

# *Compliance Applicata*

**Milano, 7 febbraio 2007**

**Dr. Jean Paul Ballerini**  
*Sr. Technology Solutions Expert*

 **INTERNET|SECURITY|SYSTEMS®**

*Ahead of the threat.™*



AAAAAAHHHH  
HH!!!!

# *Il ciclo di gestione della sicurezza*

**1. What is at risk**  
Vulnerability Mapping

**2. What to protect first**  
Protection prioritization



**4. How to show return on investment (ROI)**  
Reporting and Benchmarking

**3. How to protect the entire IT infrastructure**  
Threat prevention and shielding

# Il ciclo di gestione della compliance

1. **Analysis:**
  - Risk Analysis
  - Gap Analysis



# Avete mai sentito parlare di CIA?

Confidentiality	Integrity	Availability
Classification	Classification	Classification
Governance	Governance	Governance
Assessment	Assessment	Assessment
<b>Compliance</b>	<b>Compliance</b>	<b>Compliance</b>
Identification	Identification	Identification
Authentication	Authentication	Authentication
Authorisation	Authorisation	Authorisation
Administration	Administration	Administration
Auditing	Auditing	Auditing
Non-repudiation	Non-repudiation	Non-repudiation
Alerting	Alerting	Alerting
Assurance	Assurance	Assurance
Accountability	Accountability	Accountability

## ■ Identification

- Identify the organisation and business objectives.
- Identify the business process.
- Identify the relevant framework(s).
- Identify the relevant control practices or activities.

## ■ Cross-Reference

- Execute cross-reference mapping to all identified frameworks and standards.
- Execute cross-reference mapping to all identified compliance initiatives.
- Execute cross-reference mapping to all identified IT areas, departments and roles.

## ■ Self-Assessment/Benchmark

- Perform a “high level” self-assessment.
- Record initial results as a benchmark for maturity measurement.
- Review self-assessment results at both an aggregated level and control practice/activity level.
- Based on risk results, perform a detailed risk assessment to include asset impact and “risk realization” cost.

# *Contro cosa ci si misura?*

- **Security Standards and Best Practice**
- **Requirements and objectives for information processing in support of business operations**
- **Legal, regulatory and contractual requirements**

# Information Security Standards – Best Practice (esempi)

- **ISO/IEC 17799 – Code of Practice for Information Security Management**
  - Provides best practice for information security management.
  - Basis upon which ‘baseline’ controls can be validated
- **ITIL – IT Infrastructure Library**
  - Best practice for IT service management
- **COSO – Committee of Sponsoring Organisation (of the Tradeway Commission)**
  - Provides best practice on financial controls
- **COBIT – Control Objectives for IT and Related Technology**

# Information Security Standards – Standards (esempi)

- **ISO/IEC 17799:2005**
  - Code of Practice for Information Security Management
- **ISO/IEC 13335**
  - Guidelines for the Management of IT Security
- **NIST**
  - National Institute for Standards and Technology

# Il ciclo di gestione della compliance

1. Analysis:  
Risk Analysis  
Gap Analysis



1. Define  
Countermeasures

# Definire le contromisure

## ■ IT Risk Mitigation

- Identify potential risk mitigation options. (e.g. Products or Services)
- Identify all associated costs for each mitigation option.
- Identify any residual risk.
- Compare costs associated with risk mitigation option against “risk realization” cost to identify TCO/ROI.

## ■ Evaluate Results

- If accepted, initiate a project to implement the selected IT risk mitigation option.
- Map the value associated with the IT activity back to the organization and business objectives.
- Review the relevance of the IT activity to the cross-references for frameworks and compliance initiatives.

# *Approccio Risk Based vs Compliance Based*

## ■ **Risk Based Approach**

- Identify assets and their related values
- Identify and measure threats and associated vulnerabilities
- Determine impact levels and countermeasures to manage risk levels
- Prove due diligence through a thorough and methodical approach
- Determine controls that are specific to meet the organisations business needs

## ■ **Compliance Approach**

- Identify requirements of legislation or regulation
- Implement controls based on the requirements

