THE RISK MANAGEMENT ASSOCIATION

SARS-COV-2

Principles of Workforce Return to Facilities Addendum

SEPTEMBER 2020

ADDENDUM

SARS-COV-2 Recommendations for Third Parties Working from Home & Returning to Facilities

Each firm in the financial services sector operates a complex extended enterprise, with extensive reliance on third-party relationships, which bring many benefits and exposure to a wide variety of risks. Scenario analysis and targeted actions are the best way to anticipate and respond to risks and risk events, such as what we're experiencing while in the throes of a global pandemic.

This document is the work of senior level third-party risk management practitioners and subject matter experts, all members of RMA's Third- Party Risk Management Roundtable:

- Denise Brzakala, Director, Third Party Standards and Advisory, RBC Bank of Canada
- Lisa Hershey, Managing Director, Operational Risk Management, DTCC
- Mike Rivas, Executive Director, Head of Third-Party Risk Management, DTCC
- John Soebbing, Managing Director and Chief Procurement Officer, TD Ameritrade
- Linda Tuck Chapman, President, Ontala Performance Solutions Ltd.
- Lori Walsh, Director, Third-Party Risk/Operational Risk, Guardian Life

We will present four scenarios, targeted considerations, and specific recommendations, plus summary-level observations and recommendations that are influencing changes to risk management practices right now.

- Scenario #1: Third-Party Employees Are Working from Home (WFH)
- Scenario #2: Third Parties Are Transitioning from WFH to Return to Facilities
- Scenario #3: Third-Party Employees Return to Facilities
- Scenario #4: Third-Party Employees Revert to Work from Home

Scenario #1: Third-Party Employees Are Working from Home (WFH)

In most third parties, some or all employees are working from home. Many third parties are now requesting an extension to approved WFH arrangements, in some cases indefinitely.

Consider this:
Approvals for third-party employees to Work from Home (WFH) were intended for a limited time frame, conditional on the business segment and your firm's willingness to accept higher levels of risk for a limited period.

Recommendations

- Collaborate with legal, privacy, compliance, procurement, business relationship owners, and IT managers to ensure third parties are taking steps to secure sensitive company data and protect against cyber and business resilience risks. Determine whether additional contractual, security, and operational controls and oversight should be put in place. Determine whether an amendment to the contract is needed. Understand potential sources of legal liability – yours and your third parties' – to determine the impact on activities and communications.
- Create a formal process to track notification to a third party that WFH authorization has been extended or revoked. If WFH authorization is extended or granted permanently, recertify third-party controls, and negotiate contractual terms as required.
- Periodically remind business units to review third-party pandemic response processes that were implemented, and to extend or revoke them in a timely manner.
- Business segments should monitor third-party management of risks and controls, execution of controls against contractual terms, and test compliance. Pre-scheduling review meetings enables an appropriate cadence. Determine how the third party provides assurance and/or verifies that their remote workforce complies with policies for:
  - Security and remote access
  - Storage location of electronic data; and data retention and destruction guidelines
  - Use of personally owned devices (laptops, smartphones, tablets)
  - Access to networks, systems, and data
- Business relationship owners should validate and prioritize monitoring activities for third parties with the highest criticality and/or risk exposure. Evaluate the contingency (exit) plan for feasibility or develop a new plan.

Consider this:
Standard terms and conditions, existing agreements, and amendments don't adequately address controls necessary for third-party employees working from home.

