CHUBB®

Risk Management Checklist

NATIONAL CENTER FOR
THE MIDDLE MARKET

THE OHIO STATE UNIVERSITY
FISHER COLLEGE OF BUSINESS

Chubb and the National Center for the Middle Market (NCMM) have seen that over the past two years approximately 50% of middle market businesses have experienced some type of business disruption.[1] The research also found that nearly 40% of companies fail to recover from business disruptions and 30% lack a business continuity plan.

Workplace accidents and business disruptions can be costly and devastating to your business. At Chubb, we collaborate with independent agents and brokers to provide you with tailored, industry-specific risk management programs to mitigate the likelihood and severity of loss. For qualifying businesses, this can include on-site risk management support from Chubb. However, regardless of size, all businesses can benefit from focused risk management practices.

Use the following checklist to start the process of evaluating your risk management program.

Operational Risks

Risk that may exist in your business, exposing the business to losses resulting from property damage or bodily injury.

Questions	Yes/No	If no, further action to be taken.
Are the fire detection and suppression adequate for your operation? Have they been inspected/tested by a qualified contractor in the last 12 months?		
Do you have any flammable or combustible liquids in your operation? If so, are they used, dispensed, and stored in a manner to minimize the potential for a fire?		
Is your building's electrical system adequate for the operational load? Has an infrared thermographic scan of your main junction boxes been conducted in the last three years? Are any extension cords being used in place of permanent wiring?		
Do you maintain clear, unobstructed walking and working spaces in your facility?		
Is personal protective equipment appropriate to the hazards in your workplace being utilized by affected employees and guests?		
Does your machinery have appropriate guarding? Does each piece of machinery have a documented lockout/tagout procedure?		
Does your reception area provide a safe and controlled area for guests/customers to be received?		

Human Element Risks

Risks presented by your employees, who represent both your biggest asset and your most unpredictable variable.

Questions	Yes/No	If no, further action to be taken.
Do you have documented hiring policies that include background checks and employment history verification?		
Is there a new hire training program that provides training on corporate policies and safety programs, and documents that the training has been completed?		
Do you have an ergonomic program in place?		
Do you have an emergency evacuation plan that has been reviewed and tested in the last 12 months?		
Is there a program to conduct annual employee training on risk management issues such as safety, corporate policies and procedures, information security, and emergency response?		
Do you have policies and safeguards in place to protect against fraud and embezzlement?		
Does your security system allow you to easily remove access of former employees and contractors?		
Do employees know how to use and maintain personal protective equipment?		

Catastrophe Risks

Hurricanes, tornadoes, wildfires, and other natural disasters.

Questions	Yes/No	If no, further action to be taken.
Do you have a Business Continuity Plan (BCP) and Emergency Response Plan (ERP) in place that have been reviewed in the last 12 months?		
If you are in a hurricane zone: • Do you have a plan for securing all loose outdoor fixtures, equipment, and storage that could be turned into projectiles? • Do you have hurricane shutters or some other means of covering exterior glass? • Does your plan allow enough time for employees to protect their own dwellings and safely evacuate the area, if required?		
If you are in an earthquake zone: • Have you had your building inspected to identify structural weaknesses? • Are all racks, shelving systems, bookcases, and other furniture prone to upset in an earthquake secured to the floor and/or wall? • Do your windows have protective film to prevent them from shattering?		
If you are in an area prone to wildfires: • Have you established a 100-foot defensible space around your building? • Are all plants around the building fire-resistant and well irrigated? • Has combustible exterior storage been minimized?		
If you are in a flood zone: • Do you have a flood mitigation plan (sand bags, flood walls, etc.)? • Are all critical assets maintained at least 1 foot above the Base Flood Elevation (BFE)? • Are controls in place to prevent the release of chemicals/pollutants?		
Has the roof been inspected by a qualified roofing contractor in the last 12 months?		

Cyber Risks

IT systems, cloud computing, ecommerce, connected advanced manufacturing systems, and other technology-related risks.

Questions	Yes/No	If no, further action to be taken.
Do you have a Cyber Security Plan (actions to prevent a breach or disruption)? Additionally, is your plan based on formal, accepted cyber security standards depending on your type of operation (ISO27001, NIST 800-53, HIPAA, PCI-DSS, EU Data Protection Act, etc.)?		
Do you have a Breach Response Plan (planned actions following a breach)? Has this plan been tested?		
Is your critical data and system information backed up off-site (cloud, second location, tape storage, etc.)? Is the backup frequency adequate? Have you tested your ability to recover from the backed-up data?		
Has your cyber security and Breach Response Plan addressed ransomware attacks and how you would manage this ever-growing issue if it occurred to your organization? For example, how would your Breach Response Plan be activated if your organization was completely locked out of your computer systems?		
Has your staff received cyber security training in the last 12 months? Is the training comprehensive, and does it address key areas such as password hygiene, social engineering/phishing, and understanding how to protect sensitive information?		
Do you have an access control policy with corresponding IT and personnel that effectively restricts access to sensitive data (non-public personal information, personal health information, business sensitive information, etc.)?		
Have communications and cyber connections with customers and vendors been considered in your Cyber Security Plan?		
Do your manufacturing systems rely on “Operational Technology” to run production? If yes, are these systems hardened with dedicated cyber security control mechanisms to prevent intentional sabotage, as well as accidental mistakes by workers and trusted third parties?		

Lastly, be sure you know who to contact in the event of a claim!

This isn’t an exhaustive checklist, but it should give you a starting point for creating or enhancing your own risk management practice. Be sure to reach out and discuss these findings with your agent.

[1] NCMM