



# Driving Compliance through BPM

Dr. Shazia Sadiq<sup>1</sup>, Dr. Marta Indulska<sup>2</sup>  
School of Information Technology and Electrical Engineering<sup>1</sup>, UQ Business School<sup>2</sup>  
The University of Queensland, St Lucia, QLD 4072  
Brisbane, Australia  
email: [shazia@itee.uq.edu.au](mailto:shazia@itee.uq.edu.au); [m.indulska@business.uq.edu.au](mailto:m.indulska@business.uq.edu.au)  
ph: 0421 115 662 (Shazia), 0412 401 060 (Marta)

# Session Plan

- Introduction to Business Process Management
- Business Process Management and Compliance
  - The Role of Risk Analysis
  - A methodology for driving Compliance through BPM
- Identification of Challenges
- Summary and Discussion

# What is BPM?

# BPM (Still) The #1 Priority

## Top 10 business priorities: CIOs see executives expecting IT to play a role in current and future enterprise capabilities

To what extent will each of the following business, societal or government trends impact your enterprise in 2007?

	2007		2006	2005
Improving business processes	1	↔	1	1
Controlling enterprisewide operating costs	2	↔	2	3
Attracting, retaining and growing customer relationships	3	↔	3	**
Improving the effectiveness of the enterprise workforce	4		*	*
Need for revenue growth	5	↑	8	6
Improving enterprise competitiveness (bottom-line profitability)	6	↓	5	**
Expanding use of information/intelligence in products and services	7	↓	6	7
Deploying new business capabilities to meet strategic goals	8		*	*
Entering new markets, new products or new services	9		*	*
Faster innovation (shorter product/service life cycles)	10	↓	9	10

\* New question for 2007 \*\* New question for 2006

# BPM Origins

The age of the  
Crafts Worker

The age of the  
Factory

The age of the  
Specialist

Process  
Orientation

- Business Process Management (BPM) has been identified as the “number one business priority” and a major challenge for senior executives

Gartner EXPPremier (2005) Delivering IT's Contribution: The 2005 CIO Agenda. Gartner, January 2005.

- Increasingly, BPM is perceived as a way to align and increase the contribution of information systems to the business

Howard Smith, Peter Finger (2003) IT doesn't matter – Business Process Do. August 2003. Meghan-Kiffer Press 2003.

- Workflow management systems (a core segment in BPM solutions) and related BPM solutions will reach \$1.1 billion by 2009 (at \$416.4 million in 2003)

WinterGreen Research (2004) Business Process Management (BPM) Market Opportunities, Strategies, and Forecasts, 2004 to 2009.

Sharp and McDermott (2000)

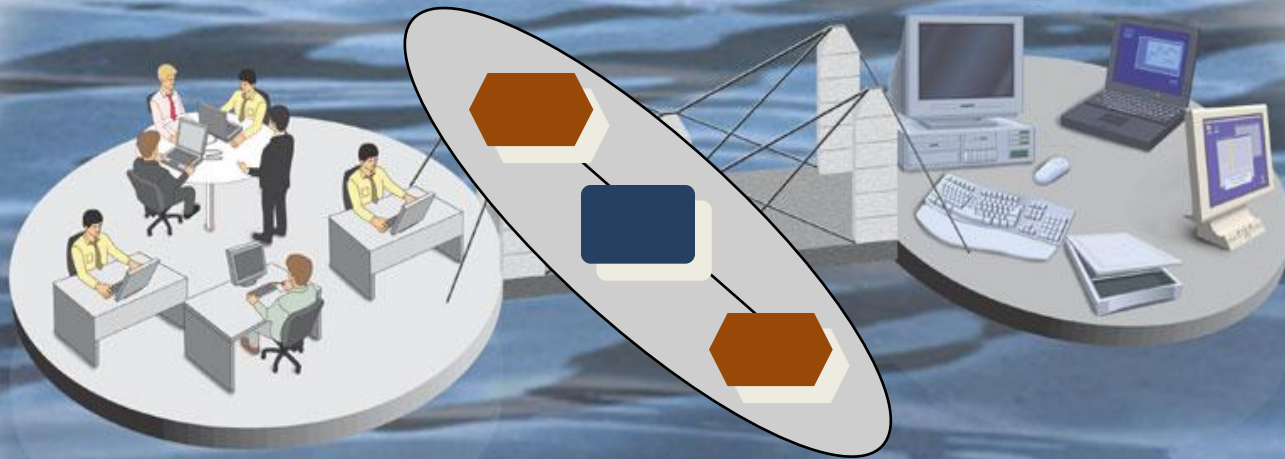
# What is BPM?

*Business Process Management is a structured, coherent and consistent way of understanding, documenting, modelling, analysing, simulating, executing, measuring and continuously changing end-to-end business processes and all involved resources in light of their contribution to business improvement.*

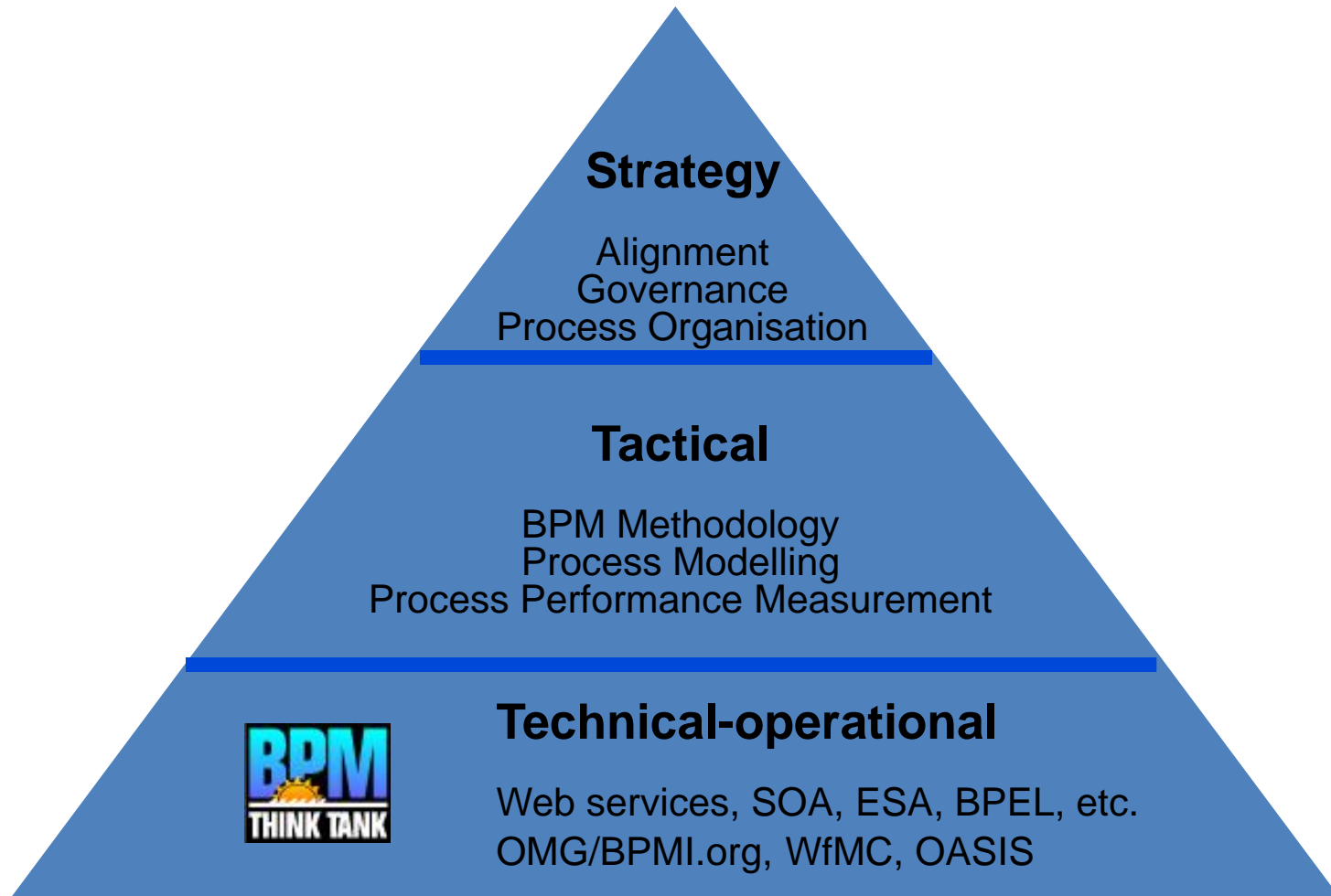
*Definition by the Australian BPM Community of Practice*



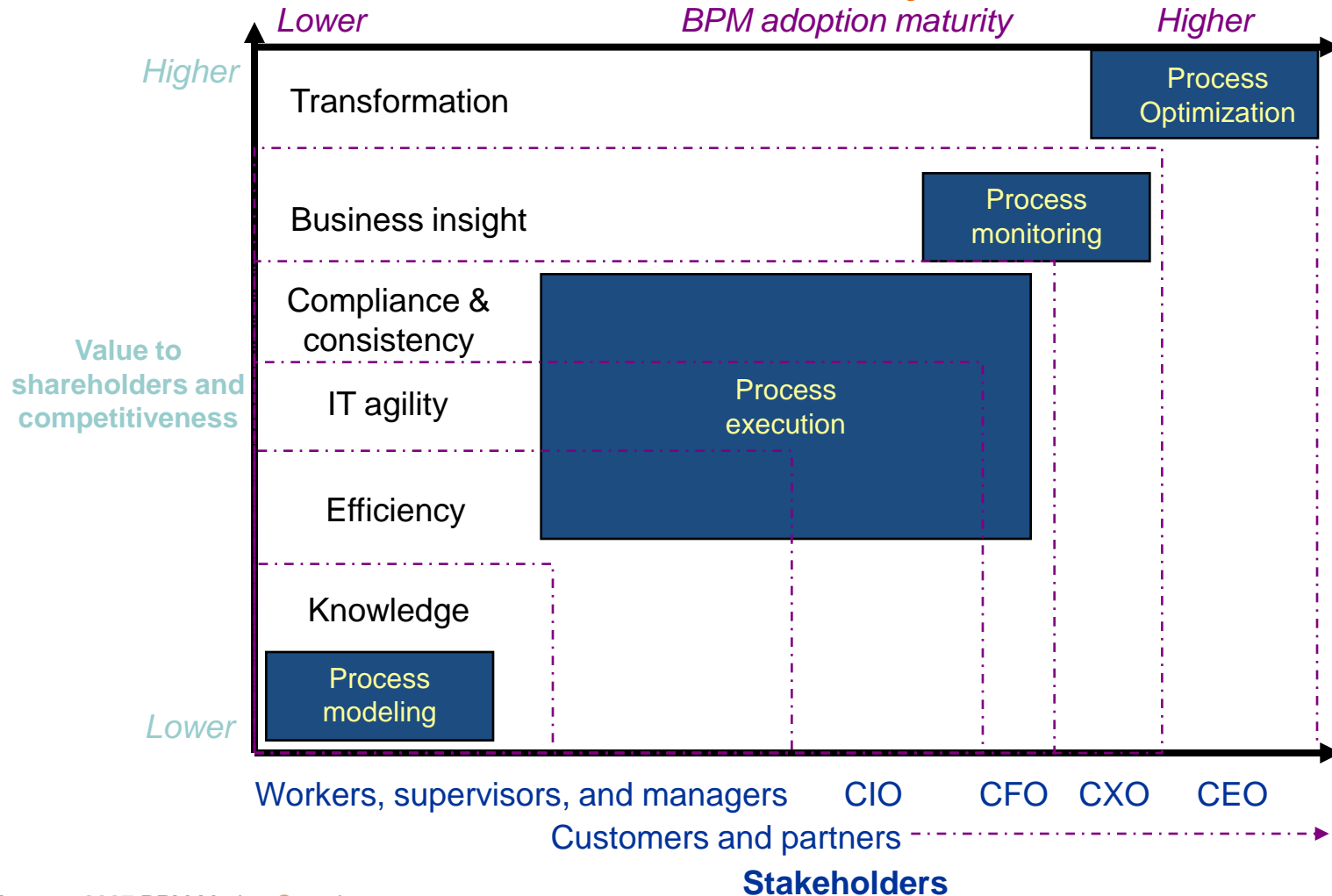
# BPM – The Missing Middle?



# The Three BPM Communities

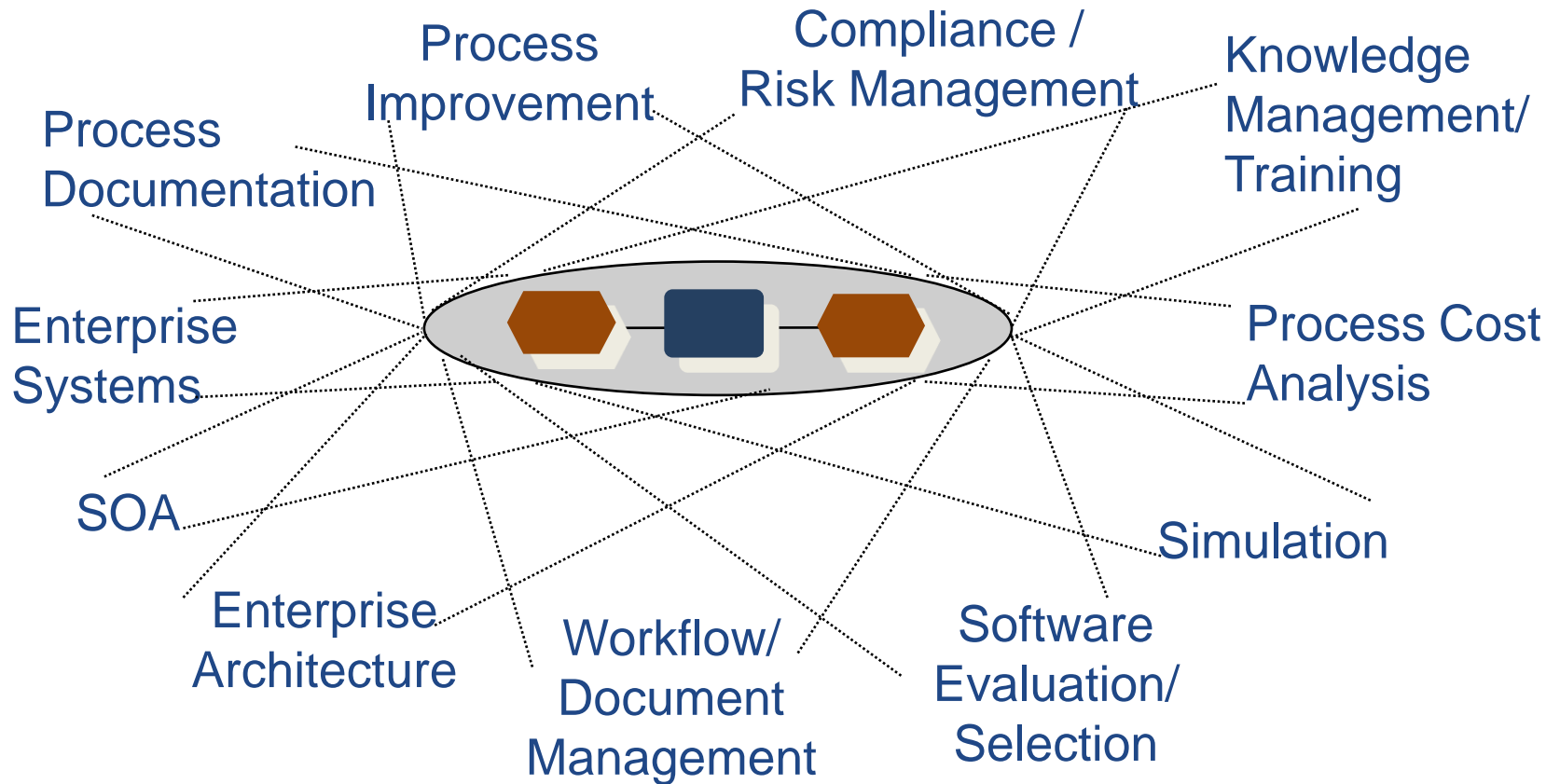


# The Value Proposition



Forester 2007 BPM Market Overview

# BPM Span



# So, what is BPM?

Business Process Management is the collection of methods and tools that allow us to:



