# VANGUARD Penetration Testing

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

**According to Gartner: "The IBM z/OS mainframe continues to be an important platform for many enterprises, hosting about 90% of their mission-critical applications... [Yet] the incidence of high-risk vulnerabilities is astonishingly high."**[1]

**Mainframe penetration testing helps organizations detect system weaknesses and vulnerabilities in advance of internal and external attacks. Proactive penetration testing can be performed periodically to evaluate system defenses, assess security policy enforcement, and ensure critical assets are properly protected.**

**Vanguard Penetration Testing helps organizations ensure their mainframe environments are protected from attack and in compliance with industry and regulatory standards.**

Although mainframes have the reputation for providing the highest level of security, in today's environment mainframes are just as prone to attack as any other server on the network. More internal and external users are accessing IBM mainframes over the Web and via cloud-based services than ever before. Mainframe systems are a key part of many cloud, big data, business intelligence and other initiatives.

Despite their increased use, many organizations have not implemented the latest security protections for System z. They still rely on mainframe security best practices and auditing procedures developed years ago, when only a small number of tightly controlled users could access mainframes over secure corporate networks. The expanded use of mainframes, combined with outdated security configurations and practices, is increasing security vulnerabilities and putting organizations at risk. These risks are compounded by the fact that, although many organizations conduct regular penetration testing, the mainframe is frequently omitted.

- **Identifies penetration risks on System z mainframes**
- **Protects mainframe security and ensures compliance**
- **Ensures penetration testing procedures meet industry and regulatory standards**
- **Provides remediation plan to correct mainframe penetration vulnerabilities**
- **Transfers knowledge to security staff to enable ongoing testing and maintenance**

# VANGUARD Penetration Testing

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

## Vanguard Penetration Testing Reduces Risk, Prevents Breaches

Vanguard Penetration Testing quickly identifies and prioritizes mainframe penetration risks, and evaluates the feasibility and potential impact of defense vulnerabilities on an organization's operations, compliance requirements and reputation, e.g. losing revenue, failing audits, or violating privacy protections.

**Vanguard Penetration Testing helps organizations:**

- Assess the business impact of the exploitation of potential attack vectors
- Ensure critical customer and corporate data are protected
- Identify high-risk and lower-risk vulnerabilities
- Enable targeted spending on security improvements
- Prove compliance with industry and regulatory standards
- Enhance productivity by reducing downtime from attacks
- Better align security and compliance resources

## Vanguard Penetration Testing Process

Vanguard Penetration Testing services discover high-risk mainframe vulnerabilities, determine if sufficient defenses are in place, offer remediation guidance, and recommend a plan and methodology for ongoing testing. The process includes a rigorous review of security policies, procedures and configuration controls to identify gaps in security that could be exploited by internal and external attackers. Through network and system scans, and full intrusion detection, Vanguard consultants determine the current security posture of the System z environment, including its defense-in-depth posture.

**Vanguard Penetration Testing services include:**

- Reconnaissance utilizing network mapping tools, networking sweepers, and port scanning tools to identify possible points of entry, including TCP and UDP ports
- Identification of TCP and UDP services that provide appropriate transport layer protection
- Vulnerability scans and analysis of discovered network services, applications, and functionality on targeted systems
- Analysis of identified exploitations of systems and services on the network layer and applications running in the environment
- Analysis of identified exploitations from within z/OS to attempt privilege escalation

**Vanguard regularly updates its penetration testing process to ensure the latest industry and regulatory standards are supported (see sidebar for list of standards supported). Findings from Vanguard Penetration Testing are documented in a comprehensive report that provides organizations with:**

- Details on specific penetration risks
- Rankings, from low to severe, of detected penetration vulnerabilities
- Instructions to remediate penetration risks
- Plans and methodologies for conducting ongoing penetration testing

**Vanguard Penetration Testing reviews for the following standards:**

- Basel II and III
- Centers for Medicare & Medicaid services (CMS)
- Control Objectives for Information and Related Technology (COBIT)
- Defense Information Systems Administration
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Information System Controls Audit Manual (FISCAM)
- Gramm-Leach-Bliley (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Trust Alliance (HITRUST)
- Security Framework (CSF)
- National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley (SOX)

# VANGUARD Penetration Testing

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

## About Vanguard Professional Services

Vanguard Professional Services offers a range of services to automate and optimize mainframe security. The Vanguard Professional Services team is the largest and most experienced group of mainframe security experts in the industry. Team members average more than 30 years of mainframe and RACF security experience. Services offered include penetration testing, comprehensive security assessments, remediation, implementations of application and RACF security, migrations to RACF security from ACF2, Top Secret and DB2®, and customized System z® security training programs.

## For more information

To find out more about Vanguard Penetration Testing and how it can help your organization, email info@go2vanguard.com or call (702) 794-0014.