Deloitte.

Turn your risk profile into an action plan using risk appetite

Three questions to ask for getting started with risk appetite

1. How much risk is the organization **willing to accept**, and where are we taking too much risk (over-exposed) or over managing risk (wasting resources)?
2. How do we define our appetite for risk-taking in the form of statements that **drive to strategic objectives** and **desired outcomes**?
3. How do we set tolerances around specific risks or performance objectives in a manner that **proactively steers** response action?

What are risk appetite and tolerance?

Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of its strategic objectives. Appetite provides a consistent measure for how much risk is acceptable to an organization and links their decision-making to objectives and risk categories.

Risk tolerance is the set of boundaries of acceptable performance variation regarding specific risks or performance objectives. Applying tolerance helps organizations tie their priority risks to measurable metrics that indicate whether—and what kind—of action is required.

Applying appetite and tolerance to the risk profile

Risk appetite gives organizational leaders a measuring tool across their risk profile to prioritize risks for response action or capitalizing on potential opportunities. Risk appetite can be used to inform a risk profile or vice versa, depending on ERM maturity. The illustration below shows high level steps to make the most out of appetite as an input to the risk profile, or to use the risk profile as a first step to developing risk appetite. See the back page for an illustration of appetite and tolerance in action. Note that when developing risk appetite statements, which are key to clear and actionable guidance, narrative or bullets are effective provided they paint a clear picture of degree of risk that can be taken.

A general approach to using risk appetite as input to the risk profile…

1. **Identify and understand objectives** for the agency or component, and their execution
2. **Identify metrics** aligned with each strategic objective that can measure performance and risk
3. **Discuss risk appetite** in reference to strategic goals, objectives, and measures (i.e., where to take more or less risk)
4. **Measure, assess, and prioritize** risks relative to appetite and tolerance – and show where action is required
5. **Complete risk profile** by adding response strategies to move risks within tolerance

Risk Profile

…or using the risk profile to form appetite and tolerance.

1. **Develop categories to group risks**, or apply categories / taxonomy if not already done
2. **Review risks within each category** with senior leaders for how much risk they are willing to accept
3. **Form appetite statements** for each risk category that establish acceptable risk levels
4. **Set tolerance levels** for individual risks by aligning performance metrics to appetite statements
5. **Plan risk response** or appropriate actions to bring risks to tolerance

Illustrating how risk appetite turns a profile into an action plan

1 **Risk appetite statements** align to **high-level groups** such as risk categories, portfolios, or strategic objectives, describe in broad terms (e.g., high, medium, low) how much risk to take, and set parameters on whether to take more or less risk.

2 **Risk tolerance** is guided by appetite, applied to **individual risks,** and establishes acceptable upper limits (U/L) and lower limits (L/L) for risk taking. Tolerance can also be established for each performance objective as a measure of acceptable variation.

Risk appetite statement	Risks & tolerance	U/L	L/L	A/P	Action / Response
IT operations. The organization has a **medium appetite** for IT operational risk, accepting balanced risk to promote operational efficiency and in pursuit of priority initiatives, with higher risk accepted for innovation pilots within the initiatives. However, operational risks resulting in Tier 1 information security incidents are not acceptable	Non-essential process transaction error rate between 2-4% (monthly)	**4%**	**2%**	**1%**	**Below tolerance.** Seek or exploit greater risk.
	Cloud server downtime of 4 – 10 hours (monthly) will be tolerated	**10 hr.**	**4 hr.**	**5 hr.**	**Within tolerance.** Accept the level of risk and monitor.
	Zero tier 1 information security incidents (quarterly) will be tolerated.	**0**	**-**	**2**	**Above tolerance**. Risk mitigation or avoidance required.

Note: *Actions taken to bring risks within tolerance reflect core risk response strategies.*

3 **Actual performance (A/P)** against tolerance drives decision making about whether risk needs to be:

- mitigated
- transferred
- exploited
- avoided
- accepted

In conclusion – principles for driving value and action using risk appetite:

- ✓ Establish ***clear and actionable boundaries*** delineating the amount of risk the agency is willing to accept when making key decisions to achieve its mission and run the business
- ✓ Acknowledge divergent views and encourage debate on ***tradeoffs*** when pursuing desired outcomes – striking a balance between value protection and value creation
- ✓ Establish ***consistency*** in the amount of risk the agency accepts in routine operational decisions, resulting in ***confidence*** that the right amount of risk is being taken
- ✓ ***Measure*** whether risks are being managed to an acceptable level
- ✓ Reinforce a more risk-aware ***culture*** by empowering employees at all levels to deliberately consider risk and act independently within established boundaries

Questions?

Cynthia Vitters
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+571 424 0046
cvitters@deloitte.com

Anthony Fratta
Specialist Leader | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+703 915 9952
afratta@deloitte.com

John Basso
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+571 214 0561
jobasso@deloitte.com

Antonio Crombie
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+617 458 1749
ancrombie@deloitte.com