CERIAS

the center for education and research in information assurance and security

Integration of COBIT, Balanced Scorecard & SSE-CMM as a strategic Information Security Management (ISM) framework

James E. Goldman, Suchit Ahuja

Computer & Information Technology, Purdue University

Background / Issues

- Multiple frameworks for Information Security Management (ISM)
    - ISO 27001 Information Security Management System
    - ISO 27002 Information Security Controls
    - COBIT Controls for processes
- Multiple frameworks for Strategic Alignment of Business & IT
    - Balanced Scorecard
    - Project Portfolio Management
- Multiple frameworks for Metrics & Measurement
    - SEI CMM
    - SSE CMM
    - COBIT process area 4.0 - “Measure & Evaluate (ME)”

Problem

- **Each framework addresses only a specific area within ISM domain**
- **Integration of two or more frameworks often consists of gaps**
- **Lack of alignment between Business + IT + InfoSec strategies**
    - **Lack of TRACEABILITY**

Proposed Solution

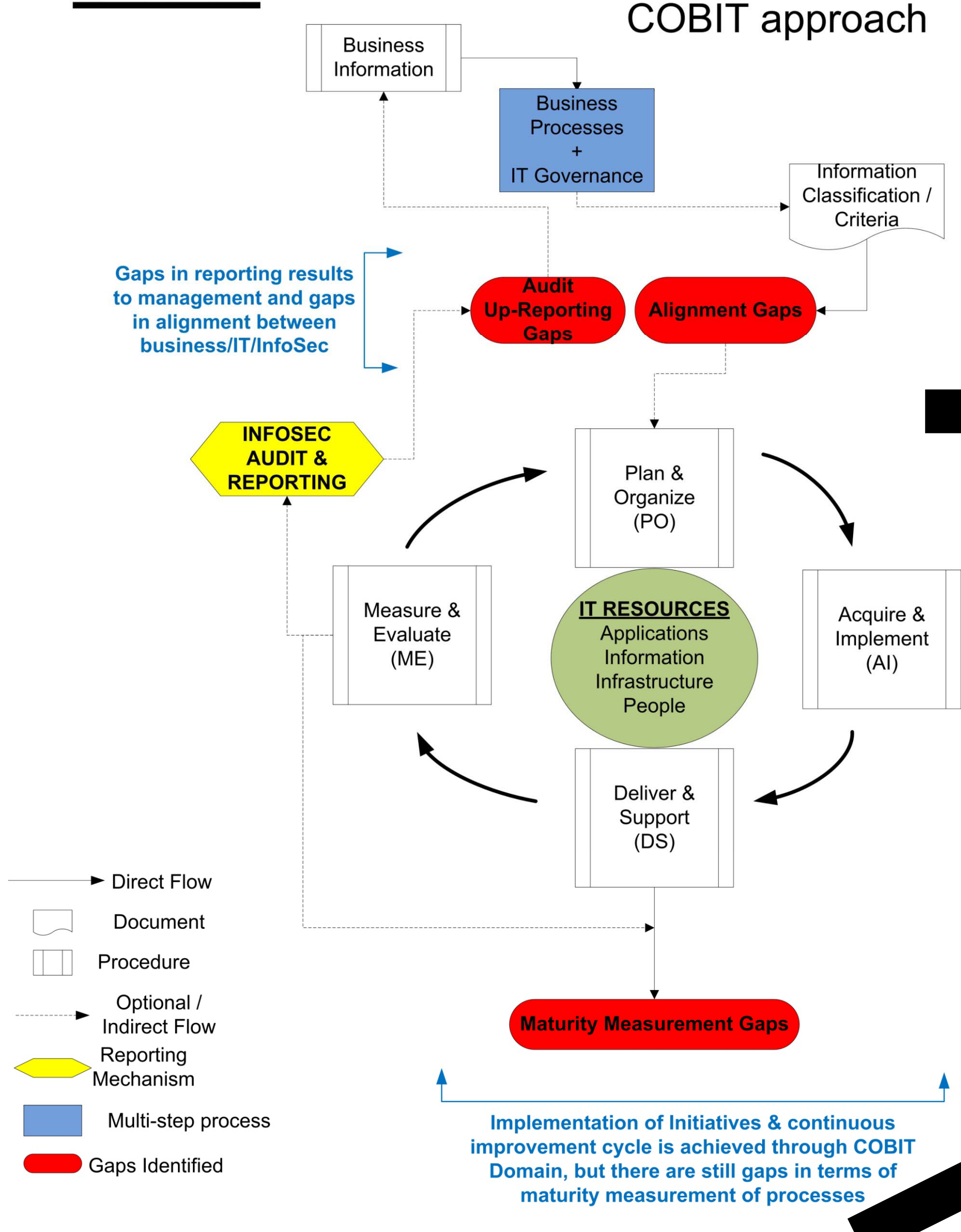
- Integration of COBIT, Balanced Scorecard & SSE-CMM for strategic ISM
    - ALIGN Business + IT + ISM Strategies
    - ESTABLISH clear TRACEABILITY + GOVERNANCE
    - USE of STANDARDIZED METRICS for Performance Management

