Cybersecurity risk assessment checklist

How to prepare for and conduct a cybersecurity risk assessment

A cybersecurity risk assessment helps you manage cyber risks and protect your business. Here's how to get started conducting and implementing one:

Action step		Status
☐	**1. Find a cybersecurity advisor**	
☐	Find a third-party cybersecurity advisor to conduct your assessment, as a comprehensive assessment benefits from external perspective and expertise.	
☐	Be sure to choose an advisory firm that knows your industry and its specific cybersecurity risk management requirements, including relevant frameworks like NIST, CMMC or ISO.	
☐	If you operate in a regulated industry, ensure your advisor also understands all relevant regulatory factors.	
☐	Consider that ideally, a cybersecurity risk assessment is done as part of a broader enterprise risk assessment, as this will help you understand and manage your risks holistically for better outcomes.	
☐	**2. Prepare for your assessment**	
☐	Prepare for your assessment by talking with your advisor about what you'll need to do and any resources it will require.	
☐	Confirm the scope of the assessment and the areas of your business it will cover, along with anticipated evidence requests.	
☐	Be sure that your advisor will be conducting a business impact analysis so you can understand what a cyber disruption in any particular department would mean for your business as a whole.	
☐	Identify the scoring criteria and reporting format, and establish which stakeholders will need to be involved.	

	Action step	Status
☐	**3. Conduct the assessment**	
☐	Collaborate with your cybersecurity advisor to conduct the assessment.	
☐	Do an inventory of your systems and data.	
☐	Identify threats and vulnerabilities and evaluate threat likelihood and impact, scoring from low to moderate to high.	
☐	Use the assessment data to calculate your business's inherent risk, which is risk level prior to implementing new security controls.	
☐	**4. Analyze what you've learned**	
☐	Review what you've learned from the risk assessment to understand your control maturity, control effectiveness and risk mitigation.	
☐	Prioritize threats or risks based on your likelihood and impact scoring, focusing on risks that score as high-likelihood, high-impact or both.	
☐	Clarify your expected residual risk, or overall risk level after implementing or maintaining effective controls.	
☐	**5. Communicate findings and develop a roadmap**	
☐	Develop an executive report, heat map, business area narratives, risk register and roadmap with prioritized risk responses.	
☐	Go over this report with your leadership team and your board to get approval to move forward with implementation.	

Action step		Status
☐	**6. Implement your roadmap**	
☐	Based on your assessment and roadmap, take action to manage your cybersecurity risks.	
☐	Implement new controls or processes as needed.	
☐	Test your new controls to assess their effectiveness.	
☐	Conduct initial training sessions to help your team adapt to new security changes.	
☐	**7. Maintain ongoing monitoring with regular reassessments**	
☐	Treat assessing and managing cyber risk as an ongoing process by doing testing, tracking metrics, conducting ongoing training, evaluating new threats and monitoring your overall risk levels.	
☐	Conduct regular reassessments to learn how the risk environment is changing and how to adapt.	

How Wipfli can help

We conduct cyber risk assessments for businesses to help you understand and manage your cybersecurity risks. Let's talk about how we can make your organization safer and stronger.

Contact us to learn more.