# A Framework to Measure BPM Maturity

## - The Six Success Factors



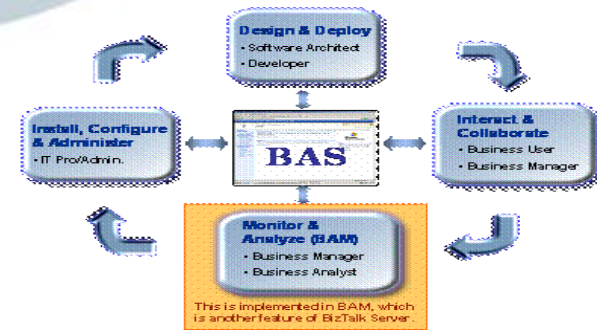
Rosemann , De Bruin & Power (2006)

# Business Process Lifecycle



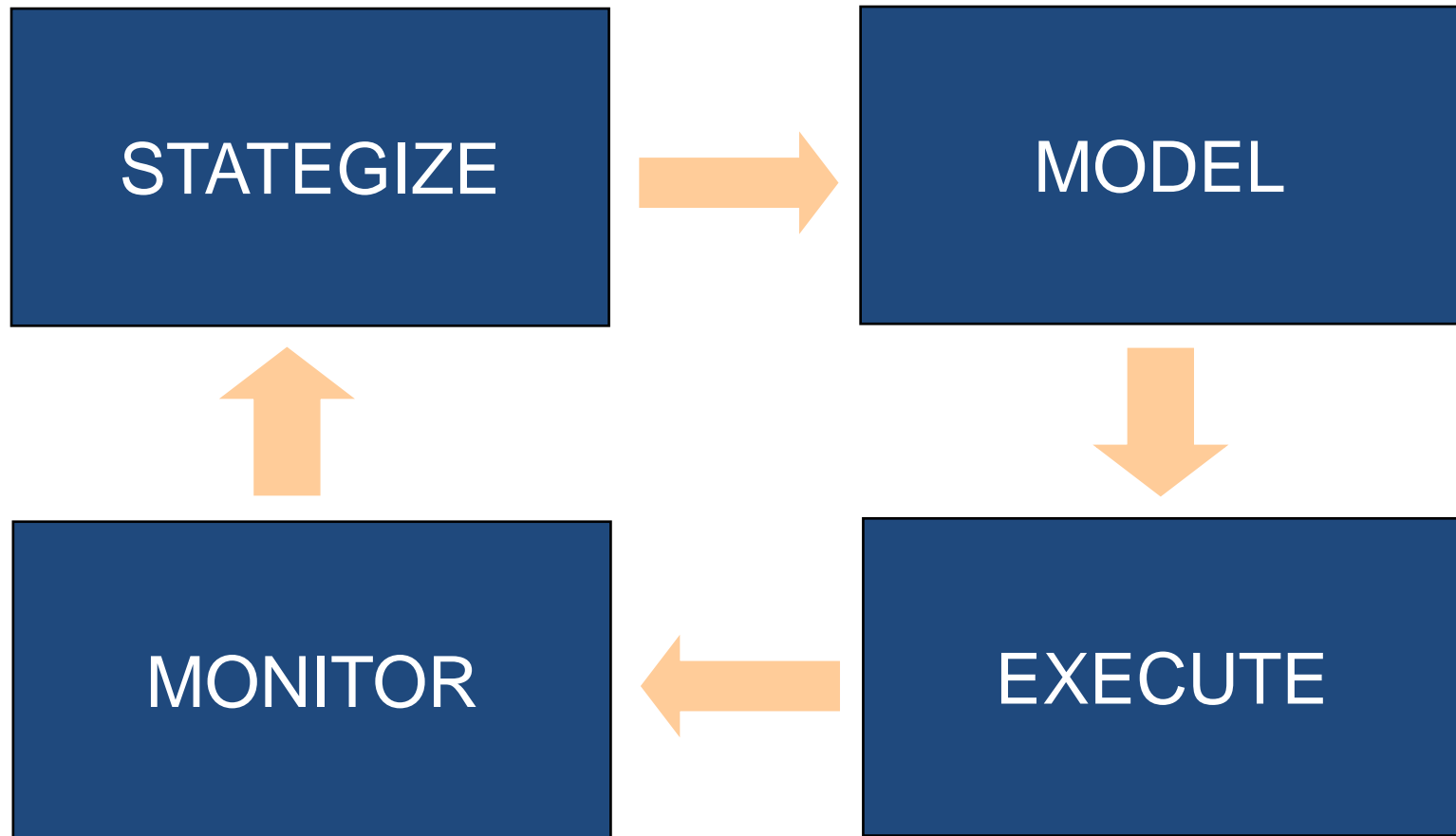
BEA Systems

IDS Scheer



Microsoft Business Activity Services for Biztalk

# Business Process Lifecycle



# Business Process and Strategy Definition

## Six Sigma

- Bill Smith (1986) Motorola University

## Porter's value chain

- Michael Porter (1985) Competitive Advantage: Creating and Sustaining Superior Performance.

## Rummler's management theory

- Geary A. Rummler, Alan P. Brache (1990) Improving Performance: How to Manage the White Space in the Organization Chart. Jossey-Bass Publishers

## SEI Capability Maturity Model Integration

- [www.sei.cmu.edu/cmmi](http://www.sei.cmu.edu/cmmi)

## Process Improvement

- Paul Harmon (2003) Business Process Change – A Manager's guide to Improving, redesigning and Automating Processes

## Process Handbook

- Thomas Malone, Kevin Crowston, George herman ((2003) Organizing Business Knowledge – The MIT Process Handbook. The MIT Press.

