonizing Practices Globally
- Contingency/Exit Plans
- Activity Concentration Risk
- Geographic Concentration Risk

COVID-19'S IMPACT ON THIRD-PARTY RISK MANAGEMENT PRACTICES

PROBLEM STATEMENT #1:

Third-party contracts and controls did not contemplate third-party employees working from home (WFH).

Where existing contracts and controls have proven to be inadequate, it is important to establish or strengthen standard contractually binding obligations, and negotiate amendments to address deficiencies and gaps.

Recommendations:

1. Where existing contracts and controls are inadequate, develop standards and negotiate amendments to strengthen controls and close gaps. At the relationship level, this may include:
    i. Work-from-home-specific approval period, expiry date, and any special conditions
    ii. Minimum security controls
    iii. Periodic controls, testing, and reporting
    iv. Activities, risk events, and notification protocols
    v. Breach reporting requirements
    vi. Retention and destruction of data and records
    vii. Evidence of periodic internal controls testing
    viii. SLAs and performance expectations

2. Negotiate a requirement for third-party work-from-home employees to comply with code of conduct, privacy, and clean desk policies that are acceptable to your firm, or have them sign yours.

3. Design and negotiate specific security controls for work-from-home third-party employees and contractors into contractual agreements. For example:
    a. Use of company-owned devices versus bring your own device (preferred)
    b. Limitations on "last mile" connectivity: not by hot spot or cellular phone
    c. Always on secure VPN connection
    d. Password protection and multi-factor authentication
    e. Full-disk encryption
    f. Installation of Data Loss Prevention agents
    g. Disabling of USB and portable devices
    h. Installation and enablement of endpoint agents
    i. Disabling of booting from active devices like CD-ROM
    j. Processes for updates and patches
    k. No local administration rights
    l. Disabling of printing/screen snipping/local storage by group policy
    m. Password/idle timeout requirements
    n. VDI connections
    o. No access to NPPI

    For more information, member companies can access an RMA Third Parties Working from Home white paper: "SARS-COV-2 Principles of Workforce Return to Facilities Addendum"

4. Negotiate requirement for access to third-party controls audits (SOC and/or SSAE reports), including disclosure of tested controls and actions taken to verify controls remain active.

5. Review the third party's Force Majeure clause in the agreement and evaluate your standard Force Majeure clause in templated contracts. Force Majeure did not take pandemics into account so this clause may need to be revisited in case things go wrong after returning to facilities.

PROBLEM STATEMENT #2:

Time to complete due diligence and onboarding for a new third-party relationship is considered excessive and particularly problematic during times of rapid change. Due diligence and onboarding can take up to three months to complete, and may exceed the company's acceptable timeframe to replace a high-risk relationship.

Recommendations:

1. A proven "best practice" for onboarding innovative third parties is to implement a Proof of Concept. A Proof of Concept (PoC) is a form of "research" to explore the design, functionality, technical requirements, and architecture before making a final decision to proceed. A PoC should be a small-scale, time-bound, and tightly controlled event. The primary purpose is to prove that the concept, innovation, process, or technology is viable, and can reasonably be expected to fulfill its intended purpose once implemented.

2. Successful strategies that accelerate onboarding can be applied to any third-party relationship.

For more information, Linda Tuck Chapman's RMA-published book titled "*Third Party Risk Management: Driving Enterprise Value*," Second Edition (chapter on innovation risk), will be available to members at a discounted price from the RMA website and on Amazon.

"The primary purpose is to prove that the concept, innovation, process, or technology is viable, and can reasonably be expected to fulfill its intended purpose once implemented.

PROBLEM STATEMENT #3:

Risk and trend analysis and risk reporting may not be delivering actionable risk insight to business owners, senior management, and the board. Controls assessments and most risk information is point-in-time data, making the current and future state of exposure to third-party risk difficult to interpret and trend. Site visits to validate the control environment may not be possible.

There are few or no predictive KRIs and risk insight data sources (e.g., model validation, SOC reports), except for cyber incident and financial health subscription services. Some third-party services offer directional indicators and forward-looking predictors for the likelihood of credit default, which may result in business failure.

Risk monitoring indicates that the full impact of COVID-19 on third-party risks and relationships is unknown, causing risk experts to struggle with providing actionable risk insight and recommendations for relationships amongst owners in the 1st Line of Defense, senior management, and the board. Board reporting must be consumable, challenging risk experts in their efforts to simplify complexity.

