

U.S. DEPARTMENT OF COMMERCE Gap Analysis and Risk Mitigation Approach

At U.S. DEPARTMENT OF COMMERCE a successful risk management program is established by (1) senior management's commitment; (2) the full support and participation of the Information Technology (IT) team; (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks.

The risk assessment process is usually repeated at least every 3 years for federal agencies, as mandated by OMB Circular A-130. However, risk management is conducted and integrated in the Software Development Life Cycle (SDLC) for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission. There are specific schedules for assessing and mitigating mission risks, but the periodically performed process are flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies (U.S DEPARTMENT OF COMMERCE, 2003).

Companies can learn from this example at U.S. DEPARTMENT OF COMMERCE and the Federal Agencies to incorporate risk management in their SDLC to enable transformational strategy and proactively mitigate risks.

CITE THIS AS:

YouSigma. (2008). "U.S. DEPARTMENT OF COMMERCE Gap Analysis and Risk Mitigation Approach." From <http://www.yousigma.com>.