Infosec is seen as a gatekeeper, not an enabler

Risk Assessments are done for compliance, not for decisions

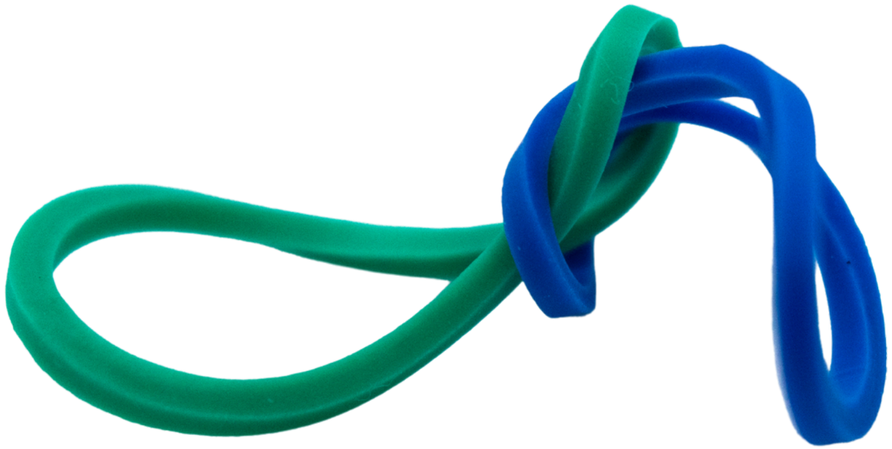
principle #1

Risk Assessments are for informed decision making

If a risk assessments doesn’t aid our decisions, we choose not to conduct it.

Risk registers are an incomplete list of unclear risks

Risks are neither defined clearly nor are they simple enough for everyone to understand



principle #2

Risks should be clear and simple

We define, clarify, and simplify risks to be understood by everyone, not just the assessors

Risk registers are **bloated** with what ‘others’ believe are risks

Audit observations, incidents, OEM reports etc. are added to the risk register without a formal validation process

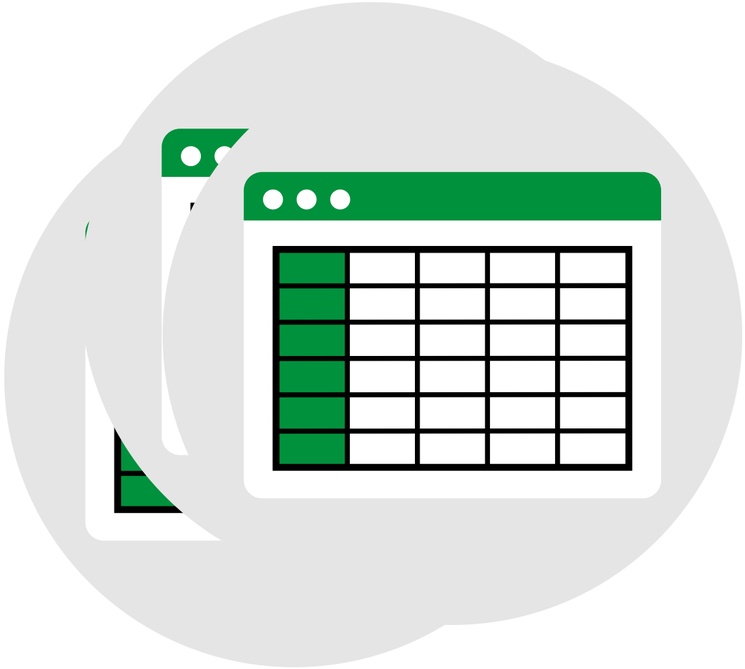
principle #3

Only validated risks in the register

We ensure all risks are verified before adding them, maintaining the integrity of our risk register

Everyone has their own list of risks and actions

A single source of clear and validated risks for the entire organisation does not exist



principle #4

One risk register for the entire organisation

One organization, one risk register, fostering consistency and cohesion.

Risks are added & monitored **after** incidents, not **before**

Risk assessment processes are reactive, not proactive. An incident becomes a risk, but an exception approval does not

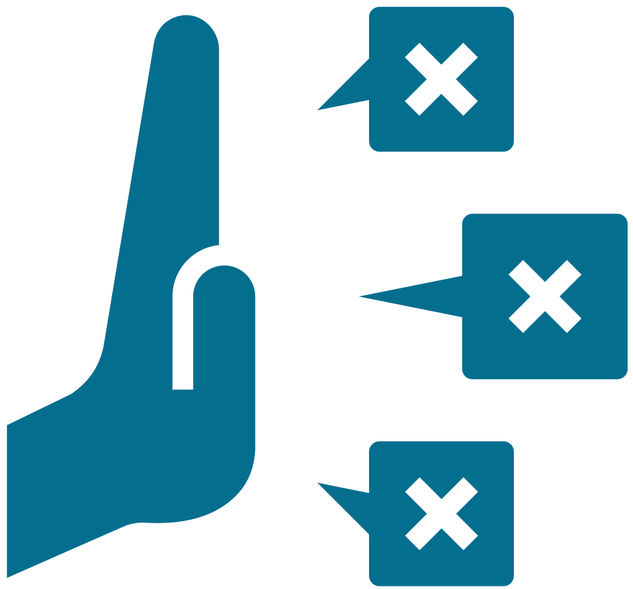
principle #5

Capture risks proactively at the source

We document risks as soon as they emerge, not months later.

An **inflexible** methodology is created and **forced** on everyone

Even if a risk requires a detailed analysis, or a simpler one, the **one** methodology has to be followed



principle #6

Value context over processes

Understanding the environment of a risk guides us more than blind adherence to procedures.

Painful risk quantification methods are touted as the smart way

Quantification is helpful, but so are intuitive decisions. Knowing when to use a particular approach helps simplify risk management

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

principle #7

Quantify high stake risks

Significant risks deserve accurate measurement to inform our strategies.

Maths on qualitative methods are used as de-facto standards

Two Medium risks do not make a High risk, just as watching 2 two star movies is not equivalent to watching one four star movie

principle #8

Recognize the limitations of qualitative risk assessments

We approach qualitative risk evaluations with awareness, understanding their constraints.