

ICANN

ANNUAL GENERAL

75

KUALA LUMPUR

Risk Concepts

Presentation by ICANN Org
Risk Management

James Caulfield
September 2022



The Nature of Risk

- ⊙ Risk is the possibility of events to have an **adverse** impact on an organization's, groups, etc. ability to achieve its mission, and could even prevent an organization from continuing to operate. Importantly, risk is characterized by **uncertainty**.

- ⊙ Uncertainty can arise from
 - the **likelihood** of a risk occurring,
 - the **severity** of the impact if the risk occurs, or
 - the effectiveness of the **controls and mitigation** in place concerning a risk.

- ⊙ The more likely an event, the more it is a certainty, not a risk. The more uncertainty, the more important risk management becomes.

- ⊙ An organization creates value by accepting and **managing** risk, not necessarily eliminating all risks.

Informed Management of Risks

Informed Management of Risks

- ⦿ Decision makers are responsible to know what risks an organization faces, how those risks are being managed, what residual risks remain, and make an **informed** decision to set the level of accepted risk.
- ⦿ In order to make decisions regarding risks, we need to **articulate** the risk and risk controls, and plan for any additional controls.
- ⦿ Adverse events will occur, but we want to anticipate risks, not be reactive. The goal is **no surprises**.

How to Articulate a Risk

- ⦿ **Risk Title (name):** Is an event, trend, or situation that could result in an adverse consequence. The event should not be confused with the consequences of the event.
- ⦿ **Consequences:** The consequence of the risk occurring, the impact, the outcome of the event.
- ⦿ **Existing Controls or Mitigation:** Provide information regarding existing controls and mitigation, explaining their effectiveness.
- ⦿ **Risk Rating:** Based on defined likelihoods and severities of impact.
- ⦿ **Proposed New or Changed Controls or Mitigation:** Describe any additional recommended controls and why, include any additional required resources for those controls.

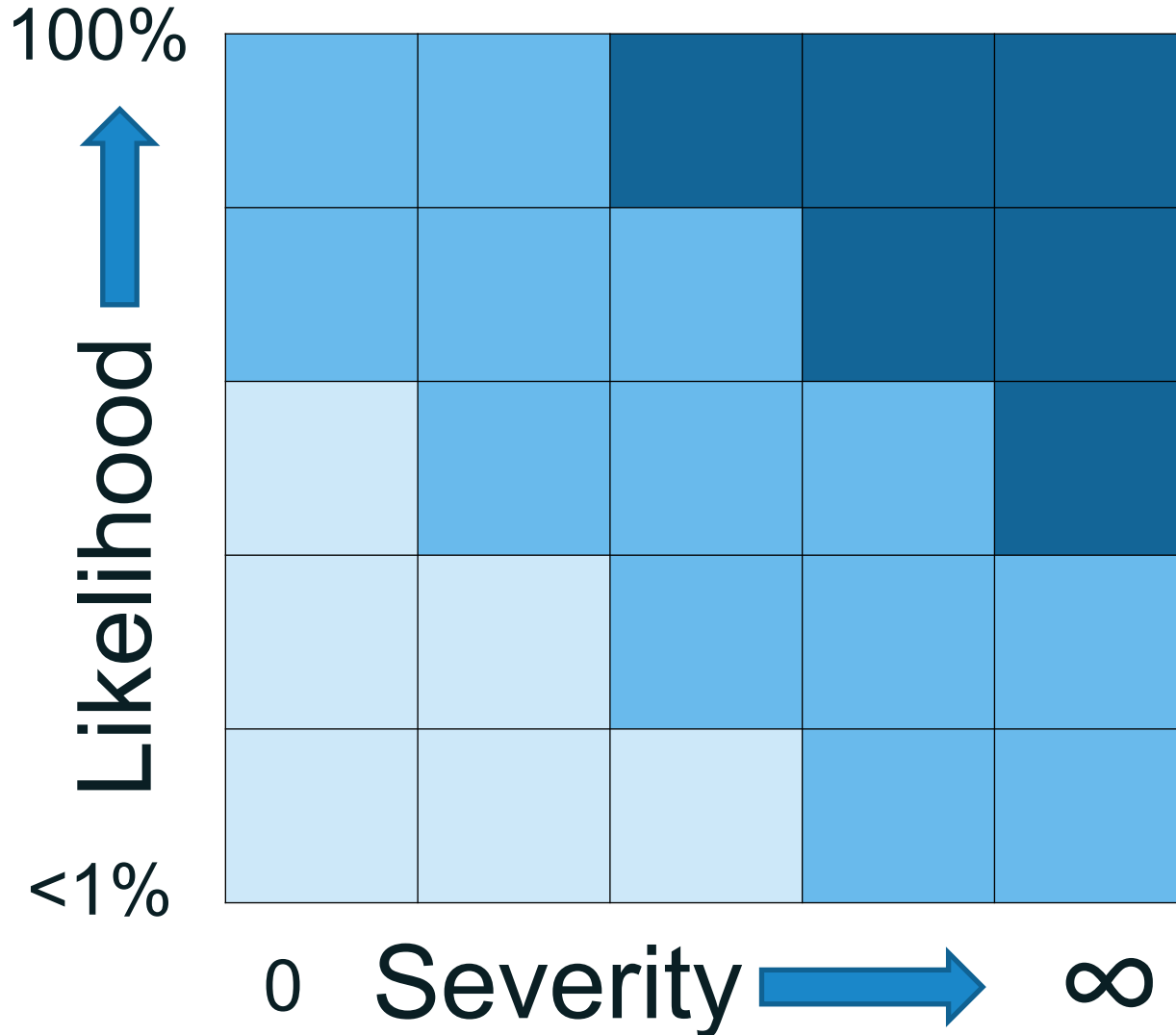
How to Articulate a Risk

Notes

- ⦿ Risk event and consequence are often confused. The risk is what happens that causes the consequence.
- ⦿ We do not include “risk” or “risk of” something in the title. Simply the event is the risk.
- ⦿ “Lack of” something is not a risk. What is lacking is usually a control.