Recommendations:

1. Recognize that there are no "silver bullets" that predict future financial health. Credit departments are a good source of sector analysis. The top two third-party providers – Dun & Bradstreet and Rapid Ratings – generate risk insight using different data sources. For example, one third party relies on payment history by firm and sector, and other data points in their risk scores (e.g., fringe financials). Another analyzes financial statements to derive a financial health score and core health score. The best course of action is to identify reliable data sources, analyze the data, and come to the most reasonable conclusion.

2. Encourage collaboration between peer group CROs to ask regulators to release the result of fintech exams much earlier. Reports are quite dated by the time they are made available.

3. Implement Third-Party Risk Management working groups and oversight committees or increase frequency of meetings. Empower them to deal with incidents and emerging risks and act.

4. Implement an exception and/or expedited approval process for COVID-19-related essential third-party relationships (e.g., PPE).

5. Build expedited pathing and processes that improve awareness, quickly escalate emerging risks, and enable coordinated response to risk events by geography and overall. The recommended approach is one of matrix management, based on severity, impact, and reach of the event.

6. Ensure any changes (temporary or permanent) to risk management policies and practices are approved by the CRO or Operational Risk Management (e.g., approval to defer security site visits).

7. Reinforce the principle that the 1st Line of Defense owns the risk. Consider hosting monthly risk forums within lines of business. This allows risk experts to present relevant data and targeted communication.

The best course of action is to identify reliable data sources, analyze the data, and come to the most reasonable conclusion.

COVID-19'S IMPACT ON BUSINESS RESILIENCE STRATEGIES

PROBLEM STATEMENT #1:

Risk insight into third-party business resilience capabilities is inadequate. Understandably, third parties provide only high-level summaries of Business Continuity Management (BCM) plans and results of Disaster Recovery testing. The process of evaluating controls and practices based on watered-down business resilience documents creates a blind spot in their clients' business reliance plans and gaps in documented evidence.

Internal exit strategies/contingency plans are often weak or impractical. Practices are ripe for change.

Recommendations:

1. Relationship Owners
   - Identify a designated relationship manager to oversee the relationship and be accountable for managing the risks and protecting the financial institution from time of contract engagement through the lifecycle of the relationship.
   - Validate the criticality and RTO for products and services. COVID-19 spotlighted those truly business critical services and those that are not. Business owners may not have an enterprise view of what constitutes a critical relationship.
   - For outsourced technology products and services, ensure the relationship manager has been trained and knows the required system availability, Recovery Time Objective (RTO), and performance metrics by which the service is internally measured.
   - Review and update criticality/materiality risk assessment, Business Impact Analysis, and technology risk assessments on a risk-adjusted basis.
   - Validate contingency plans and transition strategies for critical third parties with poor performance or financial health.

> Recovery Time Objective (RTO), and performance metrics by which the service is internally measured.

2. Risk Specialists and Other Expert Resources
   - Collaborate internally with BCM to define requirements and encourage BCM function to expand practices to be more hands-on.
   - Consider outsourcing third-party BCM plan assessments, conducted according to your firm's framework and standards.
3. Third-Party Inventory and Key Attributes
   - Each third-party relationship should be identified so that reports can be produced for lines of businesses reflecting their portfolio of third-party relationships, points of contact, and risk attributes.
   - Product and service descriptions should be aligned to the provider along with the technologies utilized and data hosting types.
   - A detailed inventory should also contain the outsourced technology primary and backup data centers so that event-impacted regions can easily be matched to third-party products and services utilized by a line of business. There should be an easily accessible record of the third party's and your institution's Single Point of Contact (SPOC).
   - The application database should capture information about reliance on third parties.
   - Third parties should be mapped back to your firm's goods and services, across business lines.

4. Due Diligence and Ongoing Risk Monitoring

   – COVID-19 revealed that current practices do not provide sufficient insight into third-party resilience capabilities. Collaborate with BCM specialists to conduct intentional conversations the third party's risk specialists often provide with sufficient risk insight. This places responsibility on the "buyer" to fill in the assessment questionnaire that would be completed by the third party as a self-assessment. Take a risk-based approach to match work effort with benefits.

   – Collaborate with peer institutions to encourage regulators to conduct BCM and DR testing with third parties that present high concentration risk.

