What is Sarbanes Oxley (SOX)

The Sarbanes-Oxley Act was signed into law on 30th July 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws".

From Gartner: Sarbanes-Oxley: The Role of Technology

The technology and business process regulated by Sarbanes-Oxley are so entwined that it's impossible to separate them, says this Analyst Report. It warns that you will face two challenges when sorting through this entanglement of business processes and technology.

Key CM Objectives of SOX

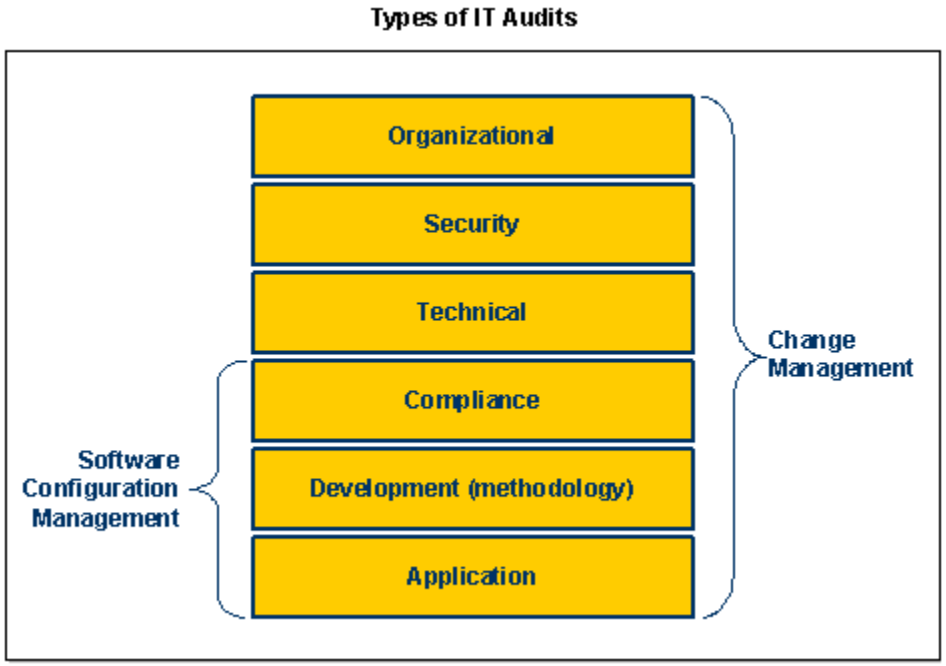
Good corporate governance also means that the applications a company develops are usable by end users, free of major defects, enable users to create business value, and lastly, free users to get their work done in the most productive manner. For management, SCM provides assurance that its mission-critical applications are not exposed to potential failure due to staff error, staff turnover, or internal or external sabotage. SCM can help the IT auditing function ensure that software development processes are defined and repeatable, minimizing risk to the organization and enabling good corporate governance. To this end, an SCM system must:

Key CM Objectives of SOX

- Allow you to assess the impact of making proposed changes
- Ensure that only planned software changes make it into production
- Enable you to quickly recover a system if an error is introduced
- Ensure that outsourcers are working only on the critical project at hand, and securing access at the member, project and development path levels;
- Produce an audit trail of all system changes with associated approvals;
- Enforce rigorous or relaxed development processes, as required;
- Provide assurance that releases/configurations are repeatable, secure and protected from tampering.

Key CM Objectives of SOX

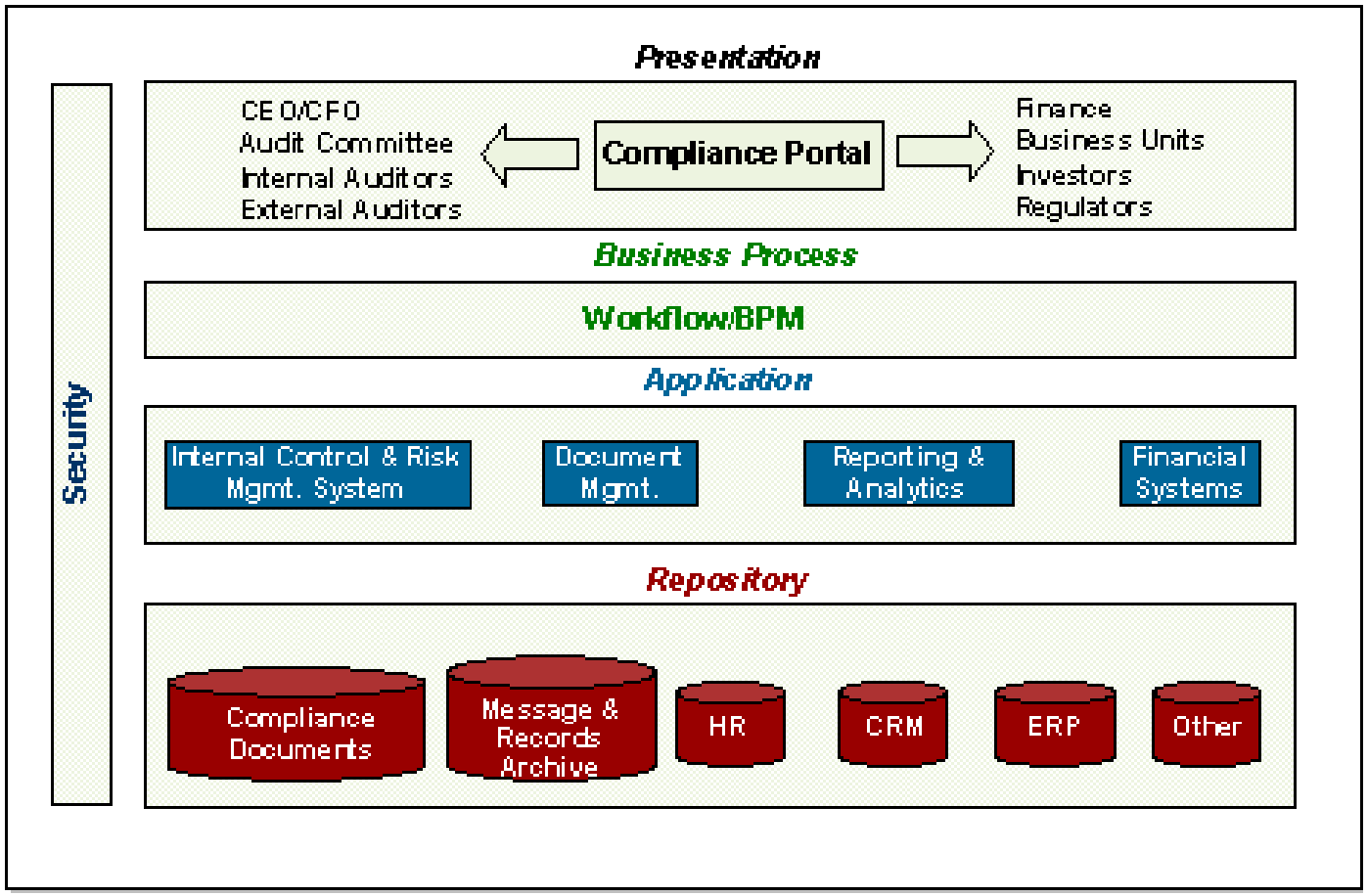
- These capabilities must support the enterprise change management function, which goes beyond the software development function and includes managing change in the production environment. The figure below depicts the type of IT audits and which types of audits are supported by change management or by SCM.



Source: Giga Research, a wholly owned subsidiary of Forrester Research, Inc.

SOX Architecture

Figure 1: Sarbanes-Oxley Compliance Architecture



Source : Giga Research, a wholly owned subsidiary of Forrester Research, Inc.

The Sarbox Conspiracy

Sarbanes-Oxley compliance efforts are eating up CIO time and budgets. Worse, CIOs are being relegated to a purely tactical role. And that may be the CFO's plan.

Jul. 1, 2004 **Issue of** CIO Magazine

The Conspiracy By the Numbers

Only 12 of 22 companies surveyed had IT representation on their Sarbox steering committees.

72% of Sarbanes-Oxley compliance teams were led by finance.

4% were led by IT.

$3 billion was spent on Sarbox compliance in 2003. About 90% of that was spent on internal staff and consultants.

Sources: Hackett Group, Gartner, AMR

The Sarbox Disconnect

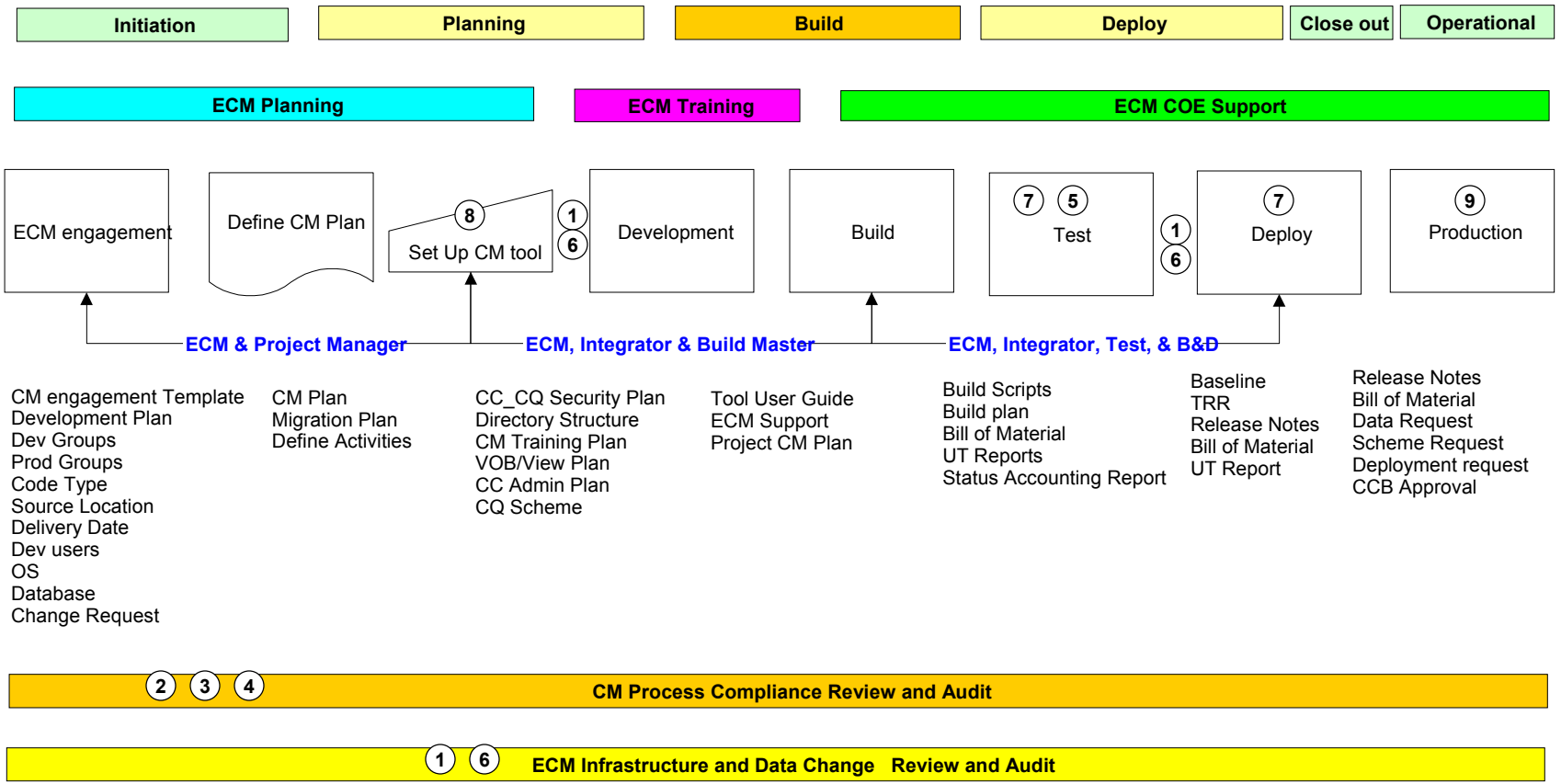
Running Sarbanes-Oxley efforts is not an option for most CIOs. Sarbox is about financial processes. And each year when they sign off on the numbers, it's the CFOs' necks on the line (along with the CEOs'). "Controls and processes around financial reporting indicate the money guy should be intimately involved [in Sarbox]," says AMR Vice President of Research John Hagerty. A recent AMR survey found that 72 percent of Sarbanes-Oxley compliance teams were led by finance, and just 4 percent by IT. (The remainder were led by other business functions, plus legal and the board of directors.) But CFOs will not be able to prove compliance without the CIO. In most cases, the CFO's expertise ends where his numbers feed into information systems.

What is ECM

Enterprise Change Management (ECM) is a management discipline that applies technical and administrative direction and surveillance to the application development life cycle, infrastructure assets and intellectual property of a company. It includes;

- Identification
- Control
- Status Accounting
- Audit

Integrated CM SOX Process Flow

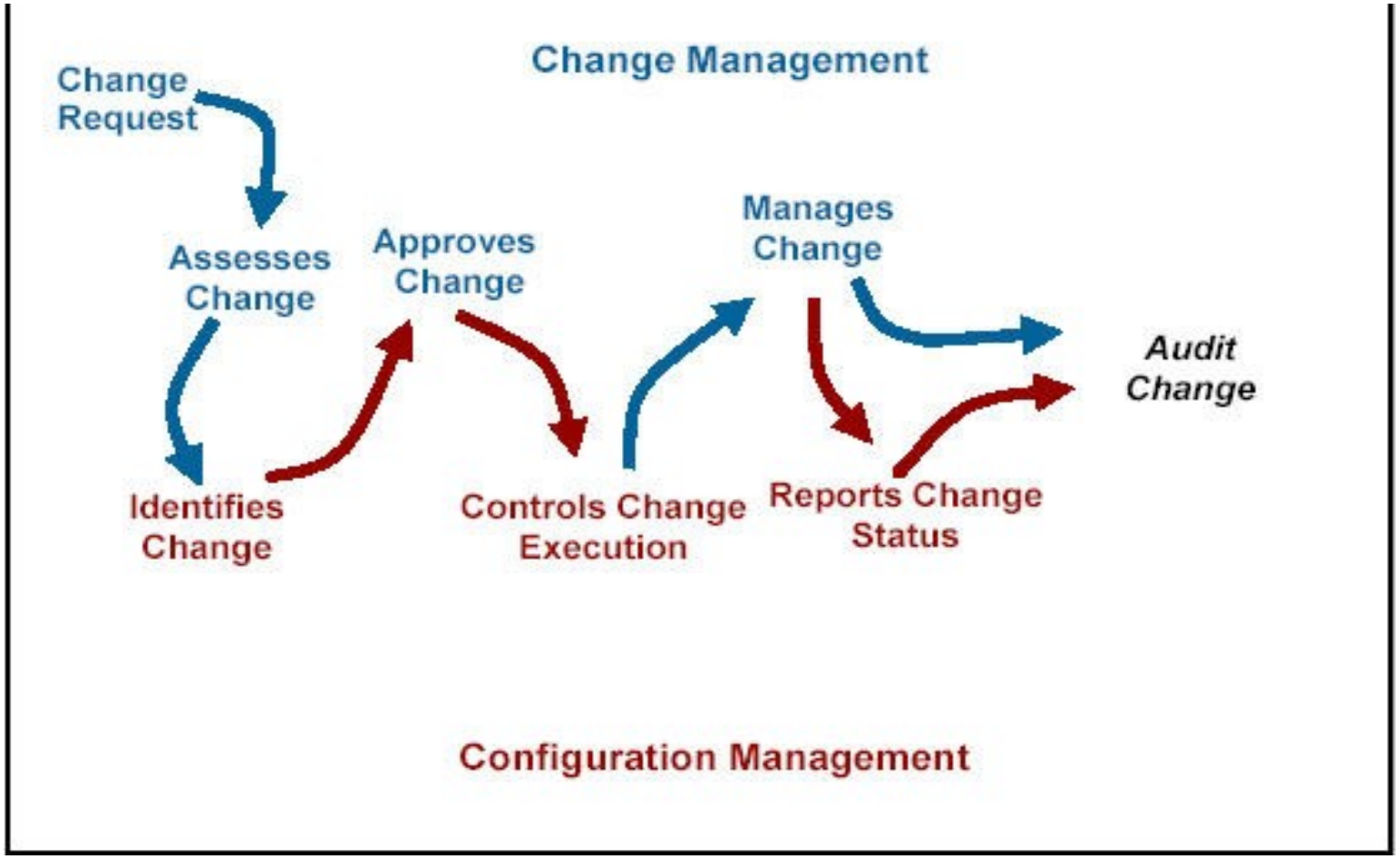


Integrated CM SOX Process Flow

Control numbers reflect ***key*** controls

1	Change Management - Overall	A formal change management process is in place to assess upstream and downstream impacts on people, process and systems for implementation of changes in business processes or operating practices. Includes ECCB.
2	ECM Process Compliance Review	Change Management compliance reviews are conducted for Mainframe & Distributed applications and Infrastructure to validate that all changes are in compliance with ECM Standards and Process.
3	Segregation of Duties - Change Management	The ECM Process and Standards define Segregation of Duties for implementing change to application source code and infrastructure.
4	ECM Process Adoption	All changes to production must follow the ECM processes.
5	Mainframe High Impact Project Operational Testing	All high impact projects must go through a coordinated Operational Test in the SHAD/RLSE environment for the mainframe. Testing of every job or module touched or impacted by a High Impact Project is required.
6	Data Management Change Control Board (DMCCB)	The data change management process defines a mechanism for capturing & validating changes to data and includes a data Management Change Control Board (DMCCB).
7	Monitor Production Program Deployment Builds	ECM Process defines that all production builds and deployments are from an established, tested baseline in an approved source version control tool. ECM will monitor all applications for compliance.
8	Production Program Version Control-Dev Artifacts	Development artifacts are required to be maintained within the ECM version control environments.
9	MainFrame Change Validation	Update access to production application libraries is limited to only ECM and Systems.

The CM Flow


Change Management
Change Request
Assesses Change
Approves Change
Manages Change
Audit Change
Identifies Change
Controls Change Execution
Reports Change Status
Configuration Management

SOX Compliance Checks

- Compliance with ECM policy and standards
  - Version control
  - Issue & Defect Tracking
  - Baseline Management
  - Status Accounting
  - CM Plan
  - CCB execution
  - ORR Approval
  - ECCB execution

Questions & Comments