**Risk avoidance** in cybersecurity refers to strategic measures taken to **prevent potential risks and threats**. [Unlike risk mitigation, which focuses on minimizing the impact of identified risks, risk avoidance aims to **sidestep the risks altogether**1](https://www.centraleyes.com/glossary/risk-avoidance/).

In more straightforward terms, here’s what it means:

1. [**Cyber Risk**: It’s the risk of **negative impact** to your organization if your information systems fail, are disrupted, damaged, or destroyed due to **unauthorized use or access**](https://www.centraleyes.com/glossary/risk-avoidance/)[2](https://www.tenable.com/principles/cyber-risk-principles).
2. **Risk Avoidance**: This approach seeks to **eliminate the possibility of risk** by avoiding activities that create exposure to risk. [Essentially, it’s about **not engaging in risky behaviors**](https://www.centraleyes.com/glossary/risk-avoidance/)[3](https://www.csoonline.com/article/554377/how-to-manage-cyber-risk.html).

Imagine it like this:

[ \text{Potential Impact of Threat} \times \text{Attack Likelihood} = \text{Cyber Risk} ]

[Risk avoidance ensures that the threat either **can’t impact your organization** or has a **probability of occurrence of zero**](https://www.centraleyes.com/glossary/risk-avoidance/). While it’s effective, keep in mind that it can also **limit opportunities** for your company.