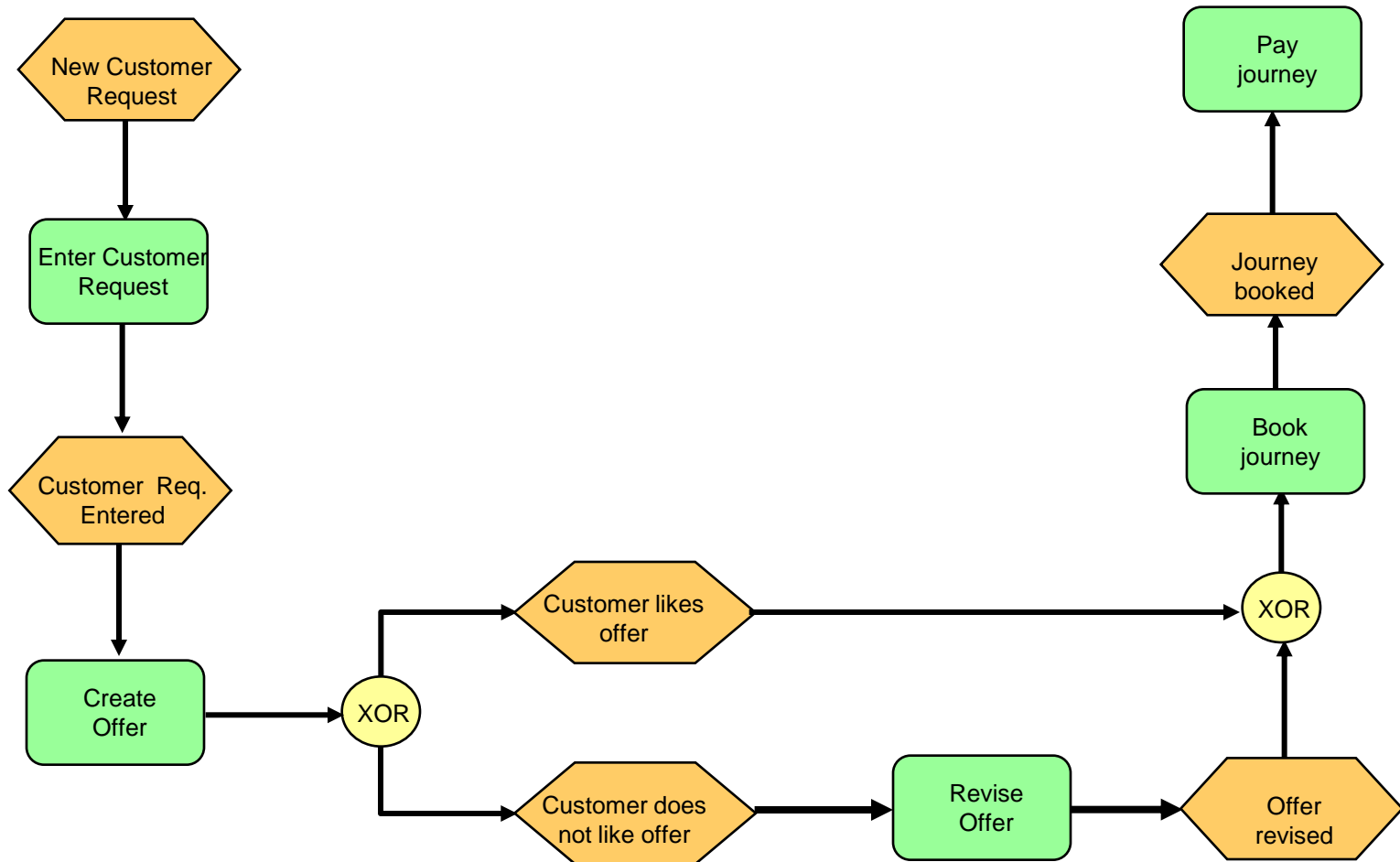
## Reference Models

- A. W. Scheer (1994) Business Process Engineering: reference Models for Industrial Enterprises. Springer.

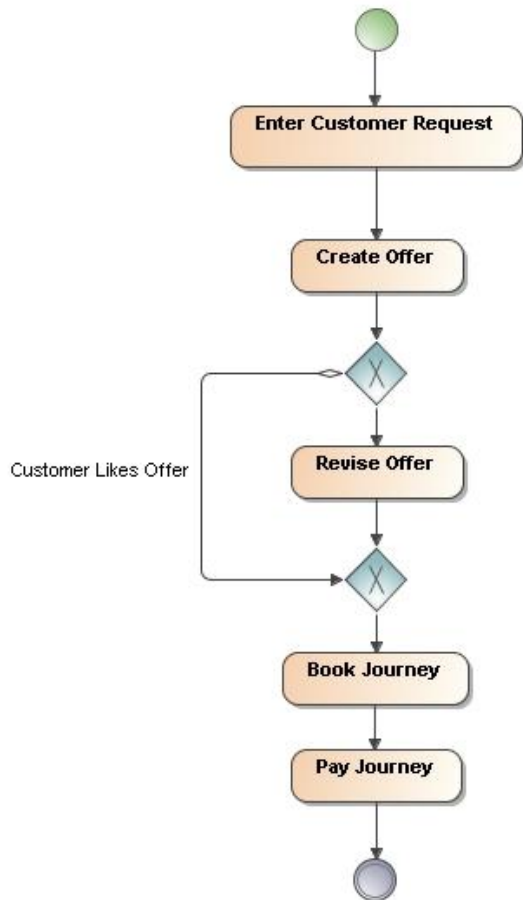
## Process Templates

- SAP Solution Maps. [www.sap.com/solutions](http://www.sap.com/solutions)

# Business Process Modeling



# Business Process Modeling



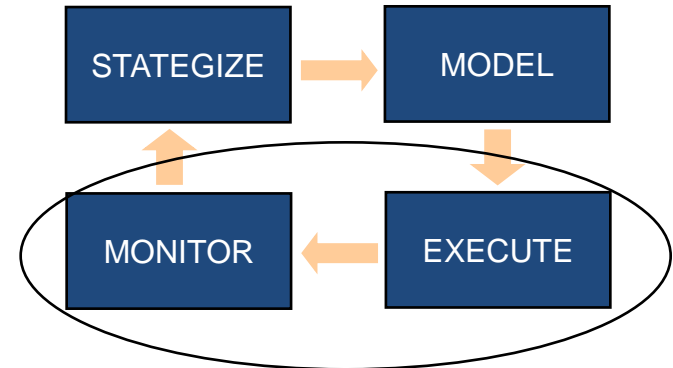
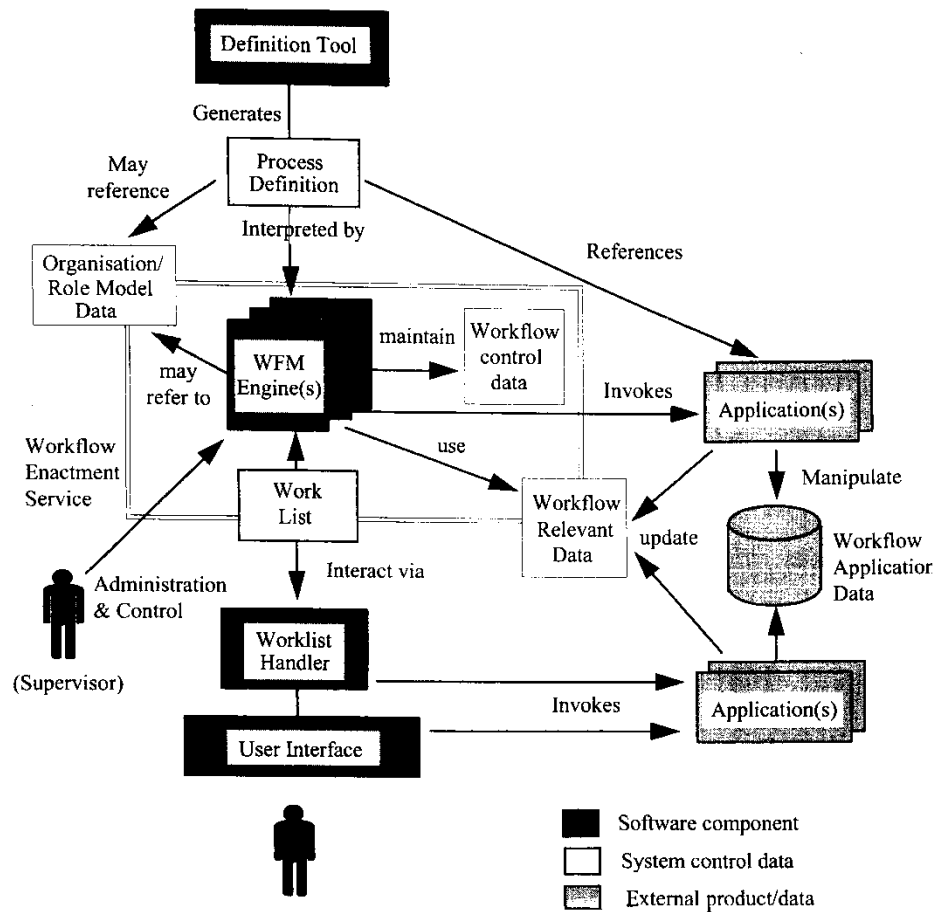
complexity & workarounds

usability vs Expressability

procedural vs. declarative

Formal vs. Commercial

# Business Process Execution and Monitoring



[www.wfmc.org](http://www.wfmc.org)

