

# Vendor Risk Management Checklist

## Understand your vendor risks

- ☐ List out your vendors
- ☐ Organize vendors into risk tiers
- ☐ Identify the risk types each vendor poses

## Create a vendor management policy

- ☐ Appoint a team comprised of key stakeholders from various internal teams to spearhead the policy creation process
- ☐ State all vendor requirements and expectations, including any regulations they must comply with
- ☐ Assign specific roles and responsibilities to your vendor management team
- ☐ Clearly state the consequences a vendor will face if they fail to follow the policy
- ☐ Detail the vendor lifecycle management process
- ☐ Review your vendor management policy annually and make adjustments as needed

## Perform vendor risk assessments

- ☐ Establish a process to ensure vendors are assessed and held accountable
- ☐ Create a process for what to do if high-risk findings are identified in risk assessments
- ☐ Determine the frequency with which vendor risk assessments will occur
- ☐ Establish a threshold for how much vendor risk the organization is willing to take on

## Set up a process for continuous monitoring

- ☐ Create a process for consistently monitoring your vendor's security posture and identifying potential threats before they impact your business
- ☐ Use an automation tool for ongoing monitoring of vendors

## Improve your vendor risk management program

- ☐ Establish metrics for evaluating your VRM program's effectiveness
- ☐ Create a process for reviewing and improving your program over time

*\*This checklist is intended as guidance only. Always consult with a compliance expert to ensure your organization is fully managing vendor risk.*