PROTECHT

E-BOOK

Risk Appetite: Taking and accepting the right amount of risk.

A comprehensive practical guide to organizational risk appetite.

Contents

PROTECHT

Introduction.

The explicit reference to an organizational risk appetite has been around for a relatively short while. The concept of risk appetite, however, has implicitly been around forever.

Like most aspects of risk management, there are the those that love risk appetite and those that loathe it and all those in between. These diverse views are healthy as they create intelligent debate.

Regardless of the many risk expert arguments for and against risk appetite, the ultimate test must be: Does it add value?

Consider the following questions:

1. Does it add value to an organization?

2. Is it used by the organization as part-of-day to day management?

3. Do non-risk specialists understand, engage with, and use risk appetite?

Overwhelmingly across Protecht's very wide client base, the answer is "Yes" – it does add value. The degree of value depends on how well risk appetite is formulated and operationalized. Like anything, it can be done really well or really poorly.

In this ebook, we will share our experiences, lessons learned, and guidance for benchmarking. If you are just starting on your risk appetite journey, the practical planning tools provided will help you get started.

This eBook covers:

Risk appetite and the related concepts of risk tolerance, risk criteria, and risk capacity

1. Risk appetite and the related concepts of risk tolerance, risk criteria, and risk capacity

2. Risk appetite purpose and value

3. A risk appetite framework

4. Articulating your risk appetite

5. A practical plan for developing your risk appetite

6. Operationalizing and using risk appetite across the organization

7. Steps to develop your risk appetite

Risk appetite and the related concepts of risk tolerance, risk criteria, and risk.

Like many other areas of risk management, there is no single common language around risk appetite, either globally or across various risk management standards.

To take a sample of the definitions of "risk appetite":

COSO	ISO 31000	FINANCIAL SERVICES REGULATORS
The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.	The ISO 31000 risk management standard on the other hand, does not directly refer to risk appetite but instead uses the terms "risk attitude" and "risk criteria":	The degree of risk an institution is prepared to accept in the pursuit of its strategic objectives and business plan
COSO Enterprise Risk Management – Integrating Strategy and Performance	• risk attitude: organization's approach to assess and eventually pursue, retain, take or turn away from risk. • risk criteria: terms of reference against which the significance of a risk is evaluated.	**Australian Prudential Regulatory Authority** The aggregate level and types of risk the board and senior management are willing to assume to achieve the firm's strategic business objectives
	ISO 31000 Risk Management Principles and Guidelines 2018	**Federal Reserve**

Similar to the variation in definitions, there is also no common meaning of the other terms often used in risk appetite. These typically are:

- risk tolerance
- risk triggers
- risk capacity

Based on Protecht's experience over the last decade or so, our standard definitions for each are:

Risk Appetite: the degree of risk an organization is prepared to accept in the pursuit of its strategic and operational objectives expressed in a *qualitative* manner.

Risk Tolerance: the degree of risk an organization is prepared to accept in the pursuit of its strategic and operational objectives expressed in a *quantitative* manner.

Risk Triggers: the degree of risk which alters the escalation, reporting and response of the risk, expressed in a *quantitative* manner.

Risk Capacity: the maximum amount of risk that an organization could take before threatening its survival expressed in a *quantitative* manner.

Risk Capacity	Represents the overall ability to absorb potential risk given resources, operational environment and obligations to stakeholders.	Outside of appetite, action required
Risk Appetite	The maximum level of risk organization is prepared to take articulated in **qualitative terms.**	Within appetite with raised attention
Risk Tolerance	The maximum level of risk organization is prepared to take articulated in **quantitative terms (measurable metrics).**	
Upper Trigger	A level of risk within risk appetite that triggers additional attention and action as to why the risk is high.	Within appetite, no action needed

Figure 1: Definitions

Risk appetite purpose and value.

The main objectives of risk appetite, which when achieved, add substantial value to the organization, include the following:

a. To enable executive management and governing body (e.g. board) to exercise appropriate oversight and governance over the risks of the organization in an efficient and effective way. The primary focus should be:

- Providing assurance

- Identification of risks outside of appetite i.e. risks that are too high

- Identification of risks that are well within risk appetite i.e. risks that may be too low

This is achieved through the use of risk appetite in evaluating and reporting risk levels based on where they fall with respect to risk appetite. Figure 2 provides an example of risk appetite based reporting.

b. To influence culture by expressing the organization's attitude to risk- taking. The risk appetite should be communicated to staff so that it influences attitudes and decisions in line with what the organization desires.

c. To form the basis of risk evaluation leading to appropriate escalation, reporting and response. The risk appetite should be used to drive workflow so that risks are escalated based on where they fall with respect to risk appetite and specific actions driven by that evaluation.

d. To limit excessive risk taking. Where parts of the organization are taking excessive risk, the risk appetite should be used to identify, report and respond based on the reporting escalation and reporting framework covered in c. above.

