

Enterprise Risk Management

A CFO's Perspective

Dr. Douglas Webster
Chief Financial Officer
U.S. Department of Labor



GAO Standards for Internal Control in the Federal Government

Internal Control is an *integral component* of an organization's management that provides *reasonable assurance* that the following objectives are being achieved:

- *Effectiveness* and *efficiency* of operations,
- *Reliability* of financial reporting, and
- *Compliance* with applicable laws and regulations.

— GAO/AIMD-00-21.3.1, November 1999

COSO's Internal Control— Integrated Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) states that:

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide **reasonable assurance** regarding the achievement of objectives in:

- ***Effectiveness*** and ***efficiency*** of operations
- ***Reliability*** of financial reporting
- ***Compliance*** with applicable laws and regulations

— <http://www.coso.org/key.htm>

How GAO Defines Risk Assessment

A precondition to risk assessment is the establishment of ***clear, consistent agency objectives***. Risk assessment is the ***identification and analysis of relevant risks*** associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.

— GAO/AIMD-00-21.3.1, November 1999

GAO Examples of Control Activities

- Top level reviews of actual performance
- Reviews by management at the functional or activity level
- Management of human capital
- Controls over information processing
- Physical control over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties
- Proper execution of transactions and events
- Accurate and timely recording of transactions and events
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control

— GAO/AIMD-00-21.3.1, November 1999

OMB Circular A-123

OMB Circular A-123 seeks to install a process that ensures compliance with Federal legislation:

- Inspector General Act of 1978, as amended (IG Act)
- Federal Managers Financial Integrity Act of 1982 (FMFIA)
- Government Performance and Results Act of 1993 (GPRA)
- Chief Financial Officers Act of 1990, as amended (CFO Act)
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- Single Audit Act Amendments of 1996
- Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)
- Federal Information Security Management Act of 2002 (FISMA)
- Improper Payments Information Act of 2002 (IPIA)

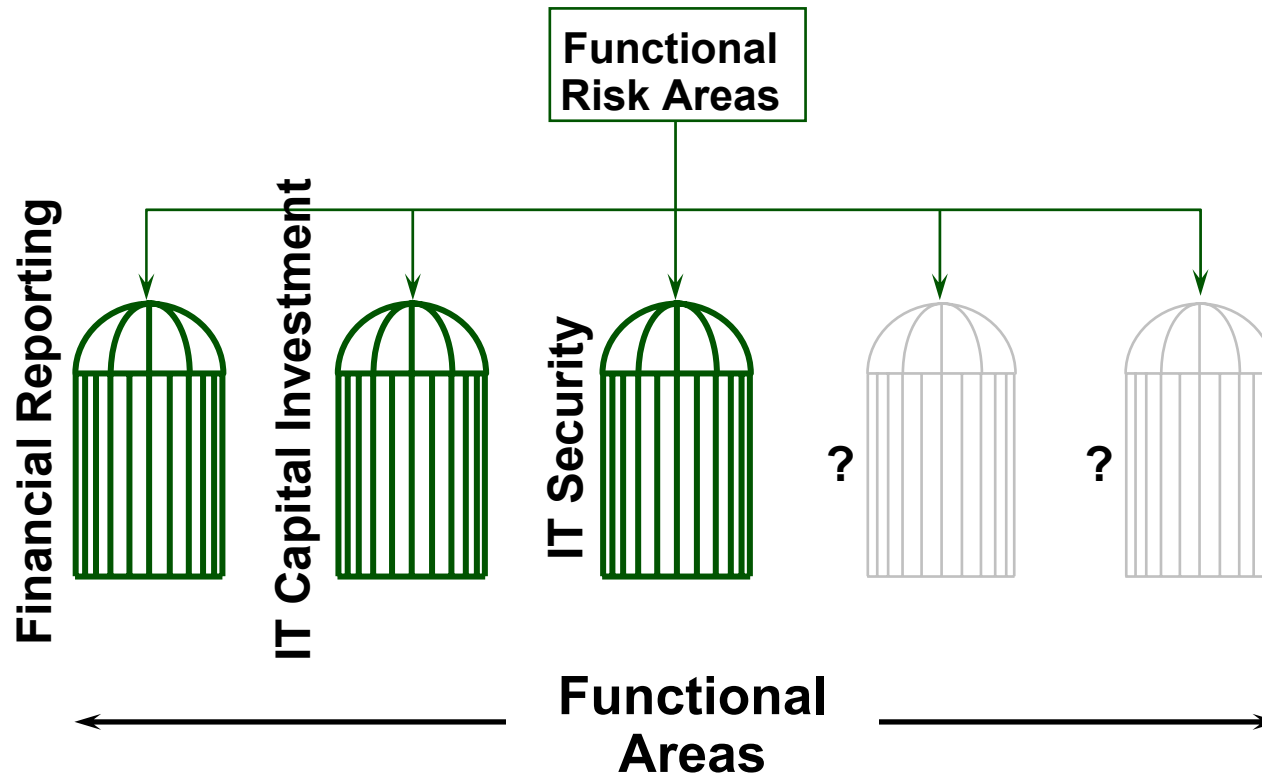
— OMB Circular A-123, Revised

A-123 ≠ ERM

While A-123 is comprehensive, it lacks in practice two attributes found in current ERM frameworks:

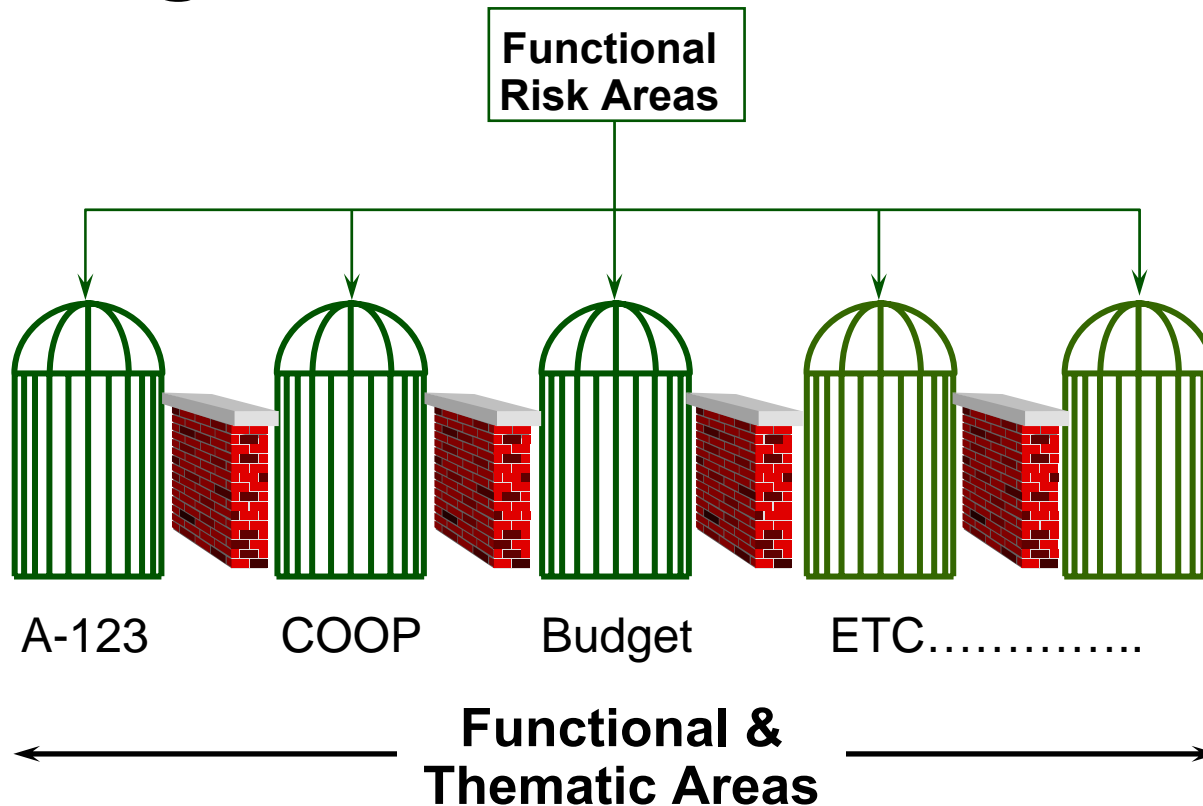
- Comprehensive (covers all relevant risks)
- Integrated (evaluates functional risks on a common basis)

Comprehensive Risk Assessment



- Functional evaluation of risk “risks” missing important hurdles to mission accomplishment

Integrated Risk Assessment



- Identification of all risks does not ensure equal treatment of impact/investment decisions due to functional “silos”
- What is lacking is an integrated approach that balances portfolio risks across the enterprise

ERM as Defined by COSO

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

—COSO Enterprise Risk Management—Integrated Framework, 2004.

ERM vs. Internal Controls

- ERM is not focused exclusively on “controls”, but on risk identification and management
- Controls tend to be operational in nature
- Audits and reviews are backward looking; ERM tends to be forward looking
- ERM focuses on projected risks, including possible events and trends external to the enterprise

ERM in the Federal Government

- Budgets are typically funded by program
- Different programs have different stakeholders making balancing of risks more difficult
- A common risk management approach can identify risks on an equal cost/benefit basis and support more informed budget justification
- ERM can be effectively applied within programs