# The Status in Australia

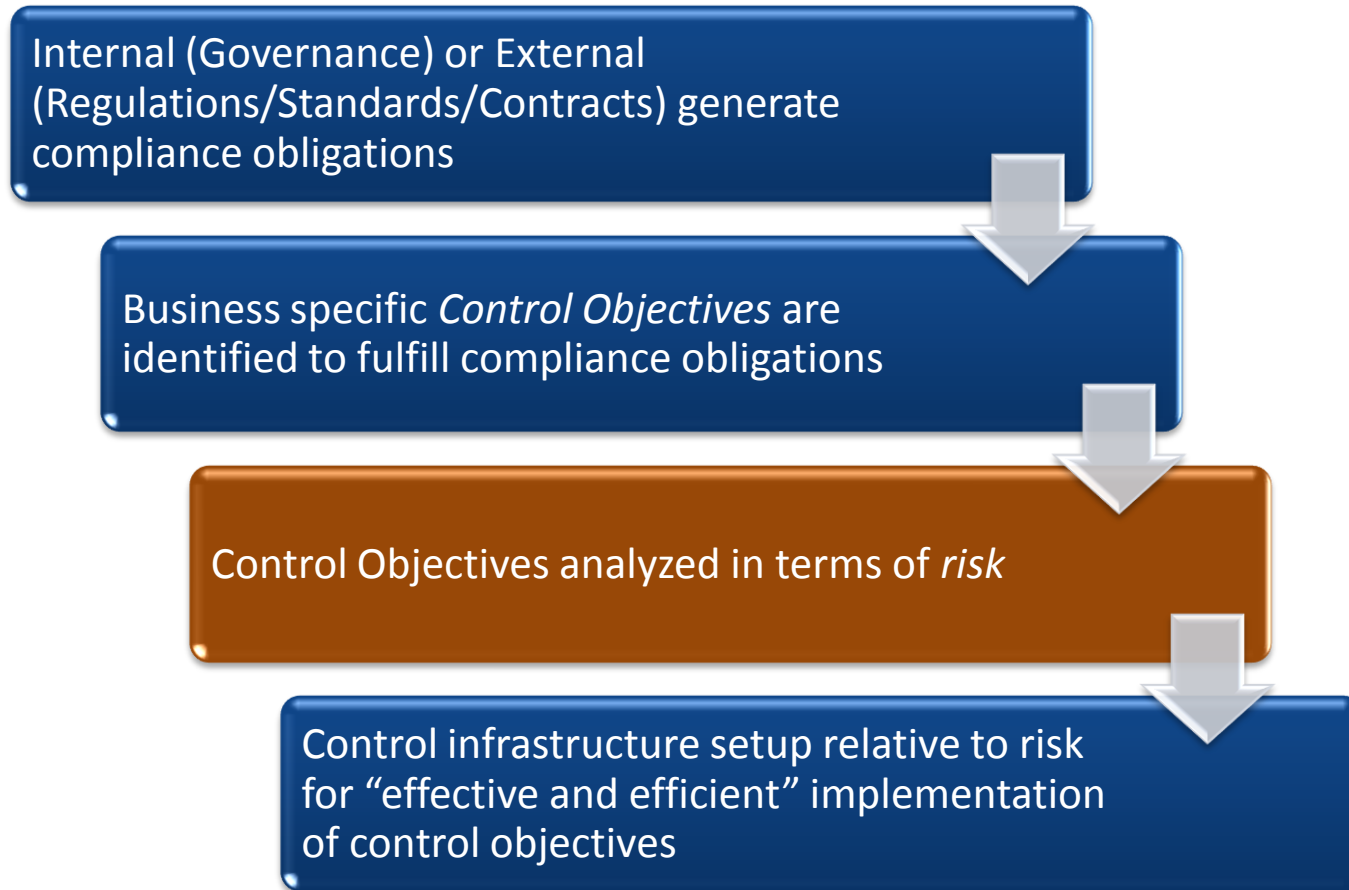
- Dedicated BPM responsibilities
- Centralisation of tools and methodologies
- First service-enabled business processes
- Local and national BPM CoPs
- High number of conferences
- First BPMG Courses
- BPM is part of university curricula
- BPM-focused consulting companies

# Compliance and BPM

# Compliance Pipeline



# Risk Assessment



# Risk Management

- Process of identifying vulnerabilities and threats to the processes used by an organisation in achieving business objectives, and deciding what *controls*, if any, to implement to reduce risk to an acceptable level.
- Effective risk management begins with a clear understanding of an organisation's *appetite for risk*.

# Risk Profile

- Each company will need to determine what “material business risks” it faces.
- When establishing and implementing its system of risk management a company should consider all material business risks.
- These risks may include but are not limited to:
  - financial reporting risks – the risk of a material error in the financial statements
  - other risks, such as operational, environmental, sustainability, **compliance**, strategic, external, ethical conduct, reputation or brand, **technological**, product or service quality and human capital which if not properly managed will affect the company.

(ASX Principles of Good Governance, Recommendation 7.1, Nov. 2006)

# Threats

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure
- *Non-compliance*

The result of any threat occurring is *impact*  
(or *loss*)

# Losses

- Direct loss of money
- Breach of legislation
- Loss of reputation/goodwill
- Endangering staff and/or customers
- Breach of confidence
- Loss of business opportunity
- Reduction in operational efficiency
- Interruption of business activity

# Impact Example

Threat	Potential Impact			
	<i>Inability to process data</i>	<i>Loss of data</i>	<i>Modified data</i>	<i>Unauthorized disclosure</i>
Acts of God	X	X		
H/W or S/W failure	X	X	X	
Human Error		X	X	
Maliciousness	X	X	X	
Crime			X	X
Invasion of Privacy				X

# Risk Analysis

## Conventional Approach

- Identify and value assets (**processes**) to be protected
- Identify potential threats
- Estimate likelihood of threat
- Evaluate existing safeguards
- ÷ Extent of potential loss

# Risk Analysis - Techniques

## ANNUAL LOSS EXPECTATION (ALE)

$$\text{ALE} = \frac{\$10^{(P+D-3)}}{4}$$

### P = RATING FOR PROBABILITY

0	IMPOSSIBLE
1	ONCE IN 400 YRS
2	40 YRS
3	4000 DAYS
4	100 DAYS
5	10 DAYS
6	1 DAY
7	10 TIMES A DAY

### D = RATING FOR ESTIMATED LOSS

0	ABOUT \$1 (\$10 <sup>0</sup> )
1	10
2	100
3	1000
4	10000
5	100000
6	1000000
7	10000000

# Handling Risk

- **Avoid** e.g., if possible, choose not to implement processes
- **Mitigate** e.g., define and implement controls
- **Transfer** e.g., share risk (insurance)
- **Accept** e.g., formally acknowledge existence of risk and monitor it
- **Eliminate** e.g., where possible, remove source of risk.

# Internal Controls

- designed to reduce threats/vulnerabilities to an acceptable level of risk
- can be preventive, detective, and/or corrective

# Process Portfolio M'gmnt

- A *process-aware organization* has a better understanding of the most important set of its business processes.
- Process portfolio management can make a first substantial contribution.
- *“What processes are exposed to the largest risk?”*
- *“What are the top five riskiest processes in the business?”*

# Risk & Business Processes

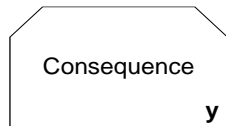
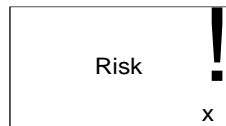
(zur Muehlen & Rosemann, 2005)

- Two process lifecycle phases:
  - *Build-time*, when the layout and input/output requirements of a process are designed, and
  - *Run-time*, when instances of the designed process are executed.