RAS Metrics Report
Periods: Oct 21, Dec 22, Aug 21

KRI	Business Unit	Risk Appetite	Scales • Green	Scales • Amber	Scales • Red	Aug 21	Dec 22	Oct 21	Trend	Comment (Oct 21)
Number of Hazards Recorded Last Month	Health and Safety		3	5	7	• 3	•	• 1		
Health and Safety Risk										
Equipment Breakdown Last Month	Health and Safety		3	5	6	• 1	•	• 1		
Number of Hazards Recorded Last Month	Health and Safety		3	5	7	• 3	•	• 1		
WHS training hours conducted during the month	Health and Safety		60	20	0	• 55	•	• 33	▲	
% of staff temperature checked on entry to company premises	People & Culture	Low	70	20	0	• 25	•	• 19	▲	Failure to process.
Number of COVID19 infected employees	People & Culture	Low	5	10	15	• 2	•	• 1	▲	
Number of employees tested for COVID19	People & Culture	Low	600	100	0	• 450	•	• 450	▲	
Insurance Risk										
The number of times an insurance review due date has been missed	Finance		1	2	4	• 1	•	• 2	▲	
Market and Investment Risk										
Interest rate risk - PVBP	Treasury		50000	75000	100000	• 23000	•	• 2200		
Operational Risk										
Number of complaints escalated to the ombudsman	Call Centre		5	10	20	• 1	•	• 2	▲	
Number of complaints relating to products, sales & service on a monthly basis	Call Centre		20	30	40	• 25	•	• 22	▲	

Figure 2: Risk appetite based reporting

e. To empower the organisation to take more risk. The deliberate taking of "intelligent" risk, risk that has a direct positive relationship with reward, should be an integral part of business management. When a business area is not performing well and the level of risk taking is minimal, one solution may be to increase the level of risk taking to enhance reward. Risk appetite communicates the boundary out to which the organisation can go, empowering the organisation to potentially take more risk.

f. To assist in better decision making. The first step of robust risk/reward decision making is to assess the risks of each alternative being considered and evaluate the size of the risks against risk appetite. Where the risk is outside of appetite, this alternative cannot be considered unless it is possible to manage the risk to within appetite. This is the "Can I?" component of "Can I?"/"Should I?" decision making.

Risk appetite driven decision making

Risk appetite should be a tool used every day, not a document that collects dust on the boardroom shelf.

Read related article

In order to deliver value, risk appetite should not be considered as a standalone concept. It should be an integral part of the Enterprise Risk Management (ERM) framework and a key part in the wider management framework. It should influence culture and decision making and empower the organisation to take the right amount of risk to achieve the right level of outcomes.

KRIs Health Score

4

Monthly Trend
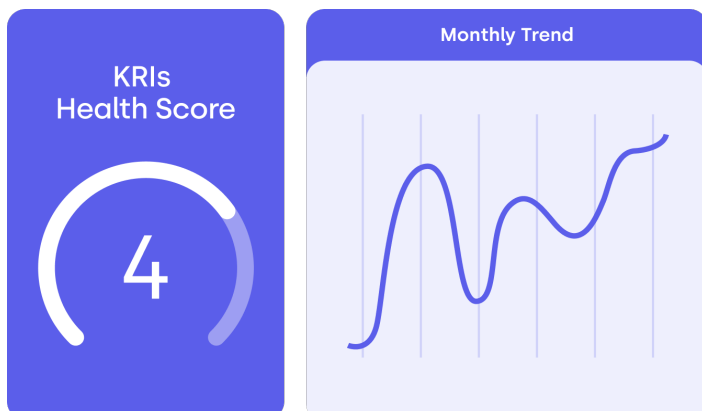
A risk appetite framework.

The Risk Appetite Framework (RAF) should form part of the overarching ERM framework. It consists of the system(s), structures, policies, processes and people used for risk appetite to assist in the evaluation, monitoring and reporting of risk.

