Risk Management Policy

VRS ANA Pty Ltd
trading as
ANA Loss Adjusters
ABN 78 163 470 255

Level 25, 100 Mount Street
North Sydney, NSW 2060

Phone (02) 8459 7056

manager@ana.net.au
www.ana.net.au

Version 4.1
Updated 15 December 2023

The identification of risk and the development of risk mitigation strategies is sound business practice, but the insurance industry has long learned that the best guide to risk is history. Incident rates. Claim rates.

We are thoroughly prepared to respond to adverse events, but the best strategies are to reduce the risk of them happening.

ANA's success in avoiding adverse events is due to its unique, foundational difference: the use of only the most qualified, most experienced, most proven Adjusters, with a business-wide focus on service quality.

We implemented and promoted that philosophy against an industry trend to price driven adjusting based on reduced skill sets, because we believed that better service would be worth it to Insurers.

Our belief has also proven worth it to ANA, making us a stronger, safer business. Training and experience are the most effective tools for mitigating risk.

Contents

Introduction

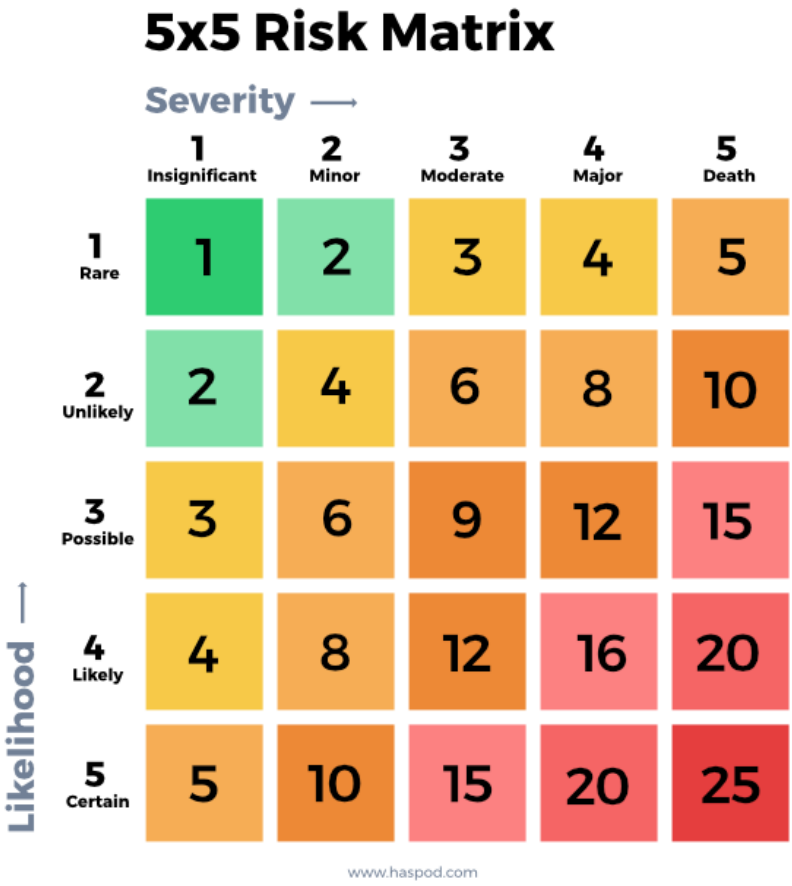
Risk management policy determines how risks to the company are identified and what action is taken in regard to them, including prioritising, actions, training, tracking and ongoing development.

The first step is a risk assessment, which determines possible mishaps, their likelihood and consequences, and the tolerance for such events.

Risk assessments commonly use a matrix assessing the severity of consequences against the likelihood of occurrence to produce a Business Impact Score.

ANA uses a popular matrix published by Haspod, a risk management consultancy, which results in a Business Impact Score range from 1 (rare events of insignificant impact) to 25 (events that are certain to happen and may cause death or business closure).

In applying the matrix, ANA pays primary attention to impacts on the continuity of business services to our clients. Continuity of service provision is the critical requirement (and, in a sense, the definition) of business continuity and disaster recovery at ANA.



Risk management structure

Risk is inherent in everything we do, so each manager has a responsibility for risk awareness and management within their area, whether territorial (by state) or subject (eg, cyber, financial etc).

Local/subject manager responsibility includes:

- Ensuring their staff have a risk-aware, pro-active culture.
- Ensuring staff know and follow risk policies.
- Encouraging staff to notice and report emerging new risks and changes to known risks.
- Reporting new risk factors and changes in risk factors to the Risk Management Committee (RMC) via the Manager – Compliance, along with suggestions for improving risk management.

Risk awareness is included in inductions and training for all staff. All staff are charged with reporting new risk factors and changes in risk factors to their manager. ANA risk management starts from the bottom and works up.

The Manager – Compliance has overall responsibility for organisation wide risks and risks spanning more than one area of management responsibility.

The Manager – Compliance chairs the Risk Management Committee.

The Risk Management Committee:

- Has a minimum of three members excluding ex officio members.
- The CEO and Managing Director are ex-officio members.
- Includes at least one staff representative.
- Members may be external to ANA (eg, contractors), chosen for their expertise.
- The Manager – Compliance may invite others (eg, external experts) to attend meetings of the Committee and may invite Clients to attend parts of meetings relating directly to them.
- The other members of the RMC are selected by the Manager – Compliance and recommended to the CEO for approval.
- The RMC meets at least once a quarter depending on need. Meetings may be virtual. Minutes will be compiled and distributed to all staff (sensitive content may be redacted) in order to encourage a risk-aware culture.

Membership of the RMC and its work is reviewed annually by the CEO in consultation with the Manager – Compliance.

