

# CERIAS

the center for education and research in information assurance and security

## Risk Management in a strategic Information Security Management (ISM) framework

James E. Goldman, Suchit Ahuja  
Computer & Information Technology, Purdue University

### Background

➤ Designed a strategic ISM framework using the following components:

- **Control Objectives for Information Technology (COBIT)**
  - ✓ IT/IS Controls & Governance
- **Cascading Balanced Scorecard (BSC)**
  - ✓ Business / IT / ISM Alignment
- **Security Engineering Capability Maturity Model (SSE-CMM)**
  - ✓ Standardized metrics for performance evaluation

➤ Presented at:

- 4<sup>th</sup> International Workshop on BUSIness /IT Alignment & Interoperability (BUSITAL '09 – Amsterdam)
- IEEE Symposium on Security and Privacy (2009 – Oakland, CA)

### Key Benefits / Goals

- **Alignment between Business / IT / Security strategies**
  - ✓ Integration of security strategy with core business & IT strategies
- **Top-down & bottom-up Traceability**
  - ✓ Justify security ROI
  - ✓ Audit & Reporting
- **Standardized metrics**
  - ✓ KPIs / KGIs / CSFs
- **Input – Process – Output methodology**
  - ✓ Continuous improvement

### Gaps / Drawbacks

#### Lack of unified Risk Management

- **COBIT - Plan & Organize (PO) domain**
  - PO-9 → Assess and Manage IT Risks
    - Lack of methodology / framework
- **Organizational processes for risk management vary with:**
  - Size, Maturity
  - Existing ERM practices
- **Use of different standards for IT risks v/s. business risks**
  - Lack of integration & communication
- **Use of other standards**
  - NIST 800-30, 800-33, 800-53
  - ISO 31000

### Proposed Solution

#### • Risk IT framework by ISACA

- ✓ Based on COBIT processes
- ✓ Integration & alignment of IT risks with overall ERM of the organization

#### • Traceability

- ✓ End-to-End IT risk management processes

- Risk Governance
- Risk Evaluation
- Risk Response

- ✓ Mapping to COBIT domains

#### • Business Focus

- ✓ Balance cost & benefit
- ✓ Risk-Aware culture
- ✓ Risk ownership

#### • Continuous Improvement

- ✓ Risk identification
- ✓ Risk Impact
- ✓ Risk Mitigation

#### • Input – Process – Output methodology

- ✓ Risk IT Domains
- ✓ COBIT Domains
- ✓ Val IT Domains
- ✓ Maturity Model
- SSE-CMM mapping