The key elements of the RAF are as follows:

a. The linkage of risk appetite with strategy, business plans and objectives

Risk appetite and strategy are inextricably linked. In order to determine strategy, you must know your risk appetite. In order to identify your key risks and determine the related appetite, you must know your strategy. They must therefore be developed and maintained in a synchronized way.

b. The linkage of risk appetite to the central taxonomy of key risks

A central risk taxonomy of key risks is a critical component of an enterprise approach to risk management. This taxonomy should be used consistently within the risk processes and systems to link all risk information and should be used to articulate appetite for each of the risks and subsequent reporting.

c. The board-level Risk Appetite Statement (RAS)

The board-level RAS is the key statement that articulates the overarching risk appetite of each key risk.

d. The various artifacts that help operationalize and communicate risk appetite across the organization's people and activities

Various artifacts are required in order to cascade and communicate risk appetite to staff. These are covered in detail in section 7.

e. The ERM system that records, analyses, measures and evaluates risk. The evaluation must be against risk appetite

Your ERM system, for us, Protecht.ERM. You can learn more about this industry leading solution here.

f. The reporting of risks against risk appetite

Risk information which informs the size of the risk should be evaluated against risk appetite and tolerance and be reported based on where the risk sits, relative to appetite.
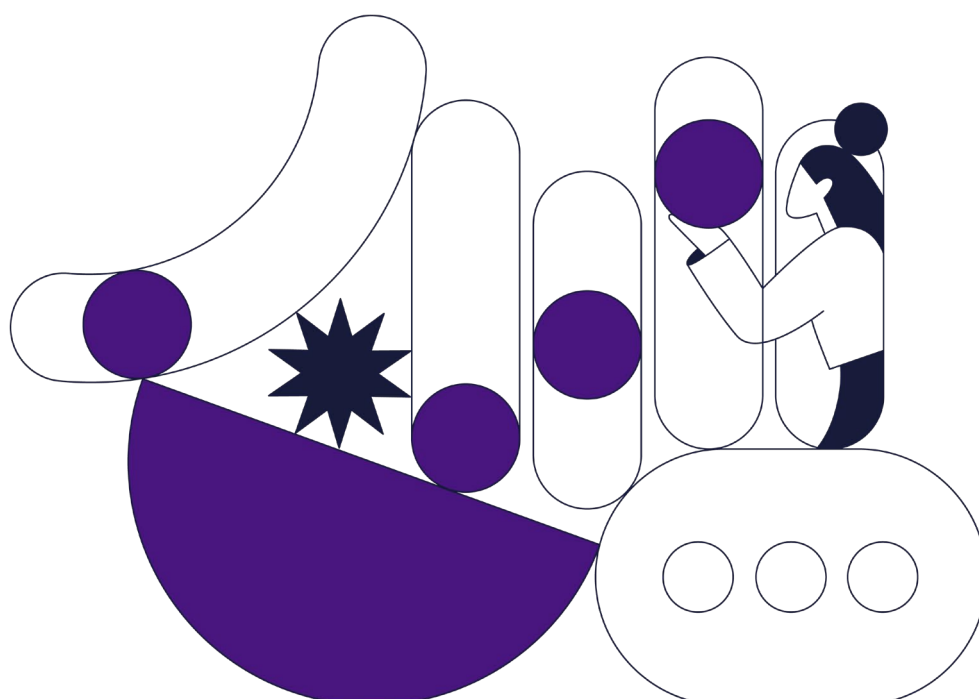
g. **The governance around risk appetite, consisting of risk appetite policy components covering such aspects as:**

- Who is responsible for developing and maintaining the risk appetite and who "owns" it?

- How often and when should the risk appetite be reviewed and updated?

- The reporting and response process against risk appetite.

- How risk appetite should be used? This should typically include:

  › To provide assurance

  › To identify risks outside of appetite, that are too high

  › To identify risks that are well within risk appetite and maybe too low

  › To provide information to assist in decision making

Figure 3: Risk Appetite Framework

Articulating your risk appetite.

The articulation of risk appetite for each key risk is important in order to:

a. Have a "measurement" scale(s) that can be used to debate and agree on the risk appetite.

b. Have a means to communicate the risk appetite to staff so that they understand and are aware of the risk boundaries for the decisions that they make.

The methods used to articulate risk appetite must be aligned to the methods used by the organization to measure risk, otherwise risk cannot be evaluated against an appetite that is articulated differently. There are a range of ways to "measure" risk so it follows that there are a range of ways to articulate risk appetite.

