



Computer Associates®

Blending Corporate Governance with Information Security

YVES LE ROUX CISSP CISM ITIL

Technology Strategist

Yves.leroux@ca.com

Plan

- What do we call « Corporate Governance » ?
- The 5 principles for an executive approach to information security
- Necessary shifts in information security perspective
- Areas of responsibility for implementation
- Building a enterprise security architecture
- Conclusion

Corporate Governance OECD Definition

Corporate governance is the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of **rights and responsibilities among different participants** in the corporation, such as, the board, managers, shareholders and other stakeholders, and spells out the **rules and procedures for making decisions** on corporate affairs. By doing this, it also provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance.

Corporate Governance World Bank Definition

Corporate governance is concerned with holding the balance between economic and social goals and between individual and communal goals. The governance framework is there to encourage the efficient use of resources and equally to **require accountability for the stewardship of those resources**. The aim is to align as nearly as possible the interests of individuals, corporations and society

European Commission Action Plan

- In the Action Plan published in May 2003, the Commission announced that it would
 - Confirm the collective responsibility of board members for financial statements and key non-financial information,
 - Increase transparency in intra group relations and transactions with related parties and
 - Improve disclosure about corporate governance practices.

5 Principles for an executive approach

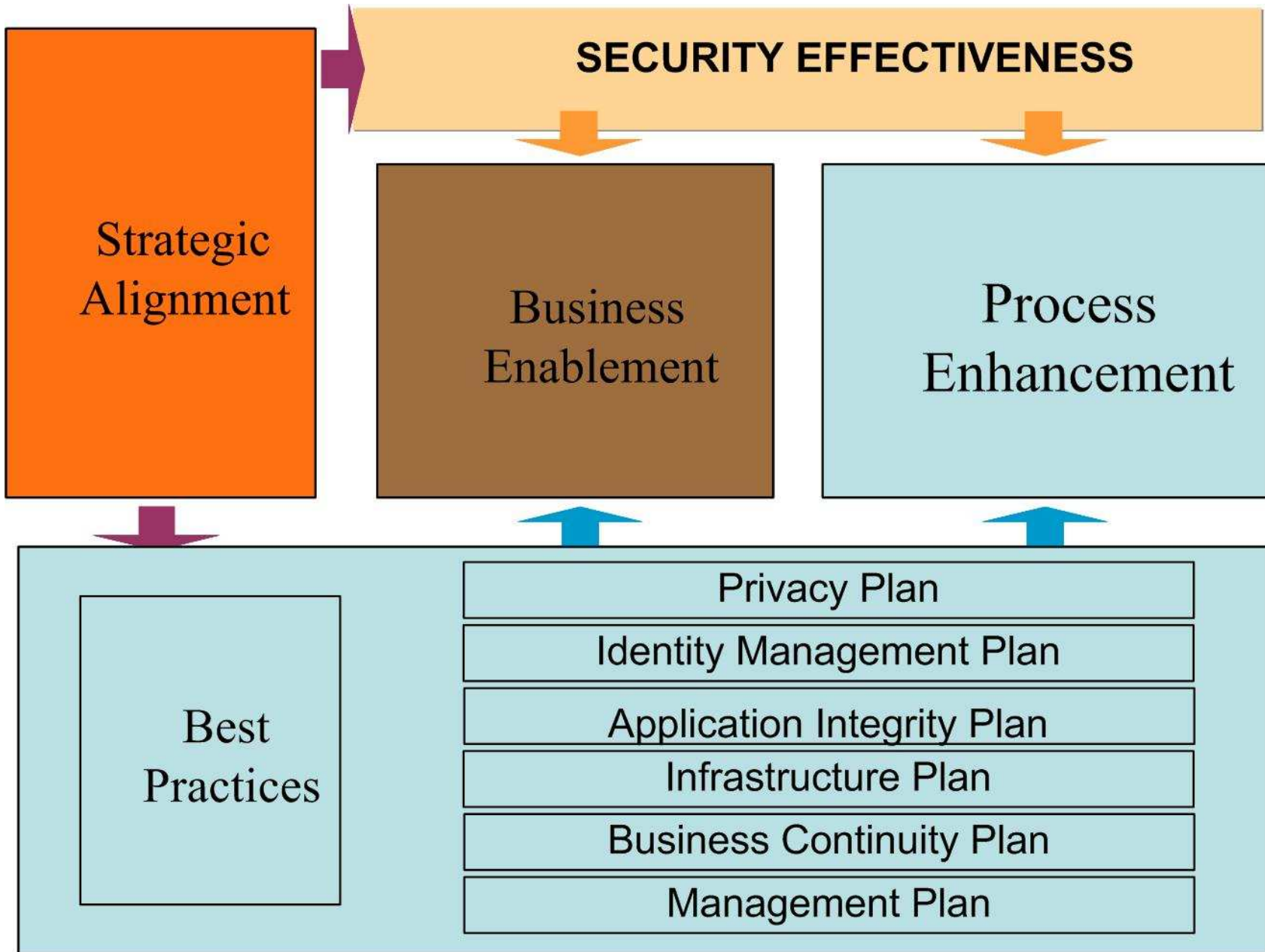
1. CEO Involvement
2. Organizational understanding of information assets
3. Integrating data storage with the system lifecycle
4. Systems must be tested
5. Comparative analysis

SHIFTS IN INFORMATION SECURITY PERSPECTIVE

- **Security is a technical problem**
- **Security has a technical owner**
- **There is an explicit focus on security**
- **Security is an expense**
- **The goal is security**
- **Security is an enterprise-wide problem**
- **Security is owned by the business**
- **Security is transparent**
- **Security is an investment**
- **The goal is business continuity and ultimately resiliency**

Five areas of responsibility

- Board of Director
- CEO
- Executive Committee
- Senior Managers
- Employees



Security Foundation

Conclusion

- Information security is not a technical issue, but rather a corporate governance responsibility.
- Without the active engagement of business unit leaders, executive management teams and boards of directors, a sustainable information security program cannot exist.
- The time to embrace information security governance is now.



Computer Associates®

Corporate Governance & Information Security

YVES LE ROUX CISSP CISM ITIL

Technology Strategist

Yves.leroux@ca.com