# Process-specific Risk Types

- Goal risk
  - Structural risk
- } **Build-time**
- Data risk
  - Technology risk
  - Organisational risk
- } **Run-time**

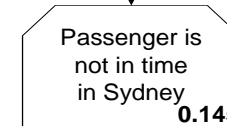
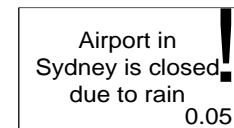
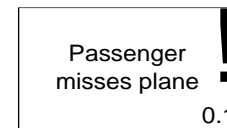
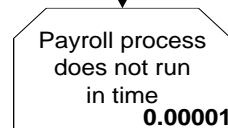
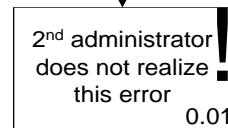
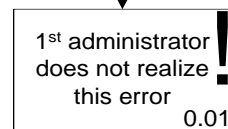
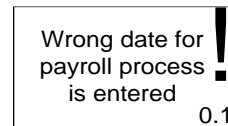
# Risk State Model



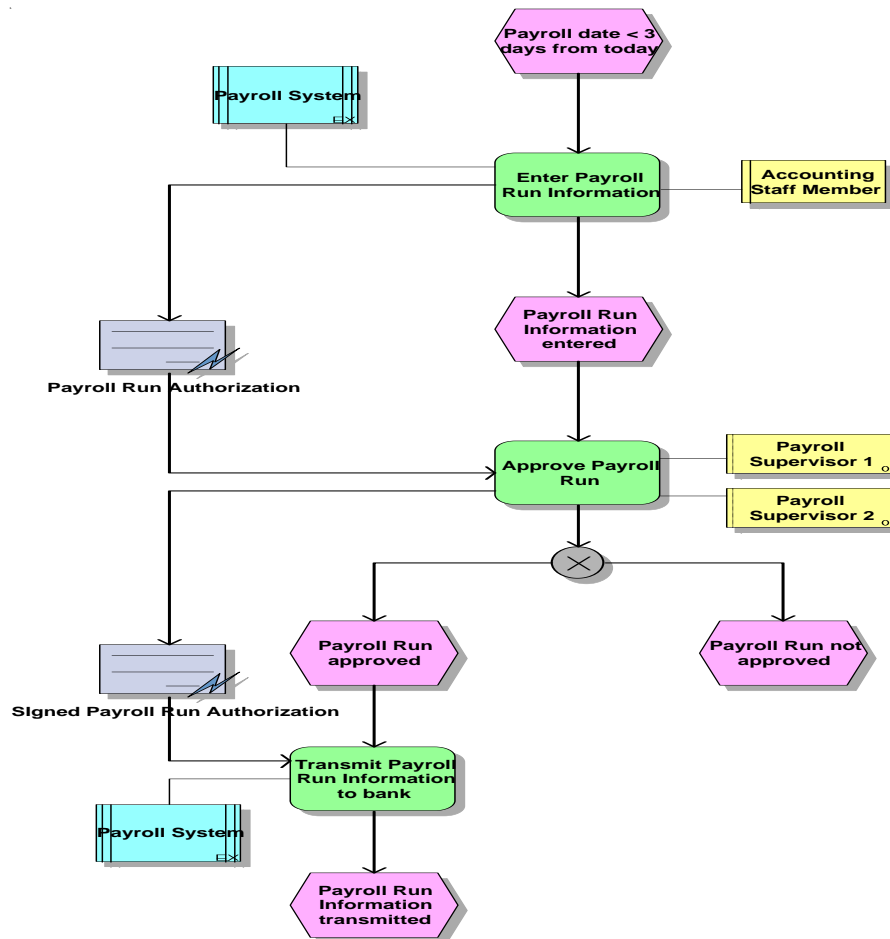
Is followed by

Causes

X: local probability  
y: global probability



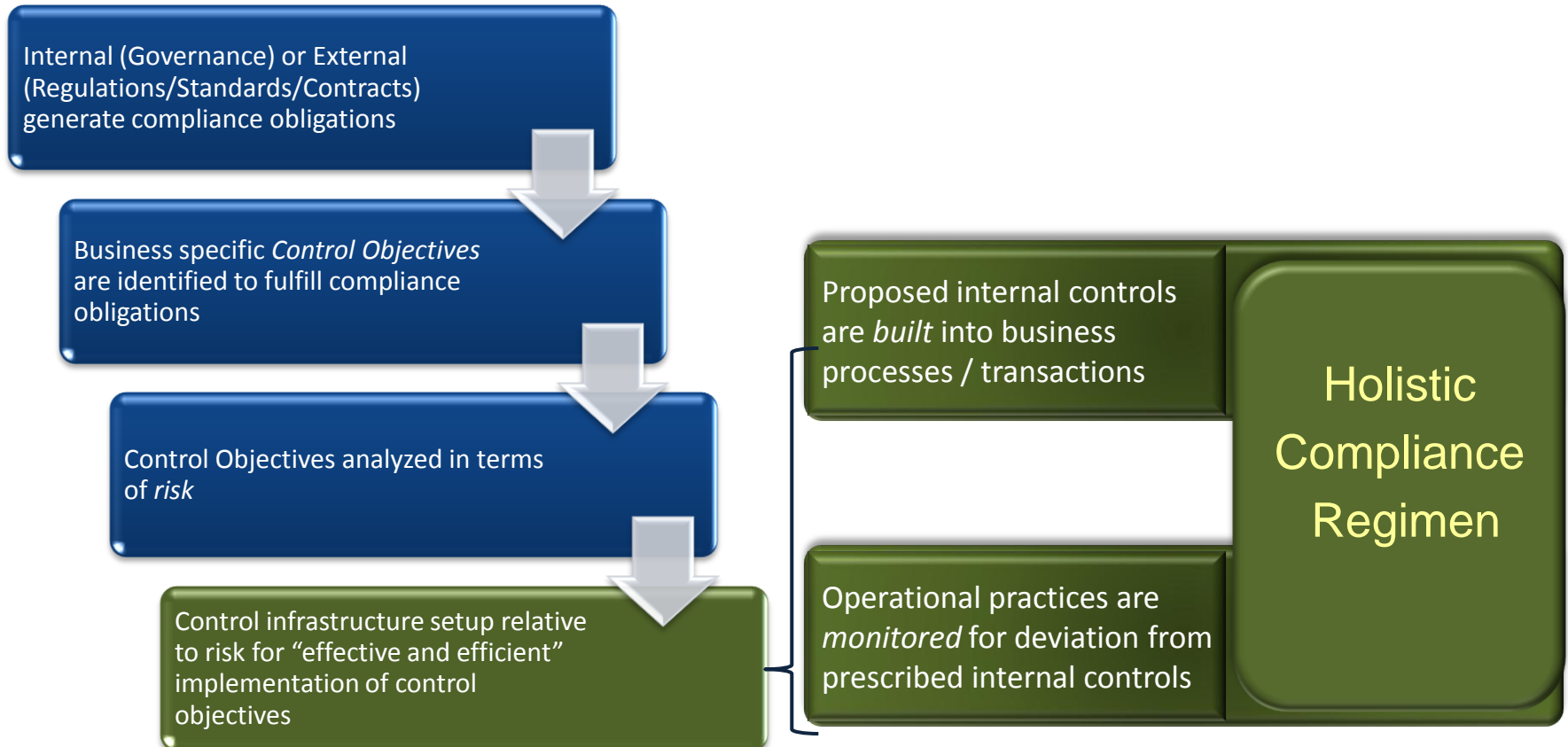
# Extended Risk Model



Structural Risk	Technology Risk	Organisational Risk
Data Entry Mistake	Payroll System Failure	
		Violation of separation of duties principle
	Transmission Failure	
	Transmission Intercepted	
	Payroll System Failure	

# A Methodology for Compliance by Design

# Compliance Pipeline



# A Methodology for Compliance by Design

- Controls Directory Management
- Ontological Alignment
- Modeling Control Objectives
- Process Model Enrichment
- Event Monitoring

# Methodology

- Controls Directory Management
- Ontological Alignment
- Modeling Control Objectives
- Process Model Enrichment
- Event Monitoring