In addition, "appetite" can be set against both risk and outcomes. Setting against risk, allows the setting of risk appetite by risk type. In addition, and using the ISO 31000 definition of risk "the effect of uncertainty on objectives", risk appetite can also be articulated based on the maximum tolerable variation in your targeted outcomes, typically measured by Key Performance Indicators (KPIs).

PROTECHT

The following are a range of typical risk "measurement" methods and resulting risk appetite articulations.

MEASUREMENT/ APPETITE ARTICULATION METHOD	EXAMPLE	BEST USE
1. Qualitative	Zero, Low, Medium, High	• Use at board and executive level to provide overall relativities of risk appetite between key risks.
2. Key Risk Indicators	Level of unforced staff turnover	• Setting risk tolerances at board level for relevant board-level metrics. • Cascading risk appetite across the organization in a meaningful and objective way. • Measuring risk against appetite across the organisation as a basis for risk reporting.
3. Key Performance Indicators	Profit	• Setting performance tolerances at board level for relevant board-level KPIs. • Cascading risk appetite across the organization in a meaningful and objective way based on the variation on objectives. • Measuring KPI performance against risk appetite across the organization as a basis for KPI reporting.
4. Likelihood and Consequence Assessment	Either qualitative as above or a score based on likelihood and consequence	• Limited use as very subjective and in its standard form the likelihood and consequence matrix does not articulate appetite by risk well.
5. Key Control Indicators/ Minimum control Standards	Minimum formal training hours for customer facing staff	• As above for key risk indicators. • For communication of staff of minimum standards, representing risk appetite.
6. Directive Statements	You will not bully other staff members	• For use in codes of conduct, policies, standards and guidelines for staff communication and compliance checking.
7. Delegations and Authorities	You have authority to approve expenditure up to $500,000	• For governance of the organization and cascading risk appetite through the different levels of the organization.

A practical plan for developing your risk appetite.

The following is a typical approach Protecht uses with clients to develop and operationalise risk appetite.

STEP	ACTIVITY
1. Define the board-level risks	• Determine whether there is a well defined central risk taxonomy of key board-level risks that are used consistently across the ERM framework. • Where required, develop/refine a central taxonomy. This would typically consist of between 10–20 risks covering all key risk types.
2. Define the content of the RAS	• Determine the layout and content of the RAS. An example of typical content is outlined below.
3. Source existing information and populate draft RAS	• Review strategic plan and business plan to identify objectives, KPIs and related targets. • Identify any existing relevant board-level key risk indicators and link them to the related key risk.
4. Set draft risk appetite levels with executive management's view	• Hold workshop(s) with executive management and set qualitative risk appetite levels and quantitative risk tolerance levels for identified metrics. • Create draft RAS ready for board review.
5. Determine and agree board view of risk appetite	• Hold workshop(s) with board to review draft RAS and executive management's views. • Board to challenge and change appetite where appropriate. • Finalize and gain board approval for RAS.
6. Operationalise	• Cascade the risk appetite through the various artifacts as identified in section 6. This will usually involve ensuring that the existing artifacts are reviewed and amended to ensure they are in line with the board-approved RAS. • Build all risk appetite and tolerance measures into your ERM system and measure risks against the appetite levels. • Report to board, committees and executives based on risks evaluated against risk appetite.

PROTECHT

Defining the content of the RAS

There is no one approach to setting out a RAS. Example content is provided below for what we see as good practice.

1. Introduction, purpose, context of the RAS.

2. Overview of strategic plan, business plan and related objectives.

3. Determining the zones and levels to be used to articulate qualitative risk appetite and quantitative risk tolerance. An example of this is as

APPETITE LEVELS	MEANING AND REQUIRED ESCALATION AND RESPONSE
Zero	XYZ Company is not willing to accept any instance of this risk occurring. It does accept that sometimes these risks could occur but if they do they will always be actioned and any weaknesses identified will be rectified.
Low	XYZ Company accepts a low amount of this risk occurring. Risks occurring greater than a low level (as reflected in tolerance levels) will be risk mitigated and any weaknesses identified will be rectified.
Medium	XYZ Company accepts a medium amount of this risk occurring. Risks occurring greater than a medium level (as reflected in tolerance levels) will be risk mitigated and any weaknesses identified will be rectified.
High	XYZ Company accepts a high amount of this risk occurring. Risks occurring will only be risk mitigated and any weaknesses identified and rectified where they fall greater than the high tolerance levels.

