Business Liability Insurance Self-Assessment Checklist

Prepare Your Business for Underwriting

Use this comprehensive checklist to ensure you have all necessary documentation and procedures in place before applying for liability insurance.

General Liability Insurance

- ☐ **Business Description**: Detailed description of your business operations.
- ☐ **Physical Safety Policies**: Documentation of workplace safety procedures.
- ☐ **Incident Records**: History of previous claims or incidents.
- ☐ **Property Information**: Details about the physical premises, including safety features.
- ☐ **Employee Training**: Records of safety training programs.

Errors and Omissions (E&O) Insurance

- ☐ **Professional Services Description**: Clear explanation of services provided.
- ☐ **Client Contracts**: Standard contract templates and signed agreements.
- ☐ **Quality Control Procedures**: Processes for ensuring service quality.
- ☐ **Complaint Resolution**: Policies for handling client complaints.
- ☐ **Previous Claims**: Record of any past E&O claims.

Cyber Liability Insurance

- ☐ **IT Infrastructure Overview**: Description of your IT systems and networks.
- ☐ **Cybersecurity Policies**: Documentation of cybersecurity protocols.
- ☐ **Incident Response Plan**: Detailed plan for responding to cyber incidents.
- ☐ **Data Protection Measures**: Policies for protecting sensitive data.

- ☐ **Employee Training**: Records of cybersecurity training for employees.
- ☐ **Vendor Management**: Procedures for managing third-party vendors.
- ☐ **Audit Reports**: Results of any cybersecurity audits or assessments.
- ☐ **Backup and Recovery Plan**: Procedures for data backup and disaster recovery.

Data Assessment

- ☐ **Identify Critical Data**: What types of data are critical to your business operations? Where is this data stored (local servers, cloud services, etc.)?
- ☐ **Data Classification**: Have you classified data based on its sensitivity (public, internal, confidential)?
- ☐ **Data Access Control**: Who has access to sensitive data? Are access controls in place?
- ☐ **Data Encryption**: Is sensitive data encrypted both at rest and in transit?

Operations Assessment

- ☐ **Process Documentation**: Are key business processes documented?
- ☐ **Operational Dependencies**: What are the critical dependencies for your operations (software, hardware, third-party services)?
- ☐ **Workflow Efficiency**: Are there any bottlenecks or inefficiencies in your current workflows?

Tech Stack Assessment

- ☐ **Inventory of Technology**: Do you have an up-to-date inventory of all hardware and software used in your business?
- ☐ **Software Licensing**: Are all software licenses up to date and compliant?
- ☐ **Hardware Maintenance**: Is all hardware regularly maintained and updated?
- ☐ **Technology Utilization**: Are you using the full capabilities of your current tech stack?

Business Continuity and Disaster Recovery Assessment

- ☐ **Business Impact Analysis (BIA)**: Have you conducted a BIA to identify critical business functions and the impact of disruptions?
- ☐ **Business Continuity Plan (BCP)**: Do you have a BCP in place? Is it documented and regularly updated?
- ☐ **Disaster Recovery Plan (DRP)**: Is there a DRP for IT systems and data recovery? Are recovery time and recovery point objectives (RTO, RPO) defined?

- ☐ **Regular Testing**: Are BCP and DRP tested regularly through drills or simulations?

Security Practices Assessment

- ☐ **Access Control**: Are strong access controls implemented (e.g., MFA, least privilege)?
- ☐ **Employee Training**: Do employees receive regular training on cybersecurity best practices and threat awareness?
- ☐ **Endpoint Security**: Are all endpoints protected with up-to-date antivirus and anti-malware software?
- ☐ **Network Security**: Are firewalls and intrusion detection/prevention systems in place and properly configured?
- ☐ **Regular Updates and Patching**: Are all systems and applications regularly updated and patched?

Compliance and Regulatory Assessment

- ☐ **Regulatory Requirements**: What regulatory requirements apply to your business (e.g., GDPR, HIPAA, PCI DSS)?
- ☐ **Compliance Status**: Are you currently compliant with these regulations? What gaps need to be addressed?
- ☐ **Policy Documentation**: Are all compliance-related policies and procedures documented and communicated to employees?

Vendor and Third-Party Risk Assessment

- ☐ **Vendor Inventory**: Do you have a list of all vendors and third-party service providers?
- ☐ **Vendor Security**: Have you assessed the security practices of your vendors? Do they comply with your security requirements?
- ☐ **Contracts and SLAs**: Are contracts and service level agreements (SLAs) in place and regularly reviewed?

Next Steps After Your Self Assessment

1. **Quantify and Prioritize Risks:** Assess and rank the most critical risks and vulnerabilities identified in your checklist.
2. **Develop an Action Plan:** Create a detailed plan with specific steps, responsible parties, and deadlines to address identified risks from the checklist.
3. **Implement Quick Wins:** Start with quick wins that can significantly improve your risk posture with minimal effort and cost.
4. **Invest in Training:** Ensure all employees are trained on cybersecurity, compliance, and safety practices.
5. **Engage Experts:** Consider engaging risk management and IT experts to implement complex solutions and provide ongoing support.
6. **Prepare Documentation:** Gather and organize all necessary documentation, such as business descriptions, safety policies, incident records, and compliance proof.
7. **Monitor and Review:** Establish a process for continuous monitoring and regular review of your risk management practices to adapt to new threats and changes in your business environment.
8. **Submit Application:** Compile the completed checklist and documentation, and submit the insurance application.