Muhammad Eissa

Regulatory IT Audit & Cybersecurity Assurance Leader | ADHICS · CBUAE ISR · ISO 27001 · NIST CSF

CISSP · CISA · CRISC · GCIH · GMON · PCIP

Abu Dhabi, UAE | +971 58 821 0538 | muhammad.a.eissa@outlook.com

linkedin.com/in/MuhammadEissa | muhammadeissa.me

Languages: Arabic (Native) | English (Fluent)

PROFESSIONAL SUMMARY

Regulatory IT audit and cybersecurity assurance leader with **11+ years** across healthcare, banking, financial services, and security operations. Currently conducting **ADHICS V2** audits of healthcare entities in Abu Dhabi, covering engagement scoping, control testing, findings, remediation, and executive reporting. Previously led information security compliance and assurance at **ADIB** and conducted regulatory IT risk assessments at the **Central Bank of Egypt**. Brings deep knowledge of **ADHICS V2**, CBUAE ISR, NESA, ISO 27001, NIST CSF, and PCI DSS, supported by hands-on SOC and security engineering experience.

CORE COMPETENCIES

- **Regulatory Audit & Assurance:** ADHICS V2, CBUAE ISR, NESA, CBE Regulations, ISO 27001, PCI DSS, SOC 2, and privacy requirements.
- **IT & IS Audit:** ITGC, application and core banking audits, risk-based planning, control testing, evidence management, findings, TeamMate, and ACL.
- **IT Risk & Controls:** Enterprise and third-party risk assessments, control design, remediation governance, and executive and board reporting.
- **Security Operations & IR:** SOC governance, incident response, cyber crisis management, threat hunting, MITRE ATT&CK, and tabletop exercises.
- **Technology Assurance:** SIEM/SOAR, EDR/NDR, vulnerability management, cloud security, network security, and secure-by-design reviews.

PROFESSIONAL EXPERIENCE

ADHICS Auditor
May 2026 – Present

Emirates Classification Society (TASNEEF) — Abu Dhabi, UAE

- Audit healthcare entities across **Abu Dhabi, Al Ain, and Al Dhafra** against **ADHICS V2**, covering Section A governance and Section B technical control requirements at the applicable Basic, Transitional, and Advanced tiers.
- Run engagements end to end: scoping and entity classification, audit planning, documentation review, physical and virtual walkthroughs, evidence validation, control testing, closing meetings, and report issuance.
- Assess controls spanning IT governance, risk management, asset and access management, health information and EMR security, third-party and cloud-hosted services, backup and recovery, incident management, and business continuity.
- Advise CIOs, CISOs, and compliance officers on remediation, translating control deficiencies into regulatory exposure and prioritized corrective action plans.

Head of Information Security Compliance & Assurance
May 2025 – Jan 2026

ADIB (Abu Dhabi Islamic Bank) — Abu Dhabi, UAE · Contract engagement

- Led enterprise-wide information security compliance governance aligned to **CBUAE ISR, ISO 27001, PCI DSS, and NIST** standards.
- Reduced audit findings by **30%** and improved risk-reporting timeliness by **40%** across the assurance function.
- Acted as **second line of defense**, providing independent assurance over security controls and risk treatment decisions.
- Coordinated internal and external security audits and gap analyses, managing the findings lifecycle and corrective action plans through to closure.
- Maintained the Information Security Assurance Framework covering all critical systems and business units.
- Reviewed implemented security configurations across enterprise platforms, identifying gaps and driving corrective action with platform owners.

Security Operations Center (SOC) Manager
May 2024 – Apr 2025

Klivvr — Cairo, Egypt

- Led **400+ incident response cases**, cutting incident resolution time by **30%** through rebuilt response playbooks.
- Reduced **MTTR by 35%** by defining SOC strategy, operating model, and SLA governance.
- Managed and mentored a team of up to **7 SOC specialists** across L1–L3, setting shift models, performance KPIs, and escalation paths.
- Deployed and tuned **Microsoft Sentinel, Splunk, and SOAR** platforms, integrating threat intelligence to reduce false positives by **30%**.

IT Risk & Cybersecurity Auditor (GRC)
Mar 2020 – Nov 2023

Central Bank of Egypt — Cairo, Egypt

- Led **14+ IT risk assessments and audits** of Egypt's top financial institutions against CBE regulations, PCI DSS, and ISO 27001.
- Designed a standardized **national cybersecurity audit program and toolkit** for financial institution reviews, improving audit efficiency by approximately **30%**.
- Developed and enforced policies aligning national IT operations with NIST, ISO 27001, and PCI DSS.
- Assessed IT infrastructure, security architecture, and control effectiveness, identifying vulnerabilities and prioritizing remediation based on regulatory risk.
- Conducted third-party vendor risk assessments to secure the national financial supply chain.
- Issued executive audit reports influencing remediation priorities and regulatory decisions.

Senior Cybersecurity Analyst — Mar 2017 – Dec 2019

Liquid C2 MENA (formerly SecureMisr) — Cairo, Egypt

- Delivered end-to-end **SIEM deployments** (log onboarding, use case development) for enterprise clients, improving event detection by **50%** and reducing false positives by **35%**.
- Led threat hunting and incident investigations across enterprise environments to mitigate APT activity.
- Established a new professional cybersecurity services line, driving a **20% revenue increase**.
- Built log source integrations and detection use cases mapped to the **MITRE ATT&CK** framework.

Network Security Engineer — Sep 2015 – Feb 2017

Sinai University — North Sinai, Egypt

- Designed and implemented security infrastructure across **3 campuses**, integrating firewalls, IDS/IPS, and SIEM, and migrating edge firewalls to next-generation platforms.
- Implemented **Network Access Control (NAC)** integrated with Active Directory, extending authenticated access coverage by **60%**.
- Deployed site-to-site VPNs and WAN optimization across branch sites, increasing data transfer efficiency by **35%**, and automated device hardening and configuration reviews.

TECHNICAL SKILLS

- **Audit & Assurance Tools:** TeamMate, ACL, Microsoft Sentinel, Splunk, IBM QRadar; KQL, SPL, and AQL.
- **Security Platforms:** SOAR, EDR/NDR, vulnerability management, FortiGate, Palo Alto, Cisco ASA, Azure, AWS, and GCP.
- **Engineering Foundations:** Python, Bash, PowerShell, Docker, Kubernetes, Ansible, Terraform, CI/CD security, and digital forensics.

CERTIFICATIONS

- **Governance, Risk & Audit:** CISSP, CISA, CRISC, PCIP (valid 12/2025 – 12/2028), BCM — EBI and IT Risk Controls (Risk Rewards Limited).
- **Defensive Operations:** GCIH, GMON, Microsoft SC-200, CEH, MITRE ATT&CK Foundations (AttackIQ), FireEye Systems Engineer (FSE), HP ATP ArcSight Security V1.
- **Architecture & Network:** Microsoft SC-100, CCNP Security, CCNA CyberOps, CCNA Security.

EDUCATION

Professional Diploma — Network & Systems Security — Nov 2013 – Jun 2014

Ministry of Communications and IT, Egypt · 924 academic training hours; CCNA R&S, CCNA Security, MCSA 2012 academic certifications

Bachelor of Science — Computer Science — Sep 2009 – May 2013

Future Academy — Cairo, Egypt

PROFESSIONAL INVOLVEMENT

- **Memberships & Volunteering:** ISACA, ISC2; ISC2 Exam Development Volunteer; Fast Company Middle East — Cybersecurity Subcommittee.
- **Founder, ESLabs Academy** — Arabic-language cybersecurity training and mentoring for the MENA security community.