---

Control objective: *prevent unauthorized use of purchase order process*

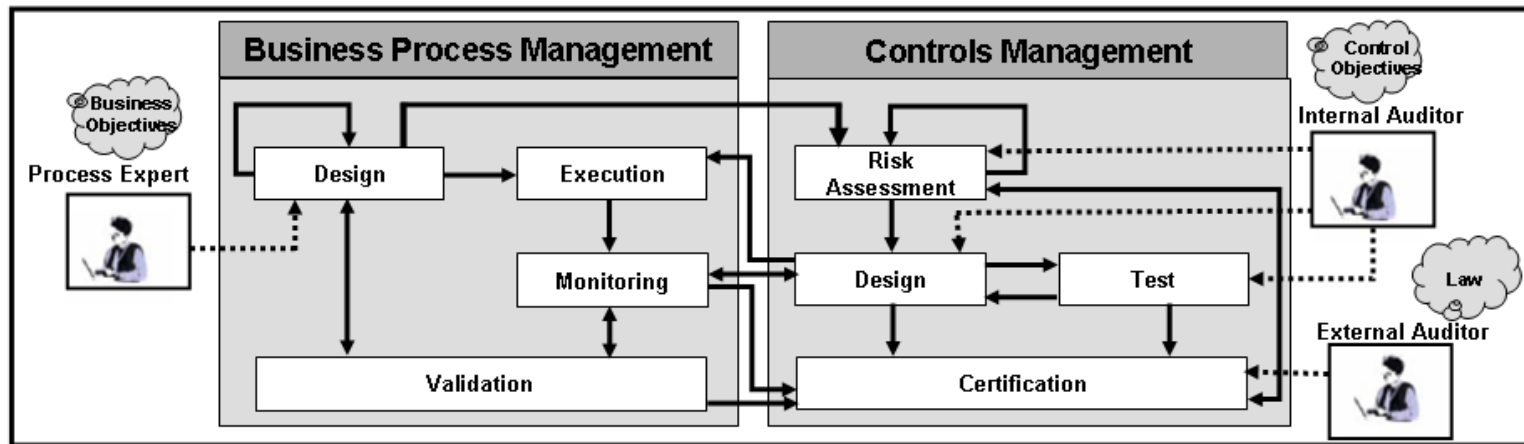
Risk: *unauthorized creation of purchase orders and payments to non-existing suppliers*

Internal control: *the creation and approval of purchase orders must be undertaken by two separate purchase officers*

---

# Methodology

- Controls Directory Management
- Ontological Alignment
- Modeling Control Objectives
- Process Model Enrichment
- Event Monitoring



# Risk Management & BPM (revisit)

## BPM

- Focus on **providing value** for stakeholders

---

- Performance depends on **effectiveness** of business processes

---

- Performance is **influenced** by process design

---

- Feedback is obtained through **performance indicators** assigned to systems and processes

---

- Performance objectives are **achieved** through optimized processes

## Risk Management

- Focus on **ensuring value** for stakeholders

---

- Risk is an **inherent property** of business processes

---

- Risk is **mitigated** by process design

---

- Feedback is obtained through **Risk Indicators** assigned to systems and processes

---

- Risk is **mitigated** through optimized processes

# Control Infrastructure & BPM



# Methodology

- Controls Directory Management
- Ontological Alignment
- **Modeling Control Objectives**
- Process Model Enrichment
- Event Monitoring

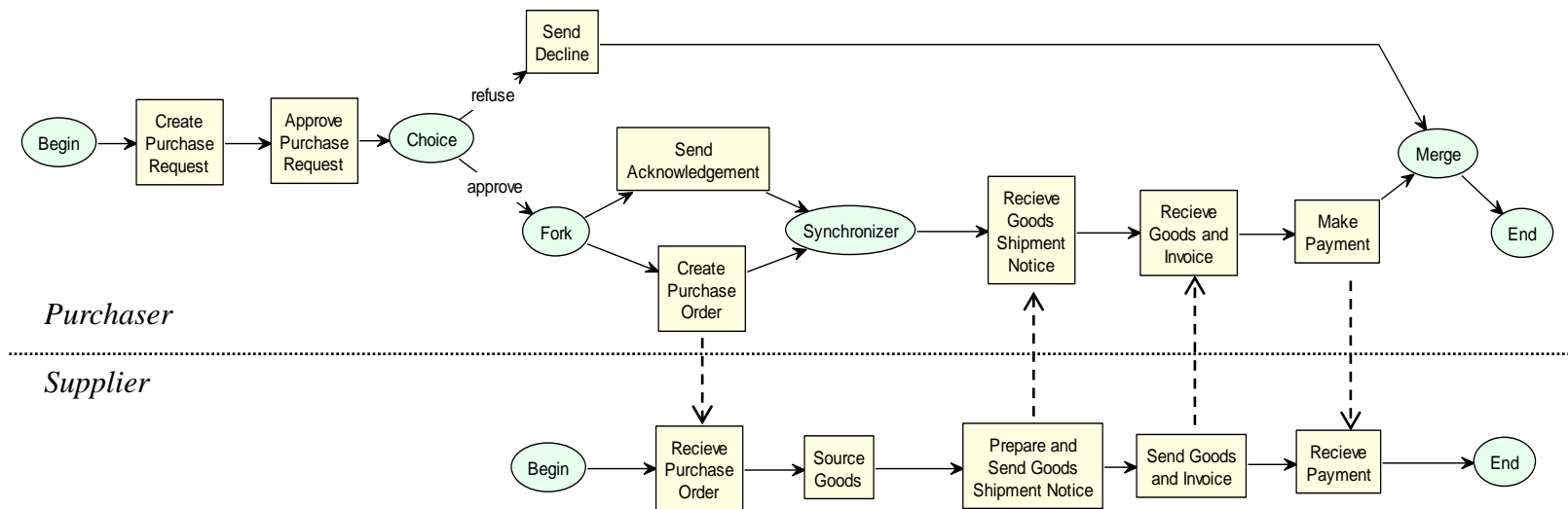
Formal language based on deontic logic to represent and analyze normative positions stemming from compliance requirements

*The creation and approval of purchase requests must be undertaken by two separate purchase officers*

$c1: \text{CreatePR}(x,y):t, \text{PurchaseOfficer}(y):t, \text{PurchaseOfficer}(z):t, y \neq z:t \Rightarrow \text{OpApprovedPR}(x,z) :t$

# Methodology

- Controls Directory Management
- Ontological Alignment
- Modeling Control Objectives
- Process Model Enrichment
- Event Monitoring

