Move vendor risk management beyond crisis response

Steps to tackle today’s increased risk, stay effective and face tomorrow stronger

Today: Understand and act

- Assess vendor exposure and potential business impacts
- Establish communication channels to stay up to date with critical vendors’ resiliency
- Evaluate current impacts to operations; monitor efforts for remediation and recovery
- Determine new security risks and attack surfaces created by new work models

Tomorrow: Build and improve

- Map your critical vendor network; create a system for documenting and keeping data current
- Review contract terms and service-level agreements; identify areas that need revisions
- Improve due diligence for business continuity plans, disaster response and financial risk
- Evaluate cyber insurance policies and update them as needed

Beyond: Strategize and evolve

- Link your VRM program to the broader enterprise risk and compliance functions
- Focus on vendor crisis management and pandemic preparedness during contracting
- Update vendor replacement planning
- Leverage technology to better manage the VRM life cycle

For details, see “Manage vendor risk during and beyond COVID-19.”