

Use the New Checklists to Comply with Regulations

By Carolina Duarte, João Ambra, Marcelo Gherman and Rosângela Caubit - August, 2006

ISO 27001

The ISO 27001 checklist is based on the information security management system structure. The standard describes a cycle of improvements guided by the PDCA model, consisting in the proposal of a security plan (Plan), implementation and execution of security controls required by the system (Do), monitoring of performance (Check), and corrective and preventive actions (Act).

By applying the checklist, the CSO can validate the implementation of requirements for certification, and demonstrate the organization's level of compliance with the ISO 27001 standard. During this phase, the checklist can function as a repository, storing evidence of implementation of the controls to be presented to the internal auditors or to the certifying body.

The checklist also supports the CSO in assessing the effectiveness of the information security management system.

System Change Management

The System Change Management checklist allows you to assess aspects, usually in the operational environment, that may put operations continuity and results at risk, and also affect user productivity. It addresses basic information security controls required by audits concerning control of the change process. The checklist is based on COSO, and helps the CSO or Compliance Manager to check the objectives that have to be covered for compliance with the Sarbanes-Oxley Act, from documentation to change approval processes.

Data and System Backup

The Data and System Backup checklist helps define which are the critical points to guarantee recovery of important information (such as organization records, financial data, plans, etc.), whose unavailability can result in considerable damage to the organization.

The checklist contains basic information security controls required by audits regarding control of the backup process, and distinguishes those under responsibility of the IT manager from those under responsibility of the application owner. The latter is the main person responsible for results that depend on the system. The checklist helps check the objectives that have to be covered for compliance with the Sarbanes-Oxley Act, regarding control of the critical financial data backup process, from documentation to media testing.

System Continuity Management

The System Continuity Management checklist addresses basic information security controls which are usually required in SOX-compliance audits focusing on the business continuity program.

The checklist supports in assessing the effectiveness of the organization's continuity process when other controls concerning the security of assets and operations present faults. Thus, use of this checklist is a requirement for risk assessments of any scope.

Configuration of Applications and Operational Environments

The Operational Application Configuration checklist evaluates basic information security controls which are usually required in SOX-compliance audits on the control of applications supporting financial processes. It allows management to individually assess each of the applications which are critical to the performance of operations, rather than to perform comprehensive analyses that tend to overlook local security faults.

The checklist describes the objectives that should be covered, from application documentation, shared access protection, and responsibilities of the application owner, to the controls that ensure traceability.