   – Educate the 1st Line of Defense about the implications of third-party BCP capabilities, and "the possibilities" for what can be negotiated and the relative cost.

   – The third party's contribution to the business owner's BCP plan and BIA is often overlooked, and what is negotiated and contracted for may inhibit the 1st Line of Defense from meeting their RTO.

   – Define timing, processes, and accountability to contract for and test DR plans, on a risk-adjusted basis.

   – Seek the risk domain owner and ERM's approval for changes and alternatives to standard practices.

5. Third-Party Controls Verification

   – Validate that the third party's business resilience objectives were met as required by the 1st Line of Defense, the business owner. Determine the most appropriate risk treatment if business resilience needs were not met.

   – If the third party's internal controls changed because of COVID-19, determine whether the revised third-party controls are "permanent" and if they have an impact on the residual risk rating. Update risk ratings and risk treatment as necessary and determine whether to expect changes to their pandemic response plan.

   – RMA White Paper: SAR-COV-2 Principles of Workforce Return to Facilities

6. Revisit Risk Analysis Practices

   – Review definitions for critical and high-risk third-party relationships and tighten where necessary. It may also be necessary to re-evaluate certain relationships.

   – Re-evaluate the frequency of risk assessments and monitoring activities and amend where appropriate (e.g., cyber, backup sites, etc.) on a risk-adjusted basis

   – Re-evaluate standard limits for limits on liability and insurance coverages for third parties for business interruption.

Update risk ratings and risk treatment as necessary and determine whether to expect changes to their pandemic response plan.

7. Standardize and, if necessary, update contractual terms
   - BCM and DR, on risk-adjusted basis.
   - Recovery time objective, recovery point objective, participation in resolution and recovery testing, and your firm's position on the third party's recovery list in comparison with their other clients.

8. Technology risk
   - Identify and assess risks arising from changes in the third party's networks and systems that are not expected to return to a pre-COVID-19 state.
   - Identify and prepare a plan to address control failures that did not match SOC report- tested controls.
   - Explore whether third parties have implemented cost control measures that will affect their technology risk profile (e.g., move to tier two cloud provider, increase the number of critical fourth-party relationships, etc.)

9. Risk acceptance should indicate when the firm is unable to negotiate standard terms and conditions, and when this occurs, determine whether the third party's controls and the contract are effective, need improvement, etc. Challenge and escalate as required.

10. Risk Monitoring
    - Strengthen monitoring practices: SLAs, negative news, compliance to contractual terms, and any monitoring that assists with predictive knowledge of emerging risks.
    - Actively manage, document, and oversee early warning indicators and remediation activities.
    - Anticipate future disruption scenarios through joint planning and testing with key stakeholders and critical providers.
    - Update contingency plans and exit strategies.
    - Schedule regular updates with critical third parties during and post serious interruption or risk event.
    - Extend monitoring to fourth parties, et. al., if they are material to your operations.

Reference materials:

- FCA: https://www.fca.org.uk/firms/information-firms-coronavirus-covid-19-response
- OCC Bulletin 2020-10: https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html
- Department of Justice: https://www.justice.gov/criminal-fraud/page/file/937501/download
- Interagency COVID-19 Examiner Guidance: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200623a1.pdf
- FIL-64-2020: https://www.fdic.gov/news/financial-institution-letters/2020/fil20064.html
- Interagency Statement on Pandemic Planning: https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf
- RMA Third Parties Working from Home white paper: "SARS-COV-2 Principles of Workforce Return to Facilities Addendum"

HARMONIZING PRACTICES GLOBALLY

PROBLEM STATEMENT #1:

As government trade and foreign national policies changed rapidly and as COVID-19 spread around the world, how did this impact global supply chains? How can we build resiliency to global shocks? There is evidence of rising protectionism whereby countries are making work visas more difficult to obtain and/or are imposing tariffs, sanctions, and new employment laws.

Over the past few decades, service delivery and supply chains have become increasingly globalized and multi-tiered. Globalization presents unique risks when foreign national policies change as quickly as they have during the COVID-19 pandemic, complicated by significant reliance on critical third, fourth and nth parties in multiple countries.

Recommendations:

1. Analyze the interconnectedness of your supply chains globally across your first few tiers (third, 4th, nth parties). Geo-map dependencies on third parties to your services, understand geographic concentrations (e.g., service delivery locations, internal functions delivering services to a region(s) or group of business units).