Approach

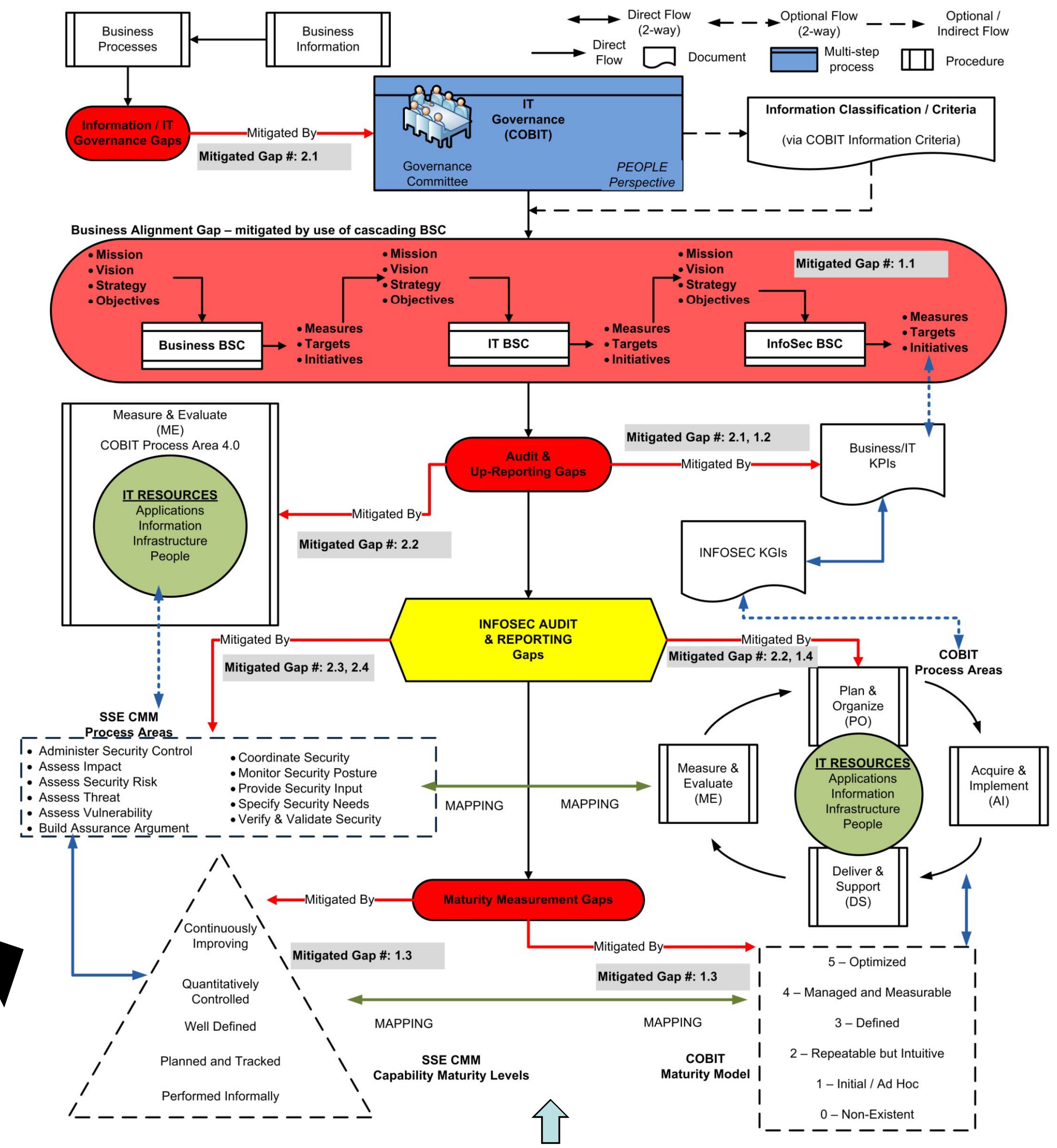
- Integration is achieved by ***bridging the gaps or mitigating the weaknesses***, that one framework inherently contains, using the methodology prescribed by the second framework and using SSE-CMM as an ***evaluation mechanism***

