An Integrated Approach to the Internal Control System

- New Methodology for Evaluating Design and Effectiveness -

Carolyn Dittmeier
President, IIA Italy
Vice President, Head of Internal Auditing Poste Italiane
Increasing legislation and regulation of governance

- Anti corruption (Law 231)
- Sarbanes (Law 262)
- Stock Exchange Governance Code
- Bank Regulations

New Corporate Governance players

Corporate Governance Paper
IIA Italy
Numerous corporate governance players

- Compliance Officer
- Audit Committee
- Board of Directors
- Board of Statutory Auditors
- Other Control Bodies
- CFO
- Quality
- Security
- Compliance Function
- Inspectorate
- Privacy
- Operational Management
- Human Resource & Organization
- Safety
Possible consequences:

Cost efficiency
Cost of governance exceeds benefits in risk reduction

Effectiveness
Inadequate/fragmented risk coverage
Corporate Governance Paper
Associazione Italiana Internal Auditors

Key points to an Integrated Corporate Governance Model:

I. Global business risk assessment

II. Unified Internal Control System
   • Three Control Levels
   • Optimizing Relationships
   • Single Evaluation Criteria

III. Mechanisms of Assurance
**Business Case**

Logistics, postal and courier express
Banking, financial services and insurance

**General Strategy**

Leveraging upon a major national network, integrating new innovative services to core businesses

- **150,000 Employees**
- **14,000 Post offices**
- **200 Logistic Centres**
- **40,000 Vehicles**
- **2,700 ATM**

**€ 15,900 Total Sales (mil)**

of which:

- **€ 5,300 Logistics/Postal**
- **€ 4,400 Financial/ Banking**
Business Case

Governance milestones

1994 - Public Economic Entity

1998 - Transformation to a stock company “Poste Italiane - Società per Azioni”

2001 - Poste Italiane is subject to supervision of Financial Regulatory Bodies

2002 - Implementation of Internal Audit replacing Inspectorship

2003 - Implementation of Ethics Officer

2005 - Code of Ethics

2006 - Implementation of Enterprise Risk Management Model

2007 – Introduction of Sarbanes – Accounting Officer
I. Global Business Risk Assessment
Global Business Risk Assessment?

Operational risks
Compliance risks
Strategic risks
Financial risks
Reputational risks
Accounting risks
Business Case

Enterprise Risk Management framework adopted in 2006

Risk Model based on Goal Model
ERM Business Maturity Checkpoints

1. Risk Framework
2. Control Risk Self-Assessment workshop
3. Strong professional development programs
4. Budget and incentive system incorporating Key Risk Indicators
5. Full risk management culture
II. A Unified Internal Control System

- Three Control Levels
- Optimizing Relationships
- Single Evaluation Criteria
Three levels of control activities within the Enterprise Risk Management Model

Company Bodies

Audit Committee

Definition of Objectives
Risk Management
Internal environment
Information and communication

COSO:

Control activities

3rd Level Assurance Activity (Internal Audit)

2nd Level Monitoring Activity (Risk Management, Compliance, Controller)

1st Level Control Activity (Line Control)
A Unified Internal Control System

Optimizing Relationships between Control bodies and functions

Informational Reporting

Communication by meetings and presentations

Providing Directives

In relation to their assurance, consulting or other roles
Overall Internal Control

Semiannual

Bimonthly

Risk Management Bancoposta
Compliance Function Bancoposta
Company Business Units and Depts

Reporting & Interchange between Governance & Control Bodies

Quarterly

Bimonthly

Internal Audit, Human Resources, Legal Affairs; CFO; Security/Risk Mgmt

Periodic :

Financial Reporting control

Risk and Compliance issues
A Unified Internal Control System

Integrated methodology for business control identification and evaluation

Focusing separately on:

- Control Design
- Control Operating Effectiveness
How to evaluate the Integrated Internal Control System

Risk Tolerance

Risk Acceptance

Control Objectives

Adequacy

Effectiveness, Efficiency and cost effectiveness

Control Design

Relevance

Strength

Coverage

Reactivity

Operating effectiveness

Resources availability

Compliance verification

Red-flag analysis
Definition of a ‘control’?
A set of activities whose purpose is to identify and correct errors and anomalies in order to reach defined control objectives, risk based.
Control Objectives, risk based (examples)

- Quality and timeliness of operations
- Reliability and integrity of Company information (financial and operational)
- Proper and effective contractual relations with customers and suppliers
- Compliance to Regulations
- Prevention of fraud
- Business continuity
How to evaluate the Integrated Internal Control System

Risk Tolerance → Control Objectives → Adequacy

Risk Acceptance

Control Design
- Relevance
- Strength
- Coverage
- Reactivity

Effectiveness, Efficiency and Cost effectiveness

Operating effectiveness
- Resources availability
- Compliance verification
- Red-flag analysis
Production of fresh cheese according to quality standards

For every fresh cheese lot, the Production Dept requests, up to 5 days before the fermentation process, requests from the Purchasing Dept quantities of milk supplies on the basis of approved monthly sales forecasts.

Upon supply of milk (<3 days) the Production Dept proceeds:
- Pasteurisation (2 hours)
- Coagulation of casein (2 hours)
- Drainage of whey (1 hour)
- Pressing and salting (1 hour)
(time frame automatically recorded in 3 of 4 phases)

The Quality Dept verifies respect of production time standards. If non compliant, it blocks the packaging process, requesting the lot to be destroyed and re-produced.

Following authorization given by Quality Dept, the Production Dept proceeds to package the fresh cheese within 24 hours for delivery by the Distribution Dept by the next day.
Case study: quality cheese production

Control objectives: Ensure fresh cheese according to quality standards

- Ensure the absence of pathogens in the milk
- Ensure production-time for avoiding pathogenic generation
- Ensure temperature-preservation for avoiding pathogenic generation

Control over Production Time Standards

Information System

Actual time frame (automatic) -> Check

- Lot destruction when out of time standard
- Replacement of Production lot
- Authorization for packaging

Time Limitation Standards
Control evaluation: scale of 1-5 (1-2 positive, 3-4-5 negative).
## Case study: quality cheese production

<table>
<thead>
<tr>
<th>Discretion</th>
<th>Integration</th>
<th>Independence</th>
<th>Segregation</th>
<th>Automation</th>
<th>Adaptability</th>
<th>Traceability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>-</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>-</td>
<td>3</td>
</tr>
</tbody>
</table>

**Strength**

3
Case study: quality cheese production

Control design evaluation: positive (2)

Scenario
- scenario 1^ Known and positive design
- scenario 2^ Known; design non positive
- scenario 3^ Unknown design

Control operating effectiveness evaluation: good (3)

Audit Program
- Test 1
  Verify Information system utilized for standard check

- Test 2
  Examine Sample of production lots checked by Quality Dept

Audit Exception Level
- Test 1: 20% - Test 2: 5%
Corporate Governance Paper
Associazione Italiana Internal Auditors

Key points to an Integrated Corporate Governance Model:

<table>
<thead>
<tr>
<th>I. Global business risk assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>II. Unified Internal Control System</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>III. Mechanisms of Assurance</td>
</tr>
</tbody>
</table>