2. Document your critical/material services on-shore, near-shore versus off-shore to understand vulnerabilities; measure these rates by region.

3. Perform internal scenario analysis on your most critical and/or higher concentration risk third parties, including what-if scenarios for critical off-shore suppliers. Evaluate the potential risk of a third party operating under crisis/stress for a prolonged period, can they sustain operations?

4. Perform joint testing with most critical third parties; define a black swan type event(s) to test. Cover both regional and global events.

5. Review the viability of previously identified alternative on-shore service providers that can be quickly enabled in the event of unexpected impacts to select geographies. Develop contingent repatriation strategies for critical operations performed off-shore.

6. Capture and identify where services are delivered from, across all locations/jurisdictions, not only head offices. Has the location changed during the pandemic?

7. Better understand critical third party's pandemic-preparedness during due diligence. Lack of infrastructure in some countries led to the inability to move to work-from-home in short order (lack of laptops, no internet in remote communities, e.g., rural India) (See work-from-home white paper.)

8. Develop new techniques to monitor third parties, particularly off-shore, who newly introduced work-from-home arrangements with a focus on information security and privacy. Heightened risk with third parties working from home on a BYOD basis.

9. Increase frequency and immediacy of country/region risk ratings as the pandemic evolves. E.g., move from quarterly to monthly. For higher concentration risk locations and/or critical services, monitor infection prevalence rates by region to assess potential workforce impacts.

10. Consider leveraging third-party contingent labor to supplement internal and third-party workforce shortfalls where the highest infection rates occurred across your geographic footprint. For example, moving services to another location or country for continuity of service, as part of contingency planning. Note: Contracts would need to allow this under extenuating circumstances, and should consider the impact on Force Majeure clauses.

Develop new techniques to monitor third parties, particularly off-shore, who newly introduced work-from-home arrangements with a focus on information security and privacy.

CONTINGENCY/EXIT PLANS

PROBLEM STATEMENT #1:

Many contingency/exit plans are “check box” exercises, and the 1st Line of Defense is facing increased pressure to improve them. As a result of COVID-19, companies need to assess contingency plans beyond initial creation or annual review, targeting third parties that support critical functions, product delivery, financial reporting, and cybersecurity.

The role of the 1st Line of Defense is even extremely important if companies plan to proactively address service delivery and/or performance concerns through increased monitoring and targeted communications with suppliers and other third parties. Ongoing management and monitoring may require new strategies and practices to increase their effectiveness. One area of immediate concern is third-party financial viability.

Recommendations:

1. Evaluate third-party pandemic planning, preparation, and impacts. Ensure required information protection and security control environments are in place, particularly for work-from-home arrangements.

2. Implement additional information-gathering and 1st Line of Defense ongoing management routines for higher-risk relationships to ensure appropriate oversight, awareness of thresholds of product/service delivery/continuity concerns.

3. Implement enhanced financial monitoring routines, especially during the next 18 months (through mid-2022) for all vendors. Employ other data-driven tools to predict future pandemics, civil unrest, geopolitical activity, and climate change concerns.