Figure 4. Example of qualitative risk appetite zones

ZONE	MEANING AND REQUIRED ESCALATION AND RESPONSE
Green	Within appetite, no action required. No escalation or specific response required. Non-urgent consideration may be given to assessing reward against risk and ensuring balance is right for risks and rewards in this zone.
Amber	Within appetite, raised attention. Escalation to board as part of the board reporting process together with an explanation as to why the risk and/or reward is in amber. Consideration to be given by the board as to ongoing acceptance of risk in amber or direction to reduce to green, dependent on the balance between risk and reward.
Red	Outside of appetite, action required. Escalation to executive management immediately and escalation to board latest at the next meeting or earlier as decided by the executive management. Actions required to be formulated to achieve at least amber as soon as possible.

Figure 5. Example of zones used to evaluate quantitative risk tolerances

4. Setting qualitative risk appetite for each objective. This should use the qualitative risk scales, e.g. Zero, Low, Medium, High to articulate the level of variation you are willing to accept regarding each objective. For example:

- Customer Satisfaction: Low. This implies we will only accept minimal variation on the downside for customer satisfaction levels.

- Profit: High. This implies we are willing to accept a wide variation to the profit target.

This may be because we are trying new markets and new innovations which are untested.

5. Setting thresholds for KPIs. Using the red/amber/green zoning noted above. This requires the setting of the green to amber threshold and the amber to red threshold.

OBJECTIVE	MEASURABLES	TARGET	APPETITE	GREEN TO AMBER	AMBER TO RED
Return on Equity	ROI	15%	Low	14.2%	13.8%
Customer Service	Net Promoter Score	85%	Medium	80%	72%
	% of customers with repeat business	60%	Medium	54%	43%
Compliance	Compliance breaches	0%	Zero	1	1
Employee well-being	Lost time injury frequency rate	1.2	Low	1.1	1.0

Figure 6. Example of setting appetite and tolerance for Objectives

6. Setting qualitative risk appetite for each key risk. This should also use the qualitative risk scales, e.g. Zero, Low, Medium, High to articulate the level of risk you are willing to accept. For example:

- Compliance Risk: Zero. This implies you are not willing to accept any compliance breaches.

- Strategic Risk: High. This implies you are

willing to accept a high amount of strategic risk and this would support innovation into new markets and new products, with an increased risk of strategy failure.

7. Setting thresholds for KRIs. Using the red/amber/green zoning noted above. This requires the setting of the green to amber threshold and the amber to red threshold.

OBJECTIVE	MEASURABLES	APPETITE	GREEN TO AMBER	AMBER TO RED
Market Risk	Unhedged FX positions	Low	USD 1m	USD 1.5m
Technology Risk	% of systems near end of life	Medium	10%	20%
	System outages	Medium	2% p.m.	4% p.m.
Cyber Risk	Number of successful intrusions	Low	1	2
HR - Quality and Quantity Risk	Unforced staff turnover	Medium	15%	22%
Strategic Decision Risk	Number of strategic decisions aborted after made %	High	20%	30%

Figure 7 Example of setting appetite and tolerances for Key Risks
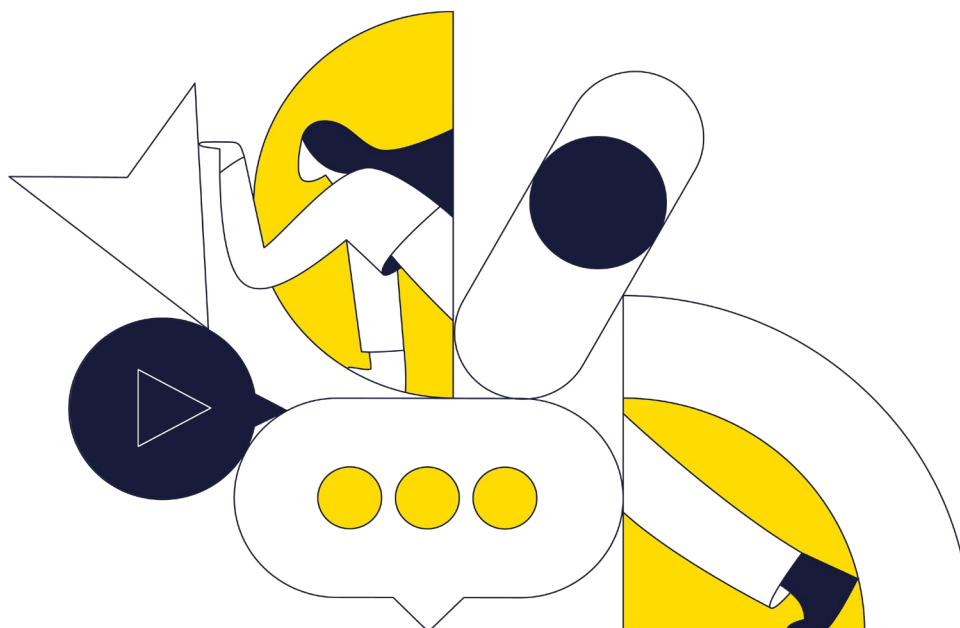
Operationalizing and using risk appetite across the organization.

