

MUHAMMAD AHMAD

CISSP, CCSP, CIPM, CRISC, CGEIT, CISM, CISA
ITIL, ISO27001 LA, ISO27005 SLRM



Kingdom of Bahrain | +973 340 33 797 | mahmad83@gmail.com | <https://www.linkedin.com/in/mahmad1983>

Summary

- ✘ Accomplished Information/Cyber Security professional with 18+ years of progressive experience in spearheading Information/Cyber Security programs and IT Governance for global organizations in Banking (Commercial & Microfinance), Payments (FinTech), FMCG, and Telecom sectors.
- ✘ Holds multiple top-tier industry certifications (CISSP, CCSP, CRISC, CISM, CGEIT, CISA, CIPM) from globally recognized bodies, including (ISC)², ISACA, and IAPP, reinforcing a deep commitment to cybersecurity governance, compliance, risk management, international standards, and industry best practices.
- ✘ Proven track record in aligning cybersecurity strategies with business objectives, securing critical infrastructure, and enhancing cybersecurity postures in fast-paced regulated environments.
- ✘ Comprehensive experience across global frameworks, including ISO 27001, ISO 20000, ISO 27005, PCI DSS, PCI CPP, PCI PIN, NIST CSF, UAE NESI Information Assurance Regulation, SBP, CBE, SAMA CSF, CBB Cyber Security regulations, and SWIFT Compliance, ensuring regulatory compliance, risk mitigation, and continuous security improvements and audit readiness across enterprise environments.
- ✘ Trusted cybersecurity governance advisor to C-level executives, skilled in stakeholder, regulatory, and internal/external auditors' engagements, and securing executive sponsorship for cybersecurity initiatives.
- ✘ Led the development and execution of multi-year Information/Cyber Security strategies, security roadmaps, implementation of related frameworks, standards, policies, and procedures, driving measurable risk reduction (KIRs and KPIs) and strengthening cyber resilience in alignment with business priorities and Enterprise Risk Management (ERM).
- ✘ Demonstrated success in leading cybersecurity governance, operations, technology integration and delivery including GRC platforms, Risk Assessment/Management, RCSA, CIS Benchmark Compliance, Cloud Security, CSA STAR Assessment, Secure Coding, Privileged Access Management (PAM), Identity and Access Management (IAM), Data Leak Prevention (DLP), Network Access Controls (NAC), Database Activity Monitoring (DAM), Mobile Security (MDM/MAM), File Integrity Monitoring (FIM), API Security, Vulnerability Management Detection and Response (Qualys VMDR), Security Assessments (VAPT), Web Application Security, Red Team/Blue Team exercises, Bug Bounty Programs, XDR/EDR, SIEM/SOC (Security Operations Center), Email and Web Security, Cyber Threat Intelligence (CTI), Incident Response (CIRT), Crisis Simulations, and Continuous Monitoring of enterprise resilience programs.
- ✘ Championed cybersecurity awareness and culture-building programs along with phishing simulations for performance improvements, resulting in measurable increases in user behavior change and risk-aware decisions.
- ✘ Strong background in Cybersecurity Budget Management, Cost Control, Financial Planning, ROI optimization, Vendor Management, Cybersecurity Third-party Risk Management (TPRM), and ensuring value-driven cybersecurity investments.
- ✘ Proven leadership in building high-performing cybersecurity teams, driving operational excellence, talent development, conflict resolution, crisis management, and driving organizational and security capability transformation.
- ✘ Excellent communication and stakeholder reporting (Board, Risk and IT Steering Committees, Regulators), Presentation, Leadership, Management, Analytical, decision-making, and Result-oriented skills with strong Negotiation flair with a track record of delivering enterprise-wide security transformation.

Key Core Competencies and Skills

✘ CISO Leadership & Board Engagement	✘ Cyber Risk Advisory, RCSA, Assessment, and Management	✘ Third-Party Risk Management (TPRM)
✘ Cybersecurity and IT Governance Strategy	✘ Security Awareness & Culture Programs	✘ Negotiation & Vendor Management
✘ Governance, Risk and Compliance Management (GRC)	✘ Vulnerability, Security Assessment, and Cyber Threat Management	✘ IT Services Management
✘ Cybersecurity Frameworks (ISO 27001, NIST CSF, PCI DSS, NESA – IAR, SAMA, NCC, CBB)	✘ Security Operations, SOC, and Incident Response	✘ Networks and Infrastructure Security
✘ Payment Systems Security	✘ Identity & Access Management (IAM/PAM)	✘ Business Continuity and Disaster Recovery
✘ Information Security Controls and Audit Management	✘ IT & Cybersecurity Budgeting, Procurement, and Vendor Management	✘ Team Leadership
	✘ Data Protection and Privacy Management	✘ Project Management
		✘ Digital Transformation

Academics

- 🎓 **MBA**, Institute of Business Administration (**IBA**), University of the Punjab, Lahore – Pakistan (2009 – 2011)
- 🎓 **MS Computer Science**, Lahore University of Management Sciences (**LUMS**), Lahore – Pakistan (2006 – 2008)
- 🎓 **B.Sc. (Hons) Computer Science**, University of the Punjab (**PUCIT**), Lahore – Pakistan (2001 – 2005)

Professional Certifications

- 🏅 **CISSP** – Certified Information Systems Security Professional, ISC2, USA (2019). *Certification ID: 348936*
- 🏅 **CCSP** – Certified Cloud Security Professional, ISC2, USA (2021). *Certification ID: 348936*
- 🏅 **CIPM** – Certified Information Privacy Manager, IAPP, USA (2024)
- 🏅 **CRISC** – Certified in Risk and Information Systems Control, ISACA, USA (2017). *Certification ID: CRISC-1926570*
- 🏅 **CGEIT** – Certified in the Governance of Enterprise IT, ISACA, USA (2016). *Certification ID: CGEIT-1908389*
- 🏅 **CISM** – Certified Information Security Manager, ISACA, USA (2015). *Certification ID: CISM-1734360*
- 🏅 **CISA** – Certified Information Systems Auditor, ISACA, USA (2014). *Certification ID: CISA-15121195*
- 🏅 **Certified ISO/IEC 27005 Senior LRM** – Certified ISO/IEC 27005 Senior Lead Risk Manager, PECB, Canada (2018)
- 🏅 **ITIL V3** – IT Infrastructure Library, AXELOS, UK (2013). *Certification ID: 4944066.20233147*
- 🏅 **ISMS Lead Auditor** – IRCA ISO 27001 Lead Auditor, UK (2012)
- 🏅 **MCSE** – Microsoft Certified Systems Engineer, Microsoft Inc., USA (2006)
- 🏅 **MCSA** – Microsoft Certified Systems Administrator, Microsoft Inc., USA (2005)
- 🏅 **CCNA** – Cisco Certified Network Associate, Cisco Inc., USA (2004)

Professional Contributions and Achievements

- 🏆 **Winner** of The World CIO 200 Virtual Summit 2021 - Country Pakistan Edition in the Leader's Category
- 🏆 **Speaker** at GITEX Ignite Conference, Dubai (2015)
- 🏆 **Speaker** at multiple Local, National, and international conferences & Webinars

Professional Development

- 🏆 **CIPM** – Certified Information Privacy Manager, InfoSec Train (2023)
- 🏆 **TOGAF Enterprise Architecture** – TLC, Karachi – Pakistan (2020)
- 🏆 **Leading with Impact** – LUMS REDC, Lahore – Pakistan (2016)
- 🏆 **Enhancing Team Effectiveness** – LUMS REDC, Lahore – Pakistan (2016)
- 🏆 **ISO 20000 Implementation** – SGS, Lahore – Pakistan (2015)

- 🏠 **Manager on Board** – CCI Learning and Development, Lahore – Pakistan (2015)
- 🏠 **Strategic Thinking** – LUMS REDC, Lahore – Pakistan (2015)
- 🏠 **PMP** – Project Management Professional, PMI Lahore Chapter, Lahore – Pakistan (2014)
- 🏠 **Finance for Non-Finance Manager (Financial Management)** – LUMS REDC, Lahore – Pakistan (2014)
- 🏠 **Diversity Management** – Narejo Human Resources, Lahore – Pakistan (2014)
- 🏠 **Situational Leadership** – CCI, Lahore – Pakistan (2014)
- 🏠 **Planning and Organizing** – Octara, Lahore – Pakistan (2014)
- 🏠 **Impacting and Influencing** – Octara, Lahore – Pakistan (2014)
- 🏠 **Change Management/Leading and Managing Change** – LUMS REDC, Lahore – Pakistan (2013)
- 🏠 **Data Savvy Decision Making** – LUMS REDC, Lahore – Pakistan (2013)
- 🏠 **Power of Synergy** – Saadilnsha, Islamabad – Pakistan (2013)
- 🏠 **Train the Trainer** – IMS Knowledge, Lahore – Pakistan (2012)
- 🏠 **ICT Workshop**, Coca-Cola İçecek, Istanbul – Turkey (2011)
- 🏠 **MCITP** – Microsoft Certified IT Professional, New Horizon, Lahore – Pakistan (2010)
- 🏠 **Business Continuity Management** – SGS, Islamabad – Pakistan (2009)
- 🏠 **Serve to Win** – Winning Edge, Lahore – Pakistan (2006)

Professional Experiences

Arab Financial Services Company B.S.C. – Kingdom of Bahrain

(17-Jul-2023 to date)

Head of Cyber and Information Security (CISO) – Bahrain, UAE, Oman, Egypt

I am a CBB (Central Bank of Bahrain)- approved person for this position, reporting directly to the Executive. AFS is the region's leading digital payment solutions provider and FinTech enabler, regulated by the Central Bank of Bahrain. The following are the core responsibilities of this role:

- Defined and executed enterprise Cyber & Information Security strategy aligned with business growth, regulatory requirements, and digital transformation objectives.
- Oversaw all facets of the organization's cyber and information security functions, driving risk reduction, operational resilience, and optimized investments while ensuring strong alignment with business priorities.
- Led and sustained the successful global compliance and audit readiness programs for ISO 27001, PCI DSS, PCI PIN, PCI CPP, UAE NESAIAR, CBB, and CBE by fulfilling rigorous regulatory, clients', and schemes requirements without any major gaps and findings for critical payment infrastructure.
- Championed and drove cybersecurity awareness and culture change initiatives across the organization.
- Directed cybersecurity budgets, governed procurement, ensured strategic and value-driven investments with cost optimization.
- Spearheaded the creation and implementation of cybersecurity frameworks, policies, procedures, and strengthened overall cyber maturity.
- Directed end-to-end security operations and technology governance covering GRC, PAM, DLP, NAC, VMDR/Qualys, Cloud Security, DDOS, DNSSec, CIS Benchmarks, AppSec, XDR/EDR, SIEM/SOC, DAM, API/Mobile/Email Security, FIM, Threat Intelligence, Red Teaming, Cloud Security Posture Management (CSPM), Bug Bounty programs, and Crisis Simulations with focus on Zero Trust Adoption, defense in depth, and privacy by design principles.
- Led the successful SIEM/SOC transformation for 24/7 threat monitoring by enhancing real-time monitoring, threat detection, MTTD/MTTR reduction, and facilitated incident response capabilities, including CERT oversight.
- Led the development of cyber and information security risk assessment methodology, RCSA, and facilitated its implementation across the organization.

- Strengthened vendor ecosystem via a robust Cyber Security TPRM program covering due diligence, evaluation, onboarding, monitoring, and remediation tracking.

FINCA Microfinance Bank Limited, Lahore – Pakistan

(01-Aug-2019 to 16-Jul-2023)

Head Information Security (CISO) – SVP

FINCA Pakistan is part of a global FINCA Impact Finance, USA network working in 20 countries around the globe and operates in 108 cities across Pakistan. This position was reported to the Chief Risk Officer. The following were significant responsibilities:

- Built the bank's Information & Cyber Security function, securing resources, establishing governance, and positioning cybersecurity as a trusted business partner.
- Developed and executed the bank's long-term cybersecurity roadmap, aligning protection of critical assets with business and regulatory priorities.
- Represented the bank's cybersecurity vision to executives, regulators, auditors, and partners, ensuring transparent communication and trusted relationships.
- Advised senior management on technology risks, control effectiveness, and security architecture decisions impacting banking operations and customer data.
- Established and maintained cyber security strategy, governance frameworks, policies, procedures, standards, and guidelines aligned with ISO 27001, Central Bank directives, SBP ETGRMF, NIST CSF, PCI DSS, and privacy principles.
- Drove continuous improvement in security practices through strong leadership, mentoring, and effective people management.
- Directed comprehensive technology risk assessments, guiding risk-based decision-making to manage and mitigate risks across the organization effectively.
- Oversaw the design and implementation of security solutions and strived to improve security posture continuously.
- Developed KPIs/KRIs for executive reporting and program maturity measurement.
- Drove organization-wide security awareness and cultural adoption through structured training and engagement programs.
- Maintained up-to-date visibility of industry threat landscapes to inform proactive risk management.
- Led proactive monitoring, analytics, and incident response operations, ensuring the capability to detect, protect, investigate, and resolve security incidents and data breaches.

Allied Bank Limited, Lahore – Pakistan

(31-Mar-2017 to 31-Jul-2019)

Manager Information Security Governance and Risk Management – VP

Allied Bank Limited (ABL) is Pakistan's 5th largest commercial bank. This strategic position is part of ABL's Information Security Group. This position was reported to the CISO. The following were significant responsibilities:

- Served as the primary advocate for Information & Cyber Security and Technology Risk Management across the bank, driving governance, compliance, and technical security uplift.
- Provided hands-on cybersecurity and risk advisory to business and technology teams, ensuring secure design, threat-aligned controls, and cyber resilience in solutions and processes.
- Designed and implemented information security governance frameworks, policies, standards, and procedures aligned with ISO 27001, ISO 27005, PCI DSS, SWIFT CSCF, and regulatory technology requirements and achieved compliance.
- Directed and executed periodic Technical Risk Assessments, security reviews, and control assessments; maintained the risk register and recommended mitigation actions to reduce technology and cyber risks.
- Built and executed the organization's cybersecurity awareness and training program to improve workforce security behavior and reduce operational risks.
- Operational oversight for Internal and External Security Assessments, including Vulnerability Assessment, Penetration Testing, Security Review, Threat Hunting, and Compromise Assessment while providing implementation support to the Security Operations Center (SOC) maturity & CERT.

Technology Services Manager, Governance

This position was reported to the CIO and was part of Pakistan's Senior IT Leadership team. The following were major responsibilities:

- Managed enterprise IT operations and governance, balancing technology enablement with business, operational, and financial objectives.
- Led IT Governance, ITSM (ServiceNow), IT Project Portfolio Management, IT Risk Management, and resource optimization with hands-on involvement in process design and control implementation.
- Strengthened IT service delivery by driving ISO 20000 (ITSM) implementation aligned with ITIL practices, improving operational maturity, IT Controls enhancements, and audit readiness.
- Enhanced efficiency through hands-on adoption of cloud services, mobility solutions, and digital workflow automation, reducing manual processes and operational overhead.
- Led the IT financial management, including budgeting, forecasting, cost control, and TCO optimization initiatives.
- Managed end-to-end vendor and procurement activities, including strategic sourcing, contract negotiation, SLA governance, and performance management.
- Delivered C-level reporting on KRIs, KPIs, scorecards, and financial performance to support informed decision-making.
- Led data center colocation, infrastructure enhancement, and outsourcing of core IT/business services (call center, service desk), improving reliability and reducing costs.

IT Infrastructure and Security Manager

This position was reported to the ICT Manager and had the following responsibilities:

- Managed and maintained enterprise IT infrastructure to ensure reliable, cost-effective, and business-aligned IT services across all locations.
- Designed and implemented secure technology architecture with risk-based controls in line with ISO 20000, ISO 27001/2700X, ITIL/ITSM, NIST, CIS, and COBIT standards.
- Ensured high availability and optimal utilization of data centers and critical IT systems, supporting business continuity and contingency planning.
- Developed and enforced IT policies, procedures, and standards covering infrastructure, cybersecurity, business continuity, systems, networks, and database management.
- Led hands-on security initiatives, including Vulnerability Assessment (VA), Penetration Testing (PT), configuration review, and security compliance reviews.
- Collaborated with internal and external stakeholders to validate ICT infrastructure compliance and recommend improvements.

IT Executive (Networks, Communication, and Security)

This position was reported to the IT Infrastructure and Security Manager and had the following responsibilities:

- Managed and optimized corporate data centers (50+ servers) and IT infrastructure across 17+ remote sites supporting 2000+ users, ensuring 24/7 availability, secure configuration, SLA/OLA compliance, and reducing operational costs by 20%.
- Implemented operational support tools including LANDesk, Active Directory consolidation (NT → Windows 2003), Bluecoat Proxy, ArcServe Backup, File Integrity Monitoring (FIM), SolarWinds, ManageEngine AD and Audit, Patch Management, Symantec Antivirus/Anti-malware Solution, and IT Asset Inventory, enhancing operational efficiency and reducing management costs by 45%.

Corporate Engineer

CyberNet is the largest ISP in Pakistan. This position was reported to the Manager – Corporate Services and had the following responsibilities:

- Deployed and managed complex network infrastructure solutions for corporate clients, integrating Frame Relay, ATM, DSL, ISDN, VSAT downlinks, and Layer 2/3 IP networks.
- Installed, configured, and maintained Windows and Linux servers, including ISA, FTP, DHCP/DNS, Web, Antivirus, File/Backup, PDC/ADC servers, supporting enterprise IT operations.

 **References**

Available upon request