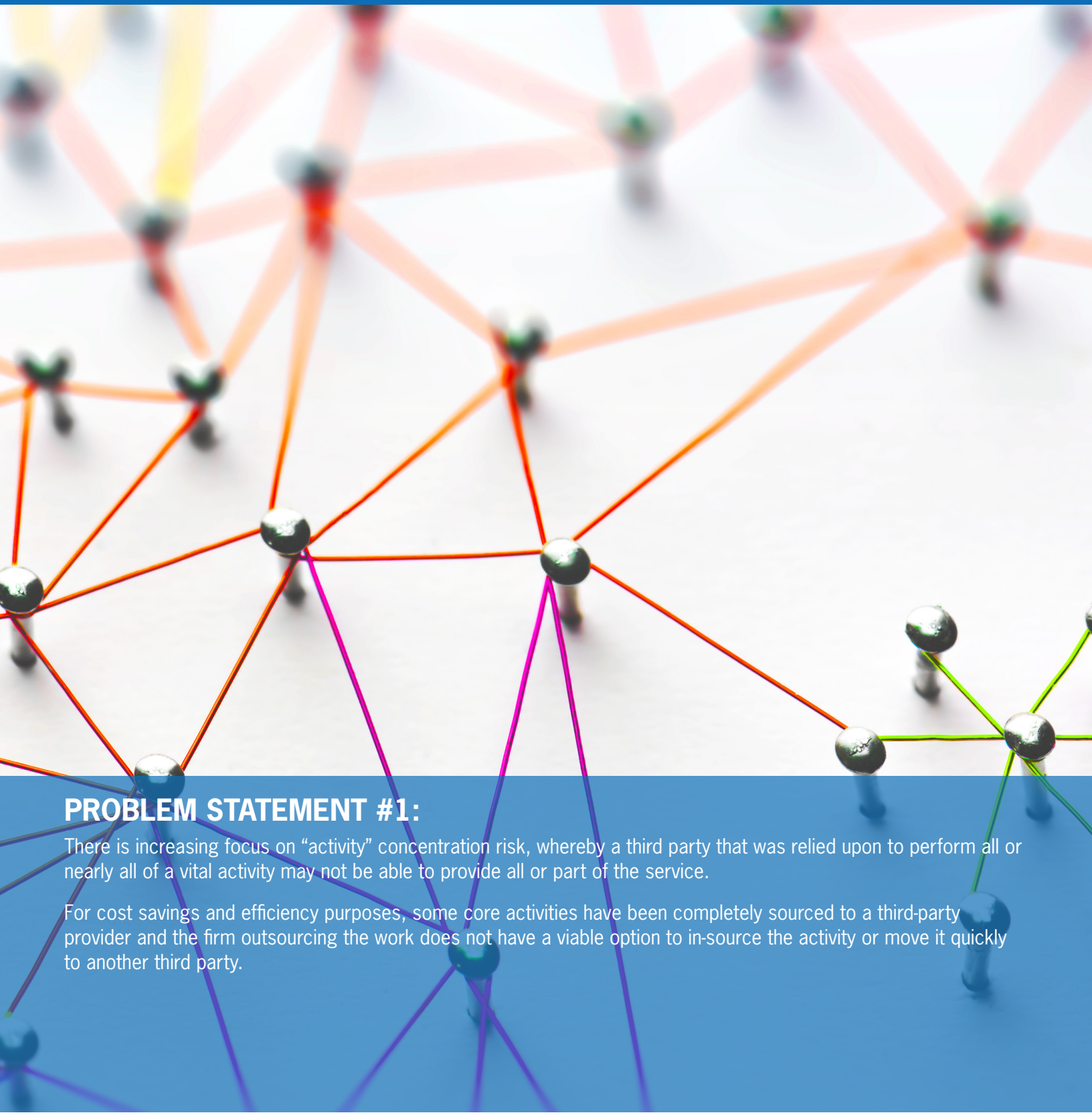
4. Review the viability of previously identified alternative service providers. Adjust contingency plan and exit strategies routines, applying risk-based approach to frequency and planning efforts.

Reference materials:

- https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200623a1.pdf

Employ other data-driven tools to predict future pandemics, civil unrest, geopolitical activity, and climate change concerns.

ACTIVITY CONCENTRATION RISK



PROBLEM STATEMENT #1:

There is increasing focus on “activity” concentration risk, whereby a third party that was relied upon to perform all or nearly all of a vital activity may not be able to provide all or part of the service.

For cost savings and efficiency purposes, some core activities have been completely sourced to a third-party provider and the firm outsourcing the work does not have a viable option to in-source the activity or move it quickly to another third party.

Recommendations:

1. Define concentration risk [KRI] for country, regional, location, single point of failure and/or credit risk. Consider geo-mapping third parties.
   - Where high concentration risk is evident, increase awareness among risk governance specialists.
   - Document risk acceptance or identify options to reduce concentration risk, exit relationships, respond to a serious event, and/or develop appropriate risk treatment and mitigation strategies.
   - Update the third-party risk management policy to define "activity" concentration risk, criteria for escalating to senior management.
   - Reassess strategic sourcing and strategic partner management approaches to identify unnecessary drivers of concentration risk.
   - Ensure management understands the trade-off between risk and efficiencies/volume discounts.