In order to ensure the boundaries for risk taking are known by all employees, especially decision makers, the RAS needs to be articulated in a manner that employees will understand and be able to be used to measure risk against. This can be achieved in a number of ways.

Articulating and communicating the risk appetite

- The board-level RAS

- The Risk Appetite Policy Statement. This usually forms part of the ERM policy.

- The various artifacts that are used to cascade and operationalize the risk appetite across the business operations. Depending on the size and nature of the organization, and as shown in Figure 3, these may consist of one of more of the following :

› **"Mini" RAS**. These would typically be used in larger organizations and groups and would operate at the subsidiary/divisional level. They are tailored statements for each subsidiary/division based on the group RAS.

› **Values and Commitments.** Many aspects of the values and commitments of an organization refer to risk taking behavior and the general boundaries expected for staff behavior.

› **Code of Conduct.** The code of conduct should clearly articulate boundaries for staff behavior, linked to risk appetite.

› **Key Risk Indicators (KRIs).** A robust set of KRIs across business operations are a key element in cascading the risk appetite tolerances set at board level.
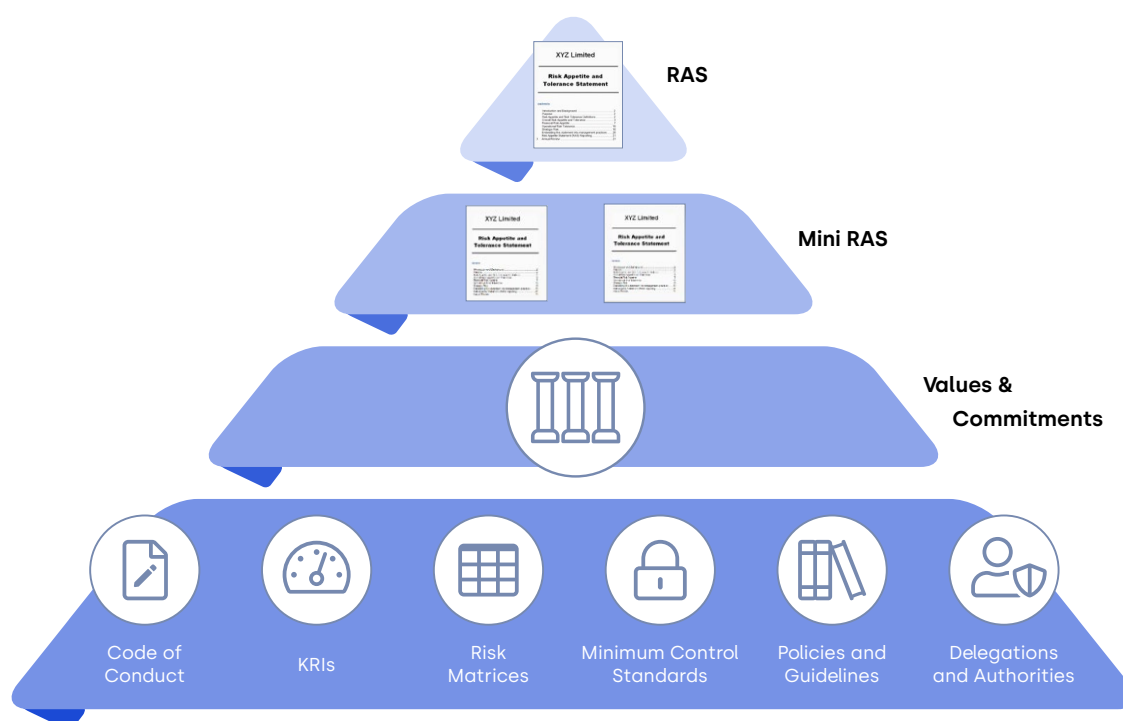

Figure 8. Artefacts to operationalise the RAS

› **Risk Matrices.** The traditional risk matrix, where risk is measured using a qualitative assessment of likelihood and consequence, is often used as a basis of setting risk boundaries and evaluating risk for subsequence escalation and response action.