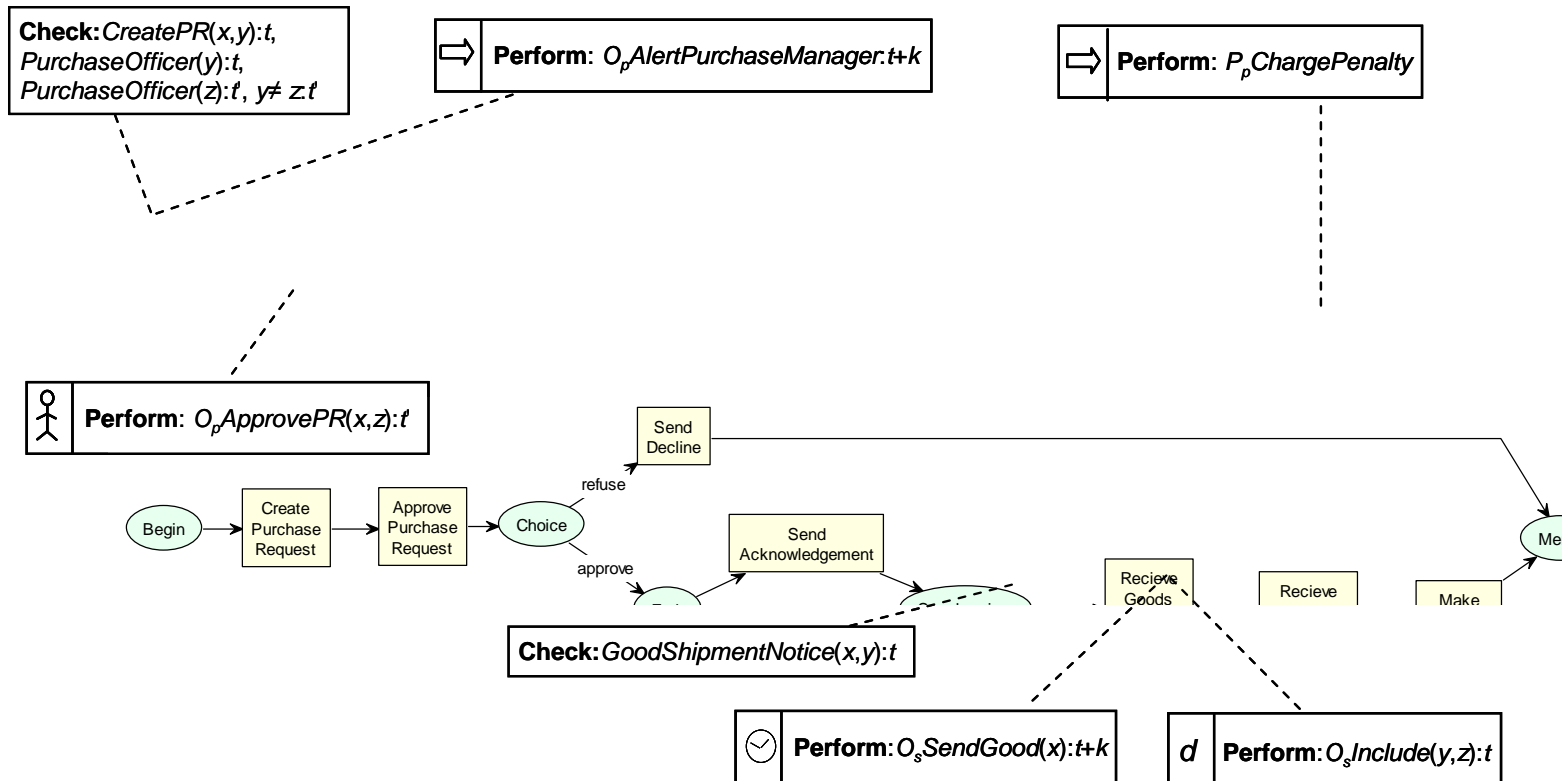


*purchase-to-pay scenario*

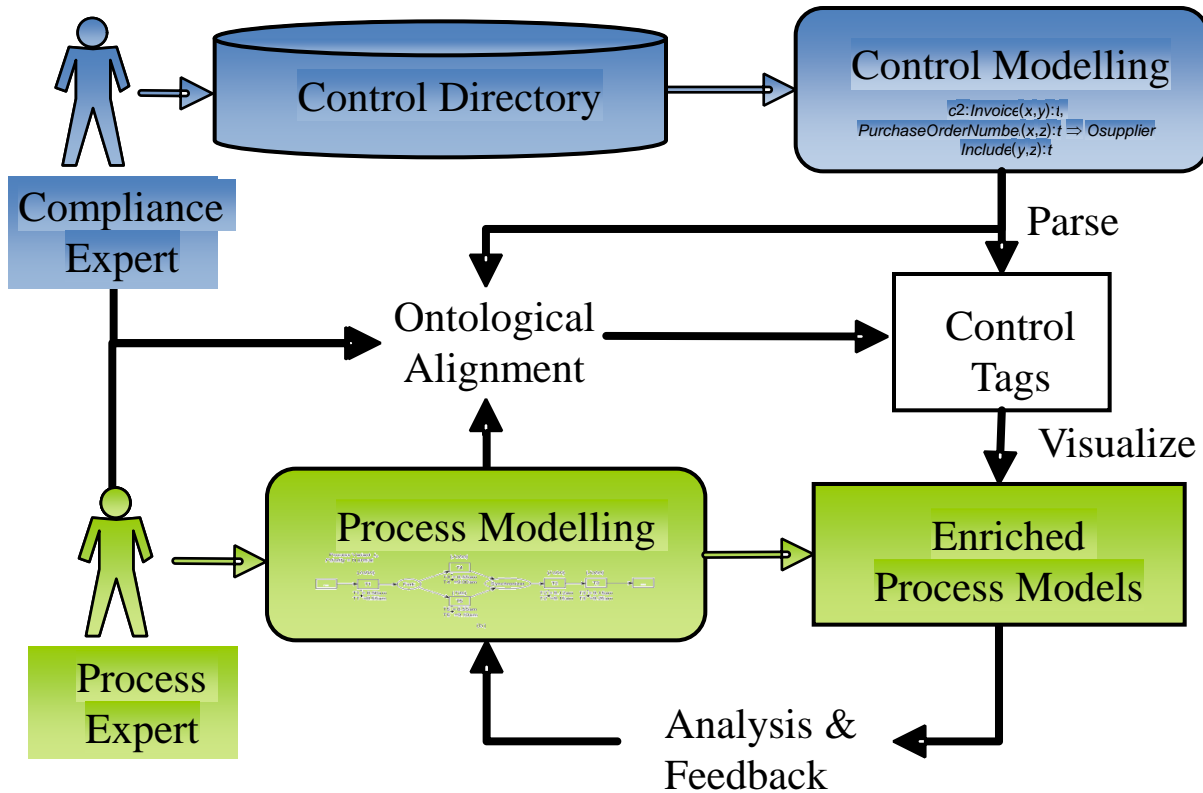
# Process Model Enrichment through *Control Tags*

- Control Tags provide a means of annotating **control objectives** (and constituent internal controls) on a business process model, thus providing a clear separation from business objectives
  - **Flow Tag:** A flow tag represents a control objective that would impact on (the flow of) the business activities, e.g. approval of leave must occur before payment for travel.
  - **Data Tag:** A data tag identifies the data retention and lineage requirements, e.g. a medical practice must retain the time of commencement of pathology tests.
  - **Resource Tag:** A resource tag represents controls relating to access, role management and authorization, e.g. persons performing cash application and bank reconciliation must be different as it allows differences between cash deposited and cash collections posted to be covered up.
  - **Time Tag:** A time tag identifies controls for meeting time constraints such as deadlines and maximum durations, e.g. a water leakage complaint must be investigated within 12 hours of lodging.

# Process Model Enrichment tag visualization



# Summary



# What do you think?

Challenges of using BPM as a vehicle  
for driving Compliance

# Summary – Top Challenges\*

- Volume of regulatory (frequency of new/updated regulations/legislation) and organizational change
- Limited \$ to be spent on improvement so manual workarounds
- Getting buy-in from staff for process design
- Constantly down in the trenches, no time to high-level view
- Pace of industry change – especially financial services sector (new ways of doing business, constantly changing requirements)
- Lack of integration between systems & legacy, hence continue with silo approach (too difficult otherwise)
- Clients' changing requirements (outsourcing, multiple countries, obligations, etc)

\* Identified by participants during discussion at end of the workshop



# Industry Driven Research Agenda for Compliance Management

Researchers from The University of Queensland are carrying out an ACI-endorsed study to develop a Compliance Management Research Agenda that aims to **address problems experienced by industry**.

Would you like to share your views on issues in Compliance Management and **help drive Compliance Management Research in the right direction?**

For more details please contact:

Dr. Shazia Sadiq<sup>1</sup>, Dr. Marta Indulska<sup>2</sup>

<sup>1</sup>School of Information Technology and Electrical Engineering, <sup>2</sup>UQ Business School

The University of Queensland, St Lucia, QLD 4072

Brisbane, Australia

email: [shazia@itee.uq.edu.au](mailto:shazia@itee.uq.edu.au); [m.indulska@business.uq.edu.au](mailto:m.indulska@business.uq.edu.au)

ph: 0421 115 662 (Shazia), 0412 401 060 (Marta)