Responsibilities of the RMC include:

- Compilation, ongoing maintenance and annual review of a *Risk Assessment and Business Impact Statement* that identifies, lists and assesses the potential business impact of all risks affecting ANA, particularly risks to the delivery of Client services. The statement is included in this policy.
- The creation, implementation and enforcement of policies to mitigate identified risks.
- Promoting risk awareness throughout the organisation, including recognition of identified risk factors, sensitivity to and reporting of new and changed risks.
- Distribution of the Risk Assessment, ANA risk management policies and minutes of RMC meetings to staff.
- Ongoing advice to the CEO on the risk environment and possible actions to improve ANA's risk management.
- Review and updating of this policy.

- The RMC also has charge of the maintenance, updating and promotion to staff of the *Business Continuity and Disaster Recovery Plan*. Managers can make suggestions regarding the Plan direct to the RMC. Staff are encouraged including through training to inform and make recommendations to their managers.
- The RMC supports the Manager – Compliance to produce an annual *Risk Management Report*.

Each July the Manager – Compliance, supported by the RMC, makes a written report on Risk Management to the CEO, that includes:

- A review of the *Risk Assessment and Business Impact Statement*, noting especially any emergent risks and risks that are becoming more significant.
- A review of this *Risk Management Policy* and recommendations for improvements. This includes supporting policies:
    - *Third Party Risk Management*
    - *Change Management*
    - *IT Security*
    - *Building Supplier Quality Assurance Protocols*
    - *COVID-19/Pandemic policy*
    - *Training*.
- A review of risk management suggestions submitted by staff and other managers to the committee.
- A review of all adverse risk outcomes for the year, with analysis and recommendations.
- A specific review of risk management in relation to third party suppliers, commenting on ways that risk management policies can help ANA get better third-party supplier contributions and ways in which the compliance burden on third party suppliers can be reduced (for example, through situation-specific and automated forms).

Where there are other internal reports specifically covering a risk area the *Risk Management Report* may comment on and refer to these reports without repeating their content.

Risk Assessment and Business Impact Analysis

The Risk Assessment and Business Impact Analysis is created by the Risk Management Committee reviewed in full at least annually by the Manger – Compliance.

You may request a copy of the current risk assessment via manager@ana.net.au.

The current business risk assessment and impact analysis identifies the major risks for ANA as:

- Pandemic risk
- Third Party risk
- Cyber security failure

Each of these major business impact areas is dealt with under its own policy, available on request. These policies are under the control of the Risk Management Committee.

Pandemic risk management

Pandemic is a high impact event with a very high probability of occurrence.

The COVID-19 pandemic demonstrated just how (unexpectedly) devastating a pandemic could be, but it also enabled significant learning by governments, health authorities and businesses.

ANA responded early to the COVID-19 with a policy that emphasized disease control and a ramping up of remote working capabilities, so disruption of client services was minimal.

When the next pandemic of COVID-19 proportions hits, ANA will be better equipped, and hopefully better supported by health services responses, to continue without any significant service interruption.

See the separate ANA *COVID-19/Pandemic Policy*. It governs ANA's risk management in relation to pandemics.

Third Party (Supplier) Risk Management

Third party risks is identified as second to the pandemic risk in total impact, but unlike the intermittent risk of a pandemic, Third Party risk is omnipresent and multiple, so management of it must be continuous.

The separate ANA *Third Party Risk Management Policy* governs ANA's risk management in relation to third parties. This policy is commercial-in-confidence, you can request a copy.

Cyber security risk management

Information security breaches have the third highest business impact score at 15, but are by far the most virulent, frequent threat for any business dependent on information. While pandemic and third-party risk are stable or even reducing (in response to mitigation measures), cyber risk is increasing rapidly.

While pandemic risks pit a business against nature and third-party risks are mostly from individuals, cyber is a 24/7 war against a well-resourced, organised human enemy.

ANA has and continues to invest heavily in cyber security. We have achieved a very secure position, but continue to move forward, knowing that cyber criminals are constantly evolving stronger attack tools.

See the separate ANA *IT Security Policy*. It governs all aspects of ANA's risk management in relation to IT, information and cyber.

Maintaining Client Services

ANA is a very successful company. It earns its income by delivering services clients buy and buy again. The only event guaranteed fatal to ANA is if it stops receiving customer instructions, and thus income.

Delivering clients services that meet client expectations is the lifeblood of the business.

The business is structured to facilitate and protect client services, particularly its enabling of remote work, structured monitoring of wok flows through process mapping and its protection of client data.

This risk management policy evaluates and responds to risk from a client services perspective.

The result is that measurable (ie, historic) risk to continuity of client services is very low.

Risk Assessment Policy maintenance and review

The Risk Management Committee, under the direction of the Manager – Compliance, has responsibility for ongoing updating and annual review of this policy, including production of an annual report on risk management and outcomes.

Ongoing updates are managed through committee meetings held at least quarterly.

Staff are encouraged through training to contribute observations and ideas on risk management.

Other policies dealing with risk

All policies should aim to reduce risk by reducing uncertainty/indecision and guiding the best outcomes. The total risk response of an organisation is thus reflected in all its policies.

Of particular importance to risk management for ANA are its:

- *Anti-corruption and Fraud Policy*
- *Bribery Policy*
- *Building Supplier Quality Assurance Protocols*
- *Business Continuity and Disaster Recovery Plan*
- *Change Management Policy*
- *Complaints Policy*
- *IT Security Policy*
- *COVID 19/Pandemic Policy*
- *Modern Slavery Policy*
- *OHS Policy Manual*
- *Privacy Policy*
- *Quality Management System*
- *Third Party Risk Management Policy*
- *Training Policy*
- *Vulnerable Customer Policy and Training*