Previous Work

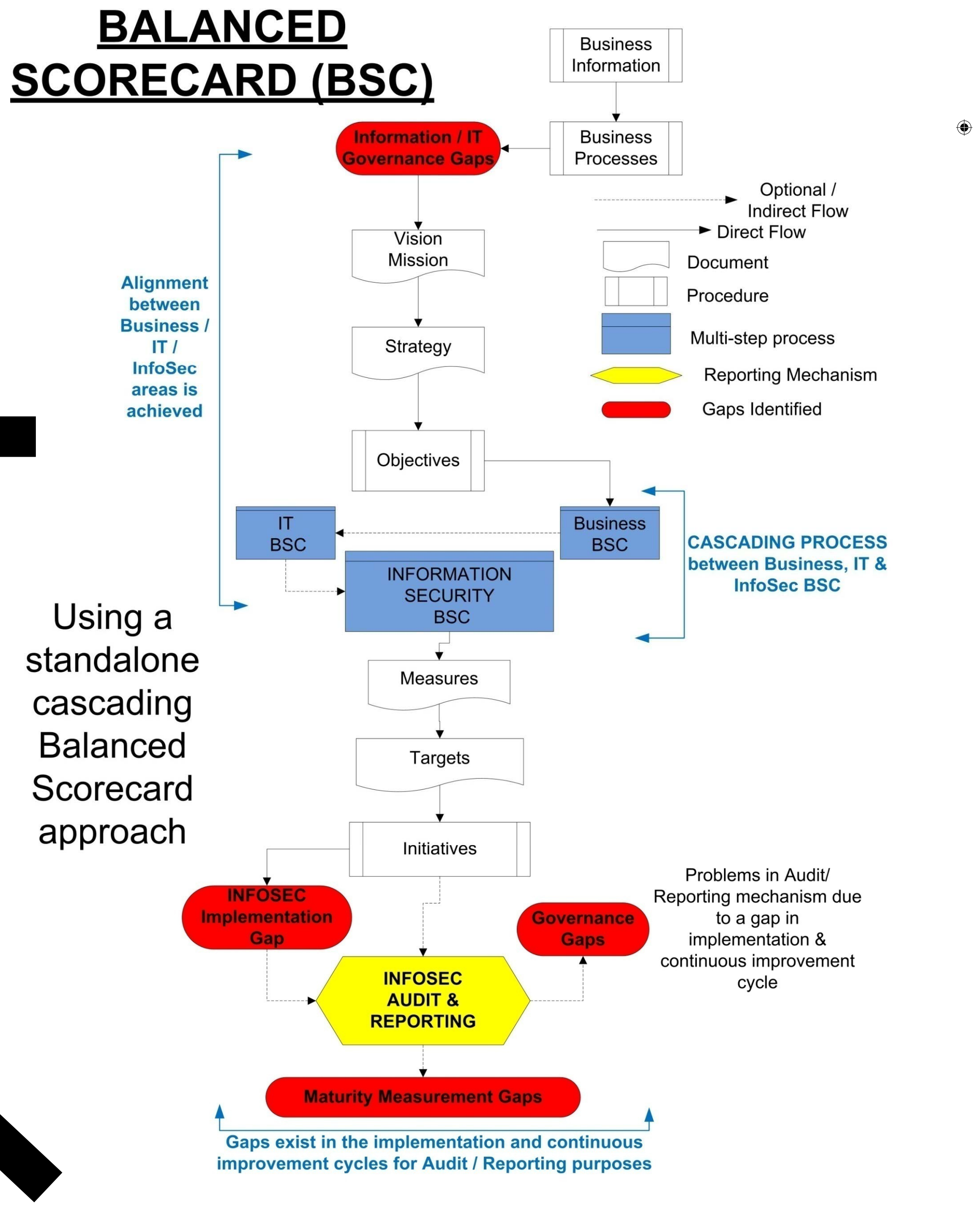
- Metrics based Security Assessment (Information Security and Ethics: Social and Organizational, 2004)
    - Using ISO 27001 and SSE-CMM
- Mapping of processes for effective integration of COBIT and SEI-CMM
    - IT Governance Institute, 2005
- Mapping of COBIT with ITIL and ISO 27002 (IT Governance Institute, 2008)
    - For effective management and alignment of IT with business