Recommendations

- Where existing contracts and controls are inadequate, develop standards and negotiate amendments to strengthen controls and address gap areas. This may include:
  - WFH-specific approval period, expiry date, and any special conditions
  - Minimum security controls
  - Periodic controls testing and reporting
  - Activities and risk events and notification protocols
  - Breach reporting requirements
  - Retention and destruction of data and records
  - Evidence of periodic internal controls testing
  - SLAs and performance expectations
- Implement a compliance attestation process to ensure third-party WFH employees are aware of the required controls. Here are some examples of controls that may be in scope:
  - Designate an appropriate work area in their home for performing services that adequately considers confidentiality and interruption factors, and minimizes the risk of others hearing or seeing sensitive information
  - Use only company approved apps or websites to get work done
  - If authorized to use a virtual desktop (e.g., Citrix) from a personal computer or device, ensure local PC antivirus is active and automated Windows updates are enabled (if applicable). For mobile devices, ensure device software is continuously updated to the most current version
  - If approved for use, personal phones should be protected to the same standard as company owned equipment
  - Use an approved means of connecting to the internet and the network
  - Use headphones and privacy screens on monitors, and guard against sensitive data being viewed by others when around others
  - NEVER take a photo of screens
  - Printing is prohibited
  - Private and confidential data must not be written down
  - NEVER share passwords with anyone
  - Lock workstations when left temporarily unattended and securely store laptop when not in use
  - Be mindful of scams/phishing that try to take advantage of the current situation, including tech support scams.

Scenario #2: Third Parties Are Transitioning from WFH to Return to Facilities

As third parties prepare to return some or all employees to facilities, it's important to understand the risks and risk mitigation strategies that will safely allow transition to occur.

Consider This…
As third parties transition employees back to facilities, visibility provides assurance of an orderly transition, uninterrupted service delivery, and resumption of contractually bound standards for productivity and performance.

Recommendations

- Identify which of the following scenarios applies to each third party authorized to WFH and determine which functions or executives are engaged in decisions and authorizations. (e.g. legal, privacy, IT, cyber risk, etc.):
  - Third party notifies you that they no longer require WFH authorization, and affected employees are returning to facilities
  - Circumstances cause your firm to revoke the WFH authorization (e.g., breach, government restrictions have been lifted)
  - Third party requests to extend WFH authorization or has not notified they will return to facilities according to the authorized term
  - Third party requests approval for permanent WFH for some or all in-scope employees
- Ensure your firm receives sufficient notice and approves proposed operating model (return to facilities, extension, hybrid).
- Take a risk-based approach to determining which third parties/vendors, and potentially phasing, are permitted to enter your facilities (e.g., case by case or an "as-needed" basis). A list of approved vendors provides clarity to all stakeholders, and the conditions of entry should be specified and communicated internally and externally.
- Define the conditions of entry to facilities, yours or the third party's, which may include:
  - Type of visits (e.g., short term for maintenance vs. long-term, project-based work)
  - Policy for limiting visitors based on number of "hops" or travel from a high-risk location. A "hop" means how many modes of transportation are required to reach the facilities by public transit including bus, subway, path, ferry, train, air
  - Attestation about potential exposure to COVID-19 (including onsite at other firms) and wellness
- Create a templated process that gives your firm visibility over third-party plans that provides assurance of orderly transition:
  - Timing, dates
  - Number of employees in each phase
  - Functions or activities they support, including key information such as access to sensitive data
  - Description of new safety measures (e.g., social distancing, PPE, food services, common areas, etc.
  - Employee training and awareness
  - Compliance management
- Establish processes to terminate any special access controls and manage return of any hardware and peripherals on loan from your firm.
- Assign seating or seating areas for approved visitors and third-party employees returning to facilities.
- Formally revoke WFH approval by contract amendment or termination letter.
- Track and monitor phases of "return to facilities." A risk-based approach may inform sequencing (e.g., employees with highest level of access return first).

Consider This…
Ongoing communication with contractors and third-party contingent workers should be included in your firm's return to facilities plan.

Recommendations

- Identify which of the following scenarios applies to contractors and contingent workers authorized to WFH and determine which functions or executives are engaged in decisions and authorizations. (e.g., HR, legal, etc.):
  - Directly contracted with your firm
  - A third party's contractor or contingent worker
  - A contractor, contingent worker, or contingent worker provider contracted to your firm via a Master Services Provider
- Ensure contractors and third parties receive timely information about your firm's plans, timing, phases, and special controls when contractors and contingent workers return to facilities, including processes/protocols they must follow.
- Ensure communication plans include contractors and contingent workers (e.g., health checks, new desk locations, safety protocols, access controls).
- Determine if and whether contractors and contingent workers will receive additional compensation for returning to facilities.
- Internal communication processes must include bilateral contractor and third-party notifications if one of more workers may have been exposed to COVID-19 on premises or outside of facilities, and when a previously infected person returns to facilities. Notifications should provide information about how infected workers' return to work will be communicated and managed.
- Engage HR and employment legal team to ensure the firm does not inadvertently enable co-employment and/or avoidable liability for your firm and the third party as a result of exchange of information or exposure to COVID-19 in your facilities.

Consider This…
Your firm may have quickly contracted with PPE suppliers without conducting a standard risk assessment.

Recommendations

- Take a risk- based approach when onboarding:
  - AML and sanctions screening for directors and offices; negative news screening; and financial viability check
- Record PPE suppliers in your third-party inventory.

Consider This…
Third parties may require periodic or ongoing access to your facilities to repair photocopiers, water plants, and clean premises, etc.

Recommendations

- Revoke badge access permissions for third-party employees. This discourages third-party employees, including those not authorized, from unnecessarily entering premises.
- Maintain a list of all authorized personnel.
- Appoint a Floor Ambassador(s) to track where third-party personnel went, communicate safety measures, etc.
- Record who enters, date/time, purpose, destination, contact information.
- Request third-party personnel sign Attestation that they don't have and have not been exposed to COVID-19, and agree to comply with safety protocols.
- Install signage detailing health and safety.
- Remember to include vendors that provide coffee, tea, and food services. Communicate your plans and keep them informed about special protocols such as closing down common areas and suspending these services, and keeping them informed about when to expect them to resume.

Consider This…
Building management company and/or third-party security protocols may differ from your firm, and/or vary across your footprint (e.g., elevator protocols, PPE, common space).

Recommendations
• Ensure there is an accountable function or person assigned to communicate with building management companies and/or third-party security personnel. • Document special requirements; reconcile differences. • Work with building management to reconfigure spaces and floors as required.

Consider This…
Your firm may be implementing or "encouraging" use of a social distancing third-party application to facilitate communication with employees and others who may have contracted or been exposed to COVID-19.

Recommendations
• Ensure the third-party risk and controls assessment is completed on third-party applications, as confidential and sensitive data will be captured.

Scenario #3: Third-Party Employees Return to Facilities

When third parties have returned to facilities, it is important to understand the risks and mitigating factors that should be in place.

Consider this:
As third-party employees return to facilities, whether in your facilities or theirs, these considerations and recommendations can be implemented internally and help your third parties manage their processes and protocols.

Recommendations
• Ensure technology, networks, and systems are performing as expected. • Review the third party's force majeure clause in the agreement or evaluate your standard force majeure clause in templated contracts. Force majeure didn't take pandemics into account, so this clause may need to be revisited in case things go wrong after return to facilities. • Verify that third-party employees have completed Safety Awareness Requirements training and signed an Attestation. • Maintain records where each employee visits (area, floor, timing). • Confirm that the third party has agreed to your COVID-specific requirements (e.g., has a pandemic plan response in place). • Develop a policy and procedures to deal with refusal to comply and/or violations of conditions of entry and safety requirements. • Create a Waiver of Consent to limit liability and track signoff. • Create Consent for Use of Contact Tracking apps for third-party employees returning to facilities, as required.

Consider this:
Technology is available that reduces the workload associated with managing information regarding return to facilities.

Recommendations
• Assess potential to implement Log/Tracking, Contact Tracking apps, areas visited, etc. • Implement an electronic Visitor Log.

Consider this:
Return to Facilities should include minimum safety protocols.

Recommendations
• Temperature check at the door • Face masks and gloves, available at the point of entry, must be worn • Limit personal items allowed in and out of the building (bags, jacket, food, etc.) • Travel in facilities is limited to required areas • Some or all visitors are escorted throughout the visit • Provide guidance for leaving and reentering facilities • Safety signs, reinforcing the above posted throughout building • Escalation procedures for incidents and violations of procedures and safety protocols • Follow-up/survey with visitors for disclosure if exposure is determined • Communications procedures if a potential COVID-19 exposure has occurred **Cross References:** • SARS-COV-2 – Principles of Workforce Return to Facilities: Phase 2, Principle 5 • SARS-COV-2– Principles of Workforce Return to Facilities: Phase 3, Principle 4

Scenario #4: Third-Party Employees Revert to Work from Home

Reverting to Work from Home (WFH) may occur for a variety of reasons, including government requirements to return to "Shelter in Place" due to a localized outbreak or second wave.

