Title : Risk Scoring Method for Cybersecurity Assessment

This document defines the scoring method used to assess cybersecurity risks for small businesses. The purpose of this scoring model is to measure the severity of risks, calculate their impact on business, and determine which risks need urgent action.

Section 1: Likelihood Scale

Score	Likelihood Level	Description
1	Rare	Unlikely to happen in the next 12 months
2	Possible	Might occur in the next 12 months
3	Likely	Expected to occur within 6 months
4	Very Likely	Expected to occur within 1 month

Section 2 : Impact Scale

Score	Impact Level	Description
1	Low	Minor interruption with no financial loss
2	Moderate	Short downtime & small financial loss
3	High	Major downtime or data loss affecting customers
4	Critical	Business unable to operate, legal or financial damage

Section 3 : Risk Calculation Formula

- **Raw Risk = Likelihood × Impact**
- **Residual Risk = Raw Risk × (1 − Controls Effectiveness)**
  - Residual Risk is the remaining risk after applying existing security controls.

Section 4 : Risk Level Categories

Score Range	Risk Level
1–4	Low
5–8	Medium
9–12	High
13–16	Critical

Section 5 : Worked Examples

Example 1: Email Phishing Attack

- Likelihood = 4
- Impact = 3
- Raw Risk = 4 × 3 = 12
- Controls Effectiveness = 0.20

Residual Risk = 12 × (1 − 0.20)
= 12 × 0.80
Show math:
12 × 0.80 = (12 × 8) ÷ 10 = 96 ÷ 10 = **9.6**