

Figure 2.8:

Alignment of I&T-Related Risk Management Principles with COBIT Risk Objectives EDM03 and APO12

Connect to enterprise objectives

Align with ERM Balance cost/benefit of I&T-related risk

Promote ethical and open communication Establish tone at the top and accountability Use a consistent approach aligned to strategy

Risk Management Principles

Aligns to EDM03 Ensured Risk Optimization

Risk Governance

Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.

Direct risk management.

Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate and that actual I&T risk does not exceed the board's risk appetite.

Monitor risk management.

Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.

Evaluate risk management.

Continually examine and evaluate the effect of risk on the current and futureuse of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.

Aligns to APO12 Managed Risk

Risk Management

Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.

Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.

Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.

Maintain a risk profile. Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.

Articulate risk. Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.

Define a risk management action portfolio. Manage opportunities to reduce risk to an acceptable level as a portfolio.

Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.