

Group Compliance

External references applicable to this Policy:

- a) All applicable laws, regulations and codes;
- b) Australian Standard AS 3806-2006 *Compliance Programs*;
- c) Board strategic objectives;
- d) Board risk policies and all other policies and process; and
- e) Compliance Framework.

The obligations of this Policy:

1 Compliance objectives

A compliance program is defined in AS 3806-2006 as *a series of activities that, when combined, are intended to achieve compliance*. It is an important element in the corporate governance and due diligence process of any organisation and has the objectives of:

- a) Identifying compliance obligations;
- b) Fostering continuous improvement in compliance processes to ensure obligations are met by establishing monitoring and reporting mechanisms that will assist in identifying instances of non-compliance and the remedial action taken;
- c) Promoting a culture of compliance within the Group through an awareness of the importance of compliance with specific obligations and as an organisational value;
- d) Maintaining the reputation of the Group in the marketplace and to demonstrate social and corporate responsibility.

2 Policy Application

This policy recognises that Community CPS Australia Ltd (Community CPS) has a number of controlled entities. Collectively Community CPS and all the controlled entities shall hereinafter be referred to as the Group. This policy and all applicable laws, regulations and codes apply to all entities and operations of the Group.

3 Compliance Approach

The compliance program at Community CPS will be structured according to the essential elements identified in Australian Standard AS 3806-2006. Those elements are:

- e) **Commitment** – through a commitment by the Board and management to effective compliance¹, alignment of compliance objectives with strategic business objectives², provision of appropriate resources³, endorsement of the compliance program by the Board⁴, and a process to identify and assess compliance obligations⁵;
- f) **Implementation** – responsibility for compliant outcomes is articulated and assigned⁶, competence and training needs are identified and addressed⁷, behaviours that create and support compliance are encouraged while those that compromise compliance are not tolerated⁸, and adequate controls are in place to manage the compliance obligations⁹;
- g) **Monitoring and Measuring** – compliance performance is monitored, measured and reported¹⁰ and is adequately documented and evidenced through practice¹¹;
- h) **Continual Improvement** – the compliance program is regularly reviewed and continually improved¹².

¹ AS 3806-2006 – Principle 1

² AS 3806-2006 – Principle 2

³ AS 3806-2006 – Principle 3

⁴ AS 3806-2006 – Principle 4

⁵ AS 3806-2006 – Principle 5

⁶ AS 3806-2006 – Principle 6

⁷ AS 3806-2006 – Principle 7

⁸ AS 3806-2006 – Principle 8

⁹ AS 3806-2006 – Principle 9

¹⁰ AS 3806-2006 – Principle 10

¹¹ AS 3806-2006 – Principle 11

¹² AS 3806-2006 – Principle 12

4 Commitment

4.1 Board and Management

The Board and management of the Community CPS Group are committed to ensuring the Group meets its compliance obligations. Compliance is concerned with not only externally imposed laws, regulations, codes and standards, but also with internal organisation standards, codes of conduct and ethics, and adoption of industry best practice.

4.2 Alignment of compliance and strategic objectives

Where appropriate, key compliance objectives will be incorporated into the Strategic Plan and planning process. As part of the planning process, a series of functional plans have been developed which are designed to ensure each of the key functions of the Group are aligned to the overall Group Strategy. A specific Compliance Functional Plan has been developed as part of this process.

4.3 Resources

Adequate resources will be provided to assist staff in meeting their compliance obligations and these resources may include:

- a) A separate Risk and Compliance Business Unit, which is resourced with appropriately skilled staff to oversee the compliance program;
- b) An in-house Legal Counsel employed to provide guidance on legislative matters to provide assurance of compliance with legislation, codes and standards;
- c) Access to detailed procedures and operational manuals on compliance matters and other relevant reference material;
- d) Appropriate training for staff to ensure understanding of, and compliance with, applicable laws, regulations, codes and organisational standards;
- e) System-based tools to provide automated compliance controls and access to specific compliance information;
- f) Access to specialised external advice on compliance matters or for assistance with compliance procedure.

4.4 Endorsement of compliance program

The Board has approved the Group Strategy, Group Compliance Policy and Compliance Framework document.

4.5 Identification of compliance matters

The Group will maintain a schedule of *external* laws, regulations and codes that are applicable to the Group in any of its operations. *Internal* compliance issues that apply as a consequence of organisational standards will be communicated to staff as appropriate but generally in the form of specified policies, procedures or codes of conduct.

Where it is considered necessary, *compliance summaries* will be maintained of the scheduled external items that identify the key compliance issues and the primary compliance measures in place. The compliance summaries will be available for review by the Group's internal auditors, the external auditors and relevant regulators as required.

The risk database maintained as a requirement of the Group Risk Management Policy of the Board will aim to identify the key internal and external compliance risks and any other compliance risks considered relevant for recording. The database should identify the related consequences of those risks and controls in place to mitigate those consequences. Each of the risk profiles, including the compliance risk profiles, are subject to an annual review by the appropriate management and Board committees.

5 Implementation

5.1 Responsibility

All staff are expected to maintain a high standard of compliance and to assist in the detection of instances of non-compliance, adoption of remedial action and recommendations for improvements in the compliance process.

All job descriptions include a summary of the relevant compliance responsibilities for each position within the Group. Specific compliance obligations are detailed for some managerial positions within the Group, where considered appropriate.

5.2 Competence and training needs

Relevant and ongoing training on compliance issues and obligations will be a core component of the Group staff training program. The training process should commence at staff induction and utilise whatever methods are deemed appropriate to ensure staff are aware of their compliance obligations and have the necessary understanding and tools to meet those obligations. Compliance training will be tailored to the position of each employee to ensure that training is provided on the relevant compliance obligations. An example of this is lending staff who require training on the *National Consumer Credit Protection Act 2009*.

5.3 Encouragement of appropriate behaviour

All staff should adhere to the compliance obligations relevant to their positions. This includes undertaking compliance training provided by the Group; identifying, reporting and escalating compliance issues in line with policy requirements; and acting lawfully. Separate policies and processes describe appropriate action to be taken in relation to matters related to non-compliance at the individual employee level.

All Business Unit managers have a prime responsibility for monitoring compliance within their areas of responsibility. The Group will maintain a designated Risk and Compliance Business Unit that reviews compliance from a Group perspective, assists operational areas in identifying compliance issues and developing appropriate compliance programs, and aims to identify potential pending compliance issues from changes to, or proposals for, new legislation, regulations and codes.

As responsibility for compliance rests with Business Unit managers, non-compliance issues will be dealt with through the existing operational level management process, requiring reporting to Executive Management as appropriate. Remedial action will depend on the nature of the non-compliance issue and whether reporting to a regulatory body is mandated. Significant compliance issues are to be referred to the Board Risk Committee and, if required, to the Board Audit and Finance Committee.

The Group Internal Audit team will undertake regular reviews of adherence to compliance processes and their effectiveness, based on the assessed risk for specific compliance items and past non-compliance events.

5.4 Controls

Where feasible and practical, appropriate preventative and corrective controls will be implemented to mitigate the consequences of identifiable compliance risks. Some of the key controls implemented by the Group to provide assurance of compliance are discussed below.

5.4.1 Education and Training

Compliance education and training will be provided to all staff, commencing at induction. Managers are to assist the Learning and Development Business Unit to identify aspects of compliance needing improvement. The Risk and Compliance Business Unit will play a key role in assisting Learning and Development with staff awareness of risk management and compliance issues.

Compliance information is to be readily available to staff. External assistance may be sought in order to clarify uncertainty over compliance obligations or to resolve specific compliance matters.

5.4.2 *Compliance policies and procedures*

Written policies and procedures are developed and maintained to assist staff in understanding and meeting their compliance obligations. Individual procedures are to be followed to ensure consistency in approach and may be deviated from only in accordance with approved deviations identified in the procedure. Specific detail and guidance to assist in meeting compliance obligations may be provided within specific compliance manuals or other documents.

Regular review of the policies and procedures is necessary to ensure they are current and reflect any applicable changes in laws, regulations and codes.

Management at its discretion may develop additional specific compliance policies and procedures to manage distinct regulatory or internal compliance obligations.

5.4.3 *System controls*

The Group utilises numerous systems to complete the functions of a financial institution. Where possible preventative controls are used to mandate compliance, which include:

- a) the use of mandatory fields with appropriate syntax to ensure the correct collection of mandatory information;
- b) automated system reports to enable the completion of regular reports required by regulators;
- c) audit logs and automated data archival to meet record retention obligations; and
- d) system prompts to notify staff of specific compliance obligations where required.

5.4.4 *Liaison*

Where it is deemed appropriate, management will appoint designated persons to undertake a liaison role with external regulators and other organisations to assist in the awareness and discussion of compliance issues and the effectiveness of the Group compliance process.

6 Monitoring and Measuring

6.1 Monitoring, Measurement and Reporting

6.1.1 Monitoring

Monitoring of compliance activity is required to confirm controls are in place, controls are effective and applied, all compliance failures are reported and actioned, and the level of compliance knowledge by staff is maintained at a high level. Various measures to monitor compliance are in place including management oversight, system reporting, and audits and reviews by internal and external parties.

6.1.2 Measurement

The Group uses a variety of methods to measure the level of compliance and risk of non-compliance, with the key indicators being detailed below:

- a) Number and nature of complaints received – a complaint process has been implemented (using the basic principles in *AS ISO 10002-2006 Customer satisfaction – Guidelines for complaints handling in organizations*) that facilitates the receipt, recording and action taken on complaints and compliance failures received from staff, members and suppliers.
- b) Number and nature of incidents reported – an incident reporting system is maintained to facilitate the reporting of all suspected issues relating to compliance or risk by staff. The number of incidents reported during a period is one means of measuring the level of compliance of the Group.

Group Compliance

- c) Number and nature of breaches recorded – Breach Registers are maintained to record all identified breaches of external legislation, codes and standards, and internal policy and process. Breaches may be detected and reported by a variety of sources including general staff, internal and external auditors, regulatory authorities and other parties.
- d) Number and nature of adverse internal audit findings – the Internal Audit Program includes a requirement to review the level of compliance with key legislation, codes and standards.
- e) Residual risk ratings of compliance risks – a risk database is maintained using the KnowRisk software to facilitate the process of identifying compliance risks and assessing their impact and mitigation, and to assess the qualitative and quantitative residual risk to which the Group is exposed. This process is conducted within the framework of *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*.

6.1.3 Reporting

The reporting of compliance failures is a key element of a robust compliance process and a process is required to suitably identify and record compliance failures and the action taken to rectify the failure. A summary of the reporting requirements are as follows:

- a) All compliance failures identified are to be reported to Risk and Compliance who will then record the details of the failure within the Breach Register;
- b) All Material compliance failures will be reported by Risk and Compliance to the Executive Committee and Board.
- c) All reportable compliance failures will be reported by Risk and Compliance to the relevant authorities.

The compliance reporting framework will include the following elements to enable the reporting of compliance failures:

- a) **Specific reporting** – each Division may develop specific reporting to facilitate management of compliance issues within their operational areas and reporting may be developed for specific compliance areas (e.g. OH&S);
- b) **General Purpose** – general purpose reporting may be employed to report on common key compliance issues applicable to the Group or defined operational areas;
- c) **Board Reporting** – the Executive is to provide an annual report to the Board as part of the APS 310 attestation that provides a summary of the level of compliance of the Group in respect of its legislative obligations;
- d) **Material/systemic matters** – a monthly compliance report is to be prepared by all Division Executives highlighting any material or systemic risk or compliance matters and an attestation on material breaches of policy or procedure and to the adequacy of the internal control framework. The report is to be provided to the CEO with a copy to the Board. That reporting will form a key element of the annual risk and compliance attestation to APRA in accordance with *APS 310 Audit and Related Matters*;
- e) **Audit reviews** – Internal Audit will undertake regular reviews of activity within operational areas of the Group in accordance with the Internal Audit Plan and risk assessment and those reviews may identify compliance risks, recommendations in relation to compliance controls and aspects of non-compliance;
- f) **Complaint handling** – an appropriate complaint handling process will be maintained and the complaint process may identify single or systemic issues of non-compliance;
- g) **Staff** – the ability is to be provided for staff to report compliance concerns, anonymously if necessary;
- h) **Breach/Incident registers** – breach registers will be maintained specifically for FSR, the National Credit Act and AML/CTF matters and an incident register will be maintained for OH&S. Other registers may be established as deemed appropriate.

6.2 Documentation

The Group's compliance program is documented using a variety of documents and registers, including:

1. The Group Compliance and Compliance policies;
2. The Compliance Framework;
3. Records of training completed by staff recorded within Learning Seat;
4. Compliance summaries and manuals in the library on the Risk and Compliance SharePoint site;
5. Record of compliance failures in the Breach Register;
6. Record of complaints within the complaints registers; and
7. Results of reviews and audits on compliance obligations and actions taken.

7 Continual Improvement

A process for continually reviewing the compliance program consists of the following.

7.1 Review and Improvement

The compliance program is to be continuously reviewed, and improved where practicable, to meet current best practice standards, to standardise and simplify compliance procedures and to meet changes in current laws, regulations or codes, or to meet expectations for proposed future compliance issues.

7.2 Compliance and Internal Audit

The Internal Audit team will undertake a key role in the risk management process through:

- a) Reviewing the qualitative and quantitative assessment of identified risks, consequences and controls, and providing recommendations as considered necessary for modifications to those assessments based on the results of related audit reviews;
- b) Providing information on potential or existing risks that have not been previously identified and assessed;
- c) Provision of advice on additional internal controls, or variations to existing controls, that might be appropriate to lower residual risk;
- d) Undertaking an independent risk assessment and examining the risk information from the Group risk database, to assist in formulating the annual Internal Audit Plan.

8 Review

This policy is to be reviewed by the Board Risk Committee at least on an annual basis or more frequently to incorporate material changes to the compliance process adopted by the Board.

Any proposed changes to subordinate Board compliance policies that materially affect the risk appetite of the Group must be first submitted to the Board, via the Board Risk Committee, for approval. Other changes to subordinate Board compliance policies may be made by the applicable management committee with a summary of such changes to be presented to the Board Risk Committee for ratification.

Acceptable deviations to this policy:

There are no acceptable deviations to this policy.