Risk Ratings

Traditional heatmap. What's the biggest risk?

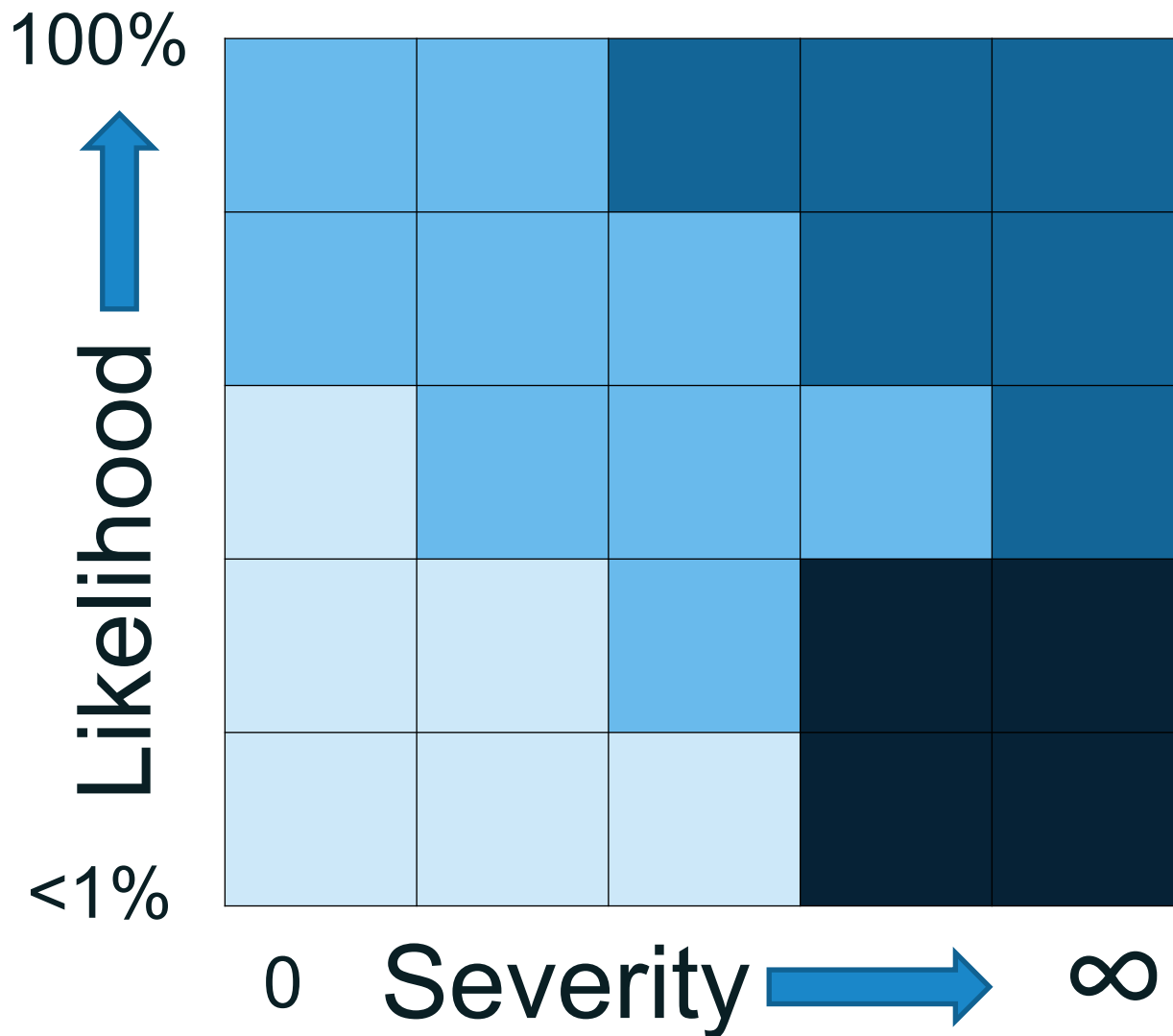


This format implies that #3 is the greatest risk, that is, the greatest likelihood x greatest severity.

We agree with that generally and is the basis for our risk ranking method.

Risk Ratings

Heatmap with severity and unexpected likelihood focus.



This format implies that risk #4 is the biggest, because the likelihood is low. The unexpected nature of #4 can cause complacency until it is too late.

We should be keenly aware of low probability / high impact risks.

Rating a Risk

Define the ratings as appropriate to your use.

Likelihood

Rating	Definition
Low - 1	Probability %: Descriptive:
Medium - 2	Probability %: Descriptive:
High - 3	Probability %: Descriptive:

Rating a Risk

Define the ratings as appropriate to your use.

Severity of Impact

Rating	Definition
Low - 1	Operational: Reputational: Financial:
Medium - 2	Operational: Reputational: Financial:
High - 3	Operational: Reputational: Financial: