National disabilityinsurance Agency

Risk Management Strategy

National Disability Insurance Agency Board

21 February 2014

Contents

1. Introduction

The National Disability Insurance Agency (NDIA; the Agency) Board has established a comprehensive Risk Management Strategy (the Strategy) as an integral part of the Board's broader Risk Management Framework. This Strategy has been prepared in accordance with *National Disability Insurance Scheme—Risk Management Rules 2013* (the Rules).

The Strategy is structured to align with requirements in rule 8 of the Rules, including:

- outlining the risk governance relationship between the Board, committees of the Board and the senior management of the Agency;
- describing the processes for the Agency to identify and assess risks, establish mitigation and control mechanisms for individual risks and monitoring and reporting issues in relation to risk;
- describing how the NDIA will raise staff risk awareness and develop an appropriate risk culture;
- setting out specific risk management roles and responsibilities and establishing a process to review the effectiveness of the framework; and
- describing the annual review process by which the Agency will assess the effectiveness of its risk management framework in identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating, material risks.

2. Risk Governance

Risk Management Rules Reference: rule 8(a) Outline the risk governance relationship between the Board, committees of the Board and the senior management of NDIA

Risk management is a fundamental responsibility for all managers and staff. At its core, risk management is about management and staff doing their jobs well and contributing to achieving the Agency's objectives.

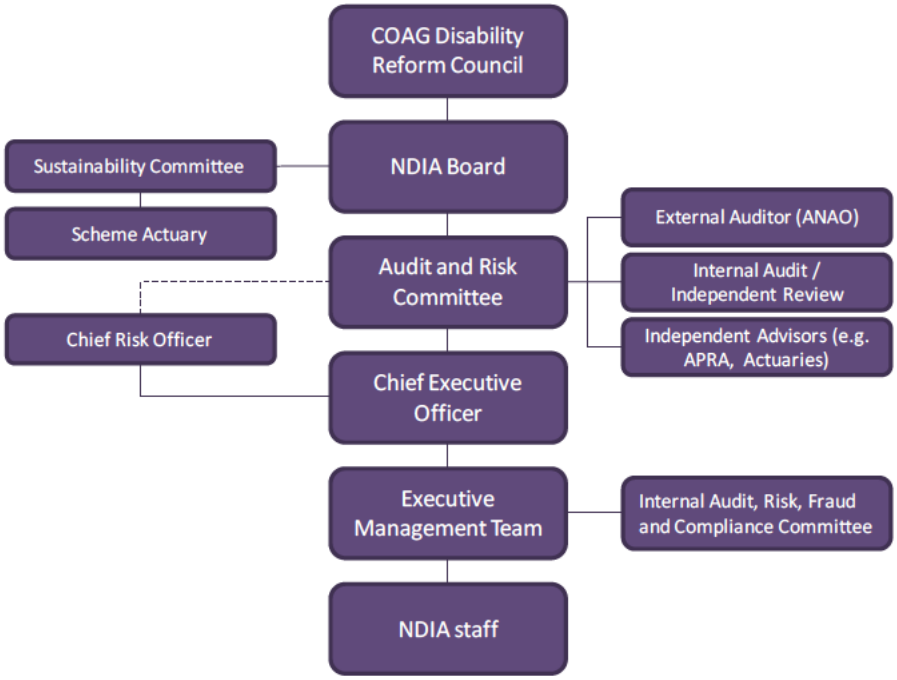
Managers at all levels are responsible for satisfying themselves that the key risks relating to their area of business are being managed appropriately and that they can provide assurance of this where required.

More specifically, as part of NDIA's risk governance arrangements:

- The Chief Executive Officer (CEO) has overall responsibility for how risks are managed by the Agency
    - The CEO and Executive Management team meet regularly as the Strategic Risk Committee to monitor risks to the achievement of the Agency's strategic plans and goals, and the management of strategic risks identified by the Board;
- The Executive is responsible for ensuring key risks to NDIA's objectives are identified, understood and adequately managed;
- The Audit and Risk Committee is responsible for monitoring the risk management process and providing independent assurance and assistance on risk management to the Board;
- The Sustainability Committee is responsible for monitoring and reporting to the Board on the sustainability of the National Disability Insurance Scheme (NDIS; the Scheme) and whether Scheme objectives are being met;
- Processes and procedures have been put in place to ensure that areas of responsibility are clearly defined between the Audit and Risk Committee and the Sustainability Committee to ensure all risks are encompassed and monitored;
- The Board, in consultation with the CEO, determines, communicates and reviews the NDIA's risk appetite in response to its dynamic operating environment;
- The Internal Audit, Risk, Fraud and Compliance Committee is responsible for internal advice and assurance to the Executive Management team and CEO on relevant matters within the Agency; and
- The Board makes an annual declaration to the COAG Disability Reform Council (CDRC) on the appropriateness and effectiveness of the Strategy.

The Board's and Agency's risk governance arrangements are illustrated in Figure 2.

Figure 2: Risk governance arrangements



A list of key roles and responsibilities is outlined in section 6 of this document.

The governance framework enables the management of risk to be integrated into all key business functions, processes, systems, programs and projects. It also provides a sound foundation for the Board and the CEO to make informed decisions which assure that proper controls are in place and that risks are well managed.

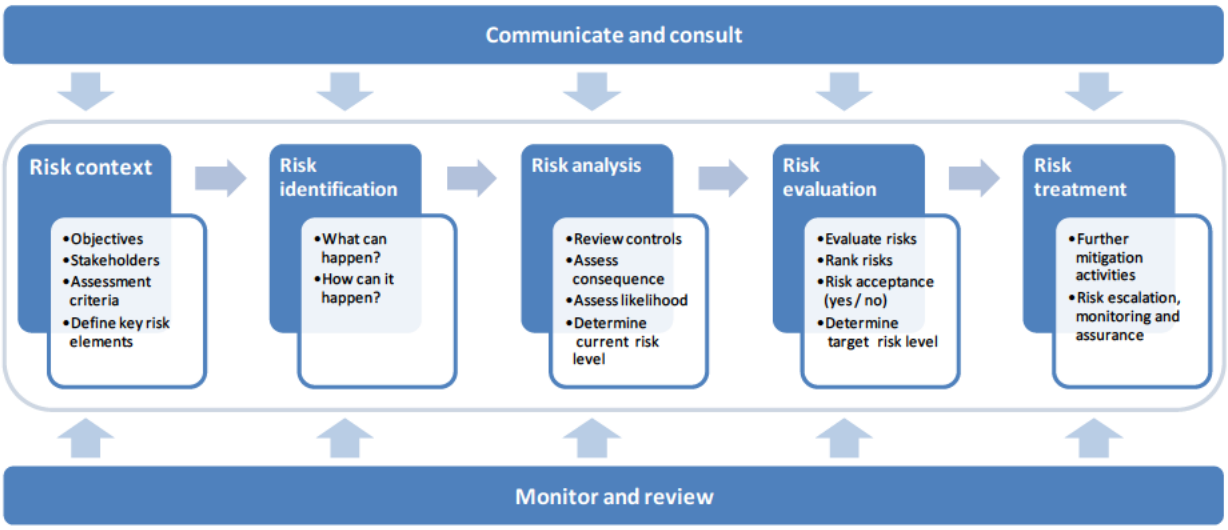
Risk influences the outcome of work at every level of the NDIA's operating environment, so staff at all levels carry responsibility for managing risk. As part of implementing this Strategy, the Board has required Management to incorporate a risk management methodology in its business planning and performance evaluation processes, enabling managers and others to identify, communicate and treat risks at the strategic, enterprise and operational levels.

3. Processes to identify, mitigate and control risks

Risk Management Rules Reference: rule 8(b) Describe the processes for NDIA to identify and assess risk; and 8(c) Describe the process for the NDIA to establish mitigation and control mechanisms for individual risks.

The Agency's risk management process is illustrated in Figure 3 and comprises five key steps to be applied to any risk process being undertaken within the NDIA.

Figure 3: National Disability Insurance Agency risk management process overview



Management and staff will be provided with the appropriate tools and training to assist them in assessing the risks they face. In turn, risk management planning will be an integral part of business planning, project management, contract negotiations and reporting against significant initiatives. The steps that Management and staff will go through in the risk management process are:

- Establish Context – stating the specific risk objectives for the assessment up front, and as clearly as possible, to identify risk areas precisely and consider their potential impact on Scheme outcomes.
- Identify risks – considering the context of the operations and reviewing as many sources of risk as possible, to identify the risks that could impact on the achievement of the Agency's objectives. Because unidentified risks can always pose a major threat, it is important to take care to ensure that the Agency maintains an open perspective on all possible threats and opportunities.
- Analyse risks – for each of the risks identified, describe how the risk might occur, what might happen if it did, and what influences already exist that mitigate it. This, in turn, facilitates a decision around the *likelihood* and *consequence* of a risk occurring to develop a risk rating.
- Evaluate risks – from the risk rating, determine whether a risk is one that is *acceptable or unacceptable*. This ensures focus on the risks of greatest overall impact to, and those that need the most immediate attention by, the Agency and the Scheme.
- Treat risks – drawing on the information gathered on each risk, choose to address or *treat* risk in a number of ways – to accept it, to avoid it, to reduce it or to transfer it. However it decides to treat the risk, the Agency must *document* what it plans to do, and then do whatever it has said it will do.

The risk assessment criteria, which translates the risk appetite statement into a consequence rating that staff can apply to individual risks is supplied to all staff through the Chief Risk Officer.

It is also important to recognise that specialist risk assessments will be undertaken from time-to-time as required by specific Commonwealth legislation with which the NDIA, as a *Commonwealth Authorities and Companies Act 1997* (CAC Act) agency, must comply. Examples include Business Continuity Management, Workplace Health and Safety, Fraud Control and Protective Security. In these instances the process by which the Agency identifies and assesses risks may vary to comply with legislative requirements, applicable international standards and best practice.

4. Monitoring and reporting risks

Risk Management Rules Reference: rule 8(d) Describe the process for monitoring and reporting issues in relation to risk (including the communication and escalation of such issues)

The NDIA's risks will be monitored and reported at a strategic, operational and project level, as illustrated in Figure 4.

Figure 4: Approach to risk monitoring and reporting

Key elements of the NDIA's monitoring and review arrangements are:

- The NDIA's strategic risks will be identified and assessed by the Board annually and reviewed by the Audit and Risk Committee at each meeting
    - The management of particular risks, identified by the Board, may be reported more frequently to the Board if appropriate;
- The Risk Management Framework, function, strategy, controls and procedures will be subject to an independent review by operationally independent and suitably trained persons;
- The Board will provide annual declarations on the adequacy and effectiveness of risk management and compliance activities, as required by rr 7 and 10 of the Rules;
- The Sustainability Committee will review risks associated with Scheme sustainability and client outcomes at each meeting, and report on them to the Board ;
- Operational risks are monitored continually, as part of normal business processes, and reported on a timely basis to the Audit and Risk Committee and Board;
- Targeted risk assessment of specialist risks including, compliance, business continuity, workplace health and safety and fraud risks will be undertaken in accordance with legislative requirements; and
- Project risk assessments will be undertaken for significant projects, specifically including transition to full Scheme, and monitored regularly in accordance with the project governance arrangements established for each project.

5. Risk communication and risk culture

Risk Management Rules Reference: rule 8(e) Describe how the NDIA is to (i) ensure that relevant staff are aware of issues relating to risk, (ii) instil an appropriate culture in relation to risk, and (iii) ensure that the risk management strategy is accessible to the NDIA's staff.

The NDIA will maintain appropriate controls in relation to risks that are consistent with its risk profile. The importance of these will be regularly communicated to staff to ensure they have an appropriate awareness of the broader risk and control environment.

Communication and consultation play an important role in all stages of the risk management process. The effective management of risk and identification of business opportunities cannot be achieved without ensuring all parties with a significant interest, including both internal and external stakeholders, are consulted.

Such consultation ensures that any differences of opinion or different perceptions of the risk are considered, understood and addressed. Similarly, it provides two-way communication to identify opportunities for business improvement. In summary, Agency management is responsible for ensuring that all relevant stakeholders are identified and consulted as appropriate as part of the risk management process.

The Agency's commitment to managing risk is demonstrated by the Board and senior executives and reflected in the organisation's culture and processes. The NDIA's culture of managing risk is a positive one, reflecting recognition of the benefits of managing risk for achieving the Agency's objectives. Understanding, managing and accepting appropriate risk is part of everyday decision-making processes.

The NDIA's approach to risk management is consistent with its organisational objectives, and ensures that as they arise, opportunities for improvement to the Scheme are identified and implemented through prudent, informed and structured decision making and, hence, risk taking. This risk management approach is driven through the Agency's governance framework and supported by clearly articulated accountabilities and the internal risk structure and reporting frameworks.

Continuous risk management learning

The NDIA has a supportive work environment where learning from experience is valued, lessons are shared and learning plans are built into management practices. Risk management is an integral and routine part of all planning processes. Education and awareness support will be provided to all work areas, including regional offices.

Driving a culture of managing risk

The NDIA is committed to developing a positive risk culture where risk is understood and managed by all staff. The development of this culture is driven by the everyday behaviour of the Agency's staff. Elements that contribute to the development of a positive risk culture are:

- all executive managers promote and implement the risk management policy;
- the benefits of risk management are well communicated;
- those who excel in managing risk in their day-to-day responsibilities are recognised and rewarded;
- risk analysis and innovation around managing risk are encouraged in order to understand the benefits and risks of new activities; and
- risk management is integrated with other key processes and systems, ensuring that risk management is part of everyday decision making.

6. Roles and Responsibilities

Risk Management Rules Reference: rule 8(f) Identify persons and positions in NDIA with roles and responsibilities in relation to risk, or groups of such persons and positions, and set out those roles and responsibilities

This section describes the roles of those who are accountable for managing risk effectively within the NDIA.

Position	Roles and Responsibilities
NDIA Board	The Board approves the overall risk strategy, policy and determines its appetite for risk. It receives risk reports by exception and directly monitors the treatment of any risk that falls outside risk tolerances (as communicated in the risk appetite statement), and those of particular strategic importance. The Board, after the end of each financial year of the Agency's operations that commences after 30 June 2013, will provide the COAG Disability Reform Council with a risk management declaration signed by at least two Board members on behalf of the Board.
Chief Executive Officer (CEO)	The CEO has ultimate accountability and overall responsibility for the Agency's performance, including the accountability for management of risk in the delivery of the Scheme's outcomes.
Chief Risk Officer (CRO)	The CRO works with other managers to establish effective risk management in their areas of responsibility. The CRO has independent access to the Audit and Risk Committee and has the resources to help effect appropriate enterprise risk management across divisions, functions, and activities. The CRO has responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down, and across the NDIA.
Executive Managers	Executive Managers are responsible for identifying, documenting, prioritising, monitoring and treating all material risks in their divisions. Executives will implement the risk management strategy and framework, promote and encourage the use of risk management tools and processes in their divisions, ensure risk management plans are regularly reviewed and updated, and monitor risks.
Audit and Risk Committee	The Audit and Risk Committee will oversee the development and implementation of the risk management strategy and the tools and templates to assist staff to implement and practice risk management. On an ongoing basis the Committee will provide assurance to the Board, independent of management, on the effectiveness and efficiency of NDIA's risk management strategy and framework, the identification and management of risks and advise on whether the internal audit plan is 'risk informed'. The Audit and Risk Committee will also notify the Board of any significant breach of, or material deviation from, the risk management strategy or framework.

Position	Roles and Responsibilities
The Internal Audit, Risk, Fraud and Compliance Committee	The Internal Audit, Risk, Fraud and Compliance Committee is responsible for internal advice and assurance to the Executive Management team and CEO on relevant matters within the Agency.
The Sustainability Committee	The Sustainability Committee is responsible for monitoring and reporting to the Board on the sustainability of the Scheme and whether Scheme objectives are being met. It does this through monitoring eligibility and access to the Scheme by participants, any cost increase in the assessment of reasonable and necessary support, cost shifting with mainstream services and price inflation. It also provides advice to the Board on potential changes to the legislation or other regulation.
Scheme Actuary	The Scheme Actuary is involved in decisions made by the Agency and the Board in relation to risk. The Scheme Actuary is also importantly linked with the Sustainability Committee as the first avenue for reporting on the financial sustainability of the scheme. This role is consistent with the duties prescribed In the *National Disability Insurance Scheme – Rules for the Scheme Actuary 2013*.
All staff	All staff carry responsibility for the identification and management of risks that impact on their work areas. All staff should recognise, communicate and respond to expected, emerging or changing risks and contribute to the development and implementation of risk treatments. In practice, this means that NDIA staff: • must be familiar with the Agency's risk management strategy and policy; • will be encouraged to alert their managers to the presence of risks and participate in their management; • will be encouraged to make use of the tools available to them so that they are better able to identify and manage risks in the workplace; and • both understand and support scheme participants through applying dignity of risk principles.

Risk function

The Agency's Chief Risk Officer (CRO):

- is responsible for providing assistance to the Board, committees of the Board and the senior management of the Agency to develop and maintain the risk management strategy and framework;
- will be maintained in line with the size, operations and complexity of the NDIS;
- is operationally independent, meaning that it has no direct involvement in the Agency's functions in relation to the funding or provision of supports under the NDIS;
- is able to brief the Board, committees of the Board and senior management of the Agency necessary to conduct its activities effectively and independently;
- is staffed by employees with relevant qualifications and experience to deliver their clearly defined roles and responsibilities;

- has access to all aspects of NDIA that have the potential to generate material risk, including information technology systems and system development resources; and
- is tasked with notifying the Board of any significant breach of, or material deviation from, the risk management framework in a timely and effective manner.

The CRO also has responsibilities for management of internal audit and fraud, consistent with the ANAO's Better Practice Guide on Internal Audit.

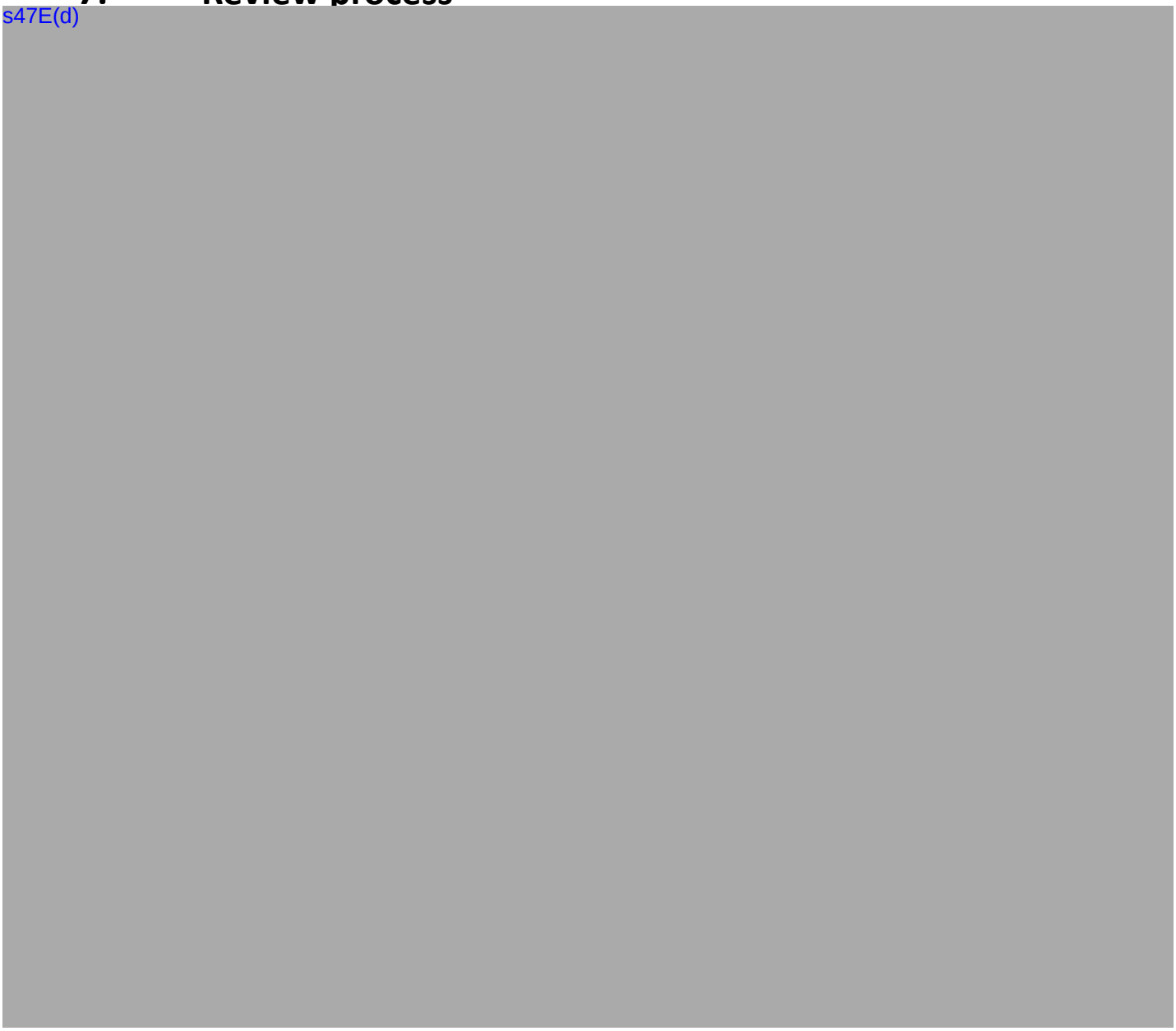
Risk assessment and reporting support

The Agency's risk management arrangements will be supported by the CRO, who will:

- maintain Risk Management Framework documentation, ensuring this is provided to staff in a format and location that is easily accessible;
- facilitate the development of individual strategic, divisional and specialist risk management plans;
- maintain a repository of risk management plans;
- design and compile risk management reports, as required, to meet the needs of the Board, the Audit and Risk Committee and the NDIA Executive; and
- provide risk management training to management and staff in order to improve risk awareness and aid the consistent application of risk management processes.

7. Review process

s47E(d)



National disabilityinsurance Agency

National Disability Insurance Agency
Risk Management Strategy

September 2015

Contents

Risk Management Strategy

Risk Context

Consistent with the responsibilities of a Board as articulated in CPS 220, and in accordance with section 8 of the *NDIS Risk Management Rules*, the Board formulates a Risk Management strategy for the Agency.

The Board's approach is to ensure that risk management is integral to the way the Agency conducts its business. In this way, the Board seeks to ensure that the benefits of a structured approach to risk management are realised.

The Board develops the NDIS Strategic Plan (with a three year horizon), identifies key risks to achieving the objectives of the Strategic Plan (the Strategic Risks), and then articulates its attitude towards the management of them through the Risk Tolerance Statement.

Of particular importance is ensuring that risks to the achievement of the Board's strategic objectives are adequately addressed through the Agency's business planning processes.

Identifying risk during the business planning process allows the Board to set realistic delivery timelines for strategies and activities, or to choose to remove a strategy or activity if the associated risks are too high or unmanageable

The Agency Corporate Plan, approved by the Board, sets out annual Agency-wide priorities for action that give effect to the objectives of the Strategic Plan, including priorities for the management of the Strategic Risks.

Responsibility for managing each Strategic Risk is allocated to members of the Executive (CEO, Deputy DEO and General Managers) in the Agency Corporate Plan. Cascading from the Agency Corporate Plan are Divisional and Branch/ Site Business Plans, and, where appropriate, Section Business Plans. Each of these plans also has a twelve month horizon.

In their Divisional Business Plans, General Managers identify, and outline management strategies for, operational risks that sit below each Strategic Risk. Operational risks are, essentially, the risks to "business as usual" deliverables that contribute to the achievement of strategic objectives.

Additionally, the Board has identified a number of projects of strategic significance – projects where additional, time-limited effort is needed to ensure the achievements of objectives. These projects are monitored by the Board separately from regular management performance reports.

Risks to the successful delivery of projects are assessed and treated as part of the project risk management process, with accountability vested at the General Manager level.

Although individual members of the Executive manage strategic, operational and project risks, information about the risks, existing controls, mitigation strategies, and progress with implementing any remedial actions is collated centrally by the Chief Risk Officer. Regular reports are provided to the Audit and Risk Committee and to the Board.

Risk Governance

The Board is ultimately responsible for ensuring efficient and effective risk management in the Agency.

The Board fulfils its responsibilities for managing risk with advice from the Audit and Risk Committee, which is responsible for monitoring the risk management process and providing independent assurance and assistance on risk management to the Board.

The Sustainability Committee pays particular attention to the management of risks around financial sustainability including the achievement of outcomes by participants.

In addition, a specialist ICT Committee has been established to oversee delivery and management of risks associated with development of a fit-for-purpose ICT system during the Scheme roll-out phase.

Recognising the importance of managing prudential risk, the Audit and Risk Committee and the Sustainability Committee work closely to ensure risks identified by the Scheme Actuary are integrated into broader Agency-wide risk management mechanisms.

The NDIS Act and Rules emphasises the Scheme Actuary's role in assessing the financial sustainability of the scheme and advising the Agency and Board of any risks to financial sustainability. Specifically under Section 180B of the NDIS Act and Rules, the Scheme Actuary in an annual report must:

- Assess the financial sustainability of the Scheme.
- Assess risks to that sustainability, consider the causes of any risks, and discuss recommendations to manage or address these risks.
- Include in an annual financial sustainability report a discussion of the Agency's risk management arrangements (all systems, structures, cultures, processes, policies and people that identify, assess, mitigate and monitor all sources of risk, both internal and external to financial sustainability) and any recommendations in relation to any inadequacies.

The Scheme Actuary has broad oversight of all risks identified and the processes for mitigating these risks through involvement in the following committees:

- Assurance, Audit and Risk Committee (a Management committee which reviews reports on operational risks, and identifies new and emerging operational risks);
- Executive Management Group (which reviews reports on strategic risks and identifies new and emerging strategic risks);
- ICT Committee (sub-committee of the Board);
- Audit and Risk Committee (sub-committee of the Board); and
- Sustainability Committee (sub-committee of the Board).

The Chief Executive Officer (CEO) has overall responsibility for how risks are managed by the Agency. The CEO and Executive Management Group (EMG) meet quarterly to monitor risks to the achievement of the Agency's strategic plan and the management of strategic risks identified by the Board.

In line with the three lines-of-defence risk governance model identified by APRA in CPS 220, the CEO and Executive Management Group are responsible for ensuring that risk ownership is clearly defined and that the risk management framework is effectively implemented and supports decision-making.

Managers at all levels – risk owners - are responsible for satisfying themselves that the key risks relating to their area of business are being managed appropriately and that they can provide assurance of this where required.

The governance framework enables the management of risk to be integrated into all key business functions, processes, systems, programs and projects. It also provides a sound foundation for the

Board and EMG to make informed decisions which assure that proper controls are in place and that risks are well managed.

Key roles and responsibilities for staff at all levels in the Agency, as well as Board members, are summarised in Table 1 below.

Table 1: Risk Management Roles and Responsibilities

Position	Roles and Responsibilities
NDIA Board	The Board approves the overall risk strategy, and determines its appetite and tolerance for risk. It receives strategic risk reports quarterly and directly monitors the treatment of any risk that falls outside risk tolerances (as communicated in the risk tolerance statement). At the end of each financial year of the Agency's operations, the Board provides the COAG Disability Reform Council with a risk management declaration signed by at least two Board members on behalf of the Board.
Audit and Risk Committee	The Audit and Risk Committee oversees the development and implementation of the risk management strategy and the tools and templates to assist staff to implement and practice risk management. On an ongoing basis the Committee provides assurance to the Board, independent of management, on the effectiveness and efficiency of the Agency's risk management strategy and framework, the identification and management of risks and advises on whether the internal audit plan is 'risk informed'. The Audit and Risk Committee also notifies the Board of any significant breach of, or material deviation from, the risk management strategy or framework
Sustainability Committee	The Sustainability Committee is responsible for monitoring and reporting to the Board on the sustainability of the Scheme and whether Scheme objectives are being met. It does this through monitoring eligibility and access to the Scheme by participants, increases in the cost of reasonable and necessary support and achievement by participants of their individual goals. It also provides advice to the Board on potential changes to the legislation or other regulation.
ICT Committee	The ICT Committee is responsible for monitoring the development and delivery of a fit-for-purpose ICT system, for the roll-out phase of the Scheme. It also advises the Board on risks and inter-dependencies of the programme.
Scheme Actuary	The NDIS legislation emphasises the Scheme Actuary's role in assessing the financial sustainability of the Scheme and advising the Board of any risks to financial sustainability. In carrying out this responsibility, the Scheme Actuary works closely with the Sustainability Committee. Risks identified by the Scheme Actuary, either to financial sustainability or to the achievement of participant outcomes, are fed into the Agency's risk management process.
Chief Executive Officer (CEO)	The CEO has ultimate accountability and overall responsibility for the Agency's performance, including the accountability for management of risk in the delivery of the Scheme's outcomes.
General Managers	General Managers are responsible for identifying, documenting, prioritising, monitoring and treating all material risks in their divisions. Executives will implement the risk management strategy and framework, promote and encourage the use of risk management tools and processes in their divisions, ensure risk management plans are regularly reviewed and updated, and monitor risks.

Position	Roles and Responsibilities
Risk Owners	Risk owners – usually General, Branch or Site Managers – are responsible for the implementation and ongoing maintenance of the risk management framework, including the identification and effective management/mitigation of risks, and issues identification, recording, escalation and management.
Chief Risk Officer (CRO)	The Chief Risk Officer assists the Board and senior management by providing independent and objective review and challenge, oversight, monitoring and reporting in relation to risk to the Agency's business operations. The CRO works with other managers to establish effective risk management in their areas of responsibility. The CRO has independent access to the Audit and Risk Committee and has the resources to help effect appropriate enterprise risk management across divisions, functions, and activities. The CRO has responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down, and across the NDIA.
Executive Management Group (EMG)	EMG will meet at least once a quarter to monitor risks to the achievement of the Agency's corporate plan and goals, and the management of strategic risks identified by the Board. It will report quarterly to the Audit and Risk Committee.
Assurance, Audit and Risk Committee	The Assurance, Audit and Risk Committee is a Management committee responsible for internal advice and assurance to EMG on relevant matters within the Agency. This Committee will have primary responsibility for Agency-wide operational risk management.
Divisional/ Site Risk Officers (Risk Champions)	Each General Manager and Site Manager will nominate an individual to co-ordinate risk management activities within that organisational unit. Division/ Site Risk Officers will act as 'risk champions' by promoting awareness and assistance with the delivery of risk management activities; assist with the identification, assessment, mitigation and monthly tracking of risks across the Division/ Site; and report to General/ Site Managers on the status of risk issues.
All Staff	All staff carry the responsibility for the identification and management of risks that impact on their work areas. All staff should recognise, communicate and respond to expected, emerging or changing risks and contribute to the development and implementation of risk treatments. In practice, this means that staff: • must be familiar with the Agency's risk management strategy and policy; • are encouraged to alert their managers to the presence of risks and participate in their management; and • are encouraged to make use of the tools available to them so that they are better able to identify and manage risks in the workplace.

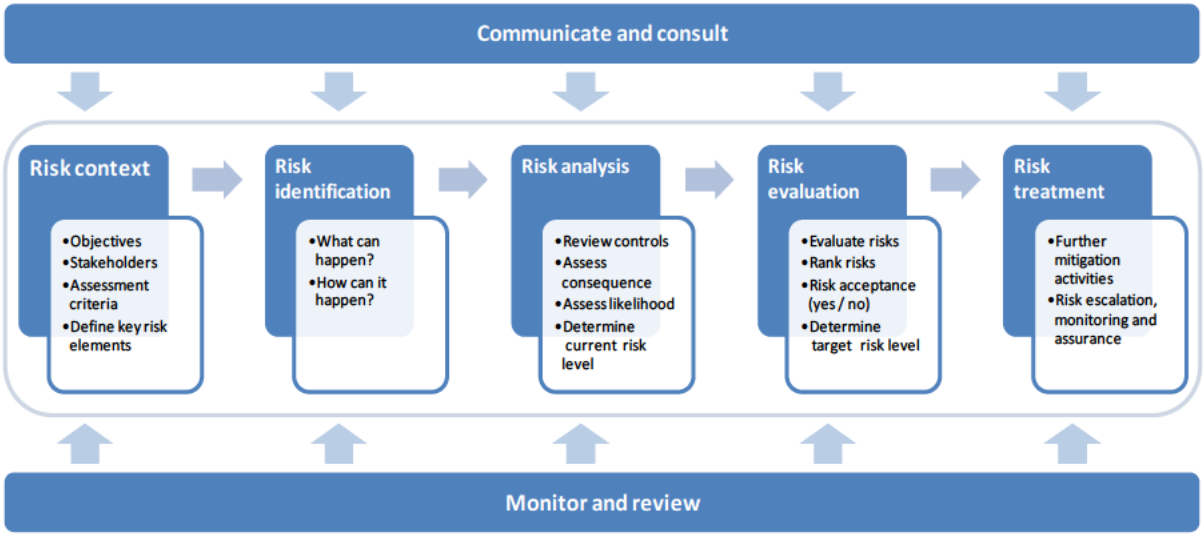
The Risk Management Process

The processes used for managing risk in the Agency are closely aligned with the Australia/New Zealand Standard on Risk Management (AS/NZS ISO 31000:2009). This involves seven key steps:

- Step 1 - Communicate and consult;
- Step 2 - Establish the context;
- Step 3 - Identify risks;
- Step 4 - Analyse risks;
- Step 5 - Evaluate risks;
- Step 6 - Treat risks; and
- Step 7 - Monitor and review.

The linkages between each step in the process are set out in Figure 1 below.

Figure 1: The NDIA's Risk Management Process



Following this process at all levels of risk management – strategic, operational or project – ensures that the Agency's approach to risk management is both comprehensive and consistent.

Step One – Communicate and Consult

Communication and consultation with internal and external stakeholders is important through all stages of the risk management process to ensure the Agency has a comprehensive picture of risks in its operating environment.

External communication and consultation is targeted at informing external stakeholders of the Agency's risk management approach; the effectiveness of that approach; and requesting feedback where appropriate. It is mainly directed at the level of the strategic risks, and as such, is primarily the responsibility of the Board and the EMG. In the case of consultation with Governments, through the CDRC, the Chair of the Board and the CEO have major carriage.

As part of its commitments to transparency and inclusiveness, the Board also seeks comment and engagement from participants and other interested stakeholders through the Scheme website.

Engagement with stakeholder governments and people with disabilities are critical for Scheme success.

Internal communication and consultation is aimed at informing internal stakeholders of the key strategic risks and their responsibilities relating to the management of these risks, as well as seeking their contribution to the identification and mitigation of operational risks. It is mainly facilitated by

Divisional and Branch/ Site Managers supported by the Assurance, Audit and Risk Committee and the Chief Risk Officer.

Step Two – Establish the Context

This involves stating the objectives of the Agency up front, as clearly as possible, in order to identify risk areas precisely, and consider their potential impact on Scheme outcomes. It means considering:

The external context

Building an understanding of external stakeholders, and the extent to which the external environment will impact on the ability to achieve corporate objectives, by considering the business, social, regulatory, cultural, competitive, financial and political environments in which the Agency operates; and the Agency's strengths, weaknesses, opportunities and threats.

The internal context

Building an understanding of organisational elements and the way they interact, including governance, organisational structure, roles and accountabilities; policies, objectives, and the strategies that are in place to achieve them; capabilities (people, time, systems, processes, technologies and capital); the relationships with and perceptions and values of internal stakeholders; the organisation's culture; information systems, information flows and decision making processes (formal and informal); standards, guidelines and models adopted by the Agency; and the form and extent of contractual relationships.

By paying attention to these and other relevant factors, the Agency can ensure that the risk management approach adopted is appropriate to the circumstances, and is supported by an appropriate level of resourcing.

Step Three – Identify Risks

This step involves reviewing as many sources of risk as possible, to identify the risks that could impact on the achievement of the Agency's objectives. Because unidentified risks can always pose a major threat, it is important to take care to ensure that the Agency maintains an open perspective on all possible threats and opportunities.

Key information sources to consider include the NDIA Strategic, Corporate and Business Plans; internal and external audit reports; post-event or post-implementation reviews; and local and overseas experience. Risks can be identified using various tools and techniques, some of which have been condensed into templates to assist in the risk identification process.

By considering these, the aim is to identify a comprehensive list of risks that could adversely impact the achievement of Agency objectives, as well as risks associated with not pursuing opportunities that could foster the achievement of objectives.

Step Four – Analyse Risks

Once a risk is identified, it is important to describe it adequately. A comprehensive risk analysis will include consideration not only of a particular risk event, but also of its causes and consequences. Risk analysis involves identifying the likelihood of the risk occurring, identifying the potential consequence or impact that would result if the risk was to occur; identifying the controls currently in place to manage those risks by reducing either the consequence of the risk, or its likelihood; and assessing the effectiveness of current controls.

Controls are aimed at bringing the risk within an acceptable level. When evaluating the effectiveness of current controls, the factors to consider include consistency of application, understanding of control content; and documentation of controls (where appropriate).

Risks are then analysed and rated after consideration of current controls, in accordance with a standard risk matrix, approved by the Board.

Step Five – Evaluate Risks

The risk evaluation stage involves using the results of the risk analysis to determine whether additional actions need to be taken to manage risks, and the priorities for treatment implementation.

This involves determining whether the risk, with the current level of controls, is acceptable or unacceptable to the Agency in accordance with the Board's approved risk tolerance statement.

Step Six – Treat Risks

Treatment actions are required where the current controls are not managing the risk within acceptable tolerance levels.

There are a number of ways of treating risk:

- Avoid the risk – change a business process or objective so as to avoid the risk, or decide not to start or continue with the activity that gives rise to the risk;
- Remove the risk source;
- Change the likelihood – undertake actions aimed at reducing the cause of the risk;
- Change the consequence – undertake actions aimed at reducing the impact of the risk;
- Share/transfer the risk – transfer ownership and liability to a third party, for example, through a contractual arrangement;
- Retain the risk – accept the impact of the risk; and
- Increasing the risk in order to pursue an opportunity.

When determining the preferred treatment option, consideration is given to the cost compared to the likely benefits that will be derived, including the risk reduction that will result, but also considering legal, regulatory and other requirements such as social responsibility and the social contract between the Agency and Scheme participants. Decisions also take into account risks which can warrant treatment other than on economic grounds, such as risks to the Agency's reputation, or levels of public confidence in the integrity of the Scheme.

Once the preferred treatment option has been selected, the cost of any actions is incorporated into the relevant budget planning process; a responsible person is designated for delivery of the action, and performance measures are determined.

The preferred option is documented in a risk treatment plan that sets out how the chosen risk treatment will be implemented. Treatment plans include the reasons for selection of treatment options, including expected benefits to be gained; those who are accountable for approving the plan and those responsible for its implementation; proposed actions; resource requirements including contingencies; performance measures and constraints; reporting and monitoring requirements; and timing and scheduling.

Risk treatment plans are also incorporated into other Agency processes, such as business or project management plans.

Risk treatment involves a cyclical process of assessing the treatment; deciding whether residual risk levels are tolerable; if not, generating a new risk treatment; and assessing the effectiveness of that treatment.

This has been built into the risk reporting process used in the Agency, and so occurs at intervals determined by the nature of the risk and the priority accorded it by the Board or senior management.

Step Seven – Monitor and Review

The Agency's risk monitoring and review processes are aimed at ensuring that controls are effective and efficient in both design and operation; obtaining further information to improve risk assessment; analysing and learning lessons from events (including near misses), changes, trends, successes and failures; detecting changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities; and identifying emerging risks.

Risks are monitored and reported at a strategic, operational and project level, as shown in Figure 2 below.

Figure 2: Risk monitoring and reporting

Key elements of the risk monitoring and review arrangements include:

- Strategic risks are identified and assessed by the Board annually and reviewed by the EMG and Audit and Risk Committee quarterly
    - The management of particular risks, identified by the Board, may be reported more frequently to the Board if appropriate;
- Operational risks are reviewed annually as part of the business planning cycle, and management of them is reviewed bi-monthly by General Managers, with High risks reported to the Assurance, Audit and Risk Committee and escalated to the EMG and Audit and Risk Committee as required;
- Targeted risk assessment of specialist risks including compliance, business continuity, workplace health and safety and fraud are undertaken in accordance with legislative requirements; and
- Project risk assessments are undertaken for significant projects and monitored monthly through the project governance arrangements.

Risk Reporting

Reporting is a key element of the "monitor and review" phase of the risk management process. The Agency's risk management reporting is designed to support a formalised, structured and comprehensive approach to the monitoring and review of its risks.

Risk Management Reporting Responsibilities

Key risk management reporting responsibilities are set out in Table 2 below.

Table 2: Risk Management Reporting Responsibilities

Role	Responsibilities
Board	• Review reports • Communicate to Agency management priorities and issues raised from consideration of risk information reports • Identify new and emerging risks
Audit and Risk Committee	• Review reports • Communicate risk information issues to Agency management • Communicate key risk issues to the Board • Identify new and emerging risks
Sustainability Committee	• Communicate key risk issues concerning sustainability and participant outcomes to the Audit and Risk Committee and the Board
CEO	• Review reports • Closely monitor high risks • Identify new and emerging risks
EMG	• Review reports • Communicate key strategic risk issues and high rated operational risks to the Audit and Risk Committee • Identify new and emerging risks
General Managers	• Review reports • Communicate key strategic risk issues to the EMG • Identify new and emerging risks
Assurance, Audit and Risk Committee	• Review reports on operational and key technical risks • Communicate key operational risk issues to the EMG • Identify new and emerging risks
Risk Owners (Strategic, Operational and Project)	• Monitor and review the risks which they own • Prepare reports for the risks which they own • Provide the Chief Risk Officer with information on the risks which they own • Identify new and emerging risks
Chief Risk Officer	• Prepare reports for the Audit and Risk Committee • Provide guidance to risk owners on the management of their risks • Prepare the suite of reports set out in Table 3 below • Maintain organisational risk registers • Identify new and emerging risks
Management and staff	• Monitor and review risks within their areas • Identify new and emerging risks • Consult with Line Managers and CRO on risks as appropriate

Risk Escalation

Risk escalation is essential to ensuring that risks are known and understood by the people with the authority to manage them appropriately in the Agency. If the risk is potentially high and requires allocation of substantial risk treatment resources, then it is managed at the Division/ Site level. The Board has overall accountability for managing risks and therefore, where a risk poses a high threat, the Board is informed immediately, through the Chair of the Board in urgent cases or the Chair of the Audit and Risk Committee in other cases.

Because previously unidentified risks can become apparent at any time during the year, everyone has the ability to identify new and emerging risks.

When a staff member identifies a new or emerging risk, they are required to raise the matter with their immediate supervisor/manager, and to work with them to undertake a risk assessment. Initial escalation should be to the Branch or Site Manager where a preliminary judgement can be made about the severity of the risk.

Branch and Site Managers review the risk information provided and, as appropriate, institute treatment action or escalate it to their General Manager and the Chief Risk Officer. The General Manager and the Chief Risk Officer consider the information provided and escalate as necessary.

If the risk has implications across more than one Branch or Site, the General Manager and Chief Risk Officer consult with other General Managers, as appropriate, before raising the matter with the CEO.

Risk Reports and Recipients

The Chief Risk Officer co-ordinates the preparation of a suite of reports on risk management across the Agency, based on input from accountable managers. The reporting regime, including target audience and frequency, is set out in Table 3 below.

Table 3: Report Recipients and Frequency

Audience	Report	Frequency
Board, ARC and EMG	Strategic Risk Report, including • Strategic risk profile • Strategic risk treatment status summary • Strategic risk treatment status details • KRI report	Quarterly
Assurance, Audit and Risk Committee	Operational Risk Report, including • Operational risk profile • Operational risk treatment status summary • Operational risk treatment status details Risk Management Implementation Update	Bi-monthly
Agency Project Committees	Project Risk Reports (as required)	Monthly

Review and Approval

The scope, content and schedule of reports are reviewed annually by the Board Audit and Risk Committee.

Access to Risk Management Reporting Framework

The Chief Risk Officer and the Risk and Assurance Team maintain all reports and risk registers.

Communication and Culture

There are three key elements in the Board's approach to ensuring the development of a healthy risk management culture across the Agency.

First, responsibilities and accountabilities for risk management are clearly delineated. The allocation to senior executive managers of responsibility for managing strategic, operational and project risks reinforces the priority given by the Board and the CEO to ensuring effective risk management aligned to the achievement of strategic goals. Senior managers are encouraged to engage with the CRO in developing strategies to mitigate risk.

Secondly, training is provided to all staff, tailored to roles and responsibilities. For example, general risk management and awareness training is provided by the Agency as part of the general onboarding program. This covers basic concepts and principles; an outline of the key components of the Risk Management Framework; and a discussion of the responsibilities of all staff in relation to risk management. A set of templates to guide staff through key steps in the risk management process is available on the staff intranet.

A network of Risk Management Champions, representing all organisational units in the Agency, meets regularly. Training that is more technical is provided to this group as required. An important part of the role of the Risk Management Champions is to raise awareness and provide advice on risk management issues to other staff in their particular work units.

Thirdly, implementation of the risk management process described previously ensures that risk management is a key element of planning and risks are identified, monitored and managed in a consistent and coordinated way.

Risk Management Function

The Agency's Chief Risk Officer (CRO) is responsible for assisting the Board, committees of the Board and the senior management of the Agency to develop and maintain the Risk Management Strategy and Framework. The CRO is operationally independent, meaning that the position has no direct involvement in the Agency's functions in relation to the funding or provision of supports under the Scheme. The CRO is able to brief the Board, committees of the Board and senior management of the Agency as necessary, and has access to all aspects of the Scheme that have the potential to generate material risk, including information technology systems and system development resources. The CRO is tasked with notifying the Board of any significant breach of, or material deviation from, the Risk Management Framework in a timely and effective manner.

The CRO fits within the second line of defence outlined in APRA's Prudential Practice Guide on Risk Management, and has independent oversight of the risk profile and risk management framework, including providing an effective challenge to activities and decisions that materially affect the risk profile. The CRO is supported by the Risk and Assurance Team with responsibilities relating to the co-ordination of risk management operations and activities that support development of an appropriate risk management culture; fraud control, prevention and detection; business continuity planning; corporate planning; and co-ordination of the internal audit function.

The internal audit program is developed in consultation with management and the Board, and approved by the Audit and Risk Committee. It is a three year program, but reviewed annually to ensure that it continues to reflect current priorities. The Audit and Risk Committee receives reports on progress with addressing audit findings.

The delivery of the internal audit program is outsourced to a specialist provider. The managing partner for the contract attends all meetings of the Audit and Risk Committee, and provides an independent report on progress with delivery of the program. The managing partner also has direct and unfettered access to the Chair of the Audit and Risk Committee and to the CRO.

Compliance

The Agency's compliance obligations can be divided into four categories: the responsibilities of Directors; administration of the Scheme, including the enabling legislation (*NDIS Act 2013* and subordinate rules), and requirements under the Intergovernmental and bilateral agreements; specific responsibilities for Commonwealth authorities under the *Public Governance Accountability and Performance Act 2013*; and general regulatory compliance with relevant Commonwealth legislation.

An annual compliance programme has been established covering all areas with results presented to the Audit and Risk Committee.

Review of the Framework

s47E(d)