› **Minimum Control Standards.** These, where implemented, should reflect the risk appetite of the organization but be expressed, not directly based on the risk but instead on the minimum level of control required over that risk. For example, the requirement to wear a minimum amount of Personal Protective Equipment (PPE) in certain situations would reflect the risk appetite for safety related risk.

› **Policies, Standards and Guidelines.** Internal policies, standards and guidelines are a common way to communicate risk appetite in a meaningful way so that staff understand the boundaries within which they need to operate. These should be written in line with the board-level risk appetite.

› **Delegations of/and Authorities.** Delegations and authorities are a very powerful and understandable way to cascade risk appetite through the organization. They also reflect the fact that as risk appetite is cascaded through the organization, the risk appetite will reduce the lower the level of the organization and the less senior is the manager.

For risk appetite to be successfully deployed across the organization, it is essential that all of the artifacts are synchronized and consistent with each other and most importantly with the board-level risk appetite. This does require recalibration of these artefacts when changes are made to risk appetite.

Escalating and reporting based on risk appetite

In order to close the loop back to the board, the key risks needed to be monitored, measured and evaluated against risk appetite. This evaluation is then used to form the basis of board, committee and executive risk reporting. The principle used should ideally be dashboard reporting with drill down capability.

8
Overdue reviews

10
Pending reviews

17
Completed reviews

Risk Appetite Statements
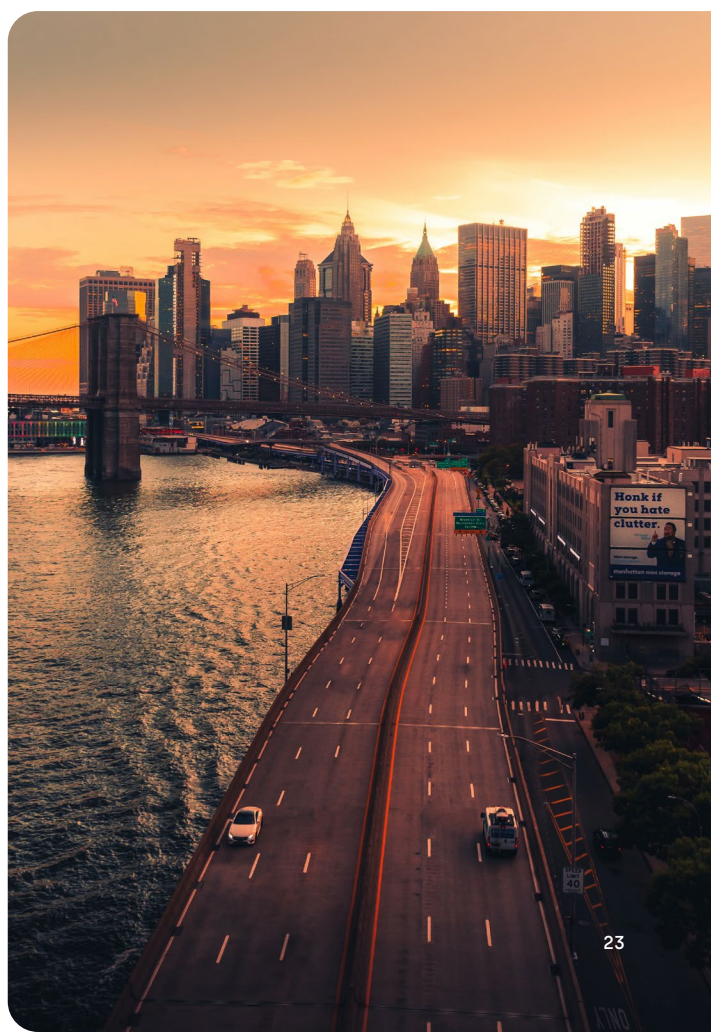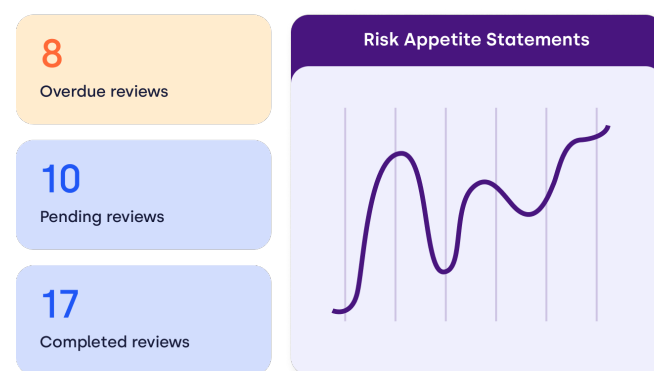
Steps to develop your risk appetite.

