

JFU Risk Management and Internal Control - Part 3 (2)

Source: JFU

25 November 2015

Setting a Policy as the Basis for C.2.4 Disclosure Statement

This note is the second part of Part 3 on the policy and disclosure statement. It also concludes our series of notes on compliance with the new risk management and internal control requirements under the Hong Kong Listing Rule.

Acknowledgement by the board - C.2.4(c)

The board acknowledges its responsibility for the design and implementation of the Systems and reviewing their effectiveness. Nevertheless, it should be emphasized that the Systems are designed to manage rather than eliminate the risk of failure to achieve business objectives, and can only provide reasonable assurance and not absolute assurance against material misstatement or loss.

Process used to review the effectiveness of the Systems - C.2.4(d)

To facilitate proper conduction of the regular review of the Systems, a handbook has been prepared as formal documentation of the Systems, with sections for respective unit, division or process "owners".

Apart from monthly work group meetings as explained in previous papers, an annual review is conducted, comprising the following elements, in order to assess the effectiveness of the Systems:

- a. a scope review to ensure the Systems cover all aspects of governance and management, together with operations, projects, units or entities of the business particularly those newly added ones during the year under review;
- b. a follow up review to ensure issues arising during the year have been properly disposed of, that is, recommendations reviewed, approved and implemented;
- c. a compliance review, that is, conduction of compliance tests on sample transactions, activities and events to confirm that the operation of the Systems conforms with the design.

The scope, follow-up and compliance reviews apply to financial controls, operational controls and compliance controls, under respective WG members.

Procedures and internal controls for handling and dissemination of inside information - C.2.4(e)

The board considers that all information in the following matters is regarded as potentially price sensitive inside information, the dissemination of which is subject to policies (see below) recommended per the SFC Guidelines by the Price Sensitive Inside Information Committee, as approved by the board:

- a. All financial information, historical reports or forecasts, including management accounts and performance reports of individual units, functional divisions, and entities before the board's explicit approval for release.
- b. All information, financial or otherwise, relating to special transactions or projects, before the board's explicit approval for release.
- c. All information as regards new products or research and development before the board's explicit approval for release.
- d. All information as regards assessment, concluded or in progress, on any risks arising from major changes in the business or its environment, before the board's explicit approval for release.

The general principle for controls over the dissemination of such information internally is "on a need to know" basis. Dissemination of such information externally is only permitted to the extent that the board has explicitly approved it for release by specified personnel and on specified channels.

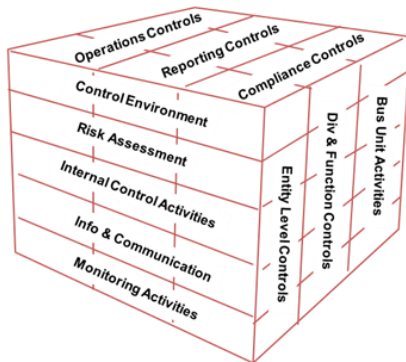
The following is an overview of the PSI policy statements approved by the board:

1. Introduction to the statutory regime for disclosure of price sensitive inside information that came into effect on 1 January 2013
 - a. Highlights of the inside information regime
 - b. Definition of inside information
 - c. Timing of disclosure
 - d. Meaning of "as soon as is reasonably practicable"
 - e. Who is an "officer" under SFO?
 - f. Manner of disclosure
 - g. Examples
2. Handling and disseminating Inside Information
 - a. Protection of Inside Information
 - b. Setting and reviewing policies and procedures
 - c. Need to know policy
 - d. Physical document management / information barriers
 - e. Information technology controls
 - f. Contact with external parties
 - g. Leak investigation
3. Insider list
4. Individual confidentiality obligations

5. Confidentiality agreements – advisors
6. Umbrella agreements - regular advisors
7. Tendering process

2013 COSO Internal Control Framework and Principles

Appendix 1



17 COSO Principles

Control Environment

1. Commitment to integrity and ethical values
2. Independent board of directors' oversight
3. Structures, reporting lines, authorities, and responsibilities
4. Attract, retain and develop competent people
5. People held accountable to internal control

Risk Assessment

6. Clear objectives specified
7. Risk identified to achievement of objectives
8. Potential for fraud considered
9. Significant changes identified and assessed

Control Activities

10. Control activities selected and developed
11. General IT controls selected and developed
12. Controls developed through policies and procedures

Information & Communication

13. Quality information obtained, generated and used
14. Internal control information internally communicated
15. Internal information externally communicated

Monitoring Activities

16. Ongoing and / or separate evaluations conducted
17. Internal control deficiencies evaluated and communicated

ISO 31000 Risk Management Principles, Framework and Process

Appendix 2

11 RM Principles (Clause 3)

1. Create Value
2. Integral part of organizational process
3. Part of decision making
4. Explicitly addresses uncertainty
5. Systematic, structured and timely
6. Based on the best available information
7. Tailored
8. Takes human and cultural factors into account
9. Transparent and inclusive
10. Dynamic, iterative and responsive to changes
11. Facilitates continual improvement and enhancement of the organization

RM Process (Clause 5)

RM Framework (Clause 4)