# Correlare le contromisure agli obiettivi aziendali

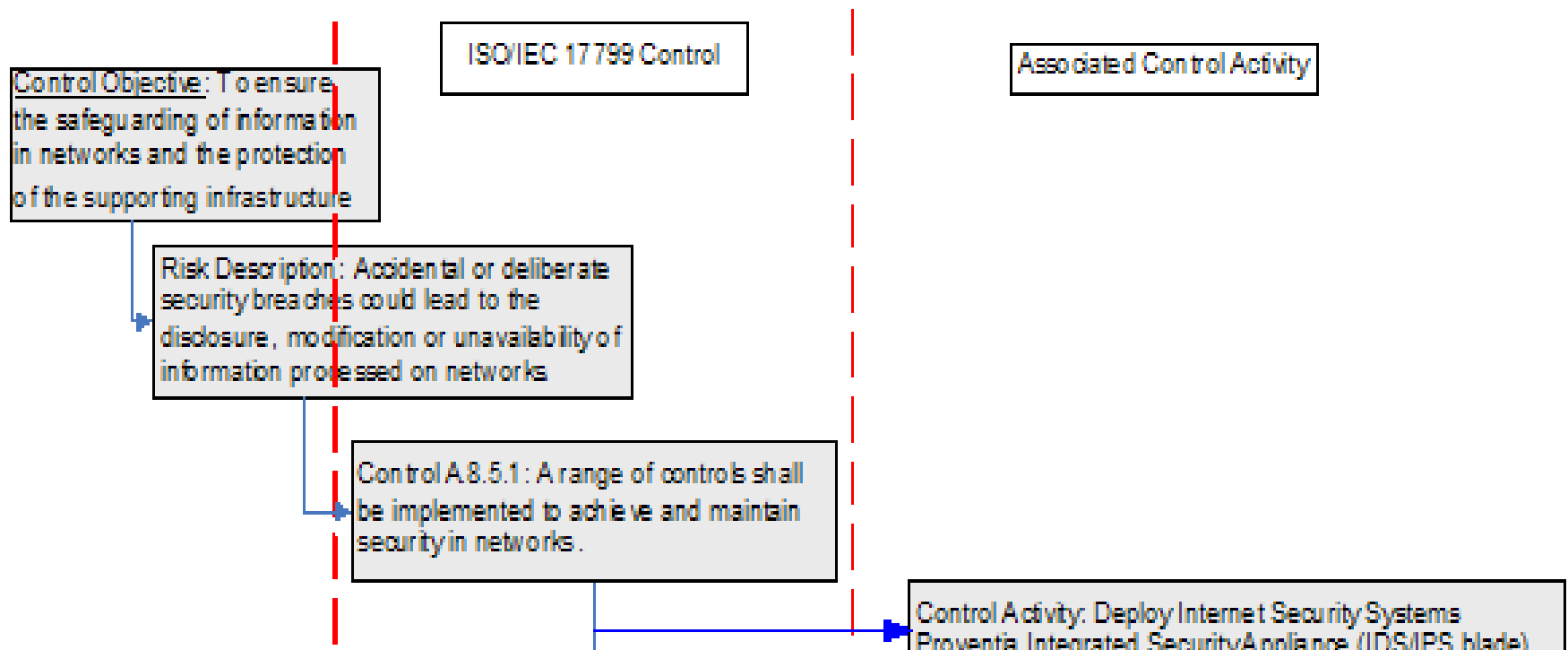
With effective IT risk management approach in place, key interests of corporates are addressed; providing IT alignment with the business.

<u>IT Risk Management</u>	<u>Key Interest</u>	<u>Key Interest Addressed?</u>
<ul style="list-style-type: none"><li>■ Identify</li></ul>	<b>Corporate</b> <ul style="list-style-type: none"><li>■ Does IT support the achievement of organizational objectives?</li><li>■ Are targeted enterprise-wide IT synergies being achieved?</li><li>■ Are IT risks being identified and managed?</li></ul>	<input checked="" type="radio"/> <b>YES</b>
<ul style="list-style-type: none"><li>■ Cross-reference mapping</li></ul>		<input checked="" type="radio"/> <b>YES</b>
<ul style="list-style-type: none"><li>■ Risk Assessment</li></ul>	<b>Business Units</b> <ul style="list-style-type: none"><li>■ Does IT deliver on its service level commitments?</li><li>■ Do IT investments positively affect business productivity?</li><li>■ Are IT costs being managed effectively?</li></ul>	<input checked="" type="radio"/> <b>YES</b>
<ul style="list-style-type: none"><li>■ Risk Mitigation Options</li></ul>		<input checked="" type="radio"/> <b>YES</b>
<ul style="list-style-type: none"><li>■ Map IT control practice/activity</li></ul>		<input checked="" type="radio"/> <b>YES</b>