Consider this:
Third parties that have Returned to Facilities are unexpectedly reverting to WFH, which may include Contingent Workers onsite in your facilities and/or third-party facilities.

Recommendations

- Define specific triggers for reverting from Return to Facilities to WFH. You may choose to rely on local governments for guidance. For example:
  - New cases/day or percentage of new cases/day
  - National, state, or local government requirements
  - Other
- Request details of the redeployment to WFH plan, including details of timing, % of employees reverting to WFH, activities they support, etc.
- Require notification of any deviations from an approved plan.
- Contractual Requirements:
  - Amend existing agreement (i.e. amendment) that enabled initial term or execute wholly new amendment with new term for WFH and, as appropriate, any modified or new requirements for WFM
  - Your firm may choose to negotiate a more conservative approach to Return to Facilities and/or WFH than recommended or required by government
- Equipment:
  - Redeploy your firm's equipment with appropriate load set including security applications for third-party employees, aligned to company requirements, or
  - If the third party is redeploying their own equipment, get assurance that it meets your firm's control standards
- Access:
  - Re-establish connectivity for third-party employees, aligned to company requirements
- Refresh security training and compliance Attestation processes.
- Monitoring:
  - Re-establish any specific monitoring and compensating controls for third-party employees aligned to company requirements (i.e. systems, financials, reporting, follow up, etc.)

In Summary

There have been many "lessons learned" and there are more to come. Effective third-party risk management is more important than ever, and changes to current practices are inevitable. Here are some considerations you may wish to act on now or in the near term.

Consider This…
Records and documentary evidence, subject to audit and regulatory exams, may not reflect the current state and actions your firm has taken.

Recommendations

- Evaluate third-party responses to the pandemic in the context of residual risk. Update as required.
- Review third-party controls audits (SOC and/or SSAE reports), noting tested controls and actions taken to verify controls remain active
- Record action items such as expiry dates for WFH approvals, new compensating controls, assessing heightened residual risk, etc.
- Update third-party records as required, including exception approvals, rationale, special Risk Acceptances, and what action was taken where control deficiencies were identified.
- Ensure pandemic-related information, survey data, and reporting are easily accessible.

Consider This…
Contract templates may need to be updated to incorporate "lessons learned" from the pandemic.

Recommendations

- Standardize the scope of acceptable force majeure events to limit future enactment to what is considered reasonable (third parties may be attempting to increase the scope). Pandemics should be addressed in BCM/Pandemic Plans, not in force majeure clauses.
- Revisit HR security requirements (e.g., education verification, references, and criminal background checks).
- Review clauses for business continuity controls (e.g., annual certification, participate in testing, etc.)
- Review notification clauses when DR and/or Pandemic Plans have been invoked (e.g., information requirements regarding availability of resources; immediate future state productivity expectations; name and contact information for single point of contact; frequency of updates; end-customer complaints).
- Review clauses for plans to outsource a critical activity to a fourth party, pre-approval prior to execution annual verification of critical fourth parties, description of services, service delivery location, data and connectivity access, etc.

Consider This…
Policies and contracts don't address third-party employees WFH, or adequately address security and controls.

Recommendations

- Negotiate specific controls into contracts for third-party WFH employees. This may include:
  - Prior notification and pre-approval for employees or groups of employees to move to WFH
  - Time-bound approval period for "temporary" WFH authorization due to a risk event
- Design and negotiate specific security controls for WFH third-party employees and contractors into contractual agreements. Controls may include some or all of the following:
  - Use of company owned devices versus BYOD (preferred)
  - Limitations on "last mile" connectivity: not by hot spot or cellular phone
  - Always on, secure VPN connection
  - Password protection and multi-factor authentication
  - Full disk encryption
  - Installation of DLP agents
  - Disabling of USB and portable devices
  - Installation and enablement of endpoint and av agents
  - Disabling of booting from active devices like CD-ROM
  - Processes for updates and patches
  - No local admin rights
  - Disabling of printing/screen snipping/local storage by group policy
  - Password/idle timeout requirements
  - VDI connections
  - No access to NPPI
- Require WFH employees to Attest to a Code of Conduct, and follow Privacy and Clean Desk policies that are acceptable to your firm – or have them sign yours. Periodically repeat, according to the risk profile of the activity/relationship.