2. Assess activity concentration risk during due diligence and on-boarding process such that LOB executives and risk committees understand the risk and a conscious decision is made to move forward. If activity concentration risk is triggered, consider:
   - Limiting additional services awarded to the third party to non-essential services or commodity activities.
   - Splitting the services between two or more third parties.
   - Maintaining a percentage of the service in-house to reduce the reliance on the third party.
   - Providing in-house FTEs training, documentation, systems access, etc. so that they can transition from their current role to the outsourced role should need be.
   - Prioritizing the activities the third party does so that lower "value" tasks are the first ones dropped if resources aren't available.
   - Developing risk-appropriate exit strategy/transition plans.
   - Enhancing the monitoring and assessment of the third party's business resiliency plans and test results including their ability to provide the activity from multiple locations, hire and train quickly, etc.

3. Review the existing portfolio periodically to identify engagements that meet activity concentration risk triggers.
   - Include activity concentration risk engagements in ERMC, TPMC. and management reporting.

Assess activity concentration risk during due diligence and on-boarding process such that LOB executives and risk committees understand the risk and a conscious decision is made to move forward.

GEOGRAPHIC CONCENTRATION RISK

PROBLEM STATEMENT #1:

Some geographic regions were severely impacted resulting in significant disruption in service delivery. The pandemic was more severe in some regions, and governments took various actions including the total lockdown of a region or country. Typical geographic concentration risk controls such as ensuring that an alternate/backup facility is a certain distance from the primary servicing location may not be effective if it is within the same region.

Recommendations:

1. Ensure the third-party inventory includes accessible information about primary and alternate locations for all activities.

2. Assess the impact if a region is not able to deliver services.

3. Develop a sourcing strategy/contingency plan for the regions; consider:
    a. Implementing a multi-region/supplier sourcing strategy.
    b. Requiring existing suppliers to provide services from a different facility.
    c. Sourcing to providers who have operations in other regions.
    d. Maintaining an in-house staff that can handle the most important activities.

4. Appoint one individual responsible for understanding and keeping abreast of the region with concentration risk.

5. Include geographic concentration risk as part of the due diligence and on-boarding process such that LOB executives and risk committees understand the risk and a conscious decision is made to move forward.

6. Review the existing portfolio periodically to identify engagements that meet geographic concentration risk triggers.

Please consider keeping this document on hand as a quick reference for proven recommendations to prevent, detect, and respond to pandemic-related third-party issues and incidents. For comments or more information, contact RMA or Linda Tuck Chapman at lindatc@thirdpartyriskinstitute.com

JOIN. ENGAGE. LEAD.

About RMA

The Risk Management Association (RMA) has been at the forefront of the development of the operational risk discipline in financial institutions since 2003.

The definition of operational risk is: *the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events, but is better viewed as the risk arising from the execution of an institution's business functions.* Operational risk exists in every organization, regardless of size or complexity, from the largest institutions to regional and community banks.

For much of the past decade, the industry has been focused on measuring operational risk losses for capital allocation purposes, but in recent years has increased the focus on the process of managing operational risk.

RMA serves operational risk practitioners in large financial institutions, as well as regional, mid-tier, and community banks, at both the corporate level and the business line. RMA provides peer sharing, professional development and networking opportunities for our members through discussion groups, conferences, round tables, forums, courses, webinars, publications, and podcasts.

RMA also conducts surveys, benchmarking studies, and range-of-practice papers. In addition, RMA's Advanced Operational Risk Group shares industry views on aspects of AMA implementation with the U.S. financial services regulatory agencies toward a goal of successful AMA implementation. *The RMA Journal®* also regularly carries articles on operational risk topics.

RMA's operational risk activities are driven by the Operational Risk Council, whose mission is to promote sound practices in the management of operational risk in financial service institutions worldwide. It promotes understanding of the causes, events, and effects of operational risk through dissemination of management methods, sound practice tools, and materials. The Operational Risk Council is focused on the needs, challenges, and opportunities of all member institutions, including community, mid-tier, regional, and large banks, as well as non-bank financial institutions.

Major issue(s)/risk(s) within the market are listed below. COVID-19 has amplified all them:

- Technology
- Cybersecurity
- Information Security
- Third-Party Risk
- Fraud
- Succession/Talent challenges
- Challenge of returning to work
- Challenge of the possibility of second major outbreak
- Reputational risk in the event of second major outbreak

To learn more about RMA or our operational risk thought leadership pieces, contact Sylwia Czajkowska at sczajkowska@rmahq.org.