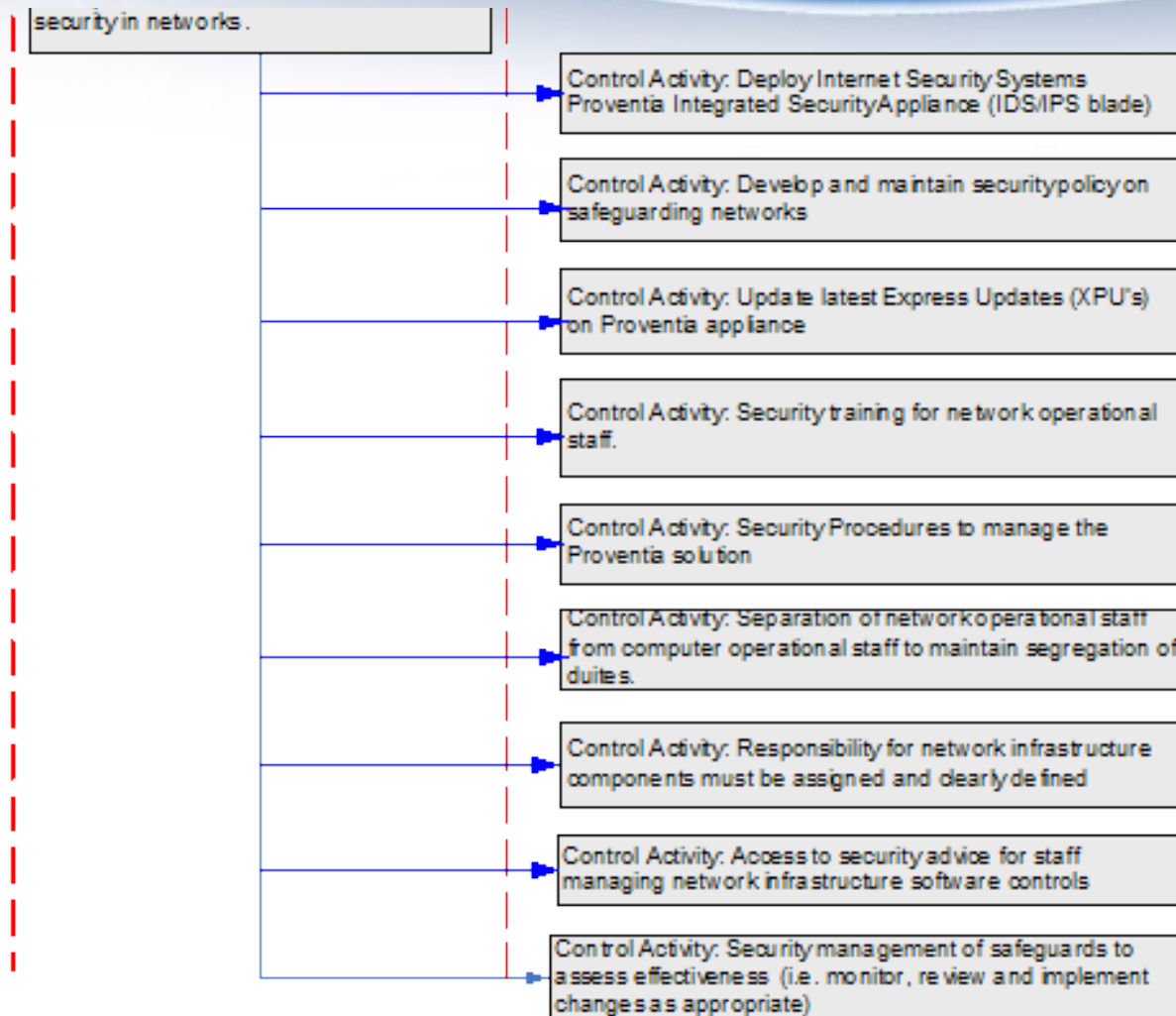
# Da politica di sicurezza a implementazione

The challenge is in balancing a control activity with business needs.

## Process – Safeguarding of information in Networks



# Da politica di sicurezza a implementazione (cont)



# Analisi delle opzioni

The objective in implementing any control is to ensure the reduction or mitigation of the risk affecting the success in achieving the business goals. The example below illustrates how IDS/IPS help in facilitating the controls to support *service availability* and *compliance with policies and regulations*.

ISO 17799-2005 Controls

## Controls against malicious software

- 10.8.6 – Business Information Systems
- 10.9.3 – Publicly available information
- 11.4.1 – Policy on use of network services
- 11.4.5 – Segregation in networks
- 11.4.6 – Network connection control
- 11.6.2 – Sensitive system isolation
- 12.5.4 – Information leakage
- 12.6.1 – Control of technical vulnerabilities
- 14.1.2 – Business continuity and risk assessment
- 15.1.4 – Data protection and privacy of personal information
- 15.1.5 – Prevention of misuse of information processing facilities
- 15.2.1 – Compliance with security policies and standards



IDS	IPS
✓	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓
	✓
✓	✓
✓	✓
	✓
	✓
✓	✓

# Il ciclo di gestione della compliance

1. Analysis:  
Risk Analysis  
Gap Analysis



1. Define  
Countermeasures

1. Be Compliant  
Mitigate Risk  
Close Gap

# *Messa in opera delle contromisure*

## ■ **Deployment of Countermeasures**

- Procedures must be implemented and adhered to.
- Security solutions must be chosen, acquired and deployed.
- Security solutions must be configured to match the countermeasures defined in the previous step.
- Changes must be managed according to the according procedures.

## ■ **Monitoring of Countermeasures**

- Make sure the security solution works and is respected.
- Make sure EVERYBODY is compliant and made aware.
- Introduce security education and culture.

- **Bit-map**

- <https://www.bit-map.com/inno/text.php/request/home> has matrixes that map products to regulations.

# Il ciclo di gestione della compliance

1. Analysis:  
Risk Analysis  
Gap Analysis

1. Prove  
Compliance



1. Define  
Countermeasures

1. Be Compliant  
Mitigate Risk  
Close Gap

## ■ Logs and Reports

- Prove due care and due diligence according to the legislation and regulation.
- Prove failure to compliance due to external factors → prove due care and due diligence.

# Il ciclo di gestione della compliance

1. Analysis:  
Risk Analysis  
Gap Analysis

1. Prove  
Compliance



1. Define  
Countermeasures

1. Be Compliant  
Mitigate Risk  
Close Gap

# In poche parole

Compliance enforces and gives a framework for IT Risk Management which is the key in maintaining a balance between the business needs and the value associated with an IT solution.

## Organization/Business Objectives

- Competitive/Leader
- Profitable Growth
- Client Satisfaction
- Employer of Choice
- Strengthen Reputation

## Business Process

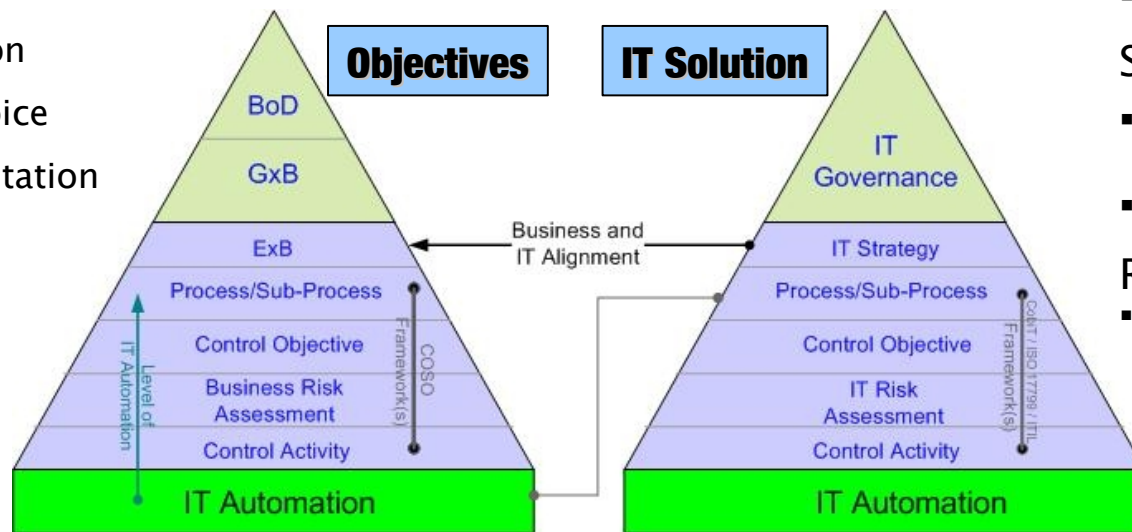
- Whichever

## IT

## Automation

- Level of Process

## Automation



## Framework(s)

- CobiT
- ISO 17799
- ITIL

## Self-Assessment

- High-level (Strategic)
- Low-level (Detailed)

## Risk Mitigation

- Pragmatic IT Risk Mitigation options align a more precise IT solution to support business needs without over-engineering.

# *Domande e Risposte*

*jpballerini@iss.net*

INTERNET SECURITY SYSTEMS  
GLOBAL SECURITY

GLOBAL SECURITY SOLUTIONS > MANAGED SECURITY SERVICES > X-FORCE RESEARCH

 **INTERNET | SECURITY | SYSTEMS®**

*Ahead of the threat.™*