COBIT
Using a standalone COBIT approach
Business Information
Business Processes + IT Governance
Information Classification / Criteria
Gaps in reporting results to management and gaps in alignment between business/IT/InfoSec
Audit Up-Reporting Gaps
Alignment Gaps
INFOSEC AUDIT & REPORTING
Plan & Organize (PO)
Measure & Evaluate (ME)
IT RESOURCES
Applications
Information
Infrastructure
People
Acquire & Implement (AI)
Deliver & Support (DS)
Direct Flow
Document
Procedure
Optional / Indirect Flow
Reporting Mechanism
Multi-step process
Gaps Identified
Maturity Measurement Gaps
Implementation of Initiatives & continuous improvement cycle is achieved through COBIT Domain, but there are still gaps in terms of maturity measurement of processes

Proposed Solution

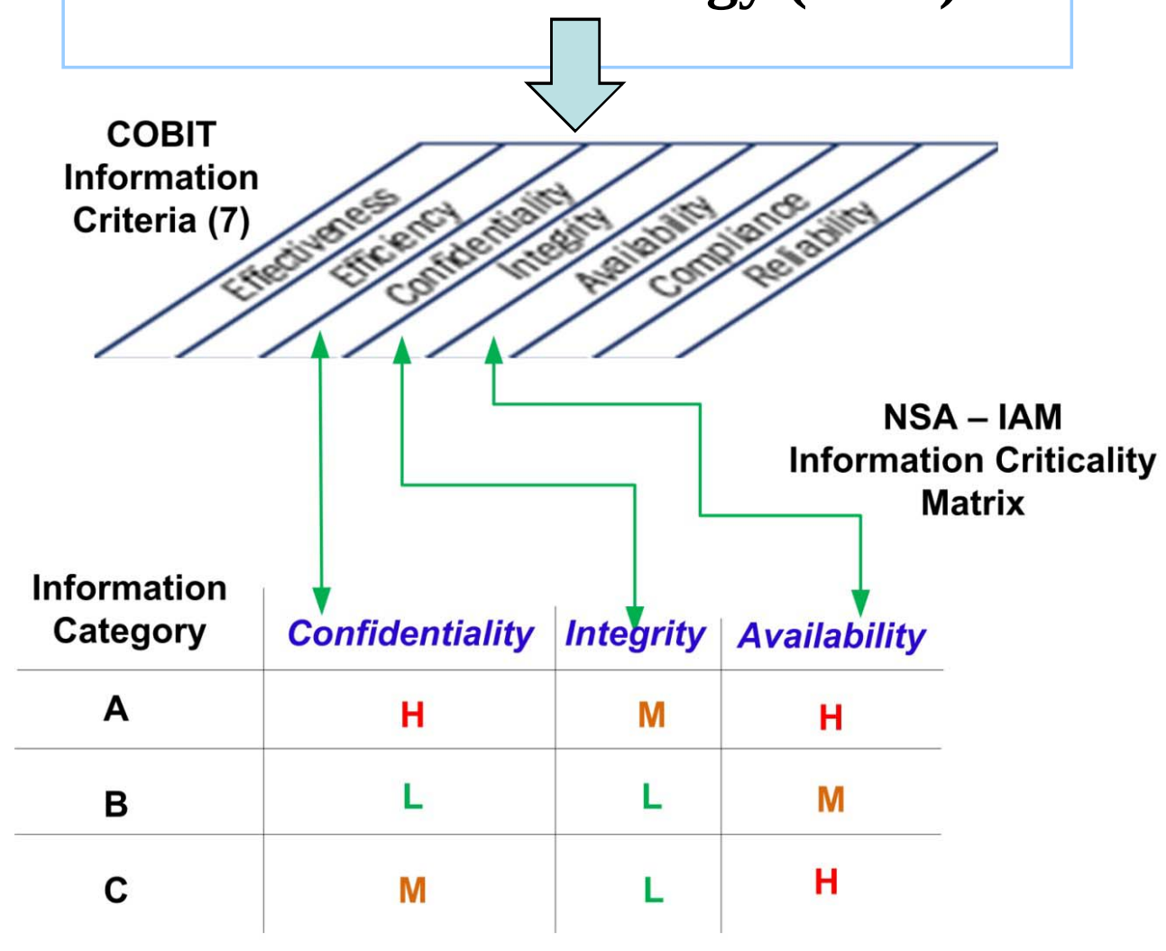


Mitigation of Gaps in BSC and COBIT frameworks


BALANCED SCORECARD (BSC)
Business Information
Business Processes
Information / IT Governance Gaps
Optional / Indirect Flow
Direct Flow
Document
Procedure
Multi-step process
Reporting Mechanism
Gaps Identified
Vision Mission
Strategy
Objectives
Alignment between Business / IT / InfoSec areas is achieved
IT BSC
Business BSC
INFORMATION SECURITY BSC
CASCADING PROCESS between Business, IT & InfoSec BSC
Using a standalone cascading Balanced Scorecard approach
Measures
Targets
Initiatives
INFOSEC Implementation Gap
Governance Gaps
Problems in Audit/ Reporting mechanism due to a gap in implementation & continuous improvement cycle
INFOSEC AUDIT & REPORTING
Maturity Measurement Gaps
Gaps exist in the implementation and continuous improvement cycles for Audit / Reporting purposes

#	Weaknesses / Risks / Gaps	Mitigation Mechanism
1	**COBIT**	
1.1	Lack of alignment of COBIT process areas with business strategy	Use a cascading balanced scorecard approach to align business strategy with information security strategy
1.2	Lack of standardized Maturity Model	Use metrics from cascading BSC and Key Performance Indicators (KPI), Key Goal Indicators (KGI) and Critical Success Factors (CSF) to aggregate the metrics
1.3	A maturity model that is mainly a stand-alone analysis tool	Use SSE-CMM mapping to COBIT areas
1.4	Audit and Information Security reporting gaps	Using a cascading BSC would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM

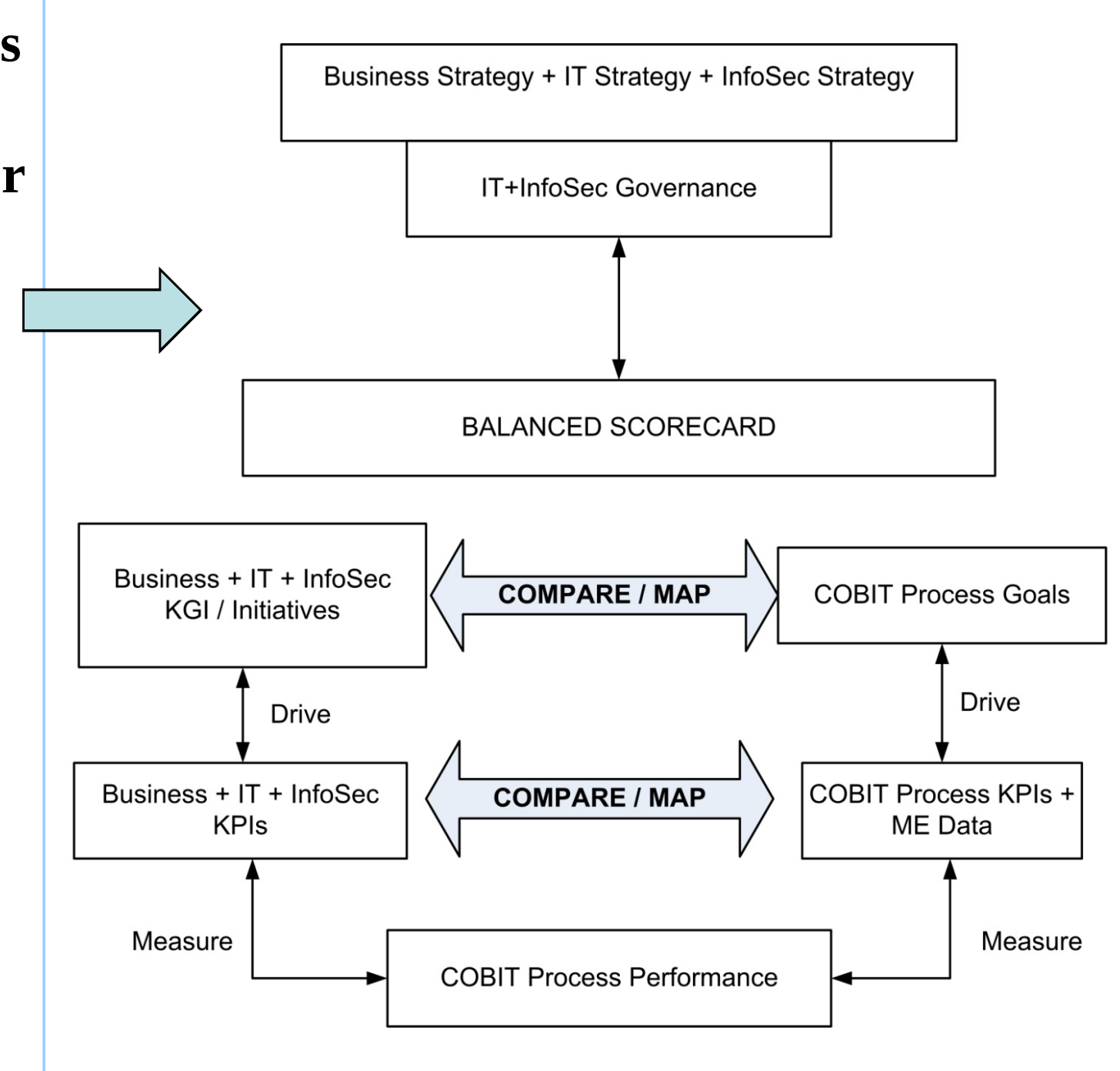
COBIT Information Criteria can help classify information directly for audit purposes. This is similar to Information Classification Matrix developed by National Security Agency (NSA) for InfoSec Assessment Methodology (IAM)



Information Category	Confidentiality	Integrity	Availability
A	H	M	H
B	L	L	M
C	M	L	H

KGI: Key Goal Indicator is defined as a measure of what has to be accomplished
KPI: Key Performance Indicator is a measure of how well the process is performing

Use of KPIs and KGIs (already defined by management and aligned with business strategy) to establish a reporting mechanism for Information Security Management (ISM) that communicates the performance of the operational processes, used in order to achieve desired ISM objectives


Business Strategy + IT Strategy + InfoSec Strategy
IT+InfoSec Governance
BALANCED SCORECARD
Business + IT + InfoSec KGI / Initiatives
COMPARE / MAP
COBIT Process Goals
Drive
Business + IT + InfoSec KPIs
COBIT Process KPIs + ME Data
Measure
COBIT Process Performance

#	Weaknesses / Risks / Gaps	Mitigation Mechanism
2	**Balanced Scorecard**	
2.1	Can cause disagreement and tension between top and middle management regarding information protection priority	The use of COBIT Information Classification / Criteria, with clear prioritization can mitigate risks arising from conflicts
2.2	Terminates at the “Initiatives” level without indicating what processes need to be implemented	Create a mapping between COBIT processes and BSC initiatives
2.3	Lack of traceability to information security level	Use of COBIT control processes over appropriate process areas that are related to information security management
2.4	Audit and Information Security reporting gaps	Using a cascading balanced scorecard approach would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM

PURDUE
UNIVERSITY

CERIAS®

Discovery Park
e-Enterprise Center