

## Road to PIPA Week 13: DETERMINING YOUR ORGANISATIONS RISK THRESHOLD

An organization's risk threshold is the measure of 'acceptable risk' for an organisation – the severity of potential harm combined with the likelihood of an incident indicates a threshold above which a risk becomes unacceptable. Risk should be viewed from both an organisational and an individual perspective.

### Information Security (organisational risk)

Risk is viewed with respect to potential damage to the organization and its assets – both tangible and intangible.

### Data Privacy (risk to individuals)

Risk depends on the impact/harm on the individuals.

*For example: critical functions, reputation, etc.*

$$\text{Risk} = \text{Likelihood} \times \text{Severity}$$

The diagram illustrates the formula Risk = Likelihood x Severity. The word 'Risk' is in a blue, italicized font. 'Likelihood' is in a light purple font and has a white bracket underneath it. 'Severity' is in a teal font and has a white bracket above it. The equals sign and the multiplication sign 'x' are in a dark grey font.

*For example: vulnerabilities, exposure, threats, mitigating controls*