So where do you go from here if you wish to develop and improve your risk appetite? We would suggest the following:

a. **Carry out a current state assessment. Where are you now?** This would include such things as:

- Do you have a current RAS?

- What is the quality of your Strategic and Business Plan?

- Are objectives well articulated?

- Are all objectives able to be measured with identified KPIs?

- Have targets been set for each KPI?

- What is the level of understand and knowledge of executive management, board and staff over risk appetite concepts?

- How well developed is the articulation of your board-level risks and central risk taxonomy?

- What existing artefacts do you have which include elements of risk appetite (e.g. Policies, Codes of Conduct etc.)?

- What current systems capability do you have to collect, evaluate and report on risk appetite measures, e.g. KRIs?

- What is the current quality of risk reporting?

b. **Determine a future state - where do you want to get to and by when?**

- What is the required content of the RAS? (refer Section 6)

- What do you want/need your Strategic Plan and Business Plan quality to be and what is required in terms of KPI setting and monitoring?

- What is the required level of understanding and knowledge required of your board, executive management and Staff?

- What is your required risk taxonomy?

- What range of artefacts will you use for communicating risk appetite?

- What systems do you required to collect, measure and evaluate risks?

- What risk reporting do you want against risk appetite?

- How do you want to use risk appetite? e.g. for Assurance, Decision Making etc.

Your ultimate aim is to create well-understood and communicated boundaries within which your staff feel safe to operate and make decisions. This will empower staff and provide confidence to the executive and board that any excess risk will be quickly identified, reported and rectified.

David Tattam

Chief Research and Content Officer

David Tattam is the Chief Research and Content Officer and co-founder of the Protecht Group. David's vision is to redefine the way the world thinks about risk and to pioneer the development of risk management to its rightful place as a key driver of value creation in each of Protecht's clients. David is the driving force behind Protecht's risk thinking, pushing risk management to the frontiers of what is possible. He is also focused on driving the uplift of people risk capability through training and content.

David is passionate about risk and risk management and in reaping the value that risk and good risk management can create for any organisation willing to embrace it. He is particularly passionate about risk management research and is prolific in creating a wide range of content delivered in blogs, ebooks, webinars and training courses. He has developed Protecht's comprehensive suite of risk management training courses and has, and continues, to train many thousands of risk practitioners across the globe. David also manages Protecht's consulting business offering a range of risk consulting capabilities from Risk Management Framework to Risk Appetite Statement development.

He is also the author of "A Short Guide to Operational Risk".

Prior to co-founding Protecht, David was the Chief Risk Officer and Head of Operations for the Australian operations of two global banks. He started his career as a Chartered Accountant and Auditor with Grant Thornton and PwC. David is an Associate of the Institute of Chartered Accountants in Australia and New Zealand and a Senior Fellow of the Financial Services Institute of Australia.

ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 20 years, we have redefined the way people think about risk management with the most complete, cutting-edge and cost-effective solutions.

Protecht helps companies increase performance and achieve strategic objectives through better understanding, monitoring and management of risk. We provide the complete risk solution, comprised of world class enterprise risk management (Protecht.ERM), compliance,

training and advisory services to large government organisations, key regulators and businesses of all sizes across the world.

Dynamically manage all your risks in a single platform: Risks, Compliance, Health and Safety, Internal Audit, Incidents, KRIs, BCP, and more.

We're with our clients for their full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

AUSTRALIA & ASIA PACIFIC

+61 2 8005 1265
Level 8
299 Elizabeth St.
Sydney NSW 2000
Australia

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 20 3978 1360
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

NORTH AMERICA

+1 (833) 328 5471
4470 W Sunset Blvd
Suite 107
PMB 95227
Los Angeles California 90027

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com