Consider This…
It may be required to refresh or redefine third-party relationship management requirements.

.

Recommendations

- Specify minimum relationship management requirements, risk-adjusted according to criticality and exposure (e.g., communication with the third party, performance monitoring, change management controls, negative news monitoring, strategic or senior management changes, financial health).
- Appoint a dedicated relationship manager for critical third parties.
- Periodic verification of deployed products and services.
- Semi-annual verification: relationship owner; contact information for the third party's "single point of contact."

Consider This…
Risk monitoring requirements would also benefit from re-evaluation/updating.

.

Recommendations

- Subscribing to risk monitoring services for critical relationships (e.g., financial health check; cybersecurity risk monitoring, negative news screening).
- Adjust focus and frequency of risk monitoring to tightly align with residual risks, by risk domain/type.
- Require periodic verification of critical fourth party relationships; record in third-party record.

Consider This…
Tiering and Residual Risk ratings may not identify critical points of failure in rapidly changing environments.

Recommendations
• Adjust and strengthen RCSAs and their linkage with third parties, reliance, criticality, risk exposure, and impact on revenue and operations.The UK's Financial Conduct Authority (1) published the following (draft) guidance for business resilience, which may apply to your firm or simply be seen as helpful advice: - Identify the important business services that, if disrupted, could cause harm to consumers or market integrity. - Identify and document the people, processes, technology, facilities, and information that support a firm's important business services (mapping). - Set impact tolerances for each important business service (i.e. thresholds for maximum tolerable disruption). - Test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios. - Conduct lessons learned exercises to identify, prioritize, and invest in their ability to respond and recover from disruptions as effectively as possible.[23] - Develop internal and external communications plans for when important business services are disrupted.

Consider This…
Business segments are in the best position to estimate the impact of a failure for third parties to meet contractual SLAs.

Recommendations
• Develop a methodology/tool that business segments can use to estimate the impact on revenue and customer satisfaction for missed SLA commitments and productivity targets (e.g., number of customers impacted, revenue, recovery costs, reputation). A higher risk impact for a specific third party may influence their inherent and/or residual risk rating and/or ongoing monitoring requirements. • As part of third-party Return to Facilities oversight, business owners should request a firm commitment or solid estimate of "return to normal" productivity and customer service for those third parties that have not been meeting their commitments. Reserve scarce resources to work on contingency plans with those business segments that have identified untenable results.

Consider This…
Return to Facilities does not necessarily mean a return to business as usual.

Recommendations
• Periodically reevaluate alignment between exposure to risk, risk management, and governance activities. • Selectively scale back or discontinue heightened requirements, where appropriate. Acquire approvals where required.

23 Financial Conduct Authority: Building operational resilience: impact tolerances for important business services CP19/32

Consider This…

Methodologies for segmentation and inherent and residual risk ratings may change as a result of "lessons learned."

Recommendations
• A current best practice is to segment third-party relationships by 1) criticality (reliance) and 2) exposure to inherent or residual risk. A future best practice may be to map third-party relationships to the services they are supporting. Controls and monitoring should then be risk-adjusted for criticality, exposure to risk, and contribution to revenue or essential core services. • Establish a time frame for initiating evaluation of the individual elements of the program. • Be prepared to respond to evolving "lessons learned."

Consider This…

There may be a need to validate Contingency Plans (exit strategies) for some critical third parties. Some have or will go out of business with little or no notice.

Recommendations
• To reduce exposure to concentration risk, firms may reconsider exposure to location risk and strategic consolidation of third parties, forgoing some benefits of higher levels of concentration. • Contingency Plans for critical third parties should be subjected to scenario analysis, then modified accordingly. • Evaluate the feasibility of proposed alternative third parties.

For comments or more information, contact Linda Tuck Chapman @ lindatuckchapman@ontala.com