

Board Policy: **Enterprise Risk Management**

Policy Type: **Operating Policies**

Monitored by: **Finance and Audit**

Board Resolution: **#1351 approved March 29, 2017**



Board Policy on Enterprise Risk Management

LIPA's ability to identify, assess, manage, and mitigate its financial, operational, supply, physical security, cyber security, legal, legislative, regulatory, reputational and other risks is integral to the Authority achieving its mission and delivering value to its customer-owners. An effective risk management program, executed in conjunction with the Authority's Service Provider, is therefore consistent with, and required by, best utility practice.

It is the policy of the Board of Trustees for the Authority to maintain an Enterprise Risk Management Program that:

- Seeks to identify and mitigate risks that could affect the Authority's ability to carry out its mission on behalf of its customer-owners;
- Enhances the effectiveness of planning and decision-making by the Authority and its Service Provider;
- Maintains prudent and appropriate levels of insurance or other coverage against insurable risks, if available and reasonably economic; and
- Provides transparency to the senior management of the Authority and its Service Provider and to the Board of Trustees regarding the Authority's risks and the actions taken by the Authority and its Service Provider to manage those risks.

Under the direction of LIPA's Chief Executive Officer, the Authority and its Service Provider shall conduct an Enterprise Risk Management program, the key provisions of which include:

- Maintaining an Executive Risk Management Committee consisting of the Chief Financial Officer and at least two other Authority staff appointed by the Chief Executive Officer, one of whom must be a member of the senior management of the Authority, to establish processes and controls and oversee the implementation of the Enterprise Risk Management program;
- Regularly assessing the risks facing the Authority, and providing updates on the status of risks and corresponding mitigation activities to the senior management of the Authority and its Service Provider as well as at least annually to the Finance and Audit Committee of the Board of Trustees;
- Annually reviewing the Authority's insurance and other forms of coverage against insurable risks, including the availability and desirability of such coverage;
- Maintaining business continuity plans for the operations of the Authority and periodically reviewing such plans of the Service Provider; and
- Requiring the Authority's Audit staff to annually undertake a review of the effectiveness and maturity of the Enterprise Risk Management program.