RSM PARTNERS
MAINFRAME

ASSURED SECURITY: SPECIALIST MAINFRAME SECURITY ASSESSMENT

Specialist Mainframe Security Assessment

Reviewing essential security controls on your IBM mainframe platform. Key to successfully protecting your mainframe data against internal fraud, accidental data breaches, hacking, malicious attacks and data loss

Expert assessment by the mainframe security experts: protecting your business

As the threat of external hacks and malicious insider attacks continues to increase, our **Specialist Mainframe Security Assessment** means you can fully understand your IBM mainframe infrastructure in security terms - helping ensure the most robust and appropriate controls are in place to guard against attack.

How you benefit

All necessary security controls are reviewed and checked by RSM mainframe security specialists:

- Reducing both risk of mainframe hacking as well as internal malicious attacks
- Providing peace of mind in receiving an industry best practice *mainframe security healthcheck*
- Fully understanding your security posture relating to your mainframe infrastructure
- Revealing any weaknesses and vulnerabilities – so you can plug gaps in your defences
- Making necessary improvements and targeting security investments in the right places

Mainframe systems are often audited by organizations and individuals with little to no knowledge of mainframe technical intricacies - instead doing a simple "Checklist Audit". This has resulted in many organizations incorrectly believing their mainframe infrastructure to be secure and infallible. RSM specialists bring detailed knowledge and understanding, helping ensure the mainframe platform is made appropriately secure.

Securing your mainframe - protecting your valuable data

Understanding weaknesses and vulnerabilities in your mainframe infrastructure is achieved via:

- An initial conversation and scoping exercise
- A detailed assessment by expert mainframe security consultants, with initial findings provided onsite
- An in-depth report, including Management Summary, issued within two weeks of onsite activity
- A face-to-face review and/or webinar to discuss the findings and the risks revealed
- A bespoke *Checklist* recommending activities for remediation and risk mitigation

Key features

- RSM Partners deploys a proven Mainframe Security Assessment methodology for any ESM: IBM's RACF; CA's ACF/2; or Top Secret
- Our in-depth Technical Assessment of Security Infrastructure uses IBM and CA utilities, including ICHDSM00, TSSCFILE and ACFRPTSL
- The Assessment reviews the current ESM Implementation and security administration for each database. This will generate recommendations and advice for improvements covering:
  - Sensitive Datasets/Libraries, including protection from unauthorised access
  - Application Data – checking whether all Production and Development data is adequately protected
  - Public Resources - are z/OS resources properly protected?
  - User SVCs - are user SVCs 200-256 being used - and if so, why?
  - Command Authority – is it possible to issue authorised MVS or JES commands?
  - Segregation controls between Development, QA and Production environments
  - The security controls implemented for UNIX System Services (USS)
- Detailed Assessment of Security Policy & Procedures, both formal and informal controls

Due to the sensitive nature of this service, RSM Partners is happy to sign any confidentiality and Non-Disclosure Agreements (NDAs) that may be required.

Security Policy and Procedures

An assessment is conducted of both the client's formal and informal security controls for managing the mainframe. Documentation is reviewed and key mainframe security and administration personnel are interviewed. Specific areas reviewed and evaluated include:

- Mainframe security policies and technical standards
- Processes and procedures for access control requests
- Processes and procedures for periodic access control reviews (recertification)
- How passwords are managed, including sensitive users, Privileged IDs, Security IDs, Audit IDs, general population
- Decentralised security administration functions
- Account management procedures e.g. new account approval, review of continued business need
- Management of backup and restore processes for the ESM database
- Deployment and exploitation of additional security tooling e.g. zSecure, Vanguard, ETF/A, Beta88
- Security Reporting including:
  - Audit settings
  - SMF data management
  - Daily, weekly and monthly report schedules
  - Review and sign-off procedures for all reports
  - Escalation procedures for issues found
  - Implementation and Management of Real Time Alerting and Monitoring Processes

Assured Security: Why RSM?

RSM Partners is a globally recognized specialist in IBM mainframe security - providing both consultancy services and niche software tools.

Working with some of the world's largest organizations - no other partner offers the same depth of knowledge and experience in ensuring mainframe security.

From specialist penetration testing and vulnerability assessments, to software tools greatly enhancing security management of the platform, clients know they can rely on RSM for quality, flexibility, and value.

In 2016 RSM Partners Security Software received Ready for IBM Security Intelligence accreditation from IBM.

Business Partner IBM

Business Partner IBM
Ready for Security Intelligence

To find out more about these and other RSM Partners services, call **+44 (0) 1527 837767** or visit **www.rsmpartners.com**

T +44 (0) 1527 837767 | **E** info@rsmpartners.com | **www.rsmpartners.com**

RSM PARTNERS
MAINFRAME

17_0047 - 13/02/V01