Governance Institute of Australia

Guidelines: Whole-of-organisation governance

February 2017

Foreword

Governance Institute of Australia (Governance Institute) is the only independent professional association with a sole focus on whole-of-organisation governance. For the last decade or more, the concentration has been on board governance. But for a governance framework to enable performance, it needs to cascade from the board throughout the organisation.

The *Guidelines: Whole-of-organisation governance* that Governance Institute has developed aims to assist organisations and their managers to understand and put in place an approach to doing this.

A clear whole-of-organisation governance framework supports the achievement of the organisation's strategic objectives by clarifying that decision-making is tied to risk and there is accountability for the exercise of authority. But it is also about empowering employees — allowing them to respond to changing circumstances, while ensuring that decisions are made within the risk appetite set by the board. Whole-of-organisation governance is inextricably linked to good risk management.

Importantly, a whole-of-organisation governance framework is not about adding layers of bureaucracy. It is about alignment of effort across the organisation to achieve strategic objectives for improved productivity; reduced risk; faster and more effective decisions; and enhanced responsiveness to the market and environment in which the organisation operates. It is about enabling performance — if the management team supports a whole-of-organisation governance framework, the organisation benefits.

I thank our members who have contributed to the development of these guidelines and commend them to you.

Andrew Horne FGIA FCIS
President
Governance Institute of Australia

About Governance Institute of Australia

Governance Institute of Australia is the only independent professional association with a sole focus on whole-of-organisation governance. Our education, support and networking opportunities for directors, company secretaries, governance professionals and risk managers are second to none.

Our postgraduate education in applied corporate governance and risk management is unrivalled in its breadth and depth of coverage. It sets the standard for entry into the profession. Postgraduate education is also the gateway to membership of Governance Institute of Australia and the Institute of Chartered Secretaries and Administrators (ICSA) — leading international associations for governance practitioners.

Our Certificates in Governance Practice, Governance and Risk Management and Governance for Not-for-Profits provide skills-based governance and risk management training, and a qualification for a wide range of professionals responsible for corporate accountability functions and processes within an organisation.

Our active membership base of more than 7,000 chartered secretaries, governance advisers and risk managers ensures that Governance Institute is at the cutting edge of knowledge of issues and support of sound practice in the continuous evolution of governance and risk management.

Contents

Overview of whole-of-organisation governance

Definition of whole-of-organisation governance

The **definition** of whole-of-organisation governance as set out in the Guidelines is a principles-based approach to good governance from the board through management to the whole organisation in order to achieve strategic objectives.

The basis of the Guidelines

Governance means the method by which an organisation is run or governed, over and above its basic legal obligations. Governance has four key components:

1. **Transparency:** being clear and unambiguous about the organisation's structure, operations and performance, both externally and internally, and maintaining a genuine dialogue with, and providing insight to, legitimate stakeholders.
2. **Accountability:** ensuring that there is clarity of decision-making within the organisation, with processes in place to ensure that the right people have the right authority for the organisation to make effective and efficient decisions, with appropriate consequences for failures to follow those processes.
3. **Stewardship:** developing and maintaining an enterprise-wide recognition that the organisation is managed for the benefit of its shareholders/members, taking reasonable account of the interests of other legitimate stakeholders.
4. **Integrity:** developing and maintaining a culture committed to ethical behaviour and compliance with the law.

As embodied in Governance Institute's definition, good governance encompasses not only the systems by which organisations are controlled, but the mechanisms by which organisations and those who comprise them are held to account.

Why is whole-of-organisation governance important?

Good governance extends beyond the boardroom. It provides the framework through which the organisation's strategic objectives are set and cascaded, and the means of attaining them are determined. The key to whole-of-organisation governance is clarity as to:

- purpose
- alignment of effort with strategic objectives, and
- accountability.

Key elements in enabling organisations to achieve their objectives are to:

- understand the risks of not achieving the strategic objectives so that these can be managed
- ensure that the effort undertaken by all employees across the organisation is aligned with the strategic objectives
- clarify individuals' roles, authorities and accountabilities in achieving strategic objectives
- empower individuals to make decisions that are aligned with strategic objectives
- clarify the controls and boundaries that apply to the exercise of authority
- provide for clear and effective accountability for the decisions taken and authority exercised.

Governance is fundamental to accountability and good performance over time and also reduces risk. A key benefit of a well-known and well deployed whole-of-organisation governance framework is that the organisation can respond in a more timely fashion as and when needed to achieve its strategic objectives. In a world of rapid information dissemination, organisations need to be able to make decisions quickly. All decision-makers — including client and customer-facing employees — need the freedom to be able to make decisions. However, appropriate boundaries on decision-making need to be in place, clearly understood and followed.

Decentralised decision-making fosters innovation and growth and sound whole-of-organisation governance provides the framework that allows for quick and effective decisions. A clear whole-of-organisation governance framework supports the achievement of the organisation's strategic objectives by clarifying that decision-making is tied to risk and there is accountability for the exercise of authority. Such a framework allows all employees to respond to changing circumstances, while ensuring that decisions are made within the risk appetite set by the board.

As a fundamental enabler of achieving the organisation's strategic objectives, whole-of-organisation governance can bring the benefits of better performance, faster decisions, alignment of effort across the organisation, improved productivity and reduced risk.

What is whole-of-organisation governance?

Whole-of-organisation governance is about how authority is exercised and controlled below the board in an organisation. Authority cascades from the board to the CEO to the executive management team and throughout the organisation. How an organisation is governed is best not left to chance, but should be actively considered by the board and the executive management team and structured accordingly.

- All decision-makers in the organisation should understand the purpose for which authority is to be exercised — to facilitate the strategic objectives of the organisation (the why).
- All decision-makers should understand how authority is exercised, who has authority to do what, and what boundaries apply (the how).

- Appropriate monitoring mechanisms should be in place to provide assurance that decisions are being made in the right way for the right purpose (the safeguard).

If everybody in the organisation:

- is empowered to do what they need to do
- understands their objectives and how they contribute to progressing the organisation's objectives
- understands what they can and cannot do, and how decisions are made, and
- complies, and holds others to account

this reduces risk and improves performance through effective, efficient decision-making. Good whole-of-organisation governance is designed to achieve these outcomes.

Culture

Culture is a key determinant in the performance of an organisation and its ability to achieve its objectives. It goes to the heart of the openness and transparency needed for effective stewardship and informed decision-making. Many factors determine an organisation's culture. Governance is but one part, but it is an important driver in producing the desired culture for an organisation.

All organisations have a culture — the question for boards and management is whether the culture is known and understood and whether the actual culture (the lived culture) represents the necessary and desired culture. It is an essential element of governance for a board and management to understand if there is any disjunction between the desired culture and the actual culture, because it is only the actual culture that ultimately matters.

While on the surface, organisations may have frameworks in place with extensive policies, procedure documents, systems and codes of conduct, it is not unusual to find that the human and organisational behaviours in the organisation are disconnected from or at odds with this framework. Rules are necessary but not sufficient to inculcate a culture where the enacted values align with the desired values.

An organisation's culture is the sum of its shared values and behaviours. It includes the values and behaviours of its people as they relate to various dimensions, such as risk, but those dimensions are not separate cultures. References are commonly made to an organisation's innovation culture, safety culture, compliance culture or performance culture — these are simply dimensions of the organisation's culture.

An organisation may have subcultures, which are intra-organisational groups of people who exhibit a set of shared values and behaviours that are identifiably different from those in other areas of the organisation. Boards and management need to identify if there are subcultures within the entity that do not align with the desired culture of the organisation as a whole: any 'rogue' subcultures should be identified.

Culture provides the context for any approach to governance and risk management. To effectively manage risk and leverage the opportunities created by uncertainty, an organisation needs a risk-aware culture. A risk-aware culture is a critical subset of the broader organisational culture that incorporates the way directors, managers and employees think, communicate and behave about all aspects of risk.

A whole-of-organisation governance framework provides the board with visibility on whether — and how — the desired culture is the enacted (lived) culture. It also provides the board with the means to make adjustments if there is a slippage in the alignment between the desired and enacted culture.

A whole-of-organisation governance framework empowers employees to make good decisions where the enacted values align with the desired values of the organisation.

Why is whole-of-organisation governance part of the governance framework of an organisation?

Whole-of-organisation governance is an extension of the governance framework at board level. A principles-based approach can cascade good governance from the board through management to the whole organisation in order to achieve strategic objectives. See Figure 1 for whole-of-organisation governance.

As defined by Justice Owen in the report on the HIH Royal Commission, corporate governance is[1]:

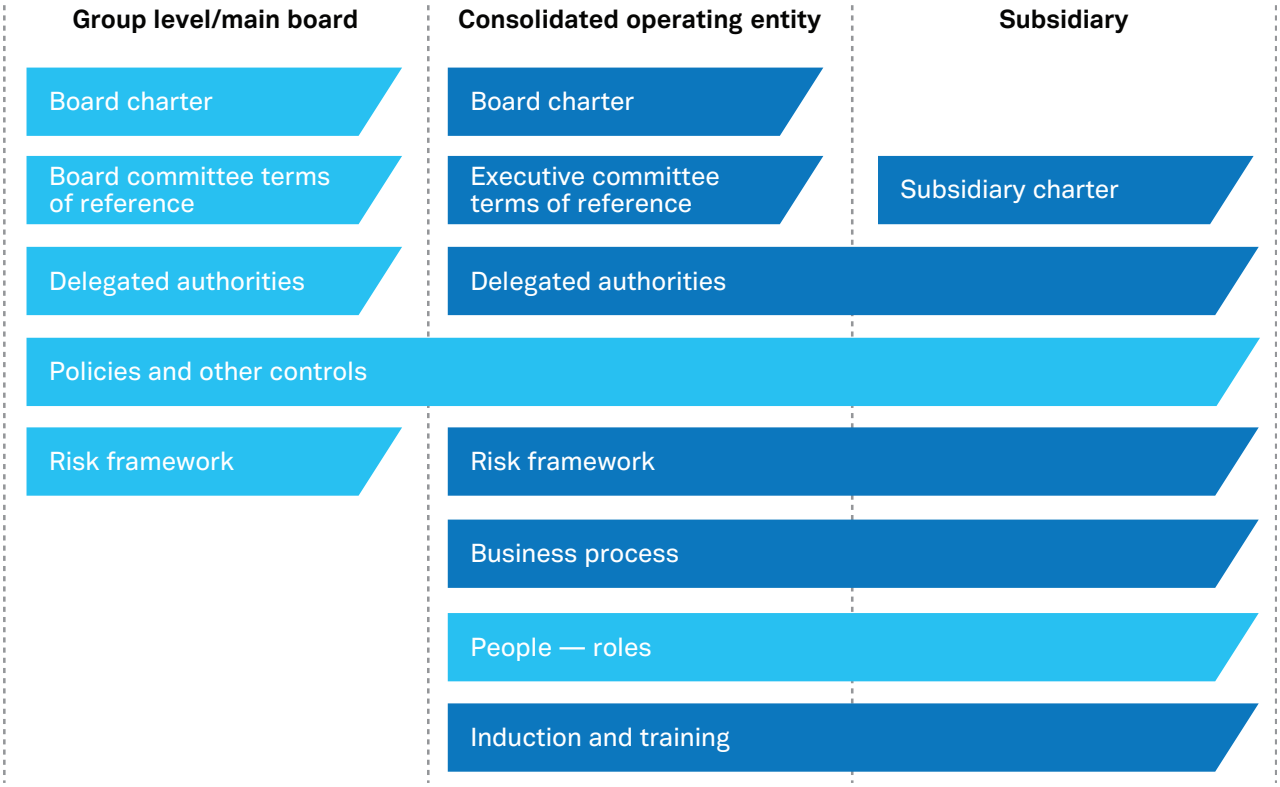
> the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations'... It encompasses the mechanisms by which companies, and those in control, are held to account.

Board governance to whole-of-organisation governance

Section 198A(1) (replaceable rule) of the *Corporations Act 2001* (Corporations Act) provides that the business of the company is to be managed by or under the direction of the directors. The directors are to exercise all the powers of a company except any that the law or the company's constitution requires the company to exercise in general meeting. The members appoint the directors to appoint and oversee the company's management, set the overall objectives and govern the company.

1 Justice Owen, HIH Royal Commission, *The Failure of HIH Insurance, Volume 1: A Corporate Collapse and Its Lessons*, Commonwealth of Australia, April 2003 — p xxxiii

Figure 1: Whole-of-organisation governance as part of the overall governance framework



Many companies in Australia have clauses in their constitutions that allow the directors to delegate their collective authority, but not their responsibility. The constitution may specifically provide for the delegation of authority to board committees, a managing director; or any other person.[2]

Directors may confer on a chief executive officer any of their authority and revoke or vary the delegation of authority

In large organisations, the CEO delegates authority to executives, who in turn delegate authority to other employees throughout the organisation in a cascading chain of authority.

The documents that set out the delegations of authority determine the accountability structure in the organisation, which is commonly that:

- the CEO (or managing director) is accountable to the board
- the executive management team is accountable to the CEO
- other employees are accountable to their managers through a chain of cascaded authority and accountability.

Whole-of-organisation governance adds value by providing a clear and accessible framework that allows for:

- decisions to be made in a timely fashion by the right people as close to the action as possible
- clear reporting of information about decisions to other stakeholders
- clear and effective accountability for decision-making.

Purpose of the Guidelines

These Guidelines are designed to:

- articulate the appropriate delegation of authority from the board to management
- facilitate better decision-making in a more timely fashion by the right people
- reduce risk and protect directors if something does go wrong
- provide for clear and effective accountability

2 The Corporations Act recognises the appropriate delegation of powers (ss 190, 198D Corporations Act).

- add value to organisations by improving performance through better decision-making, improved productivity and efficiency
- allow for fast responses in a rapidly changing world.

The application of the Guidelines

The Guidelines are intended to apply universally. However, much of the content set out in the Guidelines is drawn from the operation of large organisations and might be more detailed than is required or warranted for smaller organisations.

Key elements in whole-of-organisation governance

There are six key elements in whole-of-organisation governance, which include the dimension of risk governance:

1. **Objectives**: The board should set the strategic objectives of the organisation (this includes the organisation's mission, key performance indicators and remuneration incentives) and ensure these are appropriately cascaded throughout the organisation.
2. **Risk appetite**: The board should apply a risk lens to the organisation's strategic objectives and incentives. This means asking questions such as: What are the risks that could hinder the organisation from achieving its objectives? What is the board's appetite or tolerance for those risks?
3. **Risks and opportunities**: The board should consider the risks and opportunities that could affect the organisation's ability to achieve its strategic objective, and also the controls that management should put in place to mitigate the risks and deliver the opportunities.
4. **Delegated authorities**: The delegated authorities (that is, the decision-rights of individuals or committees) should be designed within the context of ensuring that the organisation pursues its objectives while operating within its desired appetite for risk.
5. **Boundaries on conduct**: The boundaries on behaviour and decision-making (through policies, procedures, standards, systems and controls) are developed within the context of ensuring the organisation pursues its objectives and opportunities while operating within its desired appetite for risk.
6. **Assurance mechanisms**: The assurance mechanisms, such as audits, reporting and sign-offs provide the means of monitoring if the framework is operating as intended.

See Figure 2 for the relationship of risk appetite and whole-of-organisation governance.

Figure 2: Relationship of risk appetite and whole-of-organisation governance

What is the board's role?

In setting whole-of-organisation governance, it is the board's responsibility to:

- set the mission and overall strategic objectives
- form a top-down view of the risks and opportunities that could impact on the ability to achieve the overall objectives
- determine the organisation's risk appetite (what level of risk the organisation is willing to accept)
- align the organisation's incentives with achievement of the objectives
- delegate authority to the CEO
- set the top-down view of the mandatory requirements (policies) and controls, having regard to the risk appetite and risks
- ensure that the strategic objectives, delegated authorities and policies are implemented and resourced properly
- approve key documents (for example, the code of conduct)
- establish the assurance mechanisms
- monitor performance and conformance, ensuring the whole-of-organisation governance framework is both adequate and functioning effectively.

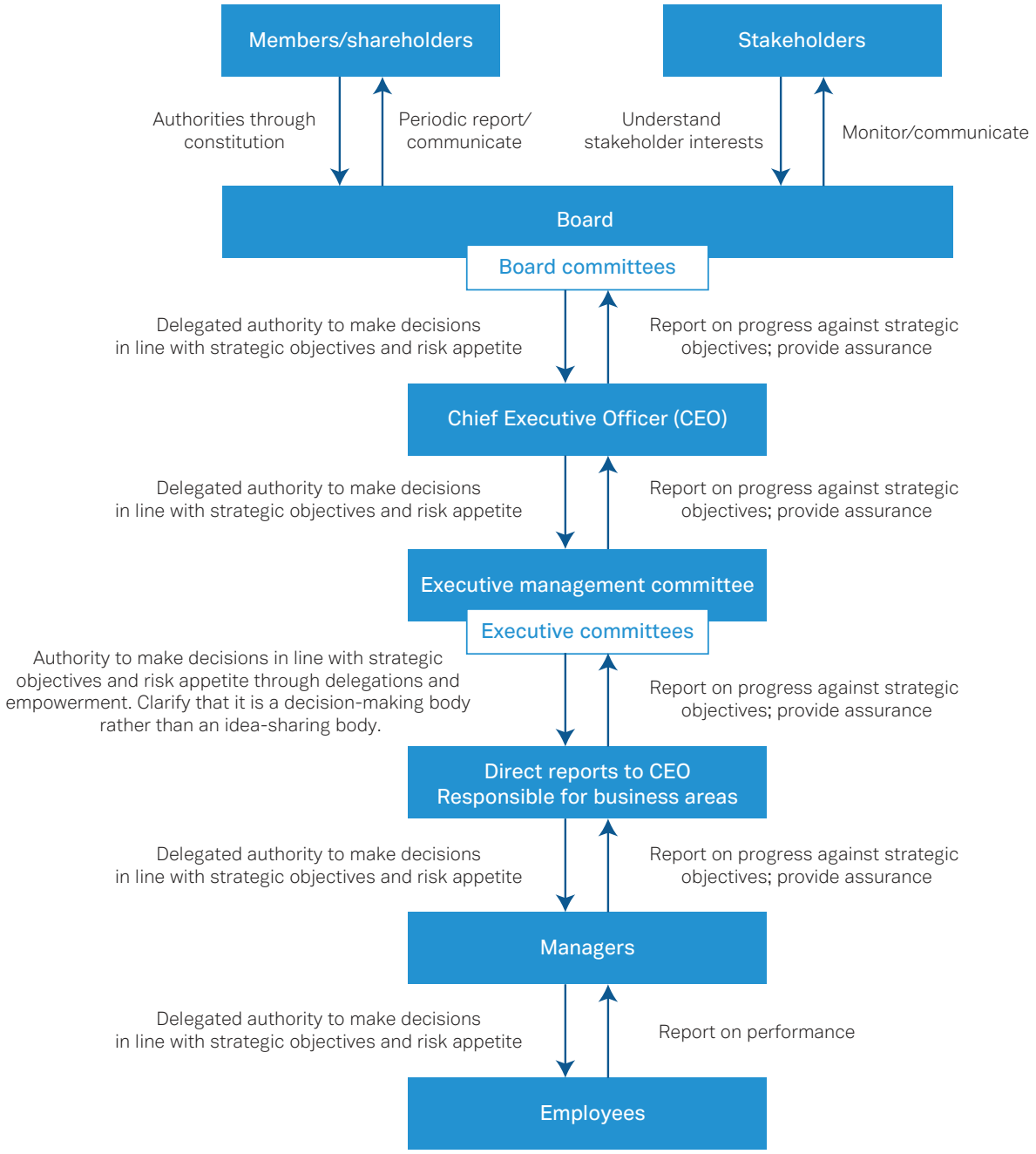
The board is also responsible for 'setting the tone from the top' in relation to culture.

Who owns whole-of-organisation governance?

With governance cascading from the board through management to the whole organisation in order to achieve strategic objectives, it is essential that a senior person who works with the board and the executive management team 'owns' the whole-of-organisation governance framework.

It should not be the CEO or CFO, who already have many key performance indicators to meet geared to achieving strategic objectives. The governance professional is the most likely candidate to be responsible for the architecture and implementation of the whole-of-organisation governance framework in an organisation.

Figure 3: Whole-of-organisation governance at a glance



Guideline 1: Decide and articulate the strategic objectives of the organisation and assign the delivery of those objectives to the executive management team

Non-executive directors should have an independence of judgment and an objectivity that is vital for effective governance and oversight of strategy and performance.

The board should facilitate long-term value outcomes through the link between high quality governance and the creation of member value.

The board should decide and articulate the strategic objectives, ensuring that the objectives assigned to the CEO and executive management team are sufficiently complete, accurate and timely to enable appropriate management to make decisions to achieve those objectives.

The organisation's strategic objectives and plans should cascade through the organisation with clear and appropriate delegation of authority conferred to relevant managers so that they can make decisions within accepted boundaries to achieve those objectives.

Recommended outcomes

- A board charter that sets out clearly the scope of the role of the board is in place.
- Board committee charters that set out the purpose, powers and responsibilities of each committee are in place.
- The board has approved the strategic objectives for the future direction of the organisation.
- The risk appetite for the organisation appropriate to the strategy has been determined by the board and communicated to the CEO and executive management team.
- The responsibilities for achieving the strategic objectives have been articulated by the board to the CEO.
- A formal delegation of authority from the board to the CEO that aligns with the CEO being able to deliver on their responsibilities has been approved by the board and communicated to the CEO.
- The responsibilities for achieving the strategic objectives have been articulated by the CEO to the executive management team.
- A formal delegation of authority from the CEO to the executive management team and employees that aligns with the executive management team being able to deliver on their responsibilities has been approved by the CEO and communicated to the executive management team.
- The responsibilities of individual employees for achieving the strategic objectives have been articulated by their executive manager and employees have the delegated authority to deliver on their responsibilities.
- A performance incentive framework for the CEO, executive management team and relevant employees that aligns to achieving the strategic objectives of the organisation is in place and communicated to the relevant people.
- Regular performance reviews by the board of the CEO, by the CEO of the executive management team and by managers of employees have been held to ensure that decisions have been made to deliver on the strategic objectives and to assess the performance in achieving the parts of the strategic objectives for which each person is responsible.
- On a regular basis the board has reviewed the organisation's strategic objectives with reference to opportunities, challenges, unforeseen events and trends in the industry and business and adjusted the strategic objectives as the board sees fit.

Commentary

The approved strategic objectives guide the work to be undertaken in an organisation. The delivery of the strategic objectives guides decision-making within the organisation. The achievement of executing the strategic objectives guides the assessment of performance and any payment of incentives.

All employees should understand the responsibilities that they have to deliver the strategic objectives and to whom they are accountable.

The CEO is accountable to the board. The executive management team is accountable to the CEO. Employees are accountable to their managers.

The organisational structure should be aligned with the strategic objectives and the types of decisions all employees will need to make to fulfil those responsibilities.

The review of employee performance in delivering the organisation's strategic objectives allows the board, CEO and executive management team to assess how well the organisation has been performing. The performance incentive framework is a way of rewarding employees for achieving the delivery of the strategic objectives and future direction of the organisation.

Tips

- Check that the constitutional source of authority is appropriate and provides the board with the power it needs.
- Operationalise the strategy in a business plan and communicate it throughout the organisation.
- Check that the formal delegation of authority from the board to the CEO aligns to the types of decisions they will have to make to execute the strategy in line with the risk appetite of the board.
- Cascade the strategic objectives throughout the organisation as well as in individual performance plans with financial and non-financial targets and completion of initiatives.
- Incentivise employees to deliver the strategic objectives and reward those employees that perform well in delivering them, both as individuals and across the organisation.
- Take time out to review the strategic objectives and make adjustments in response to a world that continues to change.
- Communicate on a regular basis as to how employees are progressing with delivering the strategic objectives, and be creative and engaging.

Guideline 2: Articulate who has authority to make which decisions in order to achieve the strategic objectives

All employees should understand who has authority to make which decisions. An effective framework of delegated authorities should be in place to make this clear.

The delegations of authority framework should be appropriate to the size and complexity of the organisation, informed by the risks associated with decision-making and aligned with the organisation's strategic objectives. Larger, more complex organisations will require more complex processes.

Employees should be appropriately empowered to make the decisions they need to make to perform their roles. Decisions should be taken by those employees with the most relevant appreciation of the context and consequences of the decision.

Authority will cascade from the board's delegation to the CEO, who further delegates authority to their direct reports and so on. The framework should be sufficiently flexible to enable rapid responses to the dynamic nature of the organisation and its external environment.

While constraints on decision-making capacity are essential to any responsible whole-of-organisation governance framework, it is important that the constraints are not so rigid that they hinder responsible decision-making.

Recommended outcomes

1. A clear framework of delegated authorities below the CEO is in place.
2. The organisation's objectives and risk appetite guide all decision-making by management.
3. Delegated authorities are framed by the organisation's risks and aligned with its objectives such that employees are appropriately empowered.
4. All material decisions, both financial and non-financial, are covered by the delegated authorities.
5. The delegated authorities are easy to understand and readily accessible to all employees.
6. Authority is delegated through all levels of the organisation, so that all decision- makers have clarity as to their delegated authority.
7. Delegated authorities are kept current and periodically reviewed.
8. Appropriate mechanisms, such as powers of attorney, are in place to support execution of documents.

Commentary

Those responsible for making decisions often need to consult with or inform others about a decision. Different rights might exist to participate or be involved in decisions in different ways.

A decision-maker does not have to be an individual, but could be a committee. Proper arrangements should be in place as to how each committee functions (see Guideline 5).

Tips

- Map the decisions that need to be made and identify who should be empowered to make them.
- Check that the delegations of authority align to the strategic objectives that need to be executed, so that the delegations do not hinder management efficiency or expose the organisation to unacceptable risk.
- Identify the employees who should make decisions, those who should be consulted beforehand and those who should be informed about particular decisions.
- Clarify the roles of executive committees in decision-making processes and their delegated authorities.
- Group decisions into sensible categories to make them easy to understand and follow.
- Delegate authority to roles, not individuals.
- Embed delegated authorities into business processes.
- Provide appropriate information, education and training to each employee to whom authority has been delegated to ensure they understand their authority and feel empowered to perform their roles.
- Define how people can change the delegations of authority.
- Constraints on decision-making should be non-legalistic and easily understood by all employees.
- Policies should be linked to the relevant delegations of authority.

Guideline 3: Establish the boundaries on conduct

Decision-makers need to know the boundaries within which they are required to act when making decisions. Most obviously, there will usually be limits on the financial authority delegated to particular decision-makers. However, there will also be a range of policies and procedures put in place by an organisation with which decision-makers must comply when exercising their delegated authority. These policies and procedures must be shaped by and consistent with the organisation's strategic objectives and risk appetite. To be effective, they must be clearly known and understood by the decision-makers to whom they apply. The culture of the organisation must reinforce the importance of the policies and procedures and the consequences of failing to comply with them.

Policies

Policies are usually high-level statements of *the way in which decisions are to be taken* and things are to be done in an organisation. They include codes of conduct and ethics, as well as policies applicable to particular types of decisions and particular parts of the organisation. Organisations often have policies in relation to a wide range of matters, such as an approvals framework; contracts and commitments; risk management; sustainable development; market disclosure and communications (for listed entities); information management; investment; financial accounting; and human resources. Polices usually also cover culture and the relationships between people.

Policies must be clearly articulated and readily accessible by all decision-makers. In some cases, policies may need to be adapted to meet the needs of different parts of an organisation. For example, policies may need to be tailored to the culture and regulatory requirements of individual jurisdictions. However, it is important to ensure that the universal values of the organisation are reflected in policies, regardless of the need to tailor aspects of them to different cultures and regulatory environments.

Effective policies establish clear expectations throughout an organisation and help to ensure that decision-makers act consistently with the organisation's values, and with each other, in exercising their powers. They allow decision-makers to know the boundaries within which they can pursue the organisation's goals. Appropriate policies materially mitigate the risk of legal and regulatory breaches occurring.

Procedures

Procedures are usually detailed statements of *how things are to be done* and how policies are to be put into effect. They rarely require the exercise of judgment. They will deal with matters such as, for example, how orders are to be placed with suppliers; transactions entered into an organisation's financial systems; and induction of new employees.

Recommended outcomes

1. A single code of conduct applicable to all employees, including the CEO, the executive management team and all directors is in place.
2. Policies that are aligned with the organisation's strategic objectives, risk appetite and risk management framework are in place.
3. Policies that are linked to the delegations of authority framework are in place.
4. Policies that are readily accessible to and understood by all decision-makers and employees, including through regular communications and training, are in place.
5. Each policy is owned by a decision-maker or decision-makers who are responsible for the review and version control of their policy.
6. Each policy is reviewed, and if necessary, updated as often as required.

Commentary

When putting in place a risk-based approach to developing policies and procedures, the policies need to be driven by the organisation's strategic objectives and risk appetite. That is, what activities does the organisation need to control because, if it does not, it may not achieve its strategic objectives? Once this has been done, the policy framework can be crafted accordingly.

It is important to understand that a good policy framework is not a single static event. Good policy frameworks evolve as the organisation evolves and should be regularly reviewed and updated to reflect changes in the organisation's strategic objectives and risk appetite, as well as the environments and markets in which it operates. Policies should be updated in response to experience, both positive and negative, of their implementation throughout the organisation. The updated policies should be promulgated through a continual learning process, with improvements implemented through training.

Tips

- Do not simply copy the policies of other organisations. An organisation can only truly own policies it has developed to meet its own unique needs.
- From the beginning, involve the business units and operational teams in the development of policies and procedures.
- Introduce policies on a risk basis, that is, what needs to be managed or controlled?
- Do not confuse a policy with a procedure. A policy is a broad statement of what 'we can do and what we can't do'. A procedure is a more detailed statement of 'how we do that'. For example, the policy is a statement that no one in the organisation accepts bribes. The procedure documents how to record each transaction.
- Policies can go further than compliance with legal obligations to protect employees and the organisation. They should reflect the organisation's values and 'DNA' of the organisation — 'the way we do things around here'.
- Ensure that policies are not so detailed or legalistic that they are difficult to follow or that there are so many that it becomes too challenging to know which policy to refer to.
- Do not implement new policies in response to one-off situations, but review existing policies to clarify if they need updating to take account of changed circumstances.

Guideline 4: Implement sound internal controls

Internal controls are required to ensure that polices and procedures are complied with. They ensure that the executive management team, and ultimately the board, receive assurance as to the actions of decision-makers and minimise the risk of developments in the organisation taking them by surprise.

Internal controls will usually have three areas of focus:

1. The effectiveness and efficiency of the organisation's operations. Are things being done as expected and are risks being appropriately managed?
2. The reliability of financial and other reporting. Can the executive management team and the board rely on and use the information they are receiving from the organisation?
3. Are applicable laws and regulations being complied with?

The components of an effective system of internal controls include the following.

- The policies and procedures put in place by the organisation to allow decision-makers to pursue the organisation's goals and the boundaries within which they are required to operate (see Guideline 5).
- Continuous risk assessment to ensure that the policies and procedures are and remain suitable to manage and mitigate the risks it faces. This is an ongoing process, as the risks faced by the organisation will constantly evolve as the organisation and its operating environment change over time.
- Effective two-way communication and reporting so that all decision-makers are aware of the organisation's expectations of them and the executive management team and the board are properly informed as to the performance of the organisation and the environment in which it operates.
- Appropriate monitoring of compliance with controls to ensure that polices and procedures are followed and that decision-makers are aware that the executive management team and the board will act on instances of non-compliance.

It is essential that controls are consistent with the organisation's strategic plan and objectives. For example, an organisation which seeks to be an innovator in a fast-developing new market should not put in place numerous layers of approvals which delay product launches by months or even years. Conversely, an organisation which relies on a premium reputation of its products in the market should put in place controls to ensure that one part of the business cannot launch a lower quality product that jeopardises that image for the entire organisation.

Recommended outcomes

1. A sound control environment is articulated and understood throughout the organisation.
2. Rigorous and regular risk assessments are implemented to ensure that the control environment responds to the real risks faced by the organisation.
3. Controls which are consistent with the organisation's strategic plan and the overall risk appetite of the organisation are in place.
4. Effective monitoring of compliance with internal controls is undertaken. Non-compliance should never be ignored. If a policy or procedure is appropriate, it should be complied with. If it is inappropriate, it should be changed.
5. An internal audit function appropriate to the needs of the organisation is in place. This function should be adequately staffed, funded and supported in order to achieve the organisation's strategic objectives.
6. Regular monitoring and reporting of financial and other data is undertaken to ensure that financial performance and operational performance are on track with the strategic objectives.
7. Performance reporting is prepared and used as a management tool, as appropriate, at all levels of the organisation, including by the board. This may include reporting between business units if their operations are intertwined.

Commentary

Internal controls help an organisation achieve its profit and performance targets. They ensure that its financial reporting is robust and reliable. They also help ensure compliance with external legal and regulatory obligations and internal policies and procedures, thereby avoiding reputational damage and other adverse consequences. An organisation which lacks sound internal controls is at risk of failing to implement its strategic plan and of not meeting its stakeholders' expectations.

Tips

- Make sure that controls are understood as the way in which performance targets are achieved, not a hindrance to their achievement.
- Make sure that the board and executive management team are, and are seen to be, supportive of policies and procedures and place importance on compliance with them.
- Periodically review controls to ensure that they remain appropriate for the risks and opportunities at which they are aimed.
- Remain aware that the assurance mechanisms are there to test conformance with the delegated authorities and policies put in place as the means to achieve strategic objectives.
- Make sure that each business unit understands the bigger picture and where it fits in.

Guideline 5: Ensure that there are appropriate mechanisms in place for gaining assurance

Boards and the executive management team need to be confident that their governance arrangements are operating effectively. A robust assurance framework provides a stronger basis for boards to be effective and better informed decision-making. A framework that identifies, manages and minimises the risks inherent in the operations will assist the board and executive management to achieve the strategic objectives.

Boards and the executive management team need to determine the level of assurance required to manage the key risks of the organisation and to assess the various methods of assurance that can be implemented. The likelihood of a risk occurring and the severity of the consequences if it should it occur should be assessed against the cost of managing it with available resources.

The board also needs to be confident that appropriate monitoring of management is in place and ensure that the system is both effective and efficient. Assurance mechanisms are there to gain confirmation that the system is adequate and working effectively, that is, that the right decisions are being taken which align with the organisation's strategic plans and objectives and that the proper accountability for those decisions is in place and operating.

The board itself is a monitoring mechanism, and it will also establish board committees to assist with its monitoring role. Management committees also not only have a decision-making role, but also a monitoring role.

The roles of the various assurance functions such as internal audit, compliance and so on should be clearly defined along with their tasks and responsibilities, and how they interact with external assurance providers.

Without assurance mechanisms, the directors are exposed to personal liability risk and the organisation and its directors are exposed to reputation risk. It is also difficult to assess the efficiency and effectiveness of the decision-making process and audit conformance without assurance mechanisms, as the question arises: Conformance to what?

Recommended outcomes

1. A top-down view of the mandatory requirements for a whole-of-organisation governance framework is in place.
2. A regular board review of the strategic objectives and plans and the delegation of authorities that facilitate operationalising plans is undertaken.
3. Regular board and board committee reviews of control policies that have been implemented, including a review of resourcing adequacy, are undertaken.
4. Assessments are made to determine the appropriate assurance program for the organisation.
5. Assurance mechanisms and functions are established that have clearly defined roles and responsibilities.
6. Methods that coordinate and share information between assurance functions are implemented.

Commentary

It is important to put in place a culture that fosters a two-way process of information sharing and monitoring. A one-way process does not provide for the learning experience that comes from sharing information gained from the monitoring process.

A two-way process of information sharing clarifies that monitoring is not about 'catching out' staff, but of ensuring that everyone benefits from the learning experience. This allows the organisation to assess what has worked well and continuously improve its processes and controls.

Tips

- Effective assurance mechanisms provide accountability for public statements and disclosures of financial outcomes by directors.
- The assurance mechanisms should be reviewed on a regular basis to ensure they remain effective within the context of changing business risks and needs.

Governance Institute provides a number of training options for you and your organisation including professional development workshops, customised training and short courses delivered face-to-face and online. Our knowledge resources provide a wealth of guidance on how to think through and manage particular governance issues. For further information please contact your local Governance Institute of Australia state office.

New South Wales & ACT
T (02) 9223 5744
F (02) 9232 7174
E nsw@governanceinstitute.com.au

Queensland
T (07) 3229 6879
F (07) 3229 8444
E qld@governanceinstitute.com.au

South Australia & Northern Territory
T (08) 8132 0266
F (08) 8132 0822
E sa@governanceinstitute.com.au

Victoria & Tasmania
T (03) 9620 2488
F (03) 9620 2499
E vic@governanceinstitute.com.au

Western Australia
T (08) 9321 8777
F (08) 9321 8555
E wa@governanceinstitute.com.au

governanceinstitute.com.au

Governance Institute of Australia