



الاتحاد المصرفي العربي
Union of Arab Banks

Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design and Regulatory Resilience



Millennium Plaza Doha Hotel

23 - 25 November 2026

DOHA – STATE OF QATAR



Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

A practical, banking-focused
seminar combining privacy
governance, regulatory compliance,
risk management and privacy

SEMINAR OVERVIEW

The rapid evolution of digital banking, artificial intelligence, cloud computing, advanced analytics, APIs and fintech ecosystems is transforming how banks collect, process, share and protect customer information. At the same time, banks face increasing regulatory and customer expectations regarding data privacy, confidentiality, transparency, accountability and responsible use of personal and financial information.

This three-day seminar provides banking professionals with a practical understanding of data privacy, privacy governance, regulatory compliance and privacy engineering, with particular attention to the regulatory and operational environment of banks operating in Qatar. It combines internationally recognized privacy-governance and privacy-engineering practices with practical banking scenarios and localized examples.

Particular attention is given to emerging banking environments involving AI, cloud services, digital banking platforms, APIs, analytics and third-party service providers.

LEARNING OBJECTIVES

- Understand key privacy principles and their application within banking and financial services.
- Understand the relationship between data privacy, banking confidentiality, cybersecurity, data governance and regulatory compliance.
- Recognize key data-protection & privacy obligations affecting banks operating in Qatar.
- Establish effective privacy governance, accountability and oversight arrangements.
- Identify and assess privacy risks throughout the banking data lifecycle.
- Apply privacy-by-design principles to banking products, systems and digital transformation initiatives.
- Conduct and evaluate Privacy Impact Assessments and Data Protection Impact Assessments.
- Address privacy risks associated with AI, analytics and automated decision-making.
- Assess privacy implications of cloud services, fintech partnerships, APIs and third-party processing.
- Select appropriate privacy-engineering and privacy-enhancing controls.
- Strengthen privacy monitoring, incident management and regulatory evidence.
- Develop practical actions for improving privacy maturity within the organization.



Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

AGENDA | Day 1 – Data Privacy, Governance & Regulatory Compliance in Banking

1. THE CHANGING DATA PRIVACY LANDSCAPE IN BANKING

- Evolution of privacy and data protection in financial services
- Digital banking, mobile banking, fintech and open ecosystems
- Growth of cloud, analytics & artificial intelligence
- Why traditional compliance approaches are no longer sufficient
- Personal, financial, transactional, behavioural and biometric information
- Personal data versus sensitive personal data
- Privacy versus confidentiality versus information security
- Banking secrecy and customer-data protection
- Privacy as a component of digital trust
- Business, regulatory, operational and reputational consequences of privacy failures

Qatar Banking Context

- Overview of the Qatar data-protection & privacy environment
- Personal Data Privacy Protection Law
- Relevant cybersecurity, cloud and technology requirements
- Data localization and cross-border considerations
- International considerations for multinational banks, including GDPR
- Managing overlapping legal, regulatory and contractual obligations

Discussion: What does a privacy failure look like in a modern Qatari bank?

Participants examine scenarios involving unauthorized customer-data access, inappropriate marketing use, third-party disclosure and digital-channel data collection.

2. BUILDING AN EFFECTIVE PRIVACY GOVERNANCE FRAMEWORK

- Privacy governance principles; accountability and ownership
- Role of the Board and senior management
- Role of the Data Protection Officer / privacy function
- Responsibilities of the CISO, CIO, Chief Data Officer, Compliance and Risk
- Data owners, system owners and business owners
- Role of Internal Audit and the Three Lines Model
- Privacy policies, standards, procedures and supporting controls
- Governance committees, escalation and integration with enterprise risk and compliance
- Regulatory evidence and demonstrating accountability
- Governance of outsourced and shared processing activities

3. GOVERNING THE BANKING DATA LIFECYCLE

Discover & Collect

- Data discovery and inventories
- Records of processing activities
- Identifying data sources
- Customer-data collection
- Purpose and lawful processing
- Consent management
- Transparency and privacy notices
- Data minimization

Use & Process

- Purpose limitation
- Access to customer information
- Secondary use of information
- Analytics and profiling
- Sharing information across business units
- Use of production data for development and testing

Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

Share & Transfer

- Internal and third-party data sharing
- Cloud processing
- Cross-border transfers
- Data-residency considerations
- Data-sharing agreements

Retain & Dispose

- Regulatory and business retention requirements
- Data-retention schedules and archival
- Legal holds
- Secure deletion and disposal
- Deletion challenges across backups, cloud and distributed environments

4. DATA SUBJECT AND CUSTOMER PRIVACY RIGHTS

- Transparency and customer information
- Consent and withdrawal
- Access to personal information
- Correction and accuracy
- Restriction of processing
- Deletion requests
- Conflicting regulatory retention requirements
- Identity verification
- Operational workflows
- Recording and demonstrating compliance

Day 1 Workshop — Designing Privacy Governance for a New Digital Banking Service

- Governance and accountability structure
- Customer-data lifecycle
- Processing inventory
- Key privacy obligations
- Initial privacy-risk scenarios

Day 2 - Privacy Risk, AI, Cloud & Third-Party Compliance

1. PRIVACY RISK MANAGEMENT

- Privacy governance versus privacy risk management
- Risk appetite, tolerance and capacity
- Identifying privacy-risk scenarios, threats, vulnerabilities and impacts
- Customer harm; regulatory, financial, operational and reputational impact
- Developing a privacy-risk register
- Risk ownership and treatment options
- Risk acceptance and residual risk
- Integrating privacy risk with enterprise and technology risk
- New customer-data uses and high-risk/sensitive processing
- Profiling and automated decision-making
- Cloud migration, new vendors and fintech arrangements, and AI implementations
- Assessing necessity and proportionality
- Mapping data flows and identifying privacy risks
- Defining mitigating controls and documenting decisions/approvals
- Risk acceptance and escalation
- Connecting PIA/DPIA with cybersecurity and enterprise-risk assessments

2. PRIVACY IMPACT ASSESSMENTS

- Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA)
- When assessments should be performed
- New banking products and major technology changes

Practical Exercise — PIA for a New Mobile Banking Feature

Participants identify data flows, processing purposes, stakeholders, privacy risks and required controls.



Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

3. AI, ANALYTICS & CUSTOMER PRIVACY

AI in Modern Banking

- Credit scoring
- Fraud detection
- AML monitoring
- Customer analytics and segmentation
- Personalized offers
- Chatbots and virtual assistants
- Generative AI
- Employee productivity tools

Privacy Risks of AI

- Large-scale data collection and secondary use
- Training versus production data
- Data quality
- Bias and discriminatory outcomes
- Transparency and explainability
- Profiling and automated decision-making
- Human oversight
- Sensitive-data inference
- Reidentification
- Model inversion and inference
- Data leakage through generative AI
- Employee use of public AI platforms

Governing AI from a Privacy Perspective

- AI governance and accountability
- Privacy-by-design for AI
- Data minimization and purpose limitation
- Human oversight
- Model and data governance
- Privacy assessments for AI use cases
- Approval, monitoring and evidence of responsible processing

4. CLOUD, FINTECH & THIRD-PARTY PRIVACY RISK

- Cloud service and deployment models; shared-responsibility model
- Customer-data processing in cloud environments
- Data location, residency & cross-border processing
- Selecting and assessing cloud service providers
- Fintech partnerships, payment processors, SaaS and external analytics providers
- Outsourced processing, subprocessors and fourth-party risk
- Contractual privacy and security requirements
- Data ownership and use limitations
- Breach-notification obligations; audit and assurance rights
- Continuous monitoring
- Exit planning, data portability and secure deletion

APIs and Data Sharing

- APIs as a privacy boundary
- Authentication and authorization
- Excessive data exposure
- Data minimization in API design
- Logging and monitoring
- Third-party API access
- Controlling and revoking access

Day 2 Banking Case Study — AI-Based Credit Scoring in the Cloud

Participants act as the bank's privacy, risk, security, technology and compliance committee and decide whether to approve, conditionally approve or reject the proposed solution, considering customer-data processing, automated decision-making, cloud architecture, data residency, third-party access, regulatory requirements and required controls.



Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

Day 3 — Privacy Engineering, Monitoring & Regulatory Resilience

1. PRIVACY BY DESIGN & PRIVACY ENGINEERING

- Privacy-by-design & privacy-by-default principles
- Moving from compliance requirements to technical controls
- Privacy engineering objectives
- Proactive versus reactive privacy controls
- Integrating privacy into project and change management and the Secure Development Lifecycle
- Privacy requirements during system design
- Data-flow analysis and trust boundaries
- Architecture reviews
- Governance gates for new digital products
- Privacy acceptance criteria

2. ENGINEERING PRIVACY INTO BANKING SYSTEMS

- Identity and access management
- Least privilege
- Role-based and attribute-based access
- Privileged access management
- Segregation of duties
- Segregation of development, testing and production
- Protecting databases and data repositories
- Secure APIs and interfaces
- Data-loss prevention
- Monitoring privileged access
- Protecting customer information in non-production environments
- Logging while minimizing unnecessary privacy exposure

3. PRIVACY-ENHANCING TECHNOLOGIES

- Encryption at rest, in transit and in use
- Key-management considerations
- Tokenization of payment & customer information
- Data masking
- Pseudonymization and anonymization
- Reidentification risk
- Differential privacy
- Synthetic data
- Homomorphic encryption
- Emerging privacy-enhancing technologies
- Selecting controls according to the banking use case

Practical Discussion — Which Privacy-Enhancing Technology Should We Use?

- Credit-card information
- Customer analytics
- AI model development
- Application testing
- Fraud analytics
- Data sharing with fintech partners

4. PRIVACY MONITORING & INCIDENT MANAGEMENT

- Continuous privacy monitoring
- Detecting inappropriate data access and unauthorized processing
- Data-loss indicators
- Privacy control testing
- Monitoring privileged users, vendors & processors
- Privacy KRIs and KPIs
- Privacy dashboards and escalation thresholds

Privacy Incidents

- Privacy incident versus cybersecurity incident
- Incident classification
- Data-breach investigation
- Determining affected information and individuals
- Containment
- Regulatory assessment
- Notification and communication
- Customer considerations
- Third-party incidents
- Evidence preservation
- Root-cause analysis
- Lessons learned and control improvement

5. ASSURANCE, AUDIT & REGULATORY READINESS

- Demonstrating privacy compliance
- Policies and procedures
- Processing inventories & data-flow documentation
- Consent and access records
- Privacy assessment evidence
- Vendor due-diligence and data-transfer records
- Incident and breach records
- Privacy control assessments
- Internal audit and compliance monitoring
- Management and Board reporting
- Regulatory examinations
- Moving from point-in-time compliance to continuous assurance



Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience

Final Banking Simulation — The Digital Banking Privacy Incident

Participants respond to a simulated incident involving a cloud service provider, compromised API, unauthorized access to customer information, an AI application using customer data, potential inappropriate third-party processing, data-residency concerns, and regulatory/customer-notification considerations.

- What happened & what customer data is affected?
- Which privacy & regulatory requirements may apply?
- Who needs to be involved?
- What immediate containment actions are required?
- What evidence must be preserved?
- What regulatory and customer communications should be considered?
- What corrective controls should be implemented?

WHO SHOULD ATTEND?

- Data Protection and Privacy Professionals
- Compliance and Regulatory Affairs Professionals
- Information Security and Cybersecurity Teams
- Chief Data Officers and Data Governance Teams
- Operational and Enterprise Risk Professionals
- Technology and Enterprise Architects
- Digital Banking and Transformation Teams
- AI, Data Science and Analytics Teams
- Cloud, Application and API Security Professionals
- Internal Auditors and IT Auditors
- Legal Professionals
- Fintech and Third-Party Risk Teams
- Business and Product Owners
- IT and Technology Management

SEMINAR METHODOLOGY

- Instructor-led presentations
- Banking-specific examples
- Qatar-focused regulatory discussions
- Practical exercises
- Group workshops
- Privacy-risk scenarios
- Case studies
- Interactive discussions
- Final banking incident simulation

The emphasis throughout the three days is on translating regulatory and privacy requirements into practical governance, risk-management and technology controls that participants can apply within their banks.

Data Privacy & Regulatory Compliance in Digital Banking

Building Trust, Privacy-by-Design
and Regulatory Resilience



TRAINER
Mr. Abdo Chalhoub

Abdo Chalhoub is a cybersecurity, governance, and digital transformation executive with more than **35 years of international experience** advising governments, financial institutions, multinational organizations, and development agencies across the Middle East, Africa, Asia, Europe, and Australia. Throughout his career, he has led enterprise technology, cybersecurity, governance, risk, compliance, privacy, AI governance, and operational resilience programs, delivering large-scale digital transformation initiatives, national digital government programs, and internationally recognized assurance and certification initiatives.

He currently serves as **Head of Information Security at Legal Ready** and as **Project Implementation and Governance Advisor** for the **US\$150 million World Bank-financed Lebanon Digital Acceleration Project (LDAP)**. Previously, he served as **Chief Information and Security Officer at Azentio Software**, **Executive Vice President at Path Solutions**, **Senior ICT Project Manager with UNDP/OMSAR**, **Network Consulting Engineer at Cisco Systems**, and **Technical Manager at Texas Instruments**, where he gained extensive experience in enterprise infrastructure, networking, systems engineering, and technology consulting.

In parallel with his executive leadership career, Abdo has contributed to higher education as a **Part-Time Instructor at the Lebanese American University (LAU)**, **ESA Business School**, and **Haigazian University**, teaching information systems, cybersecurity, governance, project management, and digital transformation while mentoring the next generation of technology professionals.

Abdo is a trusted advisor, educator, international speaker, and **ISACA Global Accredited Trainer for CISA, CISM, CGEIT, CDPSE, COBIT, and AAIR**. He is dedicated to advancing cybersecurity, AI governance, digital trust, organizational resilience, and public-sector digital transformation through executive leadership, advisory services, and professional education.



خصوصية البيانات والامتثال التنظيمي في الخدمات المصرفية الرقمية

بناء الثقة، والخصوصية حسب
التصميم، والمرونة التنظيمية



فندق ميلينيوم الدوحة
٢٣ - ٢٥ نوفمبر ٢٠٢٦
الدوحة - دولة قطر



خصوصية البيانات والامتثال التنظيمي في الخدمات المصرفية الرقمية

بناء الثقة، والخصوصية حسب
التصميم، والمرونة التنظيمية

ندوة عملية متخصصة في القطاع
المصرفي، تجمع بين حوكمة
الخصوصية، والامتثال للمتطلبات
التنظيمية، وإدارة المخاطر، وهندسة
الخصوصية، مع تطبيقات وسيناريوهات
مصرفية محلية من دولة قطر.

في ظل التوسع المتسارع في الخدمات المصرفية الرقمية، والذكاء الاصطناعي، والحوسبة السحابية، وتحليلات البيانات، وواجهات البرمجة (APIs)، تواجه المصارف تحديات متزايدة في حماية بيانات العملاء والامتثال للمتطلبات التنظيمية.

يقدم هذا البرنامج إطاراً عملياً لفهم حوكمة الخصوصية، وإدارة مخاطر البيانات، والخصوصية حسب التصميم (Privacy by Design)، والامتثال التنظيمي. ويركز على تحويل المتطلبات التنظيمية إلى ضوابط عملية في الحوكمة وإدارة المخاطر والتكنولوجيا.

نبذة

أهداف
التعلم

- فهم المبادئ الأساسية للخصوصية وتطبيقاتها في القطاع المصرفي والخدمات المالية.
- فهم العلاقة بين خصوصية البيانات، والسرية المصرفية، والأمن السيبراني، وحوكمة البيانات، والامتثال للمتطلبات التنظيمية.
- التعرف على أهم الالتزامات المتعلقة بحماية البيانات والخصوصية التي تؤثر على البنوك العاملة في دولة قطر.
- وضع أطر فعالة لحوكمة الخصوصية، وتحديد المسؤوليات، وآليات المساءلة والإشراف.
- تحديد وتقييم مخاطر الخصوصية عبر مختلف مراحل دورة حياة البيانات المصرفية.
- تطبيق مبادئ الخصوصية منذ مرحلة التصميم (Privacy by Design) على المنتجات المصرفية والأنظمة ومبادرات التحول الرقمي.
- إجراء وتقييم تقييمات أثر الخصوصية (PIA) وتقييمات أثر حماية البيانات (DPIA).
- معالجة مخاطر الخصوصية المرتبطة بالذكاء الاصطناعي، وتحليلات البيانات، واتخاذ القرارات المؤتمتة.
- تقييم الآثار المترتبة على الخصوصية عند استخدام الخدمات السحابية، والشركات مع شركات التكنولوجيا المالية (FinTech)، وواجهات برمجة التطبيقات (APIs)، ومعالجة البيانات من قبل الأطراف الثالثة.
- اختيار الضوابط المناسبة لهندسة الخصوصية وتقنيات تعزيز الخصوصية.
- تعزيز عمليات مراقبة الخصوصية، وإدارة الحوادث، وتوثيق الأدلة اللازمة للامتثال للمتطلبات التنظيمية.
- وضع إجراءات عملية لتحسين مستوى نضج الخصوصية داخل المؤسسة.

الفئات المستهدفة

العاملون في حماية البيانات والخصوصية، والامتثال، والأمن السيبراني، وإدارة المخاطر، وحوكمة البيانات، والتدقيق الداخلي وتدقيق تقنية المعلومات، والخدمات المصرفية الرقمية، والذكاء الاصطناعي وتحليلات البيانات، والحوسبة السحابية، والتكنولوجيا المالية (FinTech)، والشؤون القانونية، والهندسة التقنية وإدارة المنتجات

خصوصية البيانات والامتثال التنظيمي في الخدمات المصرفية الرقمية

بناء الثقة، والخصوصية حسب
التصميم، والمرونة التنظيمية

أجندة

اليوم الثاني – مخاطر الخصوصية والذكاء الاصطناعي والسحابة والأطراف الثالثة

1. إدارة مخاطر الخصوصية

- تحديد سيناريوهات مخاطر الخصوصية وتقييمها
- التهديدات والثغرات وتأثيرها على العملاء
- سجل مخاطر الخصوصية (Privacy Risk Register)
- معالجة المخاطر والمخاطر المتبقية (Residual Risk)
- دمج مخاطر الخصوصية مع مخاطر المؤسسة والتكنولوجيا

2. تقييم أثر الخصوصية

- تقييم أثر الخصوصية (PIA) وتقييم أثر حماية البيانات (DPIA)
- متى يجب إجراء التقييم؟
- تحديد تدفقات البيانات والمخاطر والضوابط
- تقييم الضرورة والتناسب (Necessity & Proportionality)
- توثيق القرارات والموافقات

تمرين عملي: إجراء تقييم أثر الخصوصية لخدمة مصرفية عبر الهاتف المحمول.

3. الذكاء الاصطناعي وتحليلات البيانات

- استخدامات الذكاء الاصطناعي في المصارف: الائتمان، مكافحة الاحتيال، مكافحة غسل الأموال (AML) وخدمة العملاء
- التنميط (Profiling) واتخاذ القرارات الآلية
- جودة البيانات والتحيز والشفافية
- استنتاج البيانات الحساسة وإعادة تحديد الهوية
- مخاطر تسرب البيانات عبر الذكاء الاصطناعي التوليدي
- حوكمة الذكاء الاصطناعي والرقابة البشرية

4. السحابة والتكنولوجيا المالية والأطراف الثالثة

- نموذج المسؤولية المشتركة في الحوسبة السحابية
- موقع البيانات وسيادتها ونقلها عبر الحدود
- مخاطر مزودي الخدمات السحابية وشركات التكنولوجيا المالية (FinTech)
- المتطلبات التعاقدية والرقابة المستمرة
- خصوصية وأمن واجهات البرمجة (APIs)

دراسة حالة: نظام تقييم ائتماني قائم على الذكاء الاصطناعي والحوسبة السحابية.

اليوم الأول – خصوصية البيانات والحوكمة والامتثال التنظيمي

1. خصوصية البيانات في البيئة المصرفية

- تطور مفهوم الخصوصية وحماية البيانات في القطاع المصرفي
- البيانات الشخصية والبيانات الشخصية الحساسة
- الخصوصية، السرية المصرفية وأمن المعلومات
- نقل البيانات عبر الحدود والاعتبارات الدولية

2. حوكمة الخصوصية والمساءلة

- إطار حوكمة الخصوصية وتحديد المسؤوليات
- دور مجلس الإدارة والإدارة العليا
- مسؤول حماية البيانات (DPO) ووظائف الخصوصية
- أدوار الأمن السيبراني، إدارة البيانات، المخاطر والامتثال
- السياسات والمعايير وإثبات الامتثال

3. إدارة دورة حياة البيانات

- الجمع: الغرض، الموافقة، الشفافية وتقليل البيانات
- الاستخدام والمعالجة: تحديد الغرض، الوصول، التحليلات والاستخدام الثانوي
- المشاركة والنقل: الأطراف الثالثة، السحابة ونقل البيانات عبر الحدود
- الاحتفاظ والإتلاف: مدد الاحتفاظ، الأرشفة والإتلاف الآمن
- حقوق أصحاب البيانات وإدارة طلبات العملاء

ورشة عمل: تصميم إطار حوكمة الخصوصية لخدمة مصرفية رقمية جديدة.

خصوصية البيانات والامتثال التنظيمي في الخدمات المصرفية الرقمية

بناء الثقة، والخصوصية حسب
التصميم، والمرونة التنظيمية

اليوم الثالث – هندسة الخصوصية والرقابة والمرونة التنظيمية

1. الخصوصية حسب التصميم وهندسة الخصوصية

- الخصوصية حسب التصميم (Privacy by Design)
- والخصوصية كإعداد افتراضي (Privacy by Default)
- تحويل المتطلبات التنظيمية إلى ضوابط تقنية
- دمج الخصوصية في دورة حياة تطوير الأنظمة (SDLC)
- تحليل تدفقات البيانات وحدود الثقة
- مراجعة التصميم والبنية التقنية

2. حماية البيانات في الأنظمة المصرفية

- إدارة الهوية والوصول (IAM)
- مبدأ الحد الأدنى من الصلاحيات (Least Privilege)
- إدارة الوصول المميز (PAM)
- الفصل بين المهام (Segregation of Duties)
- حماية قواعد البيانات وواجهات البرمجة (APIs)
- منع تسرب البيانات (DLP)
- التسجيل والمراقبة الأمنية

3. تقنيات تعزيز الخصوصية (PETs)

- التشفير وإدارة المفاتيح
- الترميز البديل (Tokenization)
- إخفاء البيانات (Data Masking)
- استخدام الأسماء المستعارة (Pseudonymization) وإخفاء الهوية (Anonymization)
- الخصوصية التفاضلية (Differential Privacy)
- البيانات الاصطناعية (Synthetic Data)
- التشفير المتماثل (Homomorphic Encryption)

4. مراقبة الخصوصية والاستجابة للحوادث

- المراقبة المستمرة ومؤشرات الأداء والمخاطر (KPI/KRI)
- اكتشاف الوصول والاستخدام غير المصرح به للبيانات
- التحقيق في خروقات البيانات واحتواؤها
- الإخطار التنظيمي والتواصل مع العملاء
- تحليل السبب الجذري والدروس المستفادة

5. التدقيق والجاهزية التنظيمية

- إثبات الامتثال للخصوصية
- تقييم فعالية الضوابط
- التدقيق الداخلي والمراقبة المستمرة
- التقارير للإدارة ومجلس الإدارة
- الاستعداد لعمليات الفحص التنظيمي

المحاكاة المصرفية النهائية – حادثة الخصوصية في الخدمات المصرفية الرقمية

- ماذا حدث؟ وما بيانات العملاء التي تأثرت بالحادثة؟
- ما متطلبات الخصوصية والمتطلبات التنظيمية التي قد تنطبق على هذه الحالة؟
- من الجهات والأطراف التي يجب إشراكها في التعامل مع الحادثة؟
- ما إجراءات الاحتواء الفورية المطلوبة؟
- ما الأدلة والمعلومات التي يجب الحفاظ عليها وتوثيقها؟
- ما الاتصالات والإخطارات التي ينبغي أخذها بعين الاعتبار تجاه الجهات التنظيمية والعملاء؟
- ما الضوابط والإجراءات التصحيحية التي ينبغي تنفيذها لمنع تكرار الحادثة؟
- يستجيب المشاركون لحادثة افتراضية تحاكي واقعة تتضمن مزوّد خدمات سحابية، وواجهة برمجة تطبيقات (API) مخترقة، ووصولاً غير مصرح به إلى معلومات العملاء، وتطبيقاً للذكاء الاصطناعي يستخدم بيانات العملاء، واحتمال وجود معالجة غير مناسبة للبيانات من قبل طرف ثالث، ومخاوف تتعلق بإمكان تخزين البيانات وموقعها الجغرافي (Data Residency)، بالإضافة إلى اعتبارات الإخطار للجهات التنظيمية والعملاء.

منهجية الندوة

- عروض تقديمية يقدمها المدرب.
- أمثلة متخصصة ومصممة بما يتناسب مع القطاع المصرفي.
- مناقشات تنظيمية تركز على دولة قطر.
- تمارين عملية وتطبيقية.
- ورش عمل جماعية.
- سيناريوهات لمخاطر الخصوصية.
- دراسات حالة.
- مناقشات تفاعلية.
- محاكاة نهائية لحادثة مصرفية.
- يركز البرنامج على مدى ثلاثة أيام على تحويل المتطلبات التنظيمية ومتطلبات الخصوصية إلى ضوابط عملية في مجالات الحوكمة وإدارة المخاطر والتقنية، مما يمكن المشاركين من تطبيقها عملياً داخل مؤسساتهم المصرفية

خصوصية البيانات والامتثال التنظيمي في الخدمات المصرفية الرقمية

بناء الثقة، والخصوصية حسب
التصميم، والمرونة التنظيمية

عبدو شلهوب هو مسؤول تنفيذي متخصص في الأمن السيبراني والحوكمة والتحول الرقمي، ويتمتع بخبرة دولية تزيد على 35 عاماً في تقديم الاستشارات للحكومات والمؤسسات المالية والمنظمات متعددة الجنسيات ووكالات التنمية في منطقة الشرق الأوسط وأفريقيا وآسيا وأوروبا وأستراليا. وخلال مسيرته المهنية، قاد برامج متخصصة في تكنولوجيا المؤسسات، والأمن السيبراني، والحوكمة، وإدارة المخاطر والامتثال، والخصوصية، وحوكمة الذكاء الاصطناعي، والمرونة التشغيلية، كما أشرف على تنفيذ مبادرات واسعة النطاق للتحول الرقمي، وبرامج الحكومة الرقمية على المستوى الوطني، ومبادرات دولية مرموقة في مجالات التدقيق والضمان والحصول على الشهادات والاعتمادات.

يشغل حالياً منصب رئيس أمن المعلومات في Legal Ready، كما يعمل مستشاراً لتنفيذ المشروع والحوكمة في مشروع تسريع التحول الرقمي في لبنان (LDAP)، الممول من البنك الدولي بقيمة 150 مليون دولار أمريكي. وقبل ذلك، شغل منصب الرئيس التنفيذي للمعلومات والأمن (CISO) في شركة Azentio Soft-ware، ونائب الرئيس التنفيذي في Path Solutions، ومدير أول لمشاريع تكنولوجيا المعلومات والاتصالات لدى برنامج الأمم المتحدة الإنمائي (UNDP) ووزارة الدولة لشؤون التنمية الإدارية (OMSAR)، كما عمل مهندس استشارات شبكات في Cisco Systems ومديراً فنياً في Texas Instruments، حيث اكتسب خبرة واسعة في البنية التحتية للمؤسسات، والشبكات، وهندسة الأنظمة، والاستشارات التقنية.

وبالتوازي مع مسيرته التنفيذية، ساهم عبدو في مجال التعليم العالي بصفته محاضراً بدوام جزئي في الجامعة اللبنانية الأميركية (LAU)، وكلية ESA للأعمال، وجامعة هايكايزان، حيث دُرّس مواد ونظم المعلومات، والأمن السيبراني، والحوكمة، وإدارة المشاريع، والتحول الرقمي، كما ساهم في إرشاد وتأهيل الجيل القادم من المتخصصين في مجال التكنولوجيا.

ويُعد عبدو مستشاراً موثقاً، ومعلماً، ومتحدثاً دولياً، ومدرّباً معتمداً عالمياً من قبل ISACA في شهادات وبرامج CISA وCISM وCGEIT وCDPSE وCOBIT وAAIR. وهو يكرّس خبرته وجهوده لتعزيز الأمن السيبراني، وحوكمة الذكاء الاصطناعي، والثقة الرقمية، والمرونة المؤسسية، والتحول الرقمي في القطاع العام، من خلال القيادة التنفيذية، والخدمات الاستشارية، والتعليم والتدريب المهني.



المحاضر:
السيد عبدو شلهوب