CodeCenters International

A PLATFORM FOR ENTERPRISE ANALYSIS

954.426.4248 US
0330.0012478433 UK
Sales@CodeCenters.com

Leading the way in standards based AML/CFT Technical Audits

For over 30 years, CodeCenters has been at the forefront of innovation. We have led the way in designing comprehensive standards based security frameworks for use in enterprise systems. We provide expert AML/CFT Information Security Audit Services that document and validate how your organization's AML infrastructure is addressing and meeting its regulatory obligations. More importantly, we audit to see what risks and vulnerabilities your solution inherently has or may have and how they will be addressed in your production environment.

Our team of experts focus on both your policy and technology risk assessment aspects of compliance with the specific regulations including NIST 800.xx, Gramm-Leach-Bliley (GLB), National Credit Union Administration (NCUA) Reg. 748 Appendix A and B, Bank Secrecy Act (BSA) components, Identity Theft (NCUA in 12 CFR Part 717.82, Part 717.90, and Part 717.91), COBIT and other industry related regulatory concerns.

NIST, FFIEC, COBIT, ISO, NCUA and PCI all have extensive lists defining over 2000 unique areas, checks, tests and controls in their respective checklists. CodeCenters Risk Assessments can design how to implement, support, test and audit all those specific controls. Assessments are performed by experts in the AML/CFT field with extensive data architecture and technical industry experience - all with recognized certifications from both industry specific and vendor specific environments.

These include:
ACAMS – CAMS
ACAMS CAMS-FCI
ISC2 – CISSP
ISACA – CISA
Microsoft MCSE, MCT, MCDBA

CodeCenters Cyber-focused Standards and Frameworks

NIST
National Institute of Standards and Technology released the first version of the Framework for Improving Critical Infrastructure Cybersecurity in February 2014. The framework builds on existing standards, guidelines and is the industry standard framework for infrastructure and data security.

FFIEC
The FFIEC Cybersecurity Assessment Tool (CAT) is an audit test that helps institutions identify their risk level and determine the maturity of their cybersecurity programs.

ISACA - COBIT
Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA that enables managers to bridge the gap between control requirements, technical issues and business risks.

ISO
The International Organization for Standardization developed the ISO 27000 series to address standards that enable organizations to implement processes and controls that support the principles of information security.

DISA - STIG
DISA - The Defense Information Systems Agency
STIG - Security Technical Implementation Guide (STIG)
Technical Implementation Guides (STIGs) produced by DISA are low-level specific configuration standards for devices such as database servers, computers/laptops and a range of solutions.

A project audit can cover all areas or a subset of your AML/CFT environment. If an area is not in compliance or if it does not meet the standard, we can work with your team to ensure all areas of your solution meet all required standards. These include the following:

- Threats to specific types of AML/CFT Solutions
- Vulnerabilities inherent to AML/CFT Solutions
- Security and Supervision of Cybersecurity Risk and Resources within your AML/CFT Environment
- Security and Supervision of Cybersecurity Risk for downstream and pass through systems
- Active solutions and Resources for Cybersecurity Preparedness and System Testing
- Risk Measurement and Risk Mitigation for data flows within enterprise AML solutions
- Technical Architecture of all AML Enterprise solutions

In the United States, most government and corporate computer systems are guided by the NIST 800.xx framework or other regulatory mandate similar to the FFIEC's IT Examination Handbook. For standards and framework audits, CodeCenters provides all of the documentation needed, along with all of the technical resources needed to ensure that your AML/CFT environment is compliant to the standard in which your solution is based. The table below is a simplified outline if you are conducting a "standard for AML/CFT computer system best practices" audit. For the actual audit, this list would be broken down into numerous detailed subcategories and each line item is tested and documented.

Standards II.C.1 Policies, Standards, and Procedures II.C.2 Technology Design II.C.3 Control Types II.C.4 Control Implementation II.C.5 Inventory and Classification of Assets II.C.6 Mitigating Interconnectivity Risk II.C.7 User Security Controls II.C.7(a) Security Screening in Hiring Practices II.C.7(b) User Access Program II.C.7(c) Segregation of Duties II.C.7(d) Confidentiality Agreements II.C.7(e) Training II.C.8 Physical Security II.C.9 Network Controls II.C.9(a) Wireless Network Considerations II.C.10(a) Change Management Within the IT II.C.10(b) Disaster Recovery **Environment** II.C.10(a) Configuration Management II.C.10(b) Hardening II.C.10(c) Standard Builds II.C.10(d) Patch Management II.C.11 End-of-Life Management II.C.12 Malware Mitigation II.C.13 Control of Information II.C.13(a) Storage and Data Security II.C.13(b) Electronic Transmission of Information II.C.13(c) Disposal of Information	II.C.16 Remote Access to Financial Services II.C.16(a) Vendor Security Analysis II.C.16(b) Vendor Use and Access Analysis II.C.17 Application Security II.C.18 Database Security II.C.19 Encryption **Providers** II.C.20 Oversight of Third-Party Service II.C.20(a) Outsourced Cloud Computing II.C.20(b) Cloud Computing Security II.C.20(c) Cloud Computing Encryption II.C.20(d) Cloud Computing Logging II.C.20(e) Cloud Computing Disaster recovery II.C.20(f) Managed Security Service Providers II.C.21 Business Continuity Considerations II.C.22 Log Management II.D Risk Monitoring and Reporting II.D.1 Metrics **Operations** III Security Operations III.A Threat Identification and Assessment III.B Threat Monitoring III.C Incident Identification and Assessment III.D Incident Response **Program** IV Information Security Program Effectiveness

II.C.13(d) Transit of Physical Media II.C.13(e) Rogue or Shadow IT II.C.14 Supply Chain II.C.15 Logical Security II.C.15(a) Operating System Access II.C.15(b) Application Access II.C.15(c) Remote Access II.C.15(d) Use of Remote Devices	IV.A Assurance and Testing IV.A.1 Key Testing Factors IV.A.2 Types of Tests and Evaluations IV.A.2(a) Self-Assessments IV.A.2(b) Penetration Tests IV.A.2(c) Vulnerability Assessments IV.A.2(d) Audits IV.A.3 Independence of Tests and Audits IV.A.4 Assurance Reporting