



Automating Mainframe Environments To Achieve Regulatory Compliance

Large organizations rely on mainframe computers to process and store tremendous amounts of their most highly sensitive data. Wherever data is stored, security vulnerabilities may be present. When you couple the possibility of vulnerabilities with very sensitive information, the potential for serious breaches exists. Mainframe systems can be targeted for attack from internal personnel and external sources just as distributed computers can. To prevent problems, they, too, should be tested on a regular basis to prevent compromise and to confirm that adequate security checks and balances are in place as mandated by government compliance regulations.

I.C.U...MVS from JANUS Associates is a penetration testing and security vulnerability assessment tool for mainframe environments that is designed to conduct the analysis needed for compliance requirements such as Sarbanes-Oxley. It supports vulnerability assessments, fulfills Certification and Accreditation requirements and creates "level-of-risk" based security management.

I.C.U...MVS identifies exploitable security exposures in a proactive and predictive manner. It does not require intensive technical support or system skills and is geared to be used by managerial and technical staff alike. I.C.U...MVS incorporates "expert" system capabilities and clearly shows users the exact cause of problems, not simply symptoms, thus enabling implementation of solutions before they are exploited.

An advanced feature of I.C.U...MVS is its extensive analysis of data. Traditional mainframe analytic products examine either the operating system or the access control facility residing on the system. I.C.U...MVS analyzes both of these and much more. It examines the underlying data that form the heart of an organization's information and identifies areas where internal controls may be fragile, thus resulting in a material weakness. I.C.U...MVS' use of exception reporting concentrates on corrective actions, not simply discovery. It also provides trend reporting and scoring that assists in measuring compliance.

A special feature of I.C.U...MVS is its advanced search capabilities designed to locate inadequately controlled information by scanning for strings of data that might reveal the location of reports and other unsecured information. I.C.U...MVS can also be configured to monitor MVS access control and inform management of weak passwords allowing more time to be spent working to improve password usage rather than simply identifying what problems exist. I.C.U...MVS also permits the management of security activities of operating systems located at remote sites from one central location. With the use of the included Integrity Concern Manager central controller it is no longer necessary to travel to distant locations to conduct security audits.

I.C.U...MVS provides compliance summaries of what has been reviewed, the number and type of problems discovered, and the percentage of data examined. Its Security Quotient section retains statistics that can be utilized to support substantiation of business cases to develop future security improvements. Customization for specialized mainframe environments is also available. This ensures explicit, not generalized results.

I.C.U...MVS is a comprehensive easy-to-use security compliance tool. It is designed for novice users as well as technical staff and eliminates the need for costly skilled personnel to spend hundreds of hours looking for problems. Automating your mainframe environment with I.C.U...MVS will allow you to locate problems and critical issues in minutes, not hours.

JANUS is a certified, woman-owned small business. Please call 203.251.0200 to speak with an Information Security Specialist about how your organization would benefit from our information security services.

JANUS Associates, Inc. 9 West Broad Street Stamford, CT 06902

www.JANUSassociates.com