



C  NTROLLERS Aps

www.eurosox.dk

Agenda

- **Governance, Risk, and Compliance**
- Sarbanes-Oxley
- EuroSox
- Frameworks and best practices
- What does an IT manager need to know?
- Concluding remarks

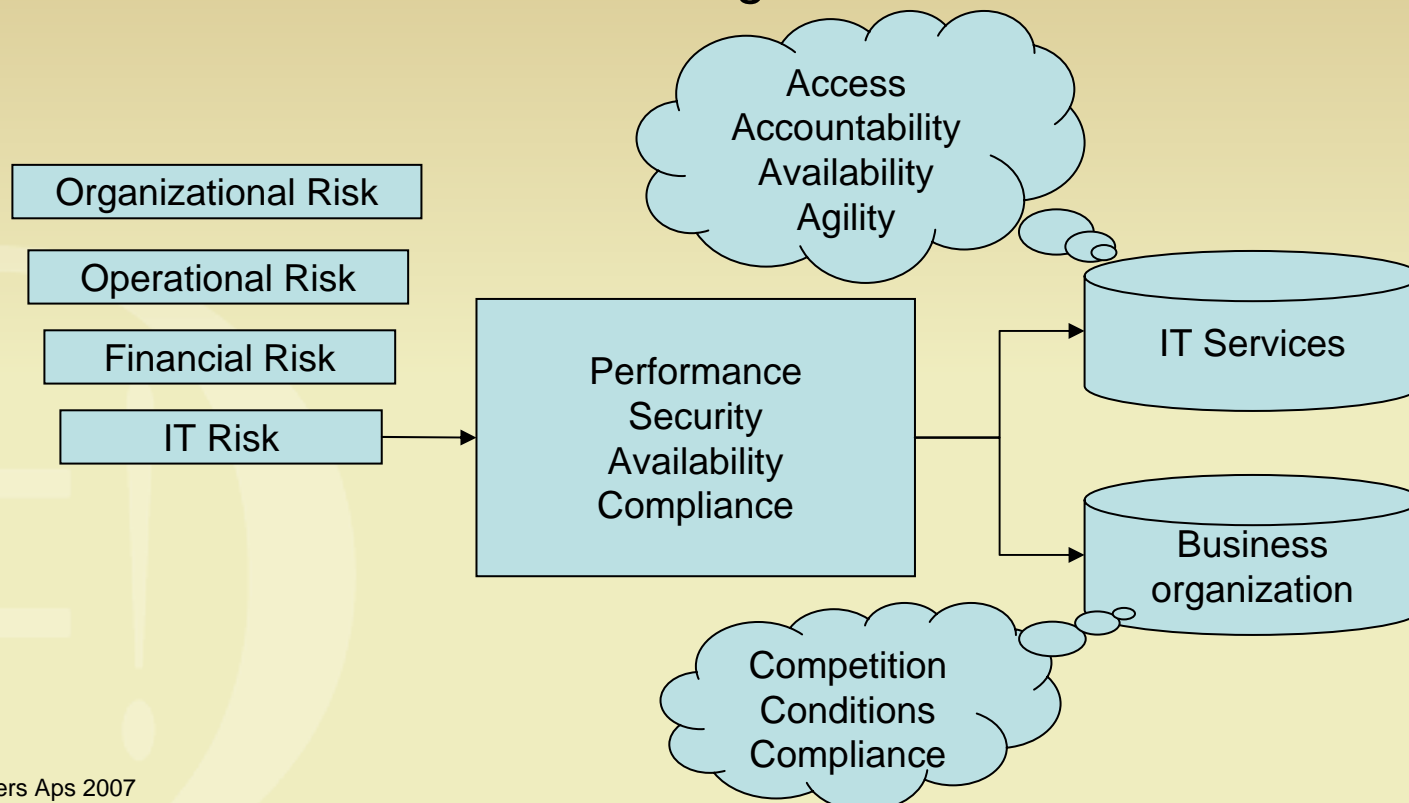


“Corporate governance is the set of processes, customs, policies, laws and institutions affecting the way in which a corporation is directed, administered or controlled. Corporate governance also includes the relationships among the many players involved (the stakeholders) and the goals for which the corporation is governed. The principal players are the shareholders, management and the board of directors.”

- Key principles
 - Rights and equitable treatment of shareholders
 - Interests of other stakeholders
 - Role and responsibilities of the board
 - Integrity and ethical behaviour
 - Disclosure and transparency

Risk Management

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."



Compliance - objectives

“Compliance is defined as an audit for monitoring the legal environment of a company, and for advising its board according to the outcome of the monitoring.”

- One of the latest methods of reducing risks is thru compliance.
- Compliance activities reduce the risk in business activities
- Compliance activities strengthens competition and market position
- Compliance terms include prevention, correction activities, and support for the monitored company during any legal procedures, building of structures and creating of procedures.

Compliance - benefits

- Strengthening the Control Environment
- Improving Documentation
- Increasing Audit Committee Involvement
- Exploiting Convergence Opportunities
- Standardizing Processes
- Reducing Complexity
- Strengthening Weak Links
- Minimizing Human Error

Agenda

- Governance, Risk, and Compliance
- **Sarbanes-Oxley**
- EuroSox
- Frameworks and best practices
- What does an IT manager need to know?
- Concluding remarks



SOX Sections requiring IT (1/2)

- Areas where IT technology is required
 - Section 302: Certify Financial Reports
 - Timely review and analysis of information
 - Automate disclosure control assessments
 - Section 404: Internal Controls Reports
 - Manage documentation, project plan
 - Management reporting and assessment
 - Automated control execution and testing
 - Section 806: Whistleblower Protection

SOX Sections requiring IT (2/2)

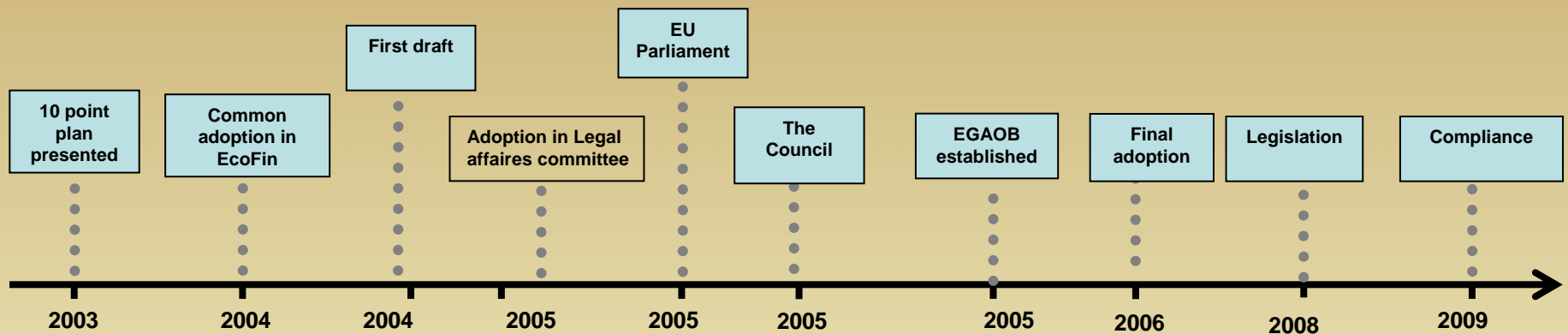
- Areas where databases are used to store electronic records
 - Section 802 regarding destruction, alteration or falsification of records; retention period for records storage and refers to the type of business records that need to be stored including all business records and communications (incl. electronic)
- Areas where IT technology will help
 - Data Quality and Reliability (404, 302)
 - Real-time Knowledge/Awareness (409)
 - Anonymity of Whistleblowers (806)

Agenda

- Governance, Risk, and Compliance
- Sarbanes-Oxley
- **EuroSox**
- Frameworks and best practices
- What does an IT manager need to know?
- Concluding remarks



The Genesis of EuroSox



2003

10 point plan from The Commission on Corporate Governance presented as the 8th directive

2004

Common adoption in ECOFIN

16. march 2004

The first draft of the directive published

21. June 2005

Adoption in The Legal Affairs Committee

29. September 2005

EU Parliament adopts directive

11. October 2005

Political acceptance of adoption in The Council of Ministers

16. December 2005

EU established EGAOB.

26. April 2006

Final adoption of the 8th directive in The Council

14. July 2006

Changes in the 4th and 7th accounting directives

April 2008

24 month adoption period.

EuroSox is a set of EU directives (1/2)

- The European Unions Financial Services Action Plan (FSAP)
- The 4th directive Annual Accounts of specific type of companies
- The 7th directive Consolidated accounts
- The 8th Company Law Directive on Statutory Audit
 - Professional ethics, independence and objectivity
 - Auditing standards
 - Audit reporting
 - Auditors' liability
- The 8th Company Law Directive and Corporate Governance
 - The impact of MiFID on corporate governance
 - Internal controls and external auditors
- The 8th Company Law Directive: Committees and Interpretations
 - The European Group of Auditors' Oversight Bodies (EGAOB)

EuroSox is a set of EU directives (2/2)

- The Transparency Directive
 - The harmonisation of transparency requirements
 - Annual financial reports
 - Half-Yearly financial reports
 - Transparency and information for holders of securities
- The Market Abuse Directive
 - Insider dealing
 - Market manipulation
 - Competent authorities with “investigatory powers”
 - How the directive is implemented under the Lamfalussy process
- The EU Data Protection Act
 - At odds with SOX 806 (Anonymity of Whistleblowers)

Agenda

- Governance, Risk, and Compliance
- Sarbanes-Oxley
- EuroSox
- **Frameworks and best practices**
- What does an IT manager need to know?
- Concluding remarks

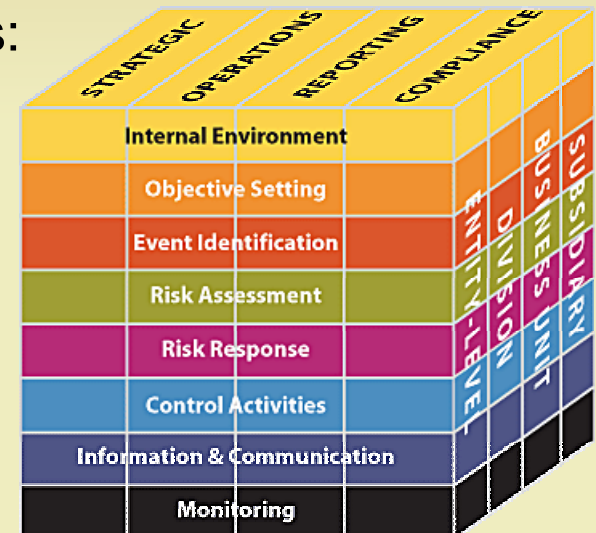


Overview of the most important frameworks

- COSO Internal Control – Integrated Framework
 - Supported, but not officially approved, by the Securities and Exchange Commission (SEC) as an internal control framework
 - COSO identifies financial reporting good practices and references
- Control Objectives for Information and Related Technology
 - COBIT is a standard for IT Governance, which is defined by ITGI and ISACA as the structure that links IT processes, IT resources, and IT information to company strategies and objectives.
 - Is approved by the EU as one among three accepted standards.
- Information Technology Infrastructure Library
 - Library of books that documents best practices for IT Service Management
 - The IT Governance Institute (ITGI) recommends using COBIT and ITIL.

COSO Integrated Control-Integrated Framework

- COSO sets out three control objectives
 - Operations: Assuming that the company is operating effectively as a business and most importantly, protecting the assets of the shareholders.
 - Financial reporting: Assuring that the financial statements of the company are produced in accordance with the Generally Accepted Accounting Principles (GAAP)
 - Compliance: Assuring that the company is in compliance with relevant laws and regulations, including SEC rules, health and safety laws, and tax laws
- COSO also sets out five control components:
 - Control Environment
 - Risk Assessment
 - Control Activities
 - Information and Communication
 - Monitoring



- COBIT advocates five main areas where IT is the foundation of controls that enable reliable financial reporting
 - Information Management and Data Classification
 - User Management
 - Real-time Reporting
 - Transaction Thresholds and Tolerance Levels
 - Data Processing Integrity and Validation
- COBIT consists of four primary domains for IT Governance
 - Planning and Organization (PO)
 - Acquisition and Implementation (AI)
 - Delivery and Support (DS)
 - Monitoring (M)
- Each primary domain consists of a number of processes for which a number of key goal indicators, key performance indicators (KPI), and critical success factors are predefined.

ITIL – a set of best practices

The Information Technology Infrastructure Library (ITIL®) is a framework of best practice approaches intended to facilitate the delivery of high quality information technology (IT) services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value, in a financial sense, in IT operations.

- Service Support
 - Service Desk
 - Incident Management
 - Problem Management
 - Configuration Management
 - Change Management
 - Release Management
- Security Management
- Service Delivery
 - Service Level Management
 - IT Service Continuity Management
 - Availability Management
 - Financial Management for IT Services
- ICT Infrastructure Management
 - ICT Design and Planning
 - ICT Deployment Management
 - ICT Operations Management
 - ICT Technical Support

Overview of relevant ISO standards

- 13335 – Guidelines for the management of IT Security
- 13888 – Non-repudiation
- 15408 – Evaluation criteria for IT security
- 15443 – A framework for IT security assurance
- 18028:2006 IT network security
- 18044 – Information security incident management
- 18045 – Methodology for IT security evaluation
- 19770 Software asset management
- 20000-1:2005 - Service Management: Specification
- 20000-2:2005 – Service Management: Code of Practice
- 27001:2005 – Information security management systems – Requirements
- 27002:2005 - Code of practice for information security management
- 27004 Information security management measurements
- 27005 Information security risk management
- 27006:2007 Requirements for bodies providing audit and certification of information security management systems

ISO 17799: Information technology – Security techniques

- The most important sections in this context are the following:
 - 4: Risk assessment and treatment - analysis of the organization's information security risks
 - 5: Security policy - management direction
 - 6: Organization of information security - governance of information security
 - 11: Access control - restriction of access rights to networks, systems, applications, functions and data
 - 15: Compliance - ensuring conformance with information security policies, standards, laws and regulations
- ISO 17799 (Danish equivalent DS484) is currently being replaced by the 27000 series

Agenda

- Governance, Risk, and Compliance
- Sarbanes-Oxley
- EuroSox
- Frameworks and best practices
- **What does an IT manager need to know?**
 - The mandates and standards discussed earlier
 - Identity Management
 - Information Lifecycle Management
 - Compliance portal requirements
 - The need for an IT Governance Board
- Concluding remarks



Core Tenets of Identity Management

- Authentication mechanisms must reflect the levels of risk and the granularity of the resources associated with that risk
- Authorise access to business functions and information at the level of each service using policy-based approaches to the definition and enforcement of access control requirements
- A federated approach is required for the mediation of the relationships at the heart of identity management
- Identity management capabilities must be delivered as distributed infrastructure services, which exploit existing services and are defined according to clear contracts which are enforced through policies
- Roles must be modelled at the intersection of identities, entitlements and organisational structures and managed as part of the broader identity management lifecycle

Information Lifecycle Management

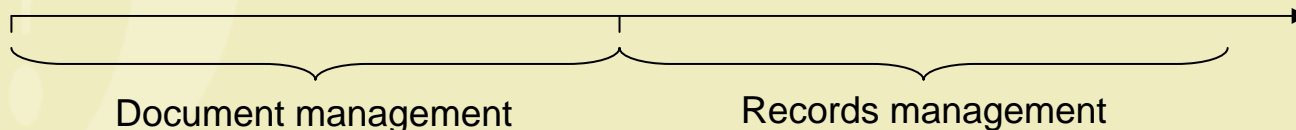
"Information Lifecycle Management is comprised of the policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost effective IT infrastructure from the time information is conceived through its final disposition."

- ILM Policy consists of the overarching storage and information policies that drive management processes.
- Policies are dictated by business goals and drivers. Therefore, policies generally tie into a framework of overall IT governance and management; change control processes, and recovery times; and service level agreements (SLA)
- Operational aspects of ILM include backup and data protection; disaster recovery, restore, and restart; archiving and long-term retention; data replication; and day-to-day processes and procedures necessary to manage a storage architecture.

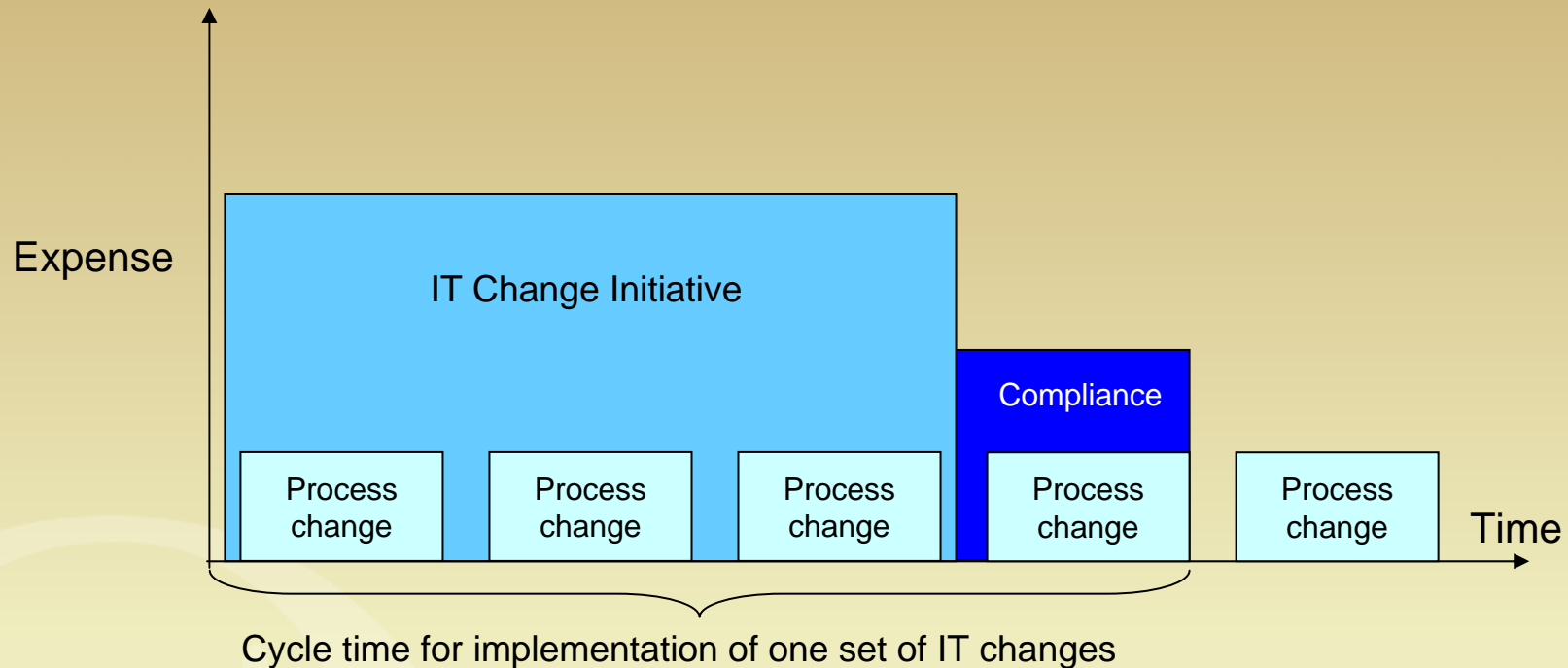
Records Management

"The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

- Creating, approving, and enforcing records policies, including a classification system and a records retention policy
- Developing a records storage plan, which includes the short and long-term housing of physical records and digital information
- Coordinate the access and circulation of records within and even outside of an organization
- Executing a retention policy to archive and destroy records according to operational needs, operating procedures, statutes, and regulations



Compliance Implications for IT change initiatives



- The cycle time for IT implementation of change initiatives to meet compliance requirements will increase significantly unless an alternative implementation strategy is chosen.

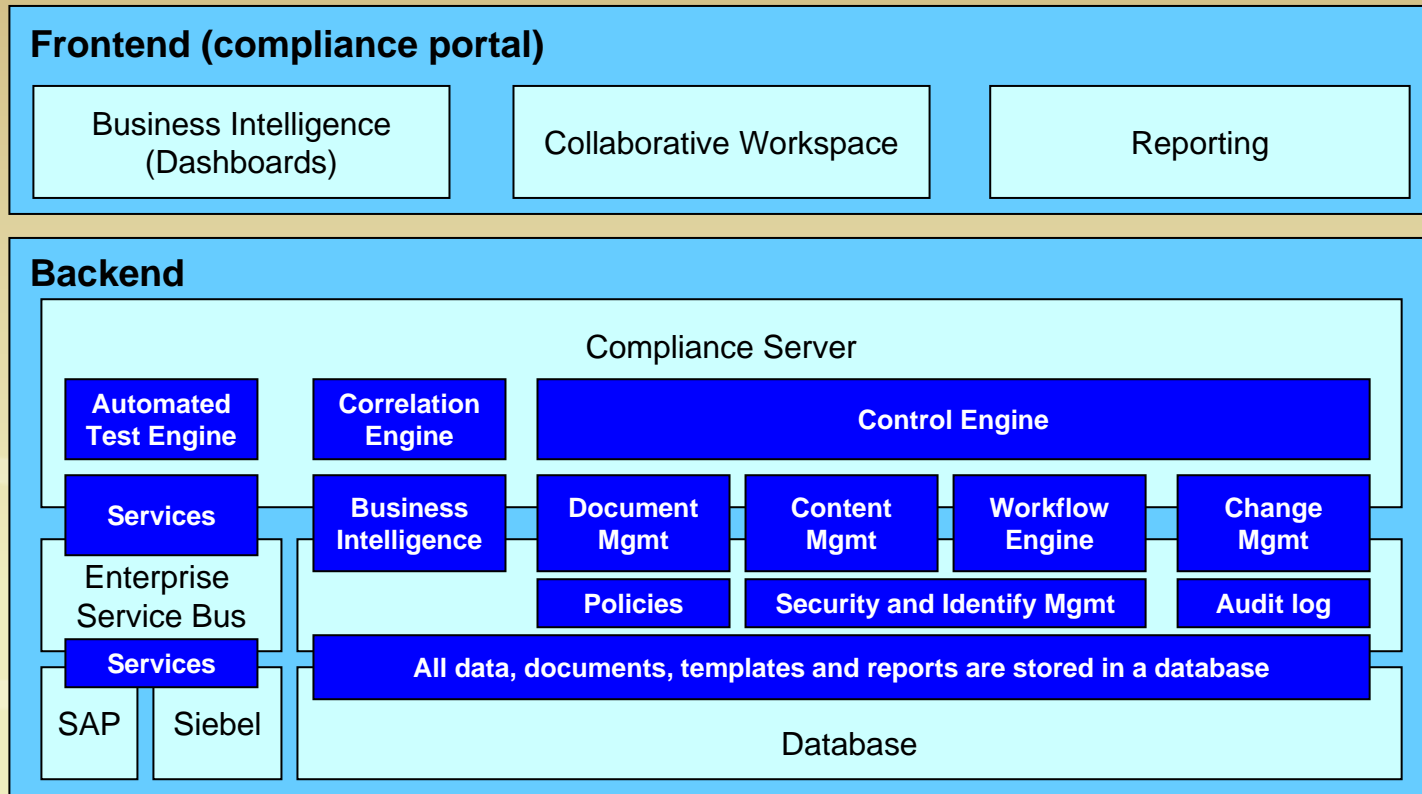
Agile compliance

- An *agile* company has the ability to respond to
 - An unprecedented level of uncertainty
 - A rapidity of change in their business-operating environment
 - Market life cycles that have become reduced
 - Technology shifts
 - Changes in ownership and organization structure (M&A, outsourcing, off-shoring, etc)
- That leads to
 - Continuously changing business processes that gives rise to new flowcharts, control points, narratives and tests
- While remaining in compliance with regulatory legislation

Requirements of a compliance IT solution

- Auditor support software
 - Questionnaires
 - Narratives
 - Process Flows
 - Control Matrixes
 - Testing
 - Remediation Reports
- Software to support compliance
 - Document management
 - Event Management
 - Contract Management
 - Supplier and Customer Collaboration Portals
 - Data Storage and Retention Programs
 - Advanced Business Intelligence and Reporting Tools

Elements of a compliance IT system



Agenda

- Governance, Risk, and Compliance
- Sarbanes-Oxley
- EuroSox
- Frameworks and best practices
- What does an IT manager need to know?
- **Concluding remarks**



Benefits of Improved IT

- Stronger Business Relationships
- Better Decision Making
- Enhanced Operational Efficiency
- Revenue Growth
- Improved Compliance Framework
- Ease of Integration
- Scalability and Sustainability (\$)

Concluding Remarks

- GRC does not regulate technology
- Using technology can reduce cost, time and risk of compliance
- Technology will be scrutinized although it is not explicitly mentioned in the Act
- Technology requirements and expectations from GRC
- The compliance platform of the future

Contact information

C^{?!=!}NTROLLERS Aps

**Kersi F. Porbunderwalla
Managing Partner**

C^{?!=!}NTROLLERS Aps
Hvidegårdsparken 14
DK-2800 Kgs. Lyngby

Tel. +45 21210616
web: www.eurosox.dk
mail: info@eurosox.dk

Disclaimer

- This presentation, its contents and the ideas therein contained, are the sole property of Controllers ApS and may not be copied, translated or distributed without the prior written consent of Controllers ApS.
- The information contained in this presentation/ documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information provided, it is provided “as is” without warranty of any kind, express or implied.
- Controllers ApS shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other documentation. Nothing contained in this presentation/ documentation is intended to, nor shall have the effect of, creating any warranties or representations from Controllers ApS (or its suppliers or licensors)
- Controllers ApS does not provide legal, accounting or audit advice or represent or warrant that its services or